Network Design, Diagnose and Tshoot

Topic 2

Write here...

Copyright ©2018 Omkar Surve. All Rights Reserved.

SSH v2 IOS/ XE:

note: for ssh on XE and ios we need atleast 2 user accounts on local router to successfully perform SSH

SSH steps:

1) complete basic settings like hostname, domain-name, username and password

2) configure line vty lines

3} configure crypto rsa

```
hostname CE19
!
!
enable password cisco
!
!
ip domain name DN.com
!
crypto key generate rsa
!
username admin password 0 admin
username omkar privilege 15 password 0 omkar
!
line vty 0 4
login local
transport input ssh
!
```

XR

Under privileged mode:

crypto key generate rsa

Under global config mode:

hostname PE1

!

ipv4 access-list SSH_ALLOWED

10 permit ipv4 10.0.0.0/24 any

!

domain name DN.com

!

ssh server v2

ssh server vrf default ipv4 access-list SSH_ALLOWED

ssh timeout 120

!

AAA can be categorised in two sub-domains--

1. Local AAA
2. External AAA

==========

Local AAA on XR:

Local AAA:

Steps:

1. User-Groups
2. Task-Groups
3. Users (defining user-groups, task-groups)

User Group example:

```
usergroup L1_READ
taskgroup L1_READ_ONLY
!
```

Task Group example:

```
taskgroup L1_READ_ONLY
 task read fr
 task read li
 task read aaa
 task read acl
 task read bfd
 task read bgp
 task read cdp
 task read cef
 task read cgn
 task read eem
 task read nps
 task read otn
 task read pbr
 task read ppp
```

task read qos
task read rib
task read rip
task read sbc
task read boot
task read diag
task read dwdm
task read hdlc
task read hsrp
task read ipv4
task read ipv6
task read isis
task read lisp
task read lpts
task read ospf
task read ouni
task read rcmd
task read snmp
task read vlan
task read vrrp
task read eigrp
task read l2vpn
task read bundle
task read fabric
task read static
task read sysmgr
task read system
task read tunnel
task read drivers
task read logging
task read monitor
task read mpls-te
task read netflow

task read network
task read pos-dpt
task read firewall
task read mpls-ldp
task read pkg-mgmt
task read interface
task read inventory
task read multicast
task read route-map
task read sonet-sdh
task read transport
task read ext-access
task read filesystem
task read tty-access
task read config-mgmt
task read ip-services
task read mpls-static
task read route-policy
task read host-services
task read basic-services
task read config-services
task read ethernet-services
description only Read access to user
!

User:

username L1_omkar

group L1_READ

password 7 143B43340309212A36

!

==========

Local Authentication:

1.

Router(config)# **aaa new-model**

- Router(config)# **aaa authentication login**{**default** | *list-name*} *method1*[*method2*...]
- Router(config)# **line** [**aux** | **console** | **tty** | **vty**] **line-number** [**ending-line-number**]
- Router(config-line)# **login authentication**

AAA Authorization Types

Cisco IOS XE software supports five different types of authorization:

- Commands--Applies to the EXEC mode commands a user issues. Command authorization attempts

  authorization for all EXEC mode commands, including global configuration commands, associated with

  a specific privilege level.

- EXEC--Applies to the attributes associated with a user EXEC terminal session.

-

Network--Applies to network connections. This can include a PPP, SLIP, or ARAP connection.

•

Reverse Access--Applies to reverse Telnet sessions.

•

Configuration--Applies to downloading configurations from the AAA server.

•

IP Mobile--Applies to authorization for IP mobile services

aaa authorization exec = Runs authorization to determine if the user is allowed to run an EXEC shell. This facility might return user profile information such as autocommand information.

aaa authorization commands = Runs authorization for all commands at the specified privilege level.

AAA Authorization:

Local AAA on IOS and XE:

```
service password-encryption ===> encrypts all pwds
!
privilege exec all level 5 show ====> sets show commands in
!
!
username admin privilege 15 password admin
username L1 privilege 5 password L1
username L2 privilege 10 password L2
username L3 privilege 15 password L3
!
aaa new-model    ===> enables AAA
!
!
aaa authentication login default local       ====> enables u
aaa authorization console                    ====> authorize
aaa authorization exec default local         ====> authorize
aaa authorization commands 5 default local   ====> authorize
aaa authorization commands 10 default local  ====> authorize
aaa authorization commands 15 default local  ====> authorize
!
!
line con 0
login authentication default     ======> use local database
authorization exec default       ======> authorize authentic
!
line vty 0 4
login authentication default     ======> use local database
authorization exec default       ======> authorize authentic
!
```

for show run on any user level (only for local):
show run view full

note: rest all show commands work. Show run command have def

Network Design, Diagnose and Tshoot

WAN L2 Technologies

PPP, CHAP, PPPoE, Frame-Relay, DWDM

Copyright ©2018 Omkar Surve. All Rights Reserved.

