#CiscoLiveAPJC

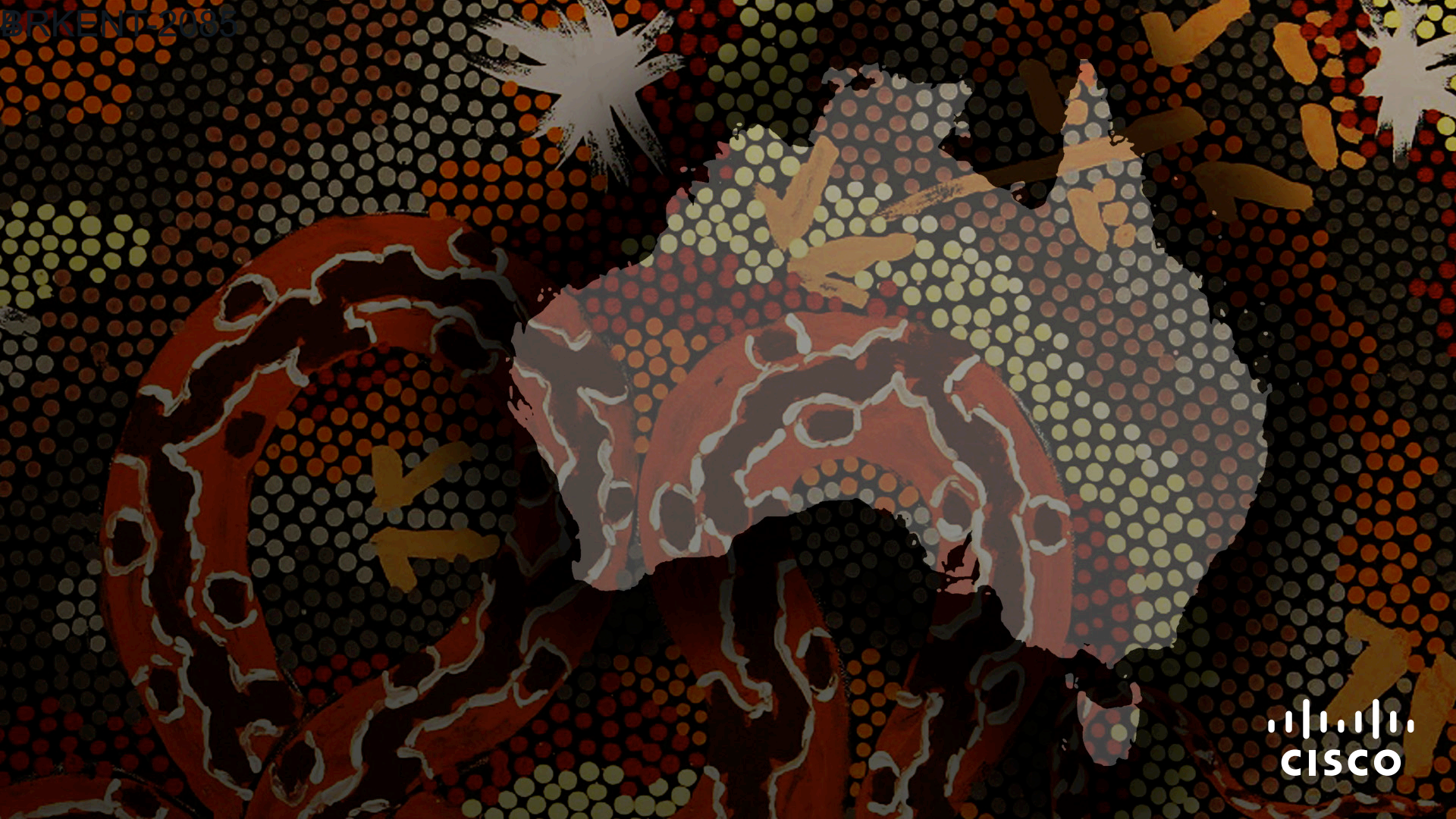
The bridge to possible

Troubleshooting Routing Protocols

OSPF | BGP

Julius Nasr – High Touch Engineer

BRKENT-2085



cisco

Cisco Webex App

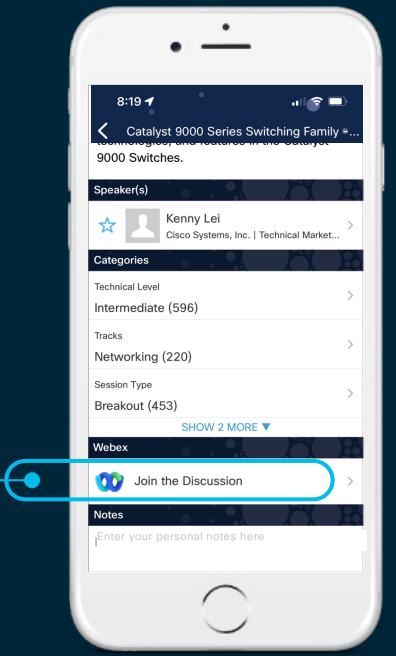
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until Thursday 22 December, 2022.

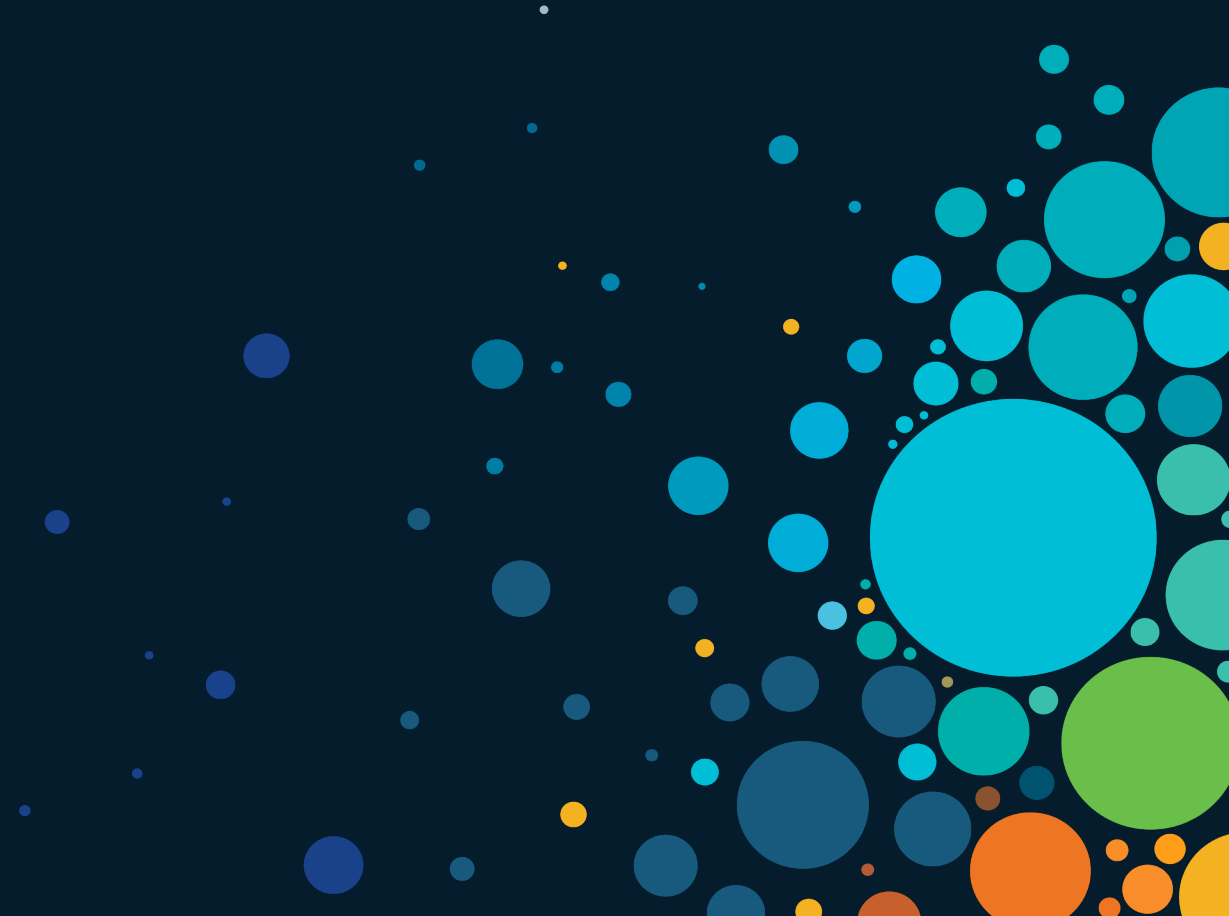


https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENT-2085

Agenda

- Introduction
- Troubleshooting OSPF
  - OSPF Neighbours
  - LSAs and LSDB
- Troubleshooting BGP
  - BGP Neighbours
  - BGP Updates
- Conclusion

Introduction



How This Session Will Help You

- Develop a tactical approach to interrogating your network
- Minimise the guesswork, offer practical takeaways
- Increase your speed in identifying issues

Approaching The Troubleshooting Process

- Trigger for troubleshooting
  - The network behaves differently from our expectations
- Our goal as troubleshooters:
  - Determine why it is not working as expected
  - Explain how to resolve the problem
- Key to successful troubleshooting
  - Good understanding of how the network should behave
  - Tools to gain insight into the network
  - Structured approach

Troubleshooting Methodology

1. Describe and document the problem
2. Gather and review information
3. Hypothesize and propose a solution
4. Test the solution
5. Problem solved? No? Repeat above steps with information learnt

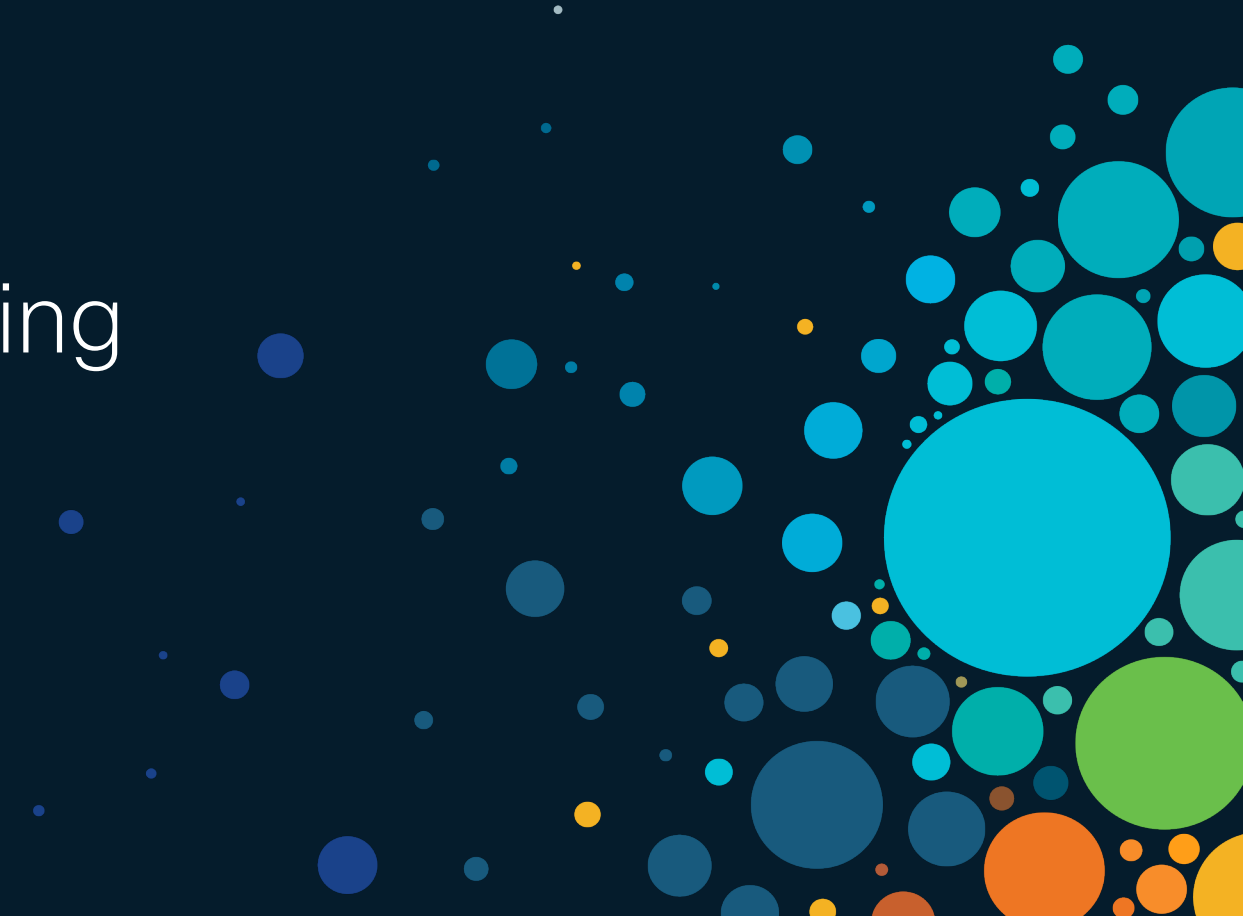
Troubleshooting Routing Protocols

Routing protocols rely on IP routing

Common flow:

1. Establishing neighbourship
2. Exchanging information about the topology
3. Perform computation locally to determine best information
4. Inject best information into routing table

Troubleshooting OSPF



OSPF Neighbours

OSPF Neighbour Intro

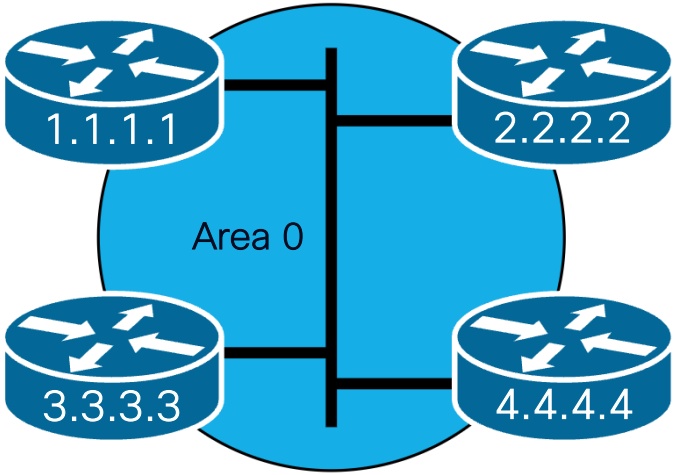
Link-state routing protocol. IP Protocol 89

Logical sequence of events for OSPF neighbours:

1. Peer with neighbors – Full adjacency
2. Exchange Link State Advertisements
3. Path computation – SPF algorithm
4. Update routing table

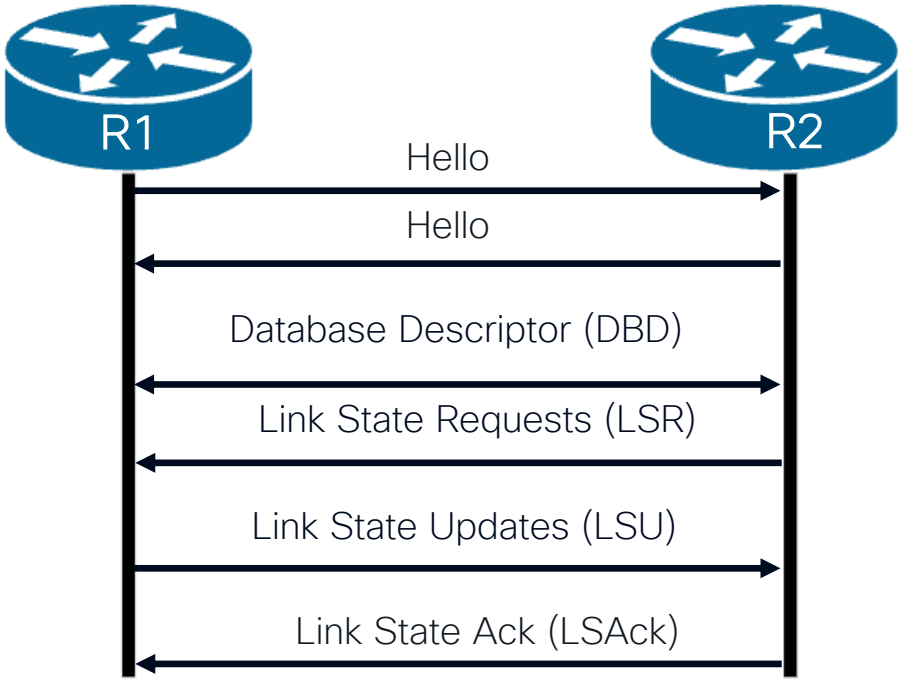
OSPF maintains several tables:

- Interfaces – #show ip ospf interface
- Neighbours – #show ip ospf neighbor
- Link State Database – #show ip ospf database



OSPF Adjacency States

- Down – No OSPF hellos received
- Init – Received OSPF Hello packet from neighbor, but our OSPF hello wasn't acknowledged
- 2-Way – OSPF hello packets exchanged. Bidirectional communication working.
  - Elect DR and BDR if more than 2 OSPF routers
- ExStart – Master/Slave election takes place to start the process of information exchange
- Exchange – DBD containing header info about LSAs
- Loading – Requests and Updates for LSAs
- Full – All information exchanged, and we agree on the network



OSPF Neighbour Command

XE-R1#**show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	1	2WAY/DROTHER	00:00:39	10.1.14.2	GigabitEthernet1
3.3.3.3	1	FULL/BDR	00:00:35	10.1.14.3	GigabitEthernet1
4.4.4.4	1	FULL/DR	00:00:31	10.1.14.4	GigabitEthernet1

- Neighbor ID – Represents neighbours router ID, does not have to be a routable address
- Pri – Priority on the neighbour interface used for DR/BDR election. Higher is more preferred.
- State – Reports the current state with your neighbours. Also describes whether they are Designated Router (DR), Backup Designated Router (BDR) or DROTHER.
- Dead Time – When this timer expires, the neighbourship is terminated. Refreshes every time hello packet is received
- Address – Your neighbours primary IP address that is used to peer with them
- Interface – Your local interface that you use to reach your neighbour

OSPF Commands cont.

- Commands
  - Show ip ospf neighbor
  - Show ip ospf interface
  - Debug ip ospf hello
  - Show run | sec router ospf

```
XE-R1#show ip ospf interface | include Hello|Router
  Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Designated Router (ID) 4.4.4.4, Interface address 10.1.14.4
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
    Adjacent with neighbor 3.3.3.3  (Backup Designated Router)
    Adjacent with neighbor 4.4.4.4  (Designated Router)
```

```
XE-R1#debug ip ospf hello
OSPF-1 HELLO Gi1: Rcv hello from 10.1.14.2 area 0 10.1.14.2
OSPF-1 HELLO Gi1: Send hello to 224.0.0.5 area 0 from 10.1.14.1
OSPF-1 HELLO Gi1: Rcv hello from 10.1.14.2 area 0 10.1.14.2
OSPF-1 HELLO Gi1: Send hello to 224.0.0.5 area 0 from 10.1.14.1
OSPF-1 HELLO Gi1: Rcv hello from 10.1.14.2 area 0 10.1.14.2
```

OSPF Neighbours – No State

- #Show ip ospf neighbor – No state revealed / Neighbor missing

```
XE-R1#show ip ospf neighbor
XE-R1#
```

- What we need?
  - IP Routing
  - Valid OSPF configuration
  - Exchange OSPF hello packets

Troubleshoot IP Routing

- Ping unicast address with source interface and VRF if required
- Ping multicast address
- Traceroute (1 hop for neighbours!)
- Show ip route
- Show ip cef
- Show ip cef exact-route *<source> <destination>*
- Show ip arp x.x.x.x

```
XE-R1#traceroute 10.1.14.2 source GigabitEthernet1
Type escape sequence to abort.
Tracing the route to 10.1.14.2
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.14.2 67 msec *  4 msec
```

```
XE-R1#ping 224.0.0.5 source GigabitEthernet1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 224.0.0.5, timeout is 2
seconds:
Packet sent with a source address of 10.1.14.1
Reply to request 0 from 10.1.14.3, 9 ms
Reply to request 0 from 10.1.14.4, 10 ms
Reply to request 0 from 10.1.14.2, 9 ms
```

```
XE-R1#show ip route 10.1.14.2
Routing entry for 10.1.14.0/24
  Known via "connected", distance 0, metric 0
(connected, via interface)
...
XE-R1#
XE-R1#show ip cef 10.1.14.2
10.1.14.2/32
  attached to GigabitEthernet1
```

Checking OSPF Configuration

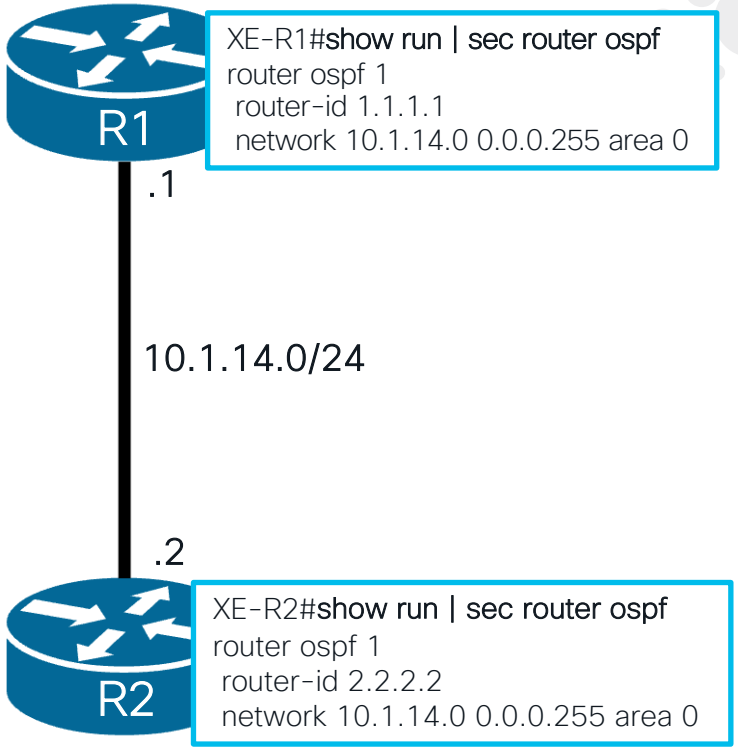
- OSPF configuration Guide:
  - Navigate cisco.com for documentation
  - Search engine – site:cisco.com IOS-XE 16.12.x ASR 1000 OSPF configuration guide
- Unique attributes: Router-ID
- Matching attributes: Area-ID, Hello/Dead timers, Network Address/Mask, MTU, Network Type, Authentication, Stub flags
- Network statement with correct wildcard mask

```
XE-R1#show run | sec router ospf
router ospf 1
 router-id 1.1.1.1
 network 10.1.14.0 0.0.0.255 area 0
```

```
XE-R2#show run | sec router ospf
router ospf 1
 router-id 2.2.2.2
 network 10.1.14.0 0.0.0.255 area 0
```

Troubleshoot OSPF No State

- Problem: New OSPF neighbourship is not forming between two OSPF routers
- Troubleshooting done:
  - No issues with power or interfaces
  - IP routing working
  - Ping OSPF multicast address of 224.0.0.5 working
  - Show run | sec router ospf
  - No authentication configured
  - Devices are directly connected

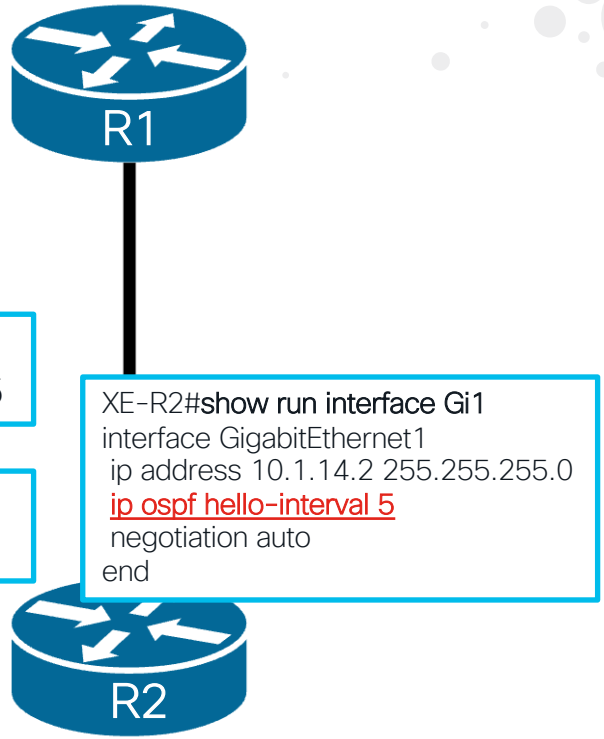


Troubleshoot OSPF No State cont.