PPP-unidirectional authentication
-standard encapsulation technique for serial links
-enabled on per interface

CHAP

- ppp with bidirectional authentication.
- Enabled on global mode

PPPoE (PPP over Ethernet)

ppp encapsulation over Ethernet

Subnet and Wildcard mask table

The following table should help in seeing a pattern between the number of bits used for the mask in a particular octet, the subnet mask in decimal and the equivalent wildcard mask:

No. of Network Bits Set to 1	0	1	2	3	4	5	6
Subnet Mask Binary	00000000	10000000	11000000	11100000	11110000	11111000	11111
Subnet Mask Decimal	0	128	192	224	240	248	252
Wildcard Mask Binary	11111111	01111111	00111111	00011111	00001111	00000111	00000
Wildcard Mask	255	127	63	31	15	7	3

The binary for the wildcard mask is the exact reverse, bit for bit, of the subnet mask. You then calculate the decimal from the reversed binary bits to obtain the dotted decimal wildcard mask.

Network Design, Diagnose and Tshoot

IGP

RIP, OSPF, ISIS and EIGRP

Copyright ©2018 Omkar Surve. All Rights Reserved.

RIPv2
-Classless == Sends sunet mask along with route
-Max Hop count 15
-Distance Vector == Hops
-Authentication
-Multicast addr == 224.0.0.9
-Auto Summarization is enabled by default

==========

Restrictions:

==========

RIPv2 is not backward compatible.

XR does not support RIP IPv6

==========

When configuring RIP on IOS/ XE special care need to taken in case of prefix. For example a /8 prefix might not work eveytime, in such cases try to use longer prefixes (/24 and above)

Configurations: IPv4

IOS/ XE

```
router rip
 version 2
 network 2.0.0.0
 no auto-summary
!
```

XRv

```
router rip
 vrf M
  interface Loopback1
  !
  interface GigabitEthernet0/0/0/3
  !
```

Configurations: IPv6

IOS/ XE

ipv6 router rip 2

interface Ethernet0/0

ipv6 rip 2 enable

XRv:

XR does not support RIP IPv6

Reachabilty Diagnosis and Troubleshoot:

1. Check IPv4/IPv6 address of port and Port up/down status.
2. ping each others physical interface
3. Ping successful, check ping loopbacks(or advertised/ received prefixes)
4. Ping unsucessful = neighborship down
5. check RIP version on both ends
6. check network prefixes in case of IPv4 and IPv6 rip config per interface in case of IPv6.
7. Ping successful, neighborship down on both ends. Routes are available via other protocol.
8. In above case, do sh ip cef on both ends.
9. When redistributing in bgp, do specify metric. It denotes the max hop the route reachable in the client network.
10. When using as PE-CE MP-BGP, nexthops must be reachable, for the remote routes to be reflected in CE FIB.

Expected Outputs:

RP/0/0/CPU0:PE1#sh route vrf M ipv4 | b Gateway
Sun Dec 16 19:23:27.539 UTC
Gateway of last resort is not set

C 2.0.0.0/24 is directly connected, 01:53:19, Loopback1
L 2.0.0.1/32 is directly connected, 01:53:19, Loopback1
R 2.0.0.18/32 [120/1] via 2.1.18.18, 01:38:56, GigabitEthernet0/0/0/3
C 2.1.18.0/24 is directly connected, 02:47:24, GigabitEthernet0/0/0/3
L 2.1.18.1/32 is directly connected, 02:47:24, GigabitEthernet0/0/0/3
RP/0/0/CPU0:PE1#

RP/0/0/CPU0:PE1#sh rip vrf M database
Sun Dec 16 19:25:35.470 UTC

Routes held in RIP's topology database:
2.0.0.18/32
  [1] via 2.1.18.18, next hop 2.1.18.18, Uptime: 8s, GigabitEthernet0/0/0/3
2.0.0.0/24
  [0] directly connected, Loopback1

2.1.18.0/24
   [0]   directly connected, GigabitEthernet0/0/0/3
2.0.0.0/8   auto-summary

RP/0/0/CPU0:PE1#sh rip vrf M statistics
Sun Dec 16 19:27:13.224 UTC

RIP statistics:
Total messages sent: 264
Message send failures: 0
Regular updates sent: 256
Queries responsed to: 3
RIB updates: 5
Total packets received: 330

==========

Auto Summarization fix (Ripv2)

router rip
version 2
network 10.0.10.0
!
===> after sh run it will appear as 10.0.0.0 due to default auto summarization.
Also show ip route on neighbor will show 10.0.0.0/8 network.