- Further Troubleshooting:
  - Show ip ospf interface
  - Show run interface GigabitEthernet1

```
XE-R1#show ip ospf interface | inc Hello
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

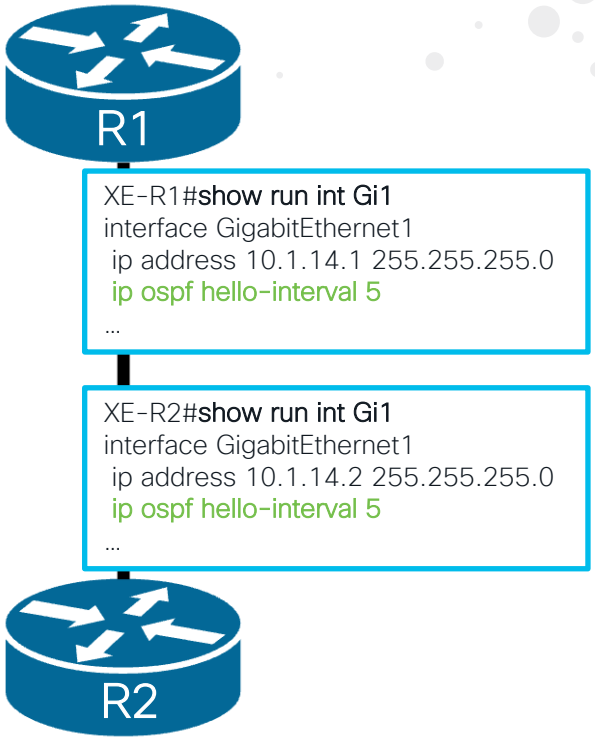
```
XE-R2#show ip ospf interface | inc Hello
  Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
```



Troubleshoot OSPF No State cont.

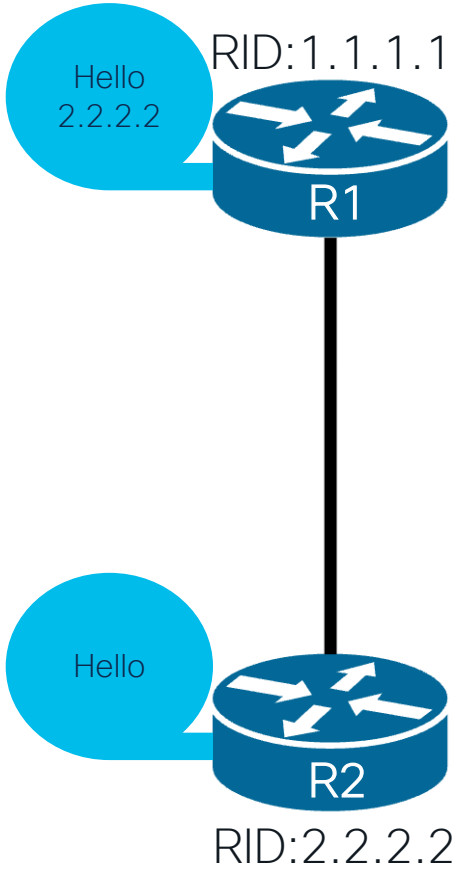
- Root cause: We had different Hello interval configured at the interface level. The Hello and Dead intervals need to match.
- Solution: Configure matching hello packet intervals

- Remember ‘show run | sec router ospf’ is not the only place where OSPF configuration can be found



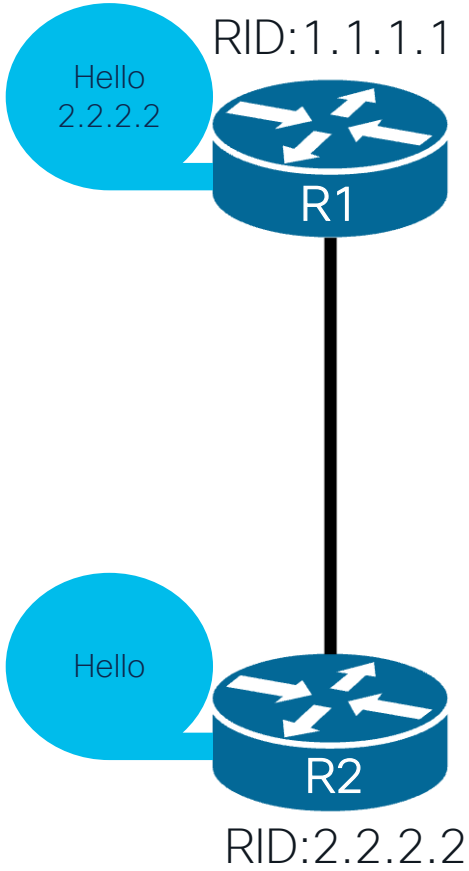
Troubleshoot OSPF State INIT

- Why are we stuck in INIT?
  - One way transport – We have received a hello packet from a neighbour, but they have not acknowledged our hello
- Verify IP routing and transport reachability
- Check OSPF and interface configuration
- Check if our OSPF packets are filtered or blocked
- Debug ip ospf hello



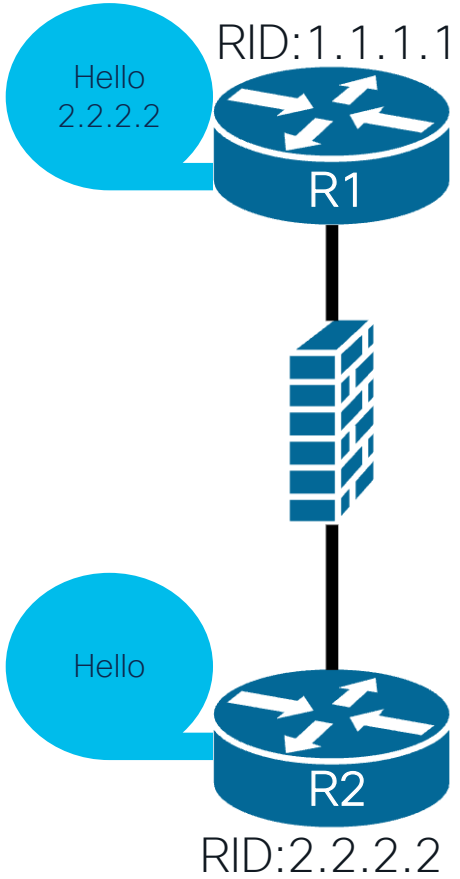
Troubleshoot OSPF INIT Case

- Problem: New OSPF neighborship is not forming between two routers
- Troubleshooting done:
  - No issues with power or interfaces
  - IP routing working. Tested with ping commands.
  - OSPF configuration looks correct at global and link level
  - Performed packet capture and confirmed packets leaving R1's interface but never arrive on R2's interface.
  - Checked and there's no ACL blocking any OSPF packets on R2's link.



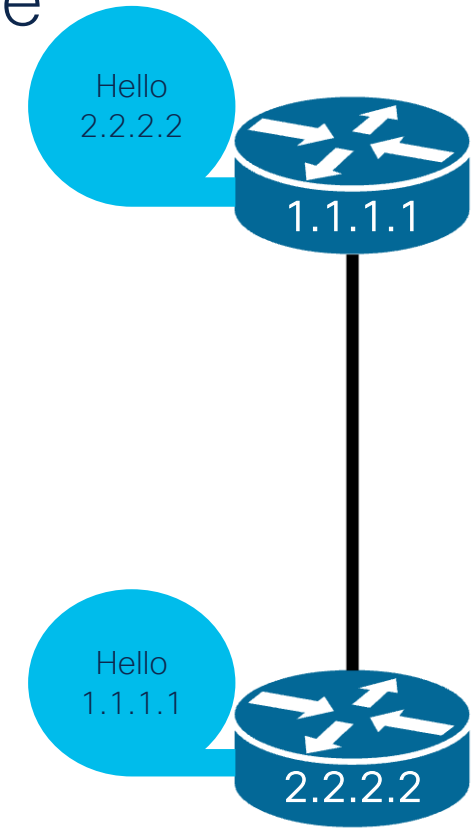
Troubleshoot OSPF INIT Case cont.

- Further Troubleshooting:
  - Clarified how our devices are connected
  - Found there's a firewall in path
  - Firewall was misconfigured and didn't have correct rule to allow our OSPF packets to pass.
- Root Cause: Firewall was dropping our OSPF packets sourced from R1 towards R2
- Solution: Configure the correct firewall rules



OSPF Neighbours – Exstart / Exchange

- Transport is working and we have bidirectional exchange of hello packets
- If we can't progress from Exchange state, it indicates issue with our exchange of DBD. Most common issue is MTU configuration on links don’t match.
- How to solve?
  - Compare OSPF and link configuration on both sides
  - Check if directly connected or any L2 transit device in between. Ensure that MTU is uniform along the path.
  - Test ping with full MTU size and DF-BIT set
  - OSPF debug – debug ip ospf adj



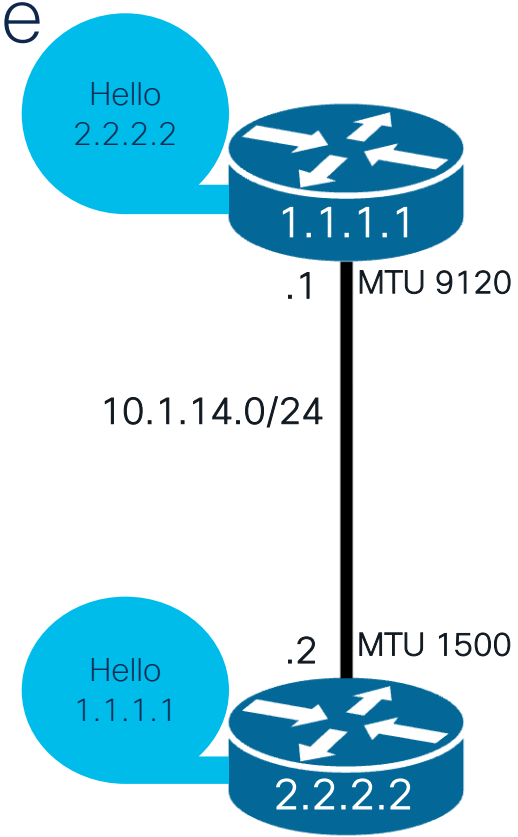
OSPF Neighbours – Exstart / Exchange

- Test ping with full MTU size and df-bit set

```
XE-R1#ping 10.1.14.2 size 9000 source GigabitEthernet1 df-bit
Type escape sequence to abort.
Sending 5, 9000-byte ICMP Echos to 10.1.14.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.14.1
Packet sent with the DF bit set
.....
Success rate is 0 percent (0/5)
```

- Debug ip ospf adj

```
OSPF-1 ADJ   Gi1: Rcv DBD from 2.2.2.2 seq 0x1EC6 opt 0x52 flag 0x7 len
32  mtu 1500 state EXCHANGE
OSPF-1 ADJ   Gi1: Nbr 2.2.2.2 has smaller interface MTU
```



OSPF Neighbours – Flapping

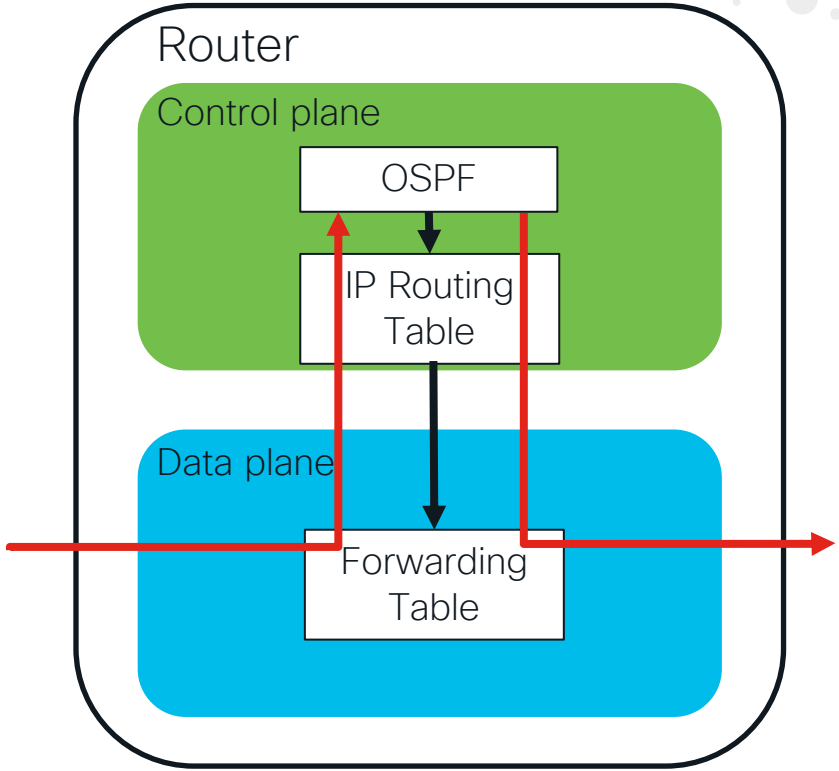
- What's happening?
  - Are we flapping between different states? Pattern?
- What do we know?
  - Depends at what state we are reaching before going back to DOWN

```
XE-R1#show log | include %OSPF-5-ADJCHG
%OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on GigabitEthernet1 from FULL to DOWN, Neighbor Down: Dead timer expired
%OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on GigabitEthernet1 from LOADING to FULL, Loading Done
%OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on GigabitEthernet1 from FULL to DOWN, Neighbor Down: Dead timer expired
%OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on GigabitEthernet1 from LOADING to FULL, Loading Done
```

- How to solve FULL to DOWN?
  - Where are my Hello packets?

OSPF Neighbours – Hello Packets

- Where are my hello packets?
- The path they take
  - Inside device: Start in control plane then exit out an interface
  - Between devices: Control plane to control plane
- Where can they get lost?
  - Route processor CPU utilization 100%
  - Interface issues
  - Blocked or filtered



OSPF Hello Packets cont.

RP CPU utilization

- Responsible for generating and processing control plane bound traffic
- #show process cpu sorted
- #show process cpu history
- Capture during time of issue to identify root cause of high CPU

```
XE-R1#show process cpu sorted
 CPU  utilization for five seconds:   100%/0%; one minute:   99%; five minutes:   81%
....
```

```
XE-R1#show process cpu history
....
100                                                                             *
 90                 *                                                           *
 80                 *              *              **                            *
 70            *    *              *            *  **          *   *
 60            *   **              *            * ***          *   *
 50            *  ***       *      *      *     ******        **   *
 40    *       ******    * *      *    ** * ********    * **** *
 30   **  *  ******** *  * *      **    ** ********** ********* *
 20   ** ** ********* *  *** *  **** **** ********** ***********
 10 ************************************************************#***
   0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0
                      CPU% per minute (last 60 minutes)
                   * = maximum CPU%   # = average CPU%
....
```

OSPF Hello Packets cont.

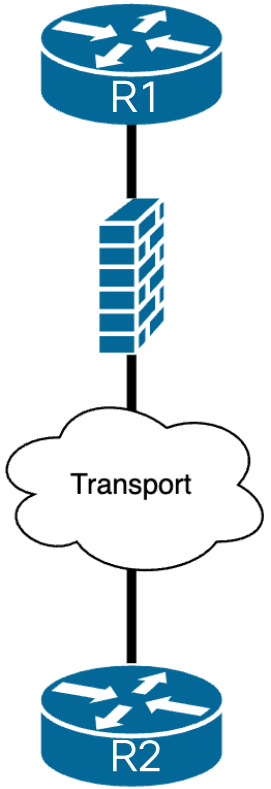
Interface Issues

- Inbound
  - Input errors
  - Input queue - can get wedged
- Outbound
  - Output errors
  - Output queue
  - Output drops
  - QoS configured?
  - #show policy-map interface GigabitEthernet1 output
    - Check class-map forwarding packets with DSCP value CS6

```
XE-R1#show interface GigabitEthernet1
GigabitEthernet1 is up, line protocol is up
...
  Internet address is 10.1.14.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
...
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Output queue: 0/40 (size/max)
...
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
...
     0 output errors, 0 collisions, 1 interface resets
...
```

OSPF Hello Packets cont.

- Filtering / Blocking
  - Is there any ACLs on the interfaces that are blocking our hellos?
  - Is there any FW/ZBFW that might be blocking our hellos?
- Transport
  - Consider if your neighbors are directly connected or if there's any intermediate devices in between
  - Consider if you are using a tunnel to peer with your neighbors. Need to verify that the tunnel is configured and working correctly.



Capture OSPF Packets

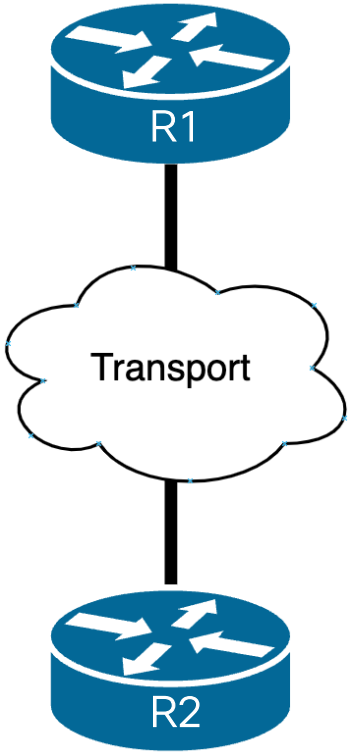
- Capture and inspect the packet
- Embedded Packet Capture (EPC)
- EPC on control–plane or interface
- Match specific or match all packets
- Buffer type:
  - Linear – Stop when buffer is full
  - Circular – Overwrite oldest data
- https://cway.cisco.com/capture-gen-analyzer