Solve this for all rip neighbors (router rip config) do ==>

router rip
no auto-summary
!

Solve for particular prefix available via particular interface ==>

int e0/0
ip summary-address rip 10.0.0.0 255.255.0.0
!

Authentication

RIP authentication is per-interface using keychains.

Key points:

Each router generates a type 1 LSA (Router LSA) and sends it to the DR
DR generates type 2 LSA (Network LSA) and sends it to all routers
LSA 3 (Network Summary LSA)as generated by Area border router (ABR). It includes prefixes from other area (inter-area)

LSA 1 and LSA 2 always stay within that particular area

OSPF Area Types:
Normal
Stub
Totally Stubby
Not-so-stubby
Totally not-so-stubby

Normal Area:
Contains LSA types 1,2,3,4 and 5

Restrictions:

- Unlike in XE, in XR we need ospfv2 for IPv4 and ospfv3 for IPv6. Also Ospfv2(in XR) cannot form neighborship with ospfv3(ipv4 in XE/IOS)
- OSPF stub routing on XRv (virtual) does not work
- OSPFv3 IPv4 nssa does not work in XE/ IOS. Use ospfv2 for ipv4 nssa
- For Stub routing to work on any one router to work, that router must have atleast one interface in area0 i.e. connected to backbone area (Hint: Use loopbacks)
- When configuring passive interface using OPSFv3 in IOS/ XE, network prefixes unlike in XR by default won't get advertised with LSA, on top of that we don't have specific command to advertise passive interface in OSPFv3 for IOS and XE. We can use tools like redistribute connected with route-maps.

Configurations IPv4

IOS/XE

```
router ospf 200
 router-id 200.0.0.23
 network 0.0.0.0 0.0.0.0 area 0
```

OR

```
router ospf 200
 router-id 200.0.0.23
!
interface Ethernet0/0
 ip ospf network point-to-point
 ip ospf 200 area 0
!
```

OR

```
router ospfv3 10
 router-id 2.2.2.2
 !
```

```
 address-family ipv4 unicast
  passive-interface Loopback0
 exit-address-family
 !
 address-family ipv6 unicast
  passive-interface Loopback0
 exit-address-family
!
interface GigabitEthernet3
 ospfv3 10 network point-to-point
 ospfv3 10 ipv4 area 0
 ospfv3 10 ipv6 area 0
!
interface GigabitEthernet4
 ospfv3 10 network point-to-point
 ospfv3 10 ipv4 area 0
 ospfv3 10 ipv6 area 0
!
```

XRv

```
router ospf 10
 log adjacency changes
 router-id 6.6.6.6
 area 0
  interface Loopback0
   passive enable
  !
  interface GigabitEthernet0/0/0/0
   network point-to-point
  !
  interface GigabitEthernet0/0/0/2
   network point-to-point
  !
 !
!
```

Configurations IPv6

IOS/XE

```
ipv6 router ospf 200
 router-id 200.0.0.23
!
interface Ethernet0/0
 ipv6 ospf 200 area 0
 ipv6 ospf network point-to-point
!
```

OR

```
router ospfv3 10
 router-id 2.2.2.2
 !
 address-family ipv4 unicast
  passive-interface Loopback0
 exit-address-family
 !
 address-family ipv6 unicast
  passive-interface Loopback0
 exit-address-family
!
interface GigabitEthernet3
 ospfv3 10 network point-to-point
 ospfv3 10 ipv4 area 0
 ospfv3 10 ipv6 area 0
!
interface GigabitEthernet4
 ospfv3 10 network point-to-point
 ospfv3 10 ipv4 area 0
 ospfv3 10 ipv6 area 0
!
```

XRv

```
router ospfv3 10
```

```
 router-id 6.6.6.6
 log adjacency changes
 area 0
  interface Loopback0
   passive
  !
  interface GigabitEthernet0/0/0/0
   network point-to-point
  !
  interface GigabitEthernet0/0/0/2
   network point-to-point
  !
 !
!
```

Reachabiliy Diagnosis and Troubleshoot

1. Check IPv4/IPv6 address of port and Port up/down status.
2. ping each others physical interface
3. Ping successful, check ping loopbacks(or advertised/ received prefixes)
4. In case of Link State protocols, the link neiborship happens via link-local address(same IP address for IPv4 adjacencies whereas link-local FE:xx for IPv6 adjacencies), check for link-local address blocking.
5. No duplicate router-ids or unavailability of router-id of neighboring router. When configuring ospf, manually mention router-id instead of letting router use it dynamically.
6. All areas (to be specific, all ospf processes) must be connected to Backbone area, Area0 because every Ospf process builts a different OSPF LSA Database, to see all the LSAs bifurcation clearly.
7. In case of Sham-Links and Virtual-Links, check their up/down states.
8. Network type(point-to-point, broadcast) mismatch.
9. Prefixes advertisement depends on Area types: Stubby, etc