```
XE-R1#show monitor capture CAP buffer brief | inc OSPF
 ----------------------------------------------------------------------
---------------------------
  #   size   timestamp     source          destination      dscp     protocol
 ----------------------------------------------------------------------
---------------------------
  0   114    0.000000      10.1.14.2       ->  224.0.0.5    48 CS6   OSPF
  9   114    5.006012      10.1.14.1       ->  224.0.0.5    48 CS6   OSPF
 10   114    5.006012      10.1.14.1       ->  224.0.0.5    48 CS6   OSPF
 11   114    5.047010      10.1.14.4       ->  224.0.0.5    48 CS6   OSPF
 12   114    5.047010      10.1.14.4       ->  224.0.0.5    48 CS6   OSPF
 13   114    6.621022      10.1.14.3       ->  224.0.0.5    48 CS6   OSPF
 14   114    6.621022      10.1.14.3       ->  224.0.0.5    48 CS6   OSPF
```

```
#monitor capture CAP match any control-plane both
#monitor capture CAP start
#monitor capture CAP stop
#show monitor capture CAP buffer brief
```

Troubleshoot OSPF Neighbours Flapping

- Problem: OSPF neighbours are flapping between DOWN and FULL sporadically throughout the day
- Troubleshooting done:
  - IP Routing is correct
  - OSPF configuration is correct
  - CPU utilization is stable over the last 24 hours
  - No packet loss or errors on local links
  - Clarified that there's L2 switching solution in between
- Hypothesis: OSPF packets are getting lost in the transport



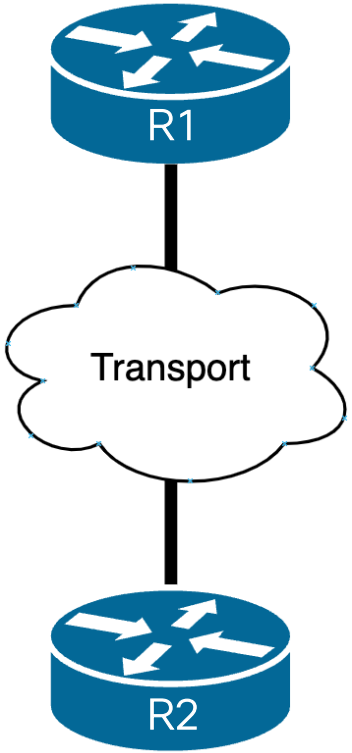
Troubleshoot OSPF Neighbours Flapping cont.

- Further troubleshooting:
  - Transport is managed by another organization
  - Configured EPC with circular buffer to capture OSPF packets on link. Leave it running in background
  - Configured EEM script to trigger when OSPF adjacency goes down. Stop and export EPC, also capture various command outputs

```
event manager applet EEM-TAC-OSPF authorization bypass
event syslog pattern "%OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on GigabitEthernet1 from FULL"
action 1.0 cli command "enable"
action 1.2 cli command "show clock"
action 2.0 cli command "monitor capture TAC stop"
action 2.2 cli command "monitor capture TAC export bootflash:OSPF-CAPTURE.pcap”
action 2.4 cli command "show run | append bootflash:TAC-TSHOOT.txt"
action 2.6 cli command "show interface | append bootflash:TAC-TSHOOT.txt"
action 3.0 cli command "show process cpu sorted | append bootflash:TAC-TSHOOT.txt"
action 3.2 cli command "show process cpu history | append bootflash:TAC-TSHOOT.txt"
action 4.0 cli command "show ip ospf neighbor | append bootflash:TAC-TSHOOT.txt"
action 4.2 cli command "show ip ospf events | append bootflash:TAC-TSHOOT.txt"
action 4.4 cli command "show ip ospf interface | append bootflash:TAC-TSHOOT.txt"
action 5.0 cli command "show logging | append bootflash:TAC-TSHOOT.txt"
action 6.0 syslog msg "EEM TAC OSPF troubleshooting script executed"
```

Troubleshoot OSPF Neighbours Flapping cont.

- Root cause: Issue with transport. Confirmed that our device did send the OSPF packets on the link leading up to flap and it was free from any CPU or interface errors
- Solution: Team that managed the transport investigated and found that there was issue with the layer 2 network between our devices



OSPF LSA and LSDB

OSPF LSAs and Routes Intro

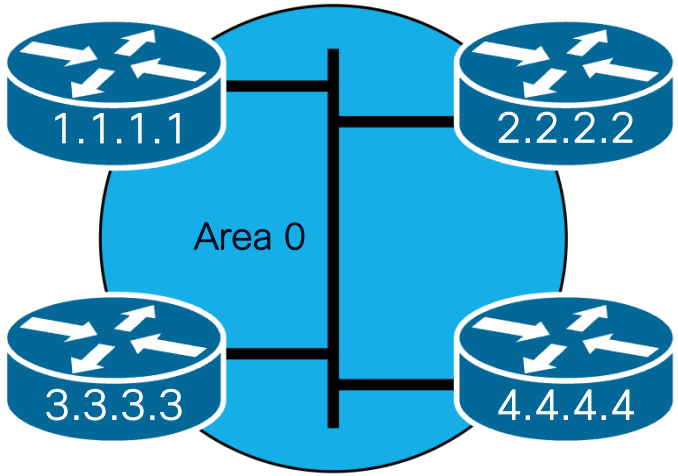
- How do we learn OSPF routes?
- Learning and exchanging LSA in our OSPF Database (LSDB)
- LSA sent and received depends on:
  - Router Type, Network Type, Area Type
- Preference of LSA
  - Cost metric (Lower is preferred)
  - Intra area > Inter area > External
- Administrative Distance of 110

LSA Type 1	Router
LSA Type 2	Network
LSA Type 3	Summary
LSA Type 4	Summary ASBR
LSA Type 5	AS External

LSA Type 1 – Router LSA

- Who: Every router in every area
- What: How routers advertise their connected interfaces
- Where: Inside an area
- #show ip ospf database router
- #show ip ospf database router self-originate

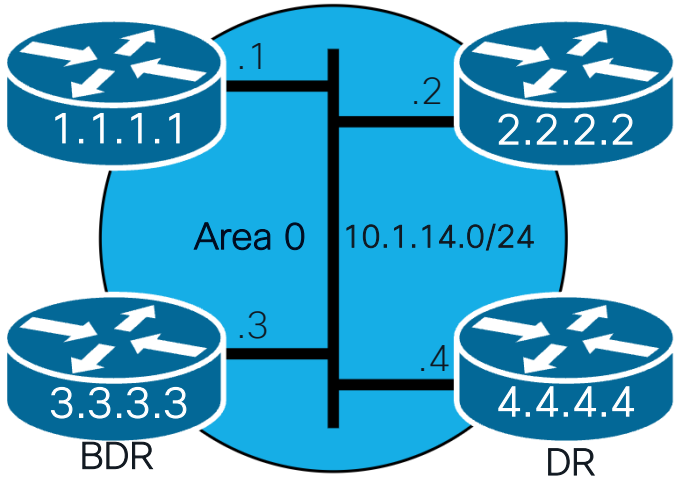
```
XE-R1#show ip ospf database
                Router Link States (Area 0)
Link ID         ADV Router      Age         Seq#       ...
1.1.1.1         1.1.1.1         650         0x800004A4 ...
2.2.2.2         2.2.2.2         651         0x800004CE ...
3.3.3.3         3.3.3.3         650         0x80000503 ...
4.4.4.4         4.4.4.4         650         0x800004C7 ...
```



LSA Type 2 – Network LSA

- Who: Designated routers (DR) on all non-point-to-point links
- What: The DR collects all the Type 1 LSAs and sends out a single Type 2 representing all the routers on the link.
- Where: Inside an area
- #show ip ospf database network

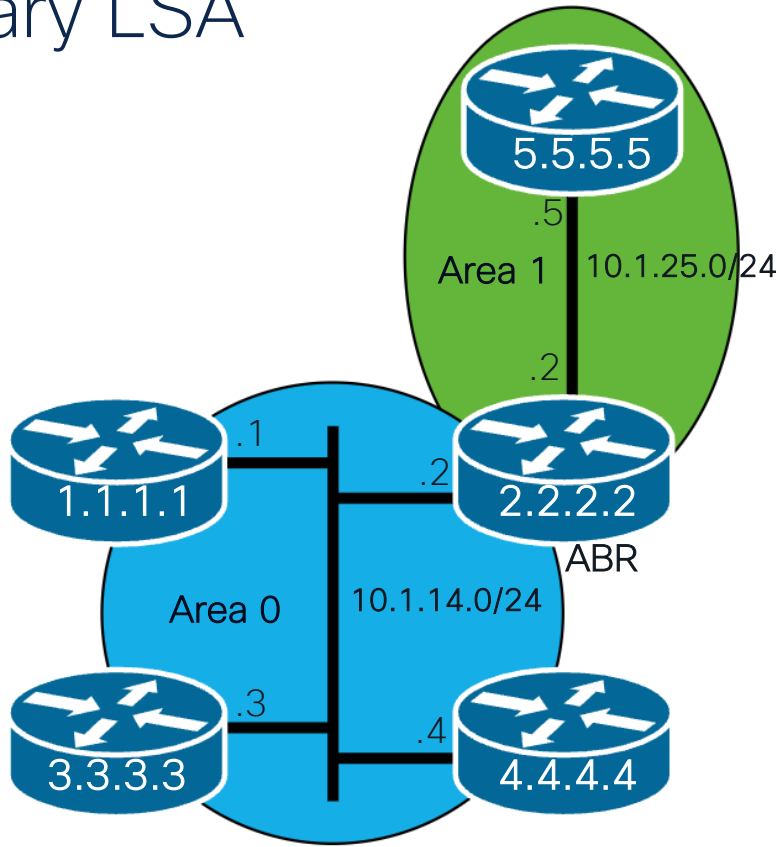
```
XE-R1#show ip ospf database
...
                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       ...
10.1.14.4       4.4.4.4         39          0x80000002 ...
```



LSA Type 3 – Network Summary LSA

- Who: Area Border Routers (ABRs)
- What: ABRs send a single LSA representing all the Type 1 and Type 2 LSAs in an area. This reduces the number of LSAs on the routers in other areas
- Where: Inter area (standard areas)
- #show ip ospf database summary

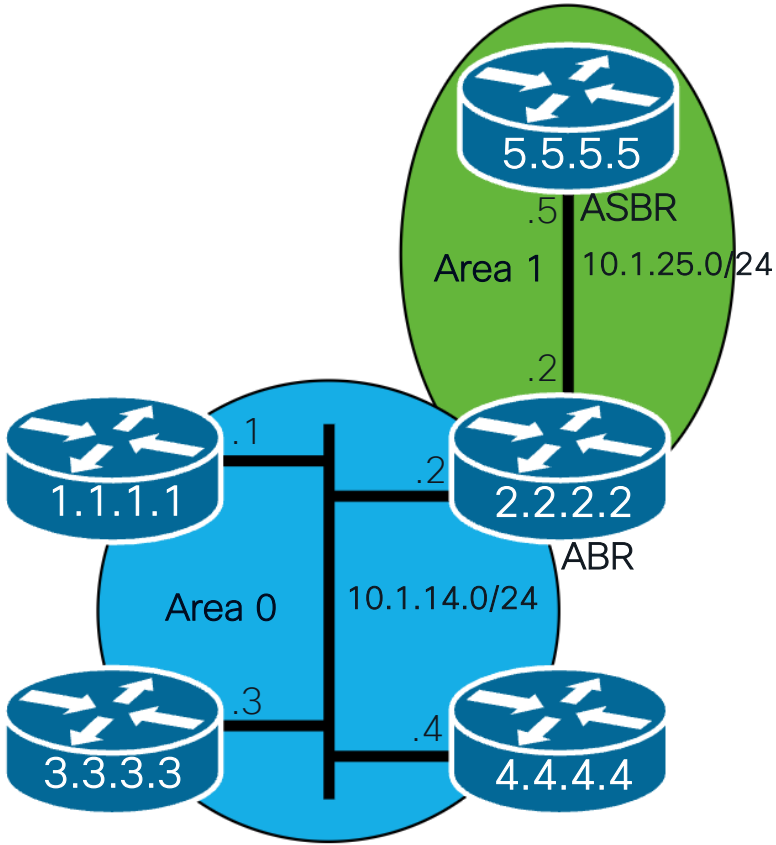
```
XE-R1#show ip ospf database
 ...
                Summary Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       ...
10.1.25.0       2.2.2.2         159         0x80000001 ...
```



LSA Type 4 – ASBR Summary

- Who: ABRs connected to an area where external routes (Type 5) are originated
- What: Type 4 LSAs are sent to other areas to build the shortest path tree to an ASBR
- Where: Inter area (standard areas)
- #show ip ospf database asbr-summary

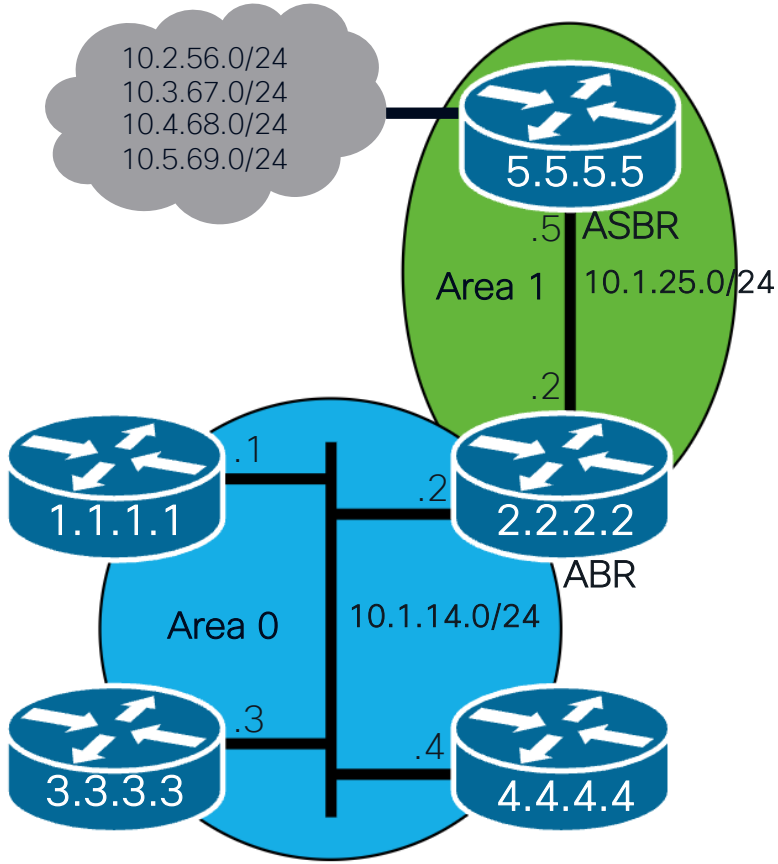
```
XE-R1#show ip ospf database
 ...
                Summary ASB Link States (Area 0)
Link ID         ADV Router      Age         Seq#       ...
5.5.5.5         2.2.2.2         205         0x80000001 ...
```



LSA Type 5 – AS External

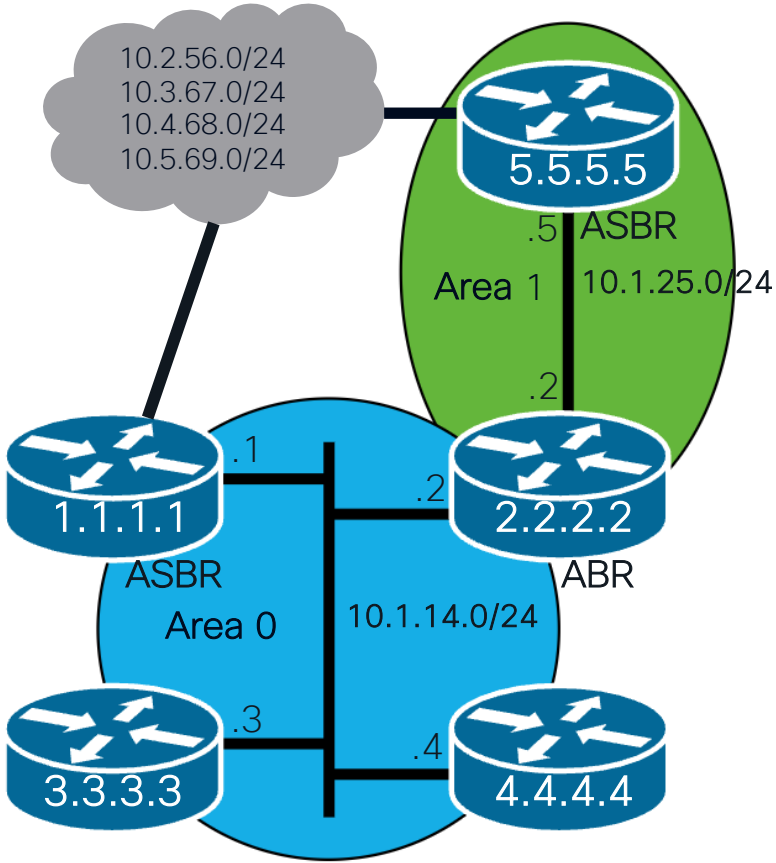
- Who: ASBR with the redistribute command that are not in a NSSA area
- What: Represents any external routes redistributed into OSPF
- Where: Inter area (standard areas)
- #show ip ospf database external

```
XE-R1#show ip ospf database
 ...
                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       ...
10.2.56.0       5.5.5.5         200         0x80000001 ...
10.3.67.0       5.5.5.5         200         0x80000001 ...
10.4.68.0       5.5.5.5         200         0x80000001 ...
10.5.69.0       5.5.5.5         200         0x80000001 ...
```



OSPF Preference of LSA

- Ordered from most preferred to least preferred:
  - Intra-Area (O)
  - Inter-Area (O IA)
  - External Type 1 (E1)
  - NSSA Type 1 (N1)
  - External Type 2 (E2)
  - NSSA Type 2 (N2)
- After picking the preferred LSA, router will pick the lowest cost path as tie breaker
  - Cost is a metric based on bandwidth of link



OSPF LSAs and Areas

- Backbone Area / Standard Areas
  - LSA type 1, 2, 3, 4 and 5
- Stub Areas
  - LSA type 1, 2 and 3 LSAs. Default route is substituted for external routes
- Totally Stubby Areas
  - LSA type 1, 2. The type 3 LSA is replaced with a default route, substituted for all external and inter-area routes

OSPF Missing LSAs

- Are they missing in the LSDB or Routing Table?
- All OSPF LSA missing from LSDB?
  - Make sure you have full adjacency with neighbours.
- Only missing summary LSA from LSDB originating from another area?
  - Make sure that area is contiguous with area 0, i.e. our ABR must have valid adjacency in both area 0 and area X
- Only OSPF external LSA missing from LSDB?
  - Are you in a stub area? Only support Type 1, 2 and 3 LSAs
  - Only Not So Stubby Areas allow for external LSAs
  - Are they being redistributed in OSPF correctly? Need to be in RIB for redistribution to work

OSPF Routes Missing from Routing Table

- Do we have the LSA in our LSDB?
  - Show ip ospf database
- Are we learning this route from different routing protocol instance?
  - Consider administrative distance. Static, eBGP, EIGRP all have lower distance compared to OSPF
- Is there any type of filtering happening within our OSPF process?
  - #Show ip protocols
  - Check configuration of route-maps, distribute-lists, access-lists.
  - Don't forget about implicit deny

```
XE-R1#show ip route 10.5.69.0
% Subnet not in table
```

```
XE-R1#show ip ospf database | begin External
            Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       ...
10.2.56.0       5.5.5.5         170         0x8000001B ...
10.3.67.0       5.5.5.5         170         0x8000001B ...
10.4.68.0       5.5.5.5         170         0x8000001B ...
10.5.69.0       5.5.5.5         170         0x8000001B ...
```

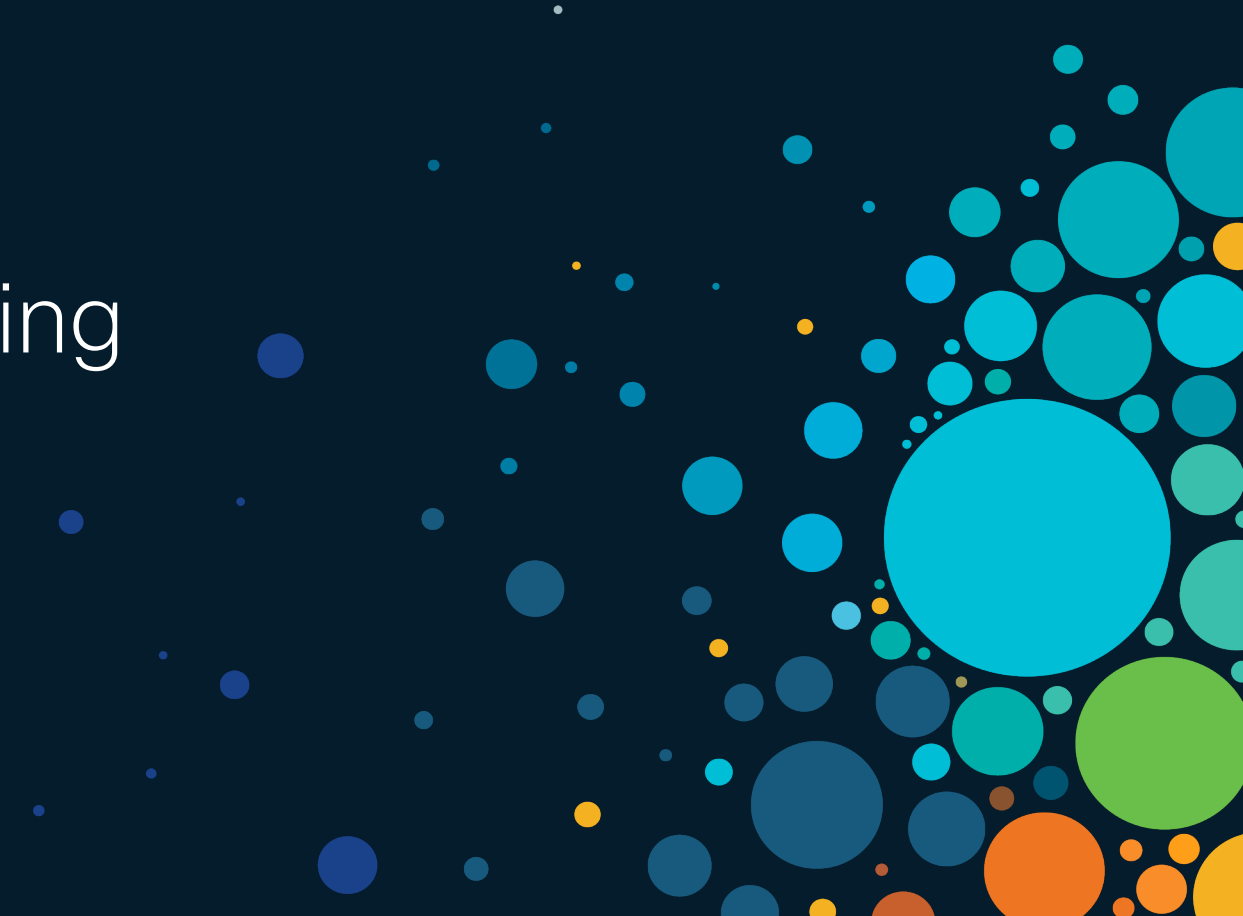
```
XE-R1#show ip protocols | sec ospf
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is EXTERNAL_IN
```

```
XE-R1#show ip access-lists EXTERNAL_IN
Standard IP access list EXTERNAL_IN
    10 permit 10.3.67.0, wildcard bits 0.0.0.255 (1 match)
    20 permit 10.4.68.0, wildcard bits 0.0.0.255 (1 match)
```

OSPF Summary

- When troubleshooting it is important to:
  - Understand what OSPF configuration is required
    - *Use Cisco documentation that is version and platform specific*
  - Understand the OSPF neighborship states and how to follow your hellos
    - *Learn how to confirm and check the path it takes through your devices*
  - Understand how to read the LSDB
    - *You will be able to understand OSPF topology just like your router*

Troubleshooting BGP

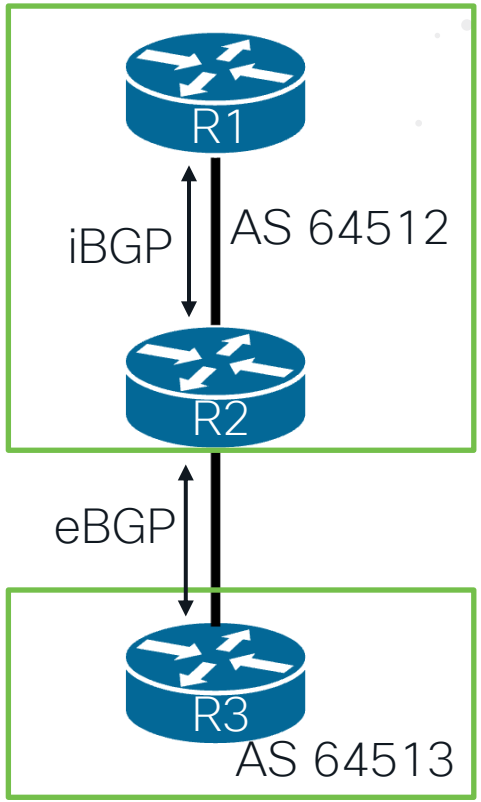


cisco Live!

BGP Neighbours

BGP Intro

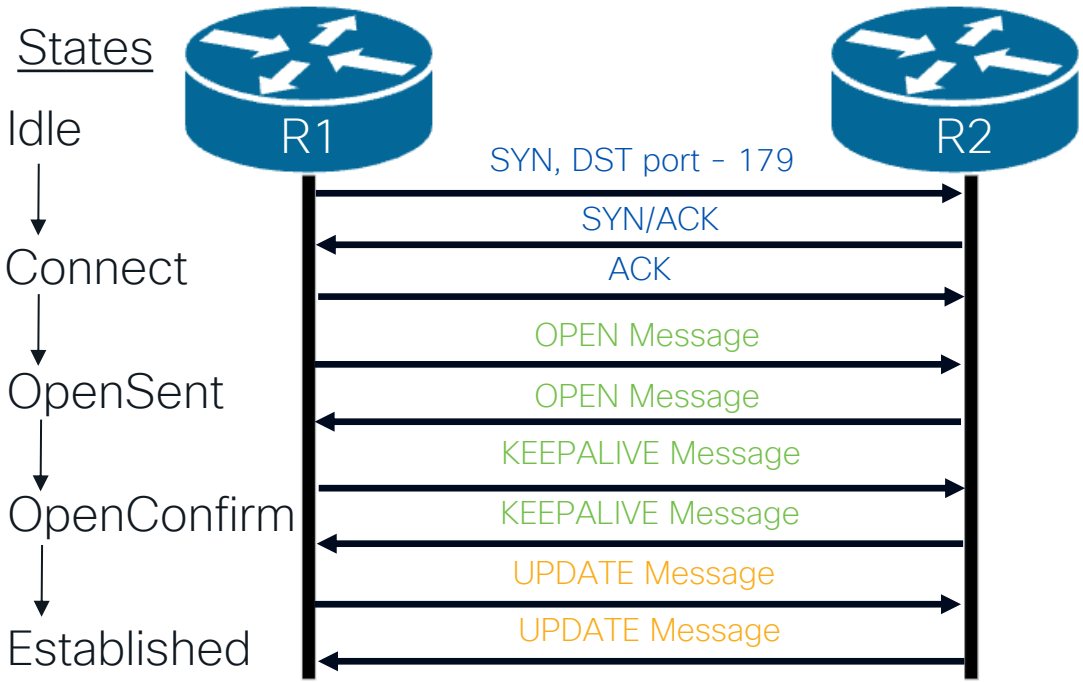
- TCP based routing protocol (Port 179)
- External BGP (eBGP) to peer with external networks
- Internal BGP (iBGP) to peer with internal routers
- Router can only be part of one Autonomous System (AS)



BGP Neighbours

1. Establish neighbourship – Explicitly configured
2. Exchange BGP path attributes
3. Path computation – Best path calculation
4. Inject information into routing table

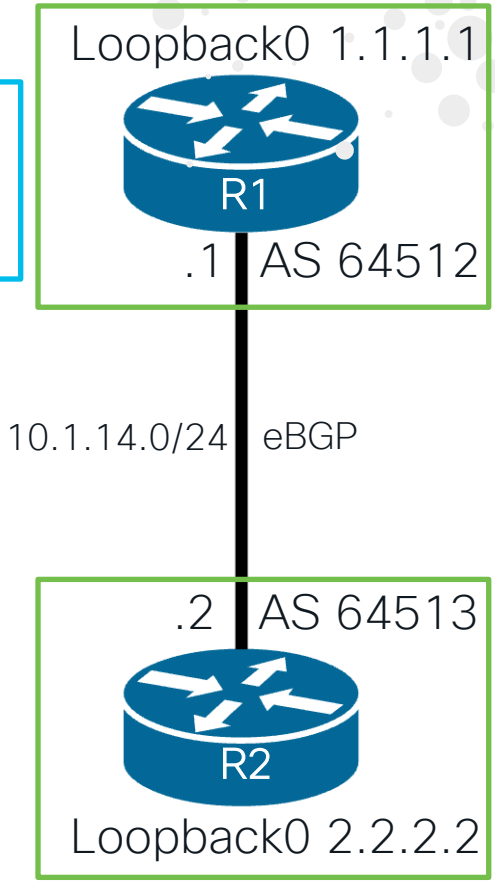
- TCP 3-way handshake
- BGP Peering Session
- Routing Database Synchronization



BGP Commands

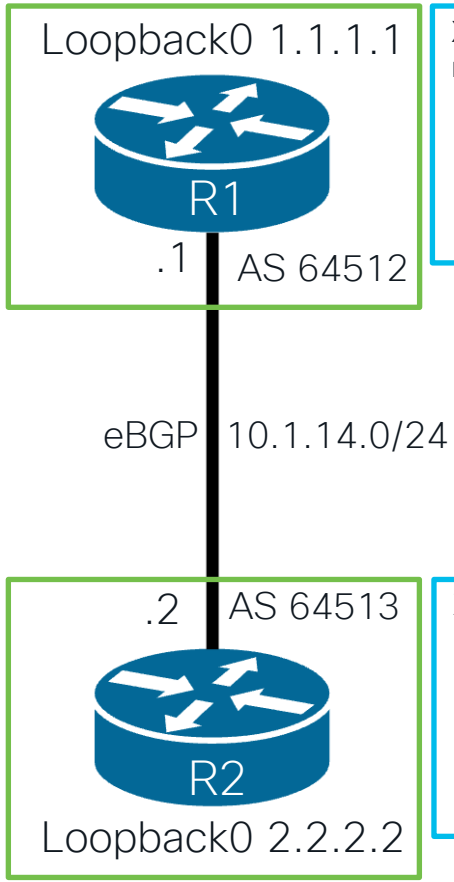
```
XE-R1#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 64512
...
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2.2.2.2         4        64513   54656   54351       24    0    0 4d07h           117
```