Show Outputs:

Stub Areas

Know LSAs 1, 2, 3, 4, 5, and 7

1 & 2 are intra-area in scope. 3 is inter-area. 5 & 7 are external. (4 is just s support mechanism for 5's, but are technically inter-area)

stub = 1, 2, 3 + 0/0 default

total stub = 1, 2 + 0/0 default

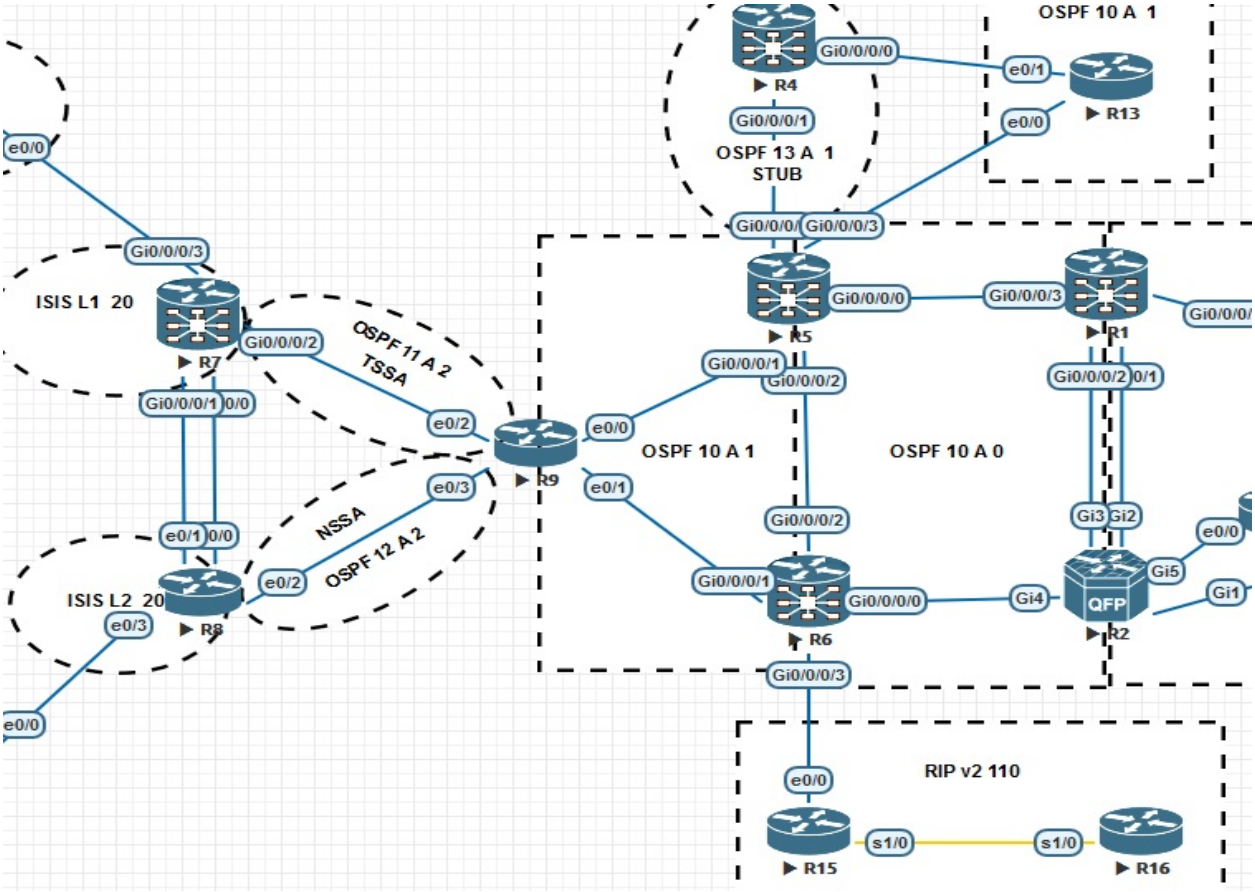
nssa = 1, 2, 3, 7 (the 0/0 is not automatically created here although you an add it)

total nssa = 1, 2, 7 + 0/0 default

Anything that says "total" is "no-summary" on the CLI. Since Type 3 = Summary LSA that should be easy to remember.