```
XE-R1#show ip bgp neighbor 2.2.2.2
BGP neighbor is 2.2.2.2,  remote AS 64513, external link
  BGP version 4, remote router ID 2.2.2.2
  BGP state = Established, up for 4d07h
  Last read 00:00:04, last write 00:00:01, hold time is 21, keepalive interval is 7 seconds
...
  Neighbor capabilities:
...
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
...
For address family: IPv4 Unicast
...
```



BGP Neighbours

- Requirements:
  - IP Routing
  - Explicit ‘neighbor’ command
  - Route to peering IP address
  - AS Number
    - eBGP peers need valid ‘remote-as’ value different to ours
    - iBGP same ‘remote-as’ value
  - Matching Authentication

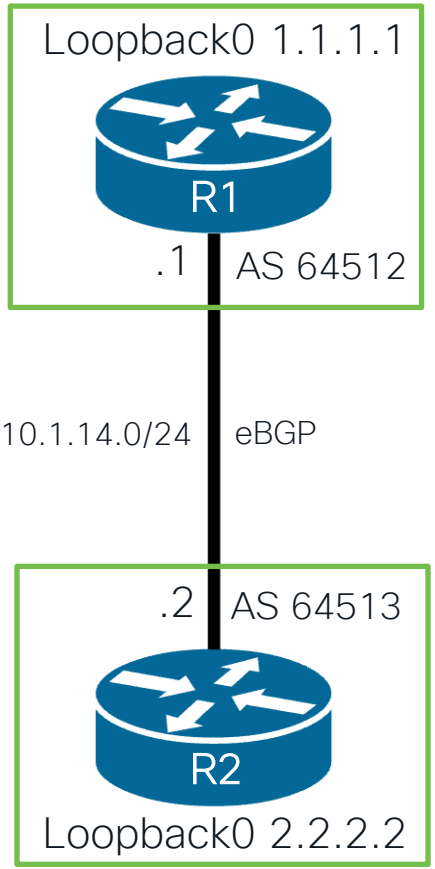



```
XE-R1#show run | sec router bgp
router bgp 64512
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 64513
 neighbor 2.2.2.2 ebgp-multihop 2
 neighbor 2.2.2.2 update-source Loopback0
 neighbor 2.2.2.2 timers 7 21
```

```
XE-R2#show run | sec router bgp
router bgp 64513
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 64512
 neighbor 1.1.1.1 ebgp-multihop 2
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 1.1.1.1 timers 60 180
```

Solve Peering Issues

- Verify Configuration
  - Peering IP address
  - AS Number
  - MD5 Authentication (Optional)
  - ebgp-multihop *hop-count* (eBGP)
- Verify Reachability
  - Ping x.x.x.x source y.y.y.y
  - Do we have a route to peering IP address
- BGP will not use the default route to reach a neighbor




```
XE-R1#show ip route 2.2.2.2
Routing entry for 2.2.2.2/32
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
  * 10.1.14.2
      Route metric is 0, traffic share count is 1
XE-R1#
XE-R1#
XE-R1#ping 2.2.2.2 source loopback0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2,
timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 6/13/39 ms
```

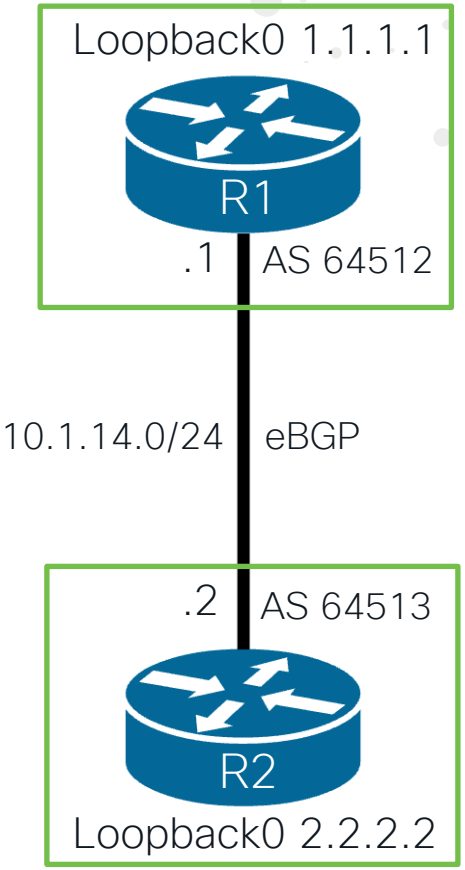
BGP Verifying TCP

```
XE-R1#show tcp brief
TCB             Local Address         Foreign Address       (state)
7F7C9A732360    1.1.1.1.179           3.3.3.3.35500         ESTAB
7F7C7025DCA0    1.1.1.1.38522         2.2.2.2.179           ESTAB
```

```
XE-R1#telnet 2.2.2.2 179 /source-interface loopback0
Trying 2.2.2.2, 179 ... Open
[Connection to 2.2.2.2 closed by foreign host]
```

```
XE-R1#telnet 2.2.2.2 179 /source-interface loopback0
Trying 2.2.2.2, 179 ...
% Destination unreachable; gateway or host down
```

```
XE-R1#telnet 2.2.2.2 179 /source-interface loopback0
Trying 2.2.2.2, 179 ...
% Connection refused by remote host
```



BGP Notifications

```
%BGP-3-NOTIFICATION: sent to neighbor 2.2.2.2 active 2/2 (peer in wrong AS) 2 bytes FC01
%BGP-3-NOTIFICATION: sent to neighbor 2.2.2.2 passive 2/2 (peer in wrong AS) 2 bytes FC01
%BGP-3-NOTIFICATION: sent to neighbor 2.2.2.2 active 2/2 (peer in wrong AS) 2 bytes FC01
```

- BGP notifications consist of an error code, sub-code and data
- Data portion may contain what triggered the notification
- Full list of error codes and sub-codes can be found here:
  - IANA BGP Parameters
  - https://www.iana.org/assignments/bgp-parameters/bgp-parameters.xhtml

Value	Name	Reference
1	Message Header Error	RFC 4271
2	OPEN Message Error	RFC 4271
3	UPDATE Message Error	RFC 4271
4	Hold Timer Expired	RFC 4271
5	Finite State Machine Error	RFC 4271
6	Cease	RFC 4271

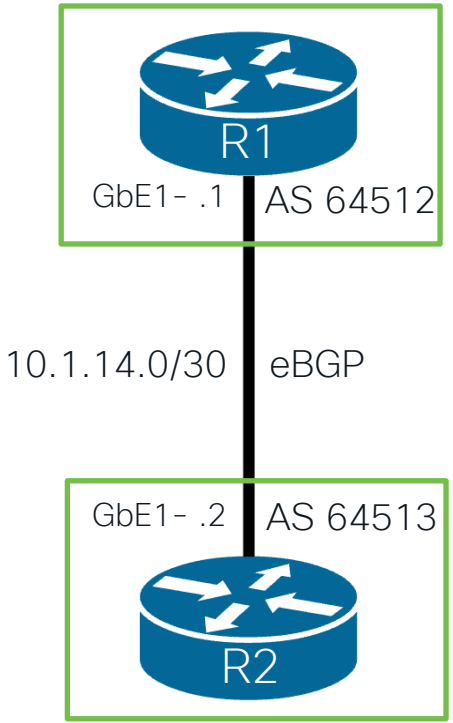
Syslog Messages

- #show logging
- Saved in devices volatile memory
- Syslog can be sent to external server
- Important to collect the messages before, during and after an issue has occurred
- Try to understand what else is happening around the time of our issue
- Collect on both sides of neighbourship

Code	Severity
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Informational
7	Debug

Troubleshoot BGP Neighbour Down

- Problem: After recently upgrading some devices in their network, eBGP peering is not establishing between two devices. Remaining in Idle state.
- Troubleshooting done:
  - eBGP configuration correct
  - Authentication removed
  - Interfaces are up and clean. No filters
  - Unicast working – ping successful
  - Packet captures on GbE1 not showing any BGP packets

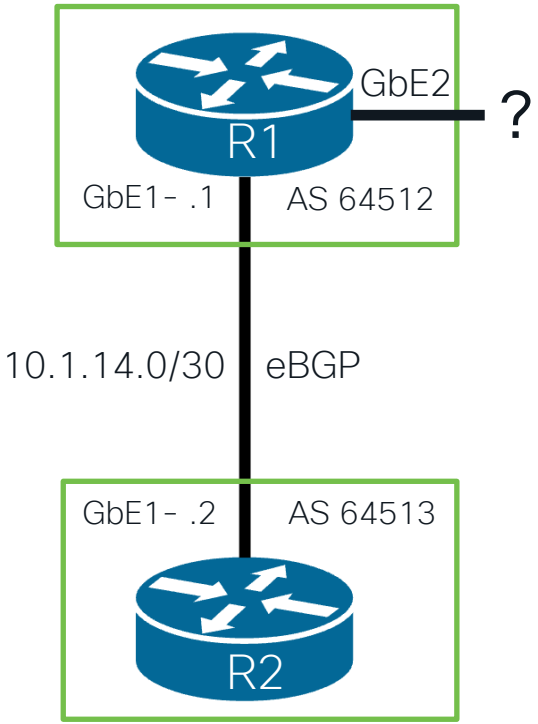



```
XE-R1#show run | sec router bgp
bgp router-id 1.1.1.1
router bgp 64512
 bgp log-neighbor-changes
 neighbor 10.1.14.2 remote-as 64513
```