1	Router LSA	Generated by Any router for any/all links	Intra-area
2	Network LSA	Generated by a DR only for DR-used-links	Intra-area
3	Summary LSA	Generated by ABRs to summarize 1 & 2's	Inter-area
4	ASBR Summary	Generated by ABRs to summarize NH of Type 5	Inter-area
5	External LSA	Generated by ASBR	Domain-wide (other than stub areas)
7	NSSA External	Generated by ASBR specific to NSSA area	Only in NSSA area - Translated to Type 5 (+ 4) for other areas

STUB area:



R5 _R4:

```
router ospfv3 13
 router-id 13.0.0.5
 area 0
  interface Loopback13
   passive
  !
 !
 area 1
  stub
  interface GigabitEthernet0/0/0/4
   network point-to-point
  !
 !
```

```
router ospf 13
 log adjacency changes
 router-id 13.0.0.5
 area 0
  interface Loopback13
   passive enable
  !
 !
 area 1
  stub
  interface GigabitEthernet0/0/0/4
   network point-to-point
  !
 !
!
router ospf 13
 log adjacency changes
 router-id 13.0.0.4
 area 1
  stub
  interface Loopback13
   passive enable
  !
  interface GigabitEthernet0/0/0/1
   network point-to-point
  !
 !
!

router ospfv3 13
 router-id 13.0.0.4
 area 1
  stub
  interface Loopback13
   passive
  !
  interface GigabitEthernet0/0/0/1
   network point-to-point
  !
```

```
 !
```

R5-R9:

```
router ospfv3 10
 router-id 5.5.5.5
 area 0
  interface Loopback0
   passive
  !
  interface GigabitEthernet0/0/0/0
   network point-to-point
  !
  interface GigabitEthernet0/0/0/2
   network point-to-point
  !
 !
 area 1
  virtual-link 9.9.9.9
  !
  interface GigabitEthernet0/0/0/1
   network point-to-point
  !
  interface GigabitEthernet0/0/0/3
   network point-to-point
  !
 !

router ospf 10
 log adjacency changes
 router-id 5.5.5.5
 area 0
  interface Loopback0
   passive enable
  !
  interface GigabitEthernet0/0/0/0
   network point-to-point
  !
  interface GigabitEthernet0/0/0/2
```

```
   network point-to-point
  !
 !
 area 1
  virtual-link 9.9.9.9
  !
  interface GigabitEthernet0/0/0/1
   network point-to-point
  !
  interface GigabitEthernet0/0/0/3
   network point-to-point
  !
 !
!

router ospf 10
 router-id 9.9.9.9
 area 1 virtual-link 6.6.6.6
 area 1 virtual-link 5.5.5.5
 passive-interface Loopback0
 network 10.0.0.9 0.0.0.0 area 0
R9#

router ospfv3 10
 router-id 9.9.9.9
 !
 address-family ipv4 unicast
 exit-address-family
 !
 address-family ipv6 unicast
  passive-interface Loopback0
  area 1 virtual-link 5.5.5.5
  area 1 virtual-link 6.6.6.6
 exit-address-family
R9#

interface Ethernet0/0
 ip ospf network point-to-point
 ip ospf 10 area 1
```

```
 ospfv3 10 network point-to-point
 ospfv3 10 ipv6 area 1
!
```

R9-R7

```
RP/0/0/CPU0:R7#sh run router ospf
Sun Mar 31 09:13:49.434 UTC
router ospf 11
 log adjacency changes
 router-id 7.7.7.7
 area 2
  stub
  interface Loopback0
   passive enable
  !
  interface GigabitEthernet0/0/0/0
   network point-to-point
  !
  interface GigabitEthernet0/0/0/2
   network point-to-point
  !
 !

RP/0/0/CPU0:R7#sh run router ospfv3
Sun Mar 31 09:14:31.891 UTC
router ospfv3 11
 router-id 7.7.7.7
 area 2
  stub
  interface Loopback0
   passive
  !
  interface GigabitEthernet0/0/0/0
   network point-to-point
  !
  interface GigabitEthernet0/0/0/2
   network point-to-point
  !
```

```
 !

R9#sh run | s r ospfv3 11
router ospfv3 11
 router-id 11.0.0.9
 !
 address-family ipv6 unicast
  passive-interface Loopback11
  area 2 stub no-summary
 exit-address-family
R9#

R9#sh run | s r ospf 11
router ospf 11
 router-id 11.0.0.9
 area 2 stub no-summary
 passive-interface Loopback11
 network 11.0.0.9 0.0.0.0 area 2
R9#

interface Ethernet0/2
 ip ospf network point-to-point
 ip ospf 11 area 2
 ospfv3 11 network point-to-point
 ospfv3 11 ipv6 area 2
!
```