```
XE-R2#show run | sec router bgp
bgp router-id 2.2.2.2
router bgp 64513
 bgp log-neighbor-changes
 neighbor 10.1.14.1 remote-as 64512
```

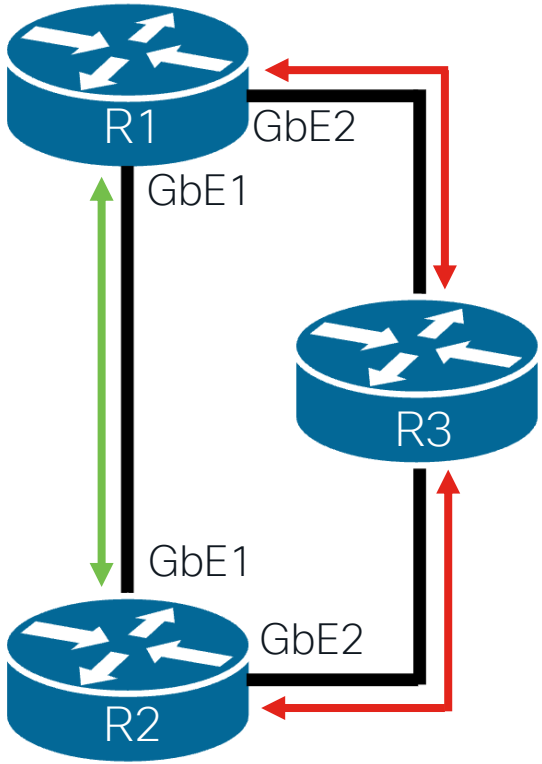
Troubleshoot BGP Neighbour Down cont.

- Further troubleshooting:
  - Traceroute 10.1.14.2 source 10.1.14.1
  - Traceroute result showed that there was 3 hops to reach our eBGP neighbours interface, we are expecting only 1 hop.
  - Expect to use 10.1.14.0/30 “connected” route
  - ‘XE-R1#Show ip route 10.1.14.2’ and we find 10.1.14.2/32 BGP route pointing in a different direction out of Interface GbE2



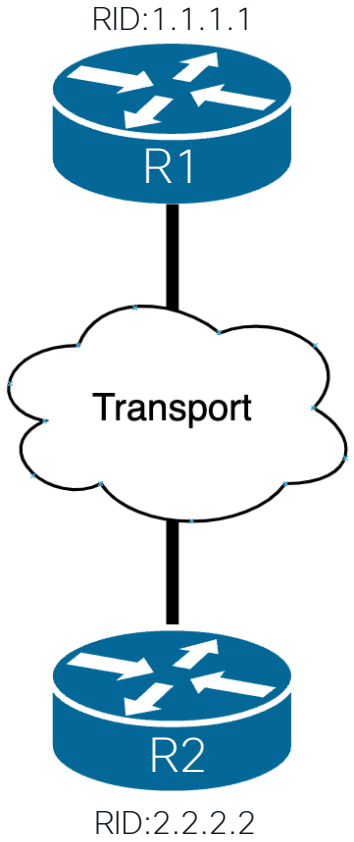
Troubleshoot BGP Neighbour Down cont.

- Root cause: R1 originally had a /30 “connected” route via GbE1 for R2’s eBGP neighbours interface.
- After network changes there was a /32 route via GbE2 in R1’s routing table for R2’s interface learnt through newly configured BGP router R3
  - BGP packets TTL expiring
  - Longest prefix match. /32 is preferred over /30
- Solution: Configure /32 static route towards desired direction.



Troubleshoot BGP Neighbour Flapping

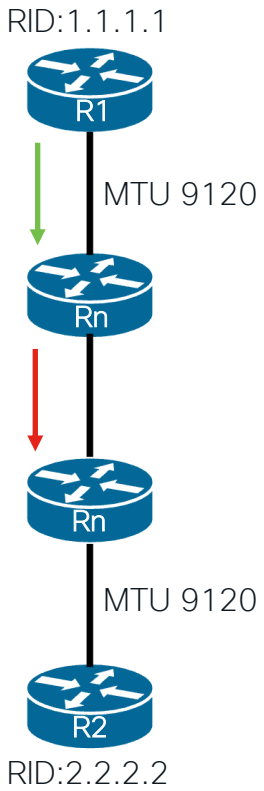
- Problem: Router eBGP Neighbour is flapping every 3 minutes. Issue began after changing the number of prefixes exchanged from 1 (default-route) to 100,000+
- Troubleshooting done:
  - IP routing is working
  - Router CPU is stable
  - Valid BGP neighbourship configuration
  - No packet loss or errors on local links
  - No memory constraint issues on the device



Troubleshoot BGP Neighbour Flapping cont.

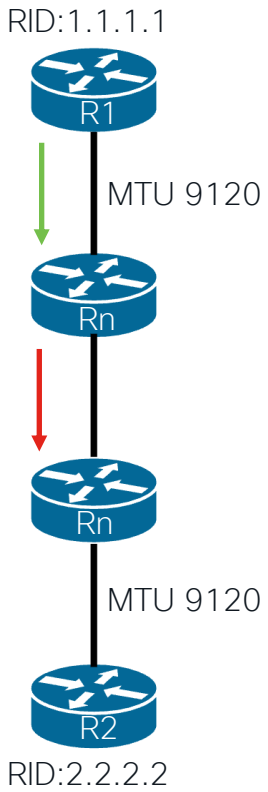
- Further troubleshooting:
  - Identified that we have large MTU configured on our BGP links
  - #show ip bgp neighbors x.x.x.x | inc max data segment
  - Ping x.x.x.x source y.y.y.y size XXXX df-bit. Failing to send packet larger than 1500 MTU. We expect to be able to send packets as large as 9120 bytes in this network

```
XE-R1#ping 2.2.2.2 source 1.1.1.1 size 1520 df-bit
Type escape sequence to abort.
Sending 5, 1520-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
Packet sent with the DF bit set
.....
Success rate is 0 percent (0/5)
```



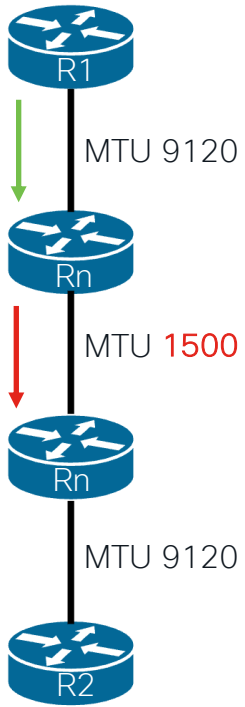
Troubleshoot BGP Neighbour Flapping cont.

- Root Cause:
  - Our BGP update packets could not fit in the path and were dropped in transport
  - BGP OPENs and Keepalives are small
  - UPDATEs can be much larger
- Solution:
  - Make the MTU/MSS value along the path uniform



Troubleshoot BGP Neighbour Flapping cont.

- Path MTU Discovery (PMTUD)
  - Enabled by default on IOS-XE for BGP
  - Used to find the smallest MTU value that can be used from source to destination
  - Sends packet with max MTU size and 'Do Not Fragment' bit set
  - Routers will respond with ICMP unreachable message if packet does not fit on link.



Troubleshoot BGP Platform Issues – CPU

High CPU

- Is BGP the culprit of the high CPU or the victim?
- CPU spike during initial convergence can be normal
- Need to capture CPU data during time of issue to isolate
- Capture in intervals
  - CPU related commands
  - BGP related commands
  - Interface related commands
  - Routing table commands
  - Show logging

BGP Route Churn

- We must understand what is baseline and “high” for each unique environment
- Spiking due to “BGP Scanner”, “BGP Router” etc?
- If we are not in the initial convergence, then route churn is the usual culprit
  - Illegal recursive lookup or some other factor causes best path changes for the entire table

```
XE-R1#show process cpu sorted
 CPU  utilization for five seconds:   100%/0%; one minute:   99%; five minutes:   81%
....
139   6795740   1020252   6660   88.34%   91.63%   74.01%   0   BGP Router
```

Troubleshoot BGP Route Churn

- How to identify route churn:
  - Run “show ip bgp summary”, note the table version
  - Wait 30~60 seconds
  - Run “show ip bgp summary” again, then compare table version
- You have 150k routes and see the table version increase by 300
  - This is likely normal route churn
  - Know how many bestpath changes your normally see per minute
- You have 150k routes and see the table version fluctuating by 20K~50K
  - This is bad and the likely cause of your high CPU

Troubleshoot BGP Route Churn cont.

```
XE-R1#show ip bgp all summary | inc table
BGP table version is 936574954, main routing table version 936574954
BGP table version is 429591477, main routing table version 429591477
XE-R1#
XE-R1#
XE-R1#show ip bgp all summary | inc table
BGP table version is 936576768, main routing table version 936576768
BGP table version is 429591526, main routing table version 429591526
XE-R1#
XE-R1#
XE-R1#show ip route | inc 00:00:0
B       187.164.0.0 [200/0] via 218.185.80.140, 00:00:00
B       187.52.0.0 [200/0] via 218.185.80.140, 00:00:00
B       187.24.0.0 [200/0] via 218.185.80.140, 00:00:00
B       187.68.0.0 [200/0] via 218.185.80.140, 00:00:00
B       186.136.0.0 [200/0] via 218.185.80.140, 00:00:00
```

Over 1800 prefixes flapped within 5 seconds

Troubleshoot BGP Route Churn cont.

- What causes large table version changes?
  - Flapping peers
    - Hold-timer expiring
    - Corrupt updates
  - Flapping links or networks
- How to resolve route churn?
  - Don’t try to troubleshoot the entire BGP table at once
  - Isolate one or two prefixes and troubleshoot

Troubleshoot BGP Route Churn cont.

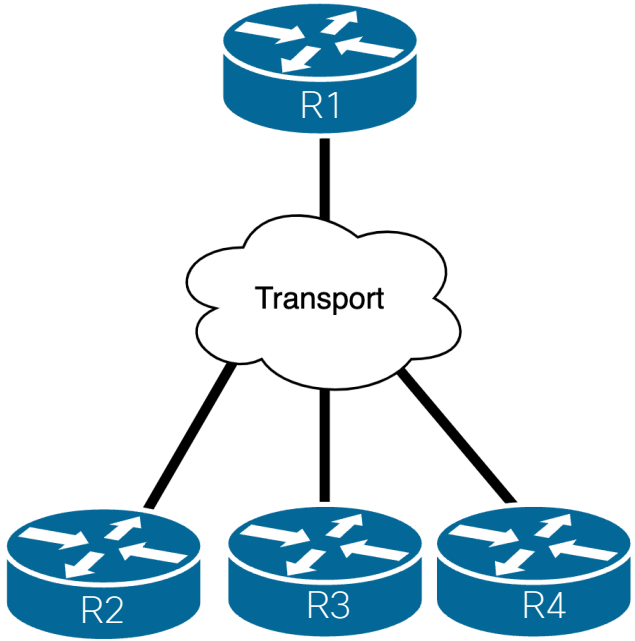
- Figuring out flapping routes from routing table (even in vrf)
- #show ip route vrf * | inc 00:00:0|VRF
- Follow who is advertising and where these prefixes originate from
- Check for any flapping protocols or links closest to the source of these routes

```
XE-R1#show ip route | inc 00:00:0
B       187.164.0.0 [200/0] via 218.185.80.140, 00:00:00
B       187.52.0.0 [200/0] via 218.185.80.140, 00:00:00
B       187.24.0.0 [200/0] via 218.185.80.140, 00:00:00
B       187.68.0.0 [200/0] via 218.185.80.140, 00:00:00
B       186.136.0.0 [200/0] via 218.185.80.140, 00:00:00
```

Troubleshooting High CPU

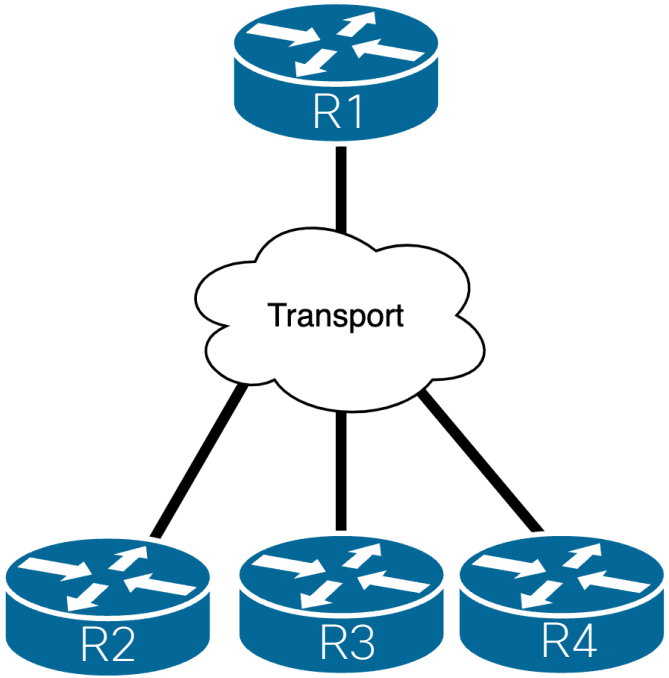
- Problem: eBGP neighbours states are sporadically flapping between. R2, R3 and R4 all reporting R1 hold timer expiring at different times

```
%BGP-3-NOTIFICATION: received from neighbor 1.1.1.1 4/0 (hold time expired) 0 bytes
%BGP-5-NBR_RESET: Neighbor 1.1.1.1 reset (BGP Notification received)
%BGP-5-ADJCHANGE: neighbor 1.1.1.1 Down BGP Notification received
%BGP_SESSION-5-ADJCHANGE: neighbor 1.1.1.1 IPv4 Unicast topology base removed
from session  BGP Notification received
%BGP-5-ADJCHANGE: neighbor 1.1.1.1 Up
%BGP-3-NOTIFICATION: received from neighbor 1.1.1.1 4/0 (hold time expired) 0 bytes
%BGP-5-NBR_RESET: Neighbor 1.1.1.1 reset (BGP Notification received)
%BGP-5-ADJCHANGE: neighbor 1.1.1.1 Down BGP Notification received
%BGP_SESSION-5-ADJCHANGE: neighbor 1.1.1.1 IPv4 Unicast topology base removed
from session  BGP Notification received
```



Troubleshooting High CPU

- Troubleshooting done:
  - BGP configuration valid. No recent changes made
  - IP routing stable. Static routes to reach neighbors loopbacks
  - Interfaces stable and free from errors
  - R1's CPU spiking very high and peaking at 100%
  - Syslog messages and BGP uptime match with spikes on CPU history graph
- Hypothesis: High CPU is causing packet loss

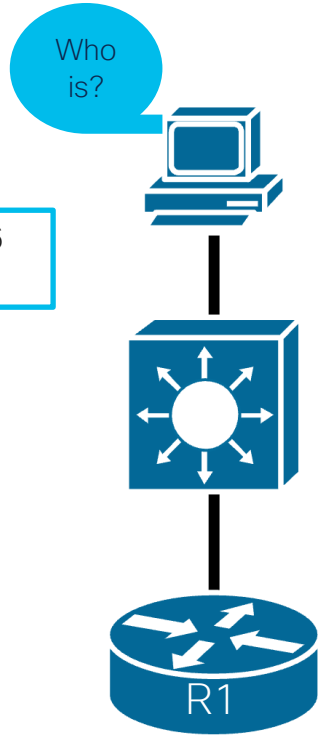


Troubleshooting High CPU cont.

- Further troubleshooting:
  - Observed following syslog message when troubleshooting

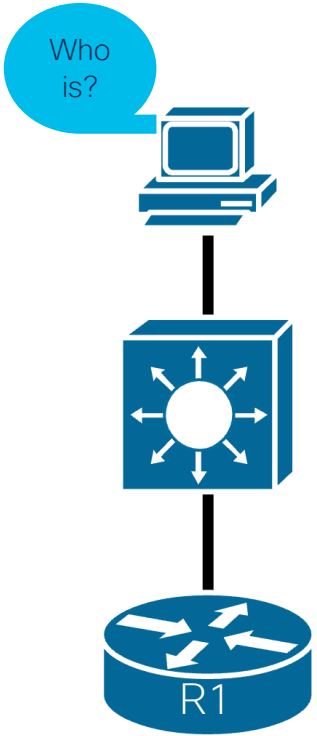
%IOSXE-5-PLATFORM: SIP0: cpp_cp: QFP:0.0 Thread:026 TS:00000408224372551936
%PUNT_INJECT-5-DROP_PUNT_CAUSE: punt cause policer drop packet cause 7

  - Configured IOS-XE packet-trace tool to capture the packets being dropped by default policer
  - Found many ARP packets that were being punted and dropped by default punt policer
  - Identified that the source MAC address for these ARP requests were coming from the same device



Troubleshooting High CPU cont.

- Root cause: ARP broadcast storm causing thousands of packets to be punted to routers control-plane and causing CPU spikes and not leaving enough cycles for our BGP packets
- Solution: Temporarily created MAC filter closest to source to stop the storm.
- Long term solution is to configure Control-plane Policer (CoPP) to protect from broadcast storms. Default punt policer is not suitable for all scenarios.



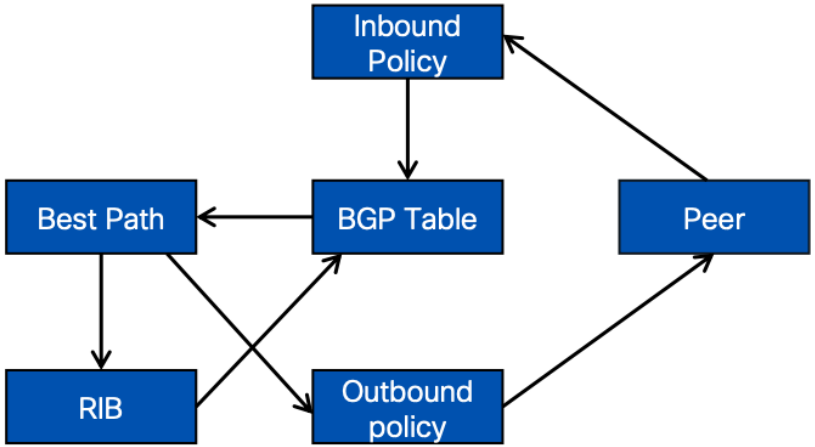
Troubleshooting High CPU – Packet Trace config

- show platform hardware qfp active infrastructure punt config cause 7
- debug platform condition ingress
- debug platform packet-trace punt code 7
- debug platform packet-trace packet 1024
- debug platform packet-trace copy packet both
- debug platform condition start
- debug platform condition stop !! Stop after some capture period
- show platform packet-trace packet X decode !! to decode and review the packets
- clear platform condition all !! to remove all the debug parameters

BGP Updates and Routes

BGP Updates

- BGP prefixes are injected by explicit configuration
- Network Statement – network <prefix> mask <mask>
  - Prefix/mask needs to match the RIB exactly
  - Does not enable BGP on an interface like IGP's
- Redistribution – redistribute ospf <PID>
  - Injects prefixes from the specified protocol
  - Does not inject 0.0.0.0/0
- Aggregate route – aggregate-address <prefix> <mask>
  - Component route must exist in BGP
  - Aggregator attribute is added
- Default Route – default-information originate
  - Neighbor x.x.x.x default-originate



BGP Best Path Selection Algorithm

- #show ip bgp [x.x.x.x]
- How it works:
  1. Prefer the path with the highest WEIGHT
  2. Prefer the path with the highest LOCAL_PREF
  3. Prefer the path that was locally originated via a **network** or **aggregate** BGP subcommand or through redistribution from an IGP
  4. Prefer the path with the shortest AS_PATH

  ….snipped…

  13. Prefer the path that comes from the lowest neighbor address
- Reference: https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html
- See the reference for full algorithm and important notes

Stuck BGP Messages