R9-R8

```
router ospfv3 12
 router-id 12.0.0.8
 area 2 nssa
 !
 address-family ipv4 unicast
  redistribute connected nssa-only route-map Lo0
  passive-interface Loopback0
 exit-address-family
 !
 address-family ipv6 unicast
```

```
  passive-interface Loopback0
 exit-address-family
R8#

interface Ethernet0/2
 ospfv3 12 network point-to-point
 ospfv3 12 ipv4 area 2
 ospfv3 12 ipv6 area 2
!

router ospfv3 12
 router-id 12.0.0.9
 area 2 nssa translate type7 always
 !
 address-family ipv4 unicast
  redistribute connected nssa-only route-map Lo12
  passive-interface Loopback12
  area 2 nssa translate type7 always
 exit-address-family
 !
 address-family ipv6 unicast
  passive-interface Loopback12
  redistribute connected route-map Lo12_v6
  area 2 nssa translate type7 always
 exit-address-family
R9#

interface Ethernet0/3
 ospfv3 12 network point-to-point
 ospfv3 12 ipv4 area 2
 ospfv3 12 ipv6 area 2
!
```

Supress / avoid unneccessary LSA updates and traffic

Three ways:

- Modify hello timers
- Demand circuit
- Flooding Reduction

Demand Circuit:

Similar feature: *OSPF Flood Reduction*
OSPF demand circuit options suppresses hello and LSA refresh functions. OSPF can establish a demand link to form an adjacency and perform initial database synchronization, the adjacency remains active even after Layer 2 of the demand circuit goes down.

How Is OSPF over Demand Circuit Different from a Normal Circuit?

There are two main features of OSPF over demand circuit that make it different from a normal circuit.

- Suppressed periodic hellos
- Suppressed periodic LSA refresh

Suppressed Periodic Hellos

When an OSPF demand circuit is configured on a link, the periodic OSPF hellos are suppressed. Periodic hellos are suppressed only on a point-to-point and point-to-multipoint network type. *On any other network type, OSPF hellos are still sent over the interface.*

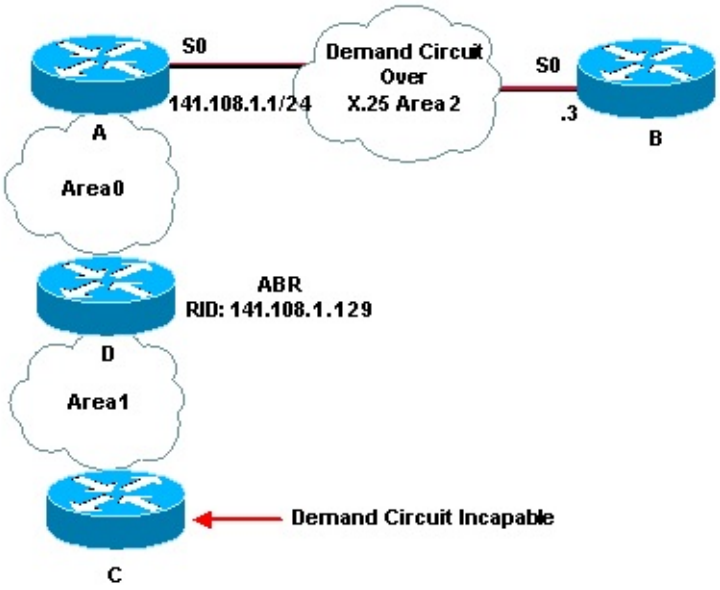
Suppressed Periodic LSA Refresh

Periodic LSA refreshes that take place every 30 minutes do not occur with OSPF demand circuit. When a demand circuit link is established a unique option bit (the DC bit) is exchanged between neighboring routers. If two routers negotiate the DC bit successfully they make a note of it and set a specific bit in the LSA Age called the DoNotAge bit (DNA). The DNA bit is the most significant bit in the LS Age field. By setting this bit the LSA stops aging, and no periodic updates are sent.

When Is a Periodic LSA Refresh Sent over an OSPF Demand Circuit?

There are only two scenarios where the periodic LSA refresh occurs when using the OSPF demand circuit feature:

- If there is a change in network topology
- If there is a router in the OSPF domain that can not understand demand circuits



Under router config mode we can configure demand circuit

<u>Flooding Reduction:</u>

The OSPF Flooding Reduction feature works by reducing unnecessary refreshing and flooding of already known and unchanged information. To achieve this reduction, the LSAs are now flooded with the higher bit set, thus making them DoNotAge (DNA) LSAs.

Configuring OSPF Flooding Reduction

Command	Purpose
Router(config-if)#ip ospf flood-reduction	Reduces unnecessary flooding and refreshing of LSAs in stable networks. You must configure this feature on a per-interface basis.

Monitoring and Maintaining OSPF Flooding Reduction

Command	Purpose
Router# show ip ospf database	Display lists of information related to the OSPF database. Should display low sequence numbers on LSAs that are not originated in the local environment.

The **no-ext-capability** keyword refers to handling one specific application of Opaque LSAs - in particular, the Router Information Opaque LSAs according to RFC 7770 (formerly RFC 4970).

These Router Information Opaque LSAs are optional extensions to OSPFv2, allowing router to advertise additional information about their capabilities (for example, support for Traffic Engineering, Stub Router, or Graceful Restart). Originally, OSPFv2 used the Options field in Hello packets and LSAs to advertise various capabilities, but since all these bits are already used up, RFC 7770 comes with an extensible way of advertising new capabilities using Opaque LSAs, and these LSAs are called, in short, the RI (Router Information) LSAs.

Depending on the nature of the capability, it can be advertised either as a link-scoped, area-scoped, or domain-local (also called AS-local) RI LSA - this naturally follows from the fact that Opaque LSAs have three flooding scopes: Type-9 Opaque LSAs are link-local, Type-10 Opaque LSAs are area-local, and Type-11 Opaque LSAs are AS-local.

With stubby and NSSA areas, ABRs do not inject external routes into these area types; that is why these areas have the "stubby" quality. However, since RI LSAs do not advertise topology or addressing information, it is not entirely clear whether it is okay for ABRs to flood received domain-local RI LSAs into stubby and NSSA areas. Flooding them certainly does not violate the stubby property of these areas, but may or may not be useful. This is what the **no-ext-capability** keyword does: If it is configured, domain-local RI LSAs will not be flooded into the respective area; without this keyword, despite the stubby area property, even domain-local RI LSAs will be flooded into stub or NSSA areas.

OSPFv2 Authentication:

*IOS / XE***Per-Area based Authentication:**

R9(config)#router ospf 11
R9(config-router)#area 2 authentication message-digest =======> *For MD5 per-area authentication*
R9(config-router)#area 2 authentication ========> *For Clear-text per-area authentication*
R9(config-router)#a
*Apr 11 13:56:06.703: %OSPF-4-NOVALIDKEY: No valid authentication send key is available on interface Ethernet0/2
/// Error: indicating autentication key missing on router interface
/// Solution:
For per-area / per-interface authentication approach we need to configure corresponding authentication key on interface.
Fixed Solution per-area:

R9(config-if)#ip ospf message-digest-key 1 md5 0 12345678910 ====> *For MD5 authentication*
R9(config-if)#ip ospf authentication-key 0 12345678 ======> *For Clear text authentication*

Per-Interface based Authentication:

For MD5 authentication:
R9(config-if)#ip ospf authentication message-digest
R9(config-if)#ip ospf message-digest-key 1 md5 0 12345678910

For Clear text authentication:
R9(config-if)#ip ospf authentication
R9(config-if)#ip ospf authentication-key 0 12345678

IOS-XR
Per-Area based Authentication:

router ospf 11
 area 2
  authentication message-digest =======> *For MD5 Authentication*

```
  message-digest-key 1 md5 12345678910
 !
!

router ospf 11
 area 2
  authentication-key 12345678910
  authentication  ========> For Clear-text Authentication
 !
!
```

Per-Interface based Authentication:

```
router ospf 11
 area 2
  interface GigabitEthernet0/0/0/2
   authentication message-digest     =======> For MD5 Authentication
   message-digest-key 1 md5 12345678910
  !
 !
!

router ospf 11
 area 2
  interface GigabitEthernet0/0/0/2
   authentication        =======> For Clear-text Authentication
   authentication-key 12345678910
  !
 !
!
```

IMP NOTE: *In case of MD5 authentication the key number must be different in different ospf processes, but can be remain same in different areas under same process. Also the md5 key number must match on both ends.*

>>

OSPFv3 Authentication:

Unlike other protocols which either uses plain-text or MD5 for authentication,

OSPFv3 uses IPSec for autenticating either per-interface or per-area.

Authentication on interface on one end and authentication on area other end doesn't work in conjunction. Same authentication must be configured on both ends.

Also on both ends SPI, MD5/SHA1 encryption(0/7 for pain-text/ excrypted), and Hex-String values must be same for authentication.

Overview

- Link-state, uses Dijkstra algorithm

Router Types

- **Level 1:** intra-area (can only form relationships with other Level 1 routers).
- **Level 2:** inter-area (can only form relationships with other Level 2 routers).
- **Level 1-2:** both.

Routing

- Level 1 ↔ Level 1
- Level 2 ↔ Level 2
- Level 1 ↔ Level 1-2 ↔ Level 2

Other Stuff

- Area borders are between routers (i.e. on the link):
  - in contrast to OSPF where the area border is within an ABR

ISIS NET Address / ISIS Multi-Area Adjancency explanation (**Case:** Unified MPLS)

Network Entity Titles (NETs) are generally 10 bytes long (they can be from 8 to 20 bytes long) and are written as 49.0001.1921.6811.9001.00.