```
XE-R1#show ip bgp summary | begin Neighbor
Neighbor        ...  MsgRcvd  MsgSent   TblVer  InQ  OutQ  Up/Down  State/PfxRcd
2.2.2.2         ...      328      520      112    0    97  00:36:38        20
```

```
XE-R1#show ip bgp summary | begin Neighbor
Neighbor        ...  MsgRcvd  MsgSent   TblVer  InQ  OutQ  Up/Down  State/PfxRcd
2.2.2.2         ...      328      520      112    0    98  00:37:45        20
```

TCP is reliable, so are our updates.

- MsgSent – Number of packets transmitted is not increasing
- OutQ – The number of packets generated is increasing
- Up/Down – Enough time has passed for at least one BGP keepalive

How to solve?

- Indicates issue with TCP connection. Check if control-plane between neighbors are clean. High CPU, slow peers, interface or MTU issues on the link

BGP Unsupported or Malformed Updates

- Receiving an update containing an unsupported or malformed attribute may cause you to lose routes or even reset neighborship
- Review the malformed update in syslog or per-neighbor logs
  - DECODE: http://bgpaste.convergence.cx/
- #show ip bgp neighbor
  - Check Neighbour capabilities for “advertised” and ”received”

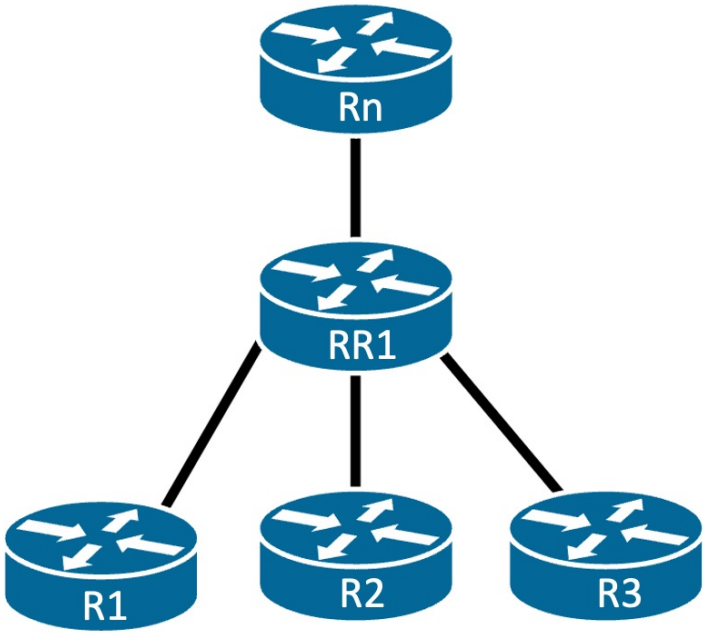
```
XE-R1#
%BGP-3-NOTIFICATION: sent to neighbor 10.1.12.1 active
2/7 (unsupported/disjoint capability) 0 bytes
XE-R1#
BGP-4-MSGDUMP: unsupported or mal-formatted message
received from 10.1.12.1:
FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF 002D 0104
0064 00B4 0101 0101 1002 0601 0400 0100 0102 0280
0002 0202 00
```

```
XE-R1#show ip bgp neighbor 2.2.2.2 | begin Last reset
Last reset 5d12h, due to BGP Notification sent, invalid or
corrupt AS path
Message received that caused BGP to send a Notification:
FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF 002D 0104
95B0 00B4 7CC3 263B 1002 0E02 0041 0400 0095 B001
0400 0100 01
```

BGP Update Groups

- Update Group is a collection of peers with identical outbound policy
- A leader is selected in the update group, which is updated first in the group
- Based on the message formatted for the master/leader, all the peers are then replicated with the same formatted message
  - Message formatting only happens once

```
XE-RR1#show ip bgp update-group
XE-RR1#show ip bgp replication
XE-RR1#show ip bgp summary slow
XE-RR1#show ip bgp update-group X summary
XE-RR1#show ip bgp neighbors x.x.x.x
```

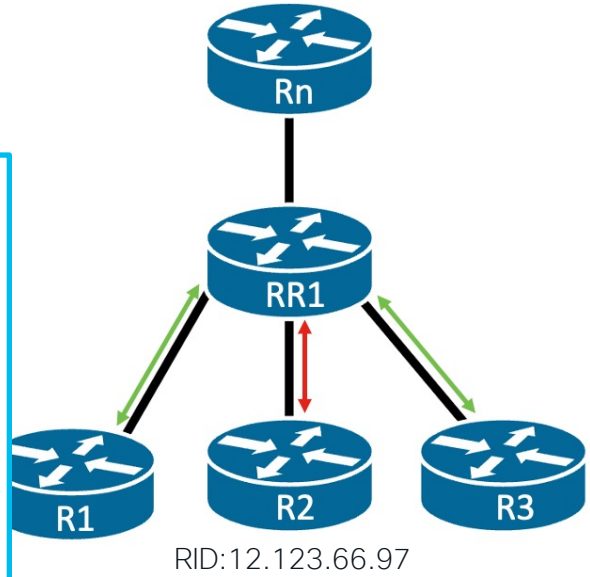


Troubleshoot BGP Slow Peers

- Symptoms: Traffic blackhole / Stale routes / Missing updates
- Causes: High CPU load / Packet loss

```
XE-RR1# show ip bgp vpnv4 all replication

                                                                  Current Next
Index    Members      Leader          MsgFmt   MsgRepl   Csize    Version Version
    1        348   12.123.67.97          ...      ...   999/1000     .../...
    2          2   12.122.78.19          ...      ...   0/200        .../...
    3          1   199.37.187.24         ...      ...   0/100        .../...
    4          2    2.122.78.249         ...      ...   0/200        .../...
XE-RR1#
XE-RR1# show ip bgp vpnv4 all summary
..
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
12.123.67.97    4   109      42    87065        0    0 1000 00:10:00        0
12.122.78.19    4   109      42    87391        0    0  674 00:10:00        0
```



Troubleshoot BGP Slow Peers

- Lookout for:
  - Keepalives being throttled?
  - Output queue, SRTT/RTTO high or increasing?
  - Number of retransmits increasing
  - Queued retransmit packets
- Resolution
  - Identify slow peers manually and resolve CPU or link quality issues
  - Separate known slow peers in their own update group
  - BGP Slow peer detection feature

```
XE-RR1#show ip bgp neighbor 12.123.66.97
...
  Last read 00:00:43, last write 00:00:17, hold time is 180, keepalive
interval
    is 60 seconds
  Keepalives are temporarily in throttle due to closed TCP window
  Neighbor capabilities:
...
  BGP table version 250001, neighbor version 200001/250001
  Output queue size : 410
...
Enqueued packets for retransmit: 15, input: 0  mis-ordered: 0 (0 bytes)
...
iss:  130287252  snduna:  131516888  sndnxt:  131532233   sndwnd:  0
...
Datagrams (max data segment is 1460 bytes):
Rcvd: 922 (out of order: 0), with data&colon; 65, total data bytes: 1261
Sent: 1463 (retransmit: 29 fastretransmit: 1),with data&colon; 1391, total
 data bytes: 1245129
...
```

BGP Missing/Stale Routes

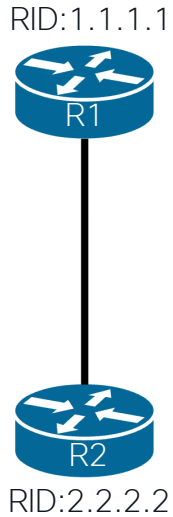
- What is difference between missing and stale?
- Missing Route
  - The remote peer has not received the route
- Stale Routes
  - A route present in the BGP table learnt from remote peer, but the route is not on that same remote peers BGP table. i.e. old information

Troubleshoot BGP Missing Route

- By default, on IOS-XE we install routes in the BGP tables for prefixes learnt from eBGP peers
- Possible causes:
  - Speaker didn't advertise the routes, or the remote peer didn't receive or process the BGP update
  - Inbound / Outbound route-maps (filtering – ACLs, prefix-list, AS list, communities etc)
- How to solve:
  - Does the path exist in the BGP table?
  - For eBGP do we have valid next hop?
  - Check any inbound and outbound filtering
  - Validate if BGP configuration is correct on router advertising BGP route
  - Recreate the issue in lab

Troubleshoot BGP Stale Route

- Can exist in both the control plane and the data plane
- Symptoms:
  - Traffic Black-hole / Outage
  - Wrong next-hop or label for BGP prefix learnt
- Possible causes:
  - BGP Slow peer
  - Sender didn't process the updates
  - Receiver didn't process the update
  - On IOS-XE it is difficult to get root cause after the problem as occurred. Need to enable conditional debugs during time of issue or reproduce issue in lab




```
XE-R1#show access-list 99
Standard IP access list 99
    10 permit 10.1.14.0, wildcard bits 0.0.0.255
XE-R1#
XE-R1#debug ip bgp 2.2.2.2 updates 99
```

Troubleshoot Filtering – Regex

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 of the set
- (Hyphen)	Indicates a range of numbers or characters in brackets
[^] (Carets in Brackets)	Excludes the characters listed in brackets; must be the first character
( ) (Parentheses)	Used for nesting of search patterns
| (Pipe)	Provides 'or' functionality of the query
. (period)	Matches a single character, including a space
* (Asterisk)	Matches zero or more preceding characters or patterns
+ (Plus Sign)	Matches on or more preceding characters or patterns
? (Question Mark)	Matches at most one preceding characters or patterns

Troubleshoot Filtering - Regex

```
XE-R1# show bgp ipv4 unicast regexp _300_
...
     Network          Next Hop            Metric LocPrf Weight Path
*>   172.16.0.0/24    192.168.200.3            0             0 300 80 90 21003 455 i
*>   172.16.4.0/23    192.168.200.3            0             0 300 878 1190 1100 1010 i
*>   172.16.16.0/22   192.168.200.3            0             0 300 779 21234 45 i
*>   172.16.99.0/24   192.168.200.3            0             0 300 145 40 i
*>   172.16.129.0/24  192.168.200.3            0             0 300 10010 300 1010 40 50 i
*>i 192.168.129.0    10.12.1.1                0    100      0 100 10010 300 1010 40 50 i
```

```
XE-R1# show bgp ipv4 unicast regexp ^300_
...
     Network          Next Hop            Metric LocPrf Weight Path
*>   172.16.0.0/24    192.168.200.3            0             0 300 80 90 21003 455 i
*>   172.16.4.0/23    192.168.200.3            0             0 300 878 1190 1100 1010 i
*>   172.16.16.0/22   192.168.200.3            0             0 300 779 21234 45 i
*>   172.16.99.0/24   192.168.200.3            0             0 300 145 40 i
*>   172.16.129.0/24  192.168.200.3            0             0 300 10010 300 1010 40 50 i
```

Q&A

Session Surveys

We would love to know your feedback on this session!

- Complete the session surveys in the Cisco Events mobile app. You'll earn some points in the Cisco Live Game and potentially win a prize.
- Complete a minimum of four session and the overall event surveys to claim a Cisco Live cable bag.

Continue your education

Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Expert meeting

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

The bridge to possible

Thank you

#CiscoLiveAPJC