The first three bytes of the address form the area ID. The area ID can be up to 13 bytes long. The first byte of the area ID is the Address Family Identifier of the authority, which is the space assigned to a particular enterprise (equivalent to an IP address space that is assigned to an enterprise). The value of 49 is the well-known Address Family Identifier used for private addressing, which is the equivalent of RFC 1918 addressing for IP protocols. The last two bytes in the area ID identify an IS-IS area within the AS, here 0001 means are 1.

The next six bytes (here, 1921.6811.9001) are the system identifier, which identifies each node(router) on the network. Although IS-IS supports a variable-length system field, in practice this field is always six bytes.The final two bytes

of the NET are the NET selector (NSEL) and, for IS-IS, they must always be zero to indicate "this system".

Restrictions:

- XR by default supports multitopology (both IPv4 and IPv6 under same isis process) whereas IOS and XE supports single-topology (IPv4 or IPv6).
- The selection bits in NET address must be always set to 0.
- Cannot configure same NET address on multiple isis process on the same router. Even configuring same NET address on different routers running single isis process is not allowed.
- When is-type (under isis process) and circuit-type(under isis interface) both are configured, isis will prefer is-type over circuit-type.
- In case of passive interfaces, we cannot use same interface in different isis process.
- In case of Multi-instance(process) isis, starting 1byte(eg: '49.' in '49.0001' area) must be same to differentiate multiple sub-areas under same router and avoid prefixes migrating from one area to other.

Configuration:

IOS / XE:

```
router isis 20
 net 49.0020.2000.0008.00
 metric-style wide
 redistribute isis ip level-2 into level-1 route-map FOR_L1
 passive-interface Loopback0
 !
 address-family ipv6
  multi-topology
  advertise passive-only
  redistribute isis level-2 into level-1 route-map FOR_L1
 exit-address-family
!
interface Ethernet0/0
 ip router isis 20
 isis circuit-type level-1
 ipv6 router isis 20
```

```
 isis network point-to-point
!
```

XRv:

```
router isis 20
 net 49.0020.2000.0007.00
 address-family ipv4 unicast
  metric-style wide
  advertise passive-only
 !
 address-family ipv6 unicast
  metric-style wide
  advertise passive-only
 !
 interface Loopback0
  passive
  address-family ipv4 unicast
  !
  address-family ipv6 unicast
  !
 !
 interface GigabitEthernet0/0/0/0
  circuit-type level-1
  point-to-point
  address-family ipv4 unicast
  !
  address-family ipv6 unicast
  !
 !
 interface GigabitEthernet0/0/0/1
  circuit-type level-2-only
  point-to-point
  address-family ipv4 unicast
  !
  address-family ipv6 unicast
  !
 !
 interface GigabitEthernet0/0/0/3
```

```
  point-to-point
  address-family ipv4 unicast
  !
  address-family ipv6 unicast
  !
 !
!
```

Reachabiliy Diagnosis and Troubleshoot

1. Check IPv4/IPv6 address of port and Port up/down status.
2. ping each others physical interface
3. Ping successful, check ping loopbacks(or advertised/ received prefixes)
4. In case of Link State protocols, the link neiborship happens via link-local address(same IP address for IPv4 adjacencies whereas link-local FE:xx for IPv6 adjacencies), check for link-local address blocking.
5. Area types(Level 1, Level 2, and Level 1-2) mismatch. NET areas mismatch. Network type(point-to-point, broadcast) mismatch.
6. Topology mismatch(single, Multi).
7. Wrong consideration while interconnecting different isis levels.
8. ISIS metrics and metric-type mismatches.

Show Outputs

```
RP/0/0/CPU0:R7#sh isis neighbors
Sun Mar 24 16:53:21.928 UTC

IS-IS 20 neighbors:
System Id      Interface        SNPA           State Holdtime Type IETF-NSF
R8             Gi0/0/0/0        *PtoP*         Up    29       L1   Capable
R8             Gi0/0/0/1        *PtoP*         Up    29       L2   Capable
R11            Gi0/0/0/3        *PtoP*         Up    22       L2   Capable

Total neighbor count: 3
RP/0/0/CPU0:R7#


RP/0/0/CPU0:R7#sh isis database
Sun Mar 24 16:56:46.474 UTC

IS-IS 20 (Level-1) Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
R7.00-00            * 0x0000000e   0xac76        1043          0/0/0
R8.00-00              0x00000012   0x73b9        653           0/0/0
```

```
R12.00-00           0x0000000f   0x418a       1152           0/0/0

 Total Level-1 LSP count: 3     Local Level-1 LSP count: 1

IS-IS 20 (Level-2) Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
R7.00-00            * 0x00000012   0xcf1f        1065          0/0/0
R8.00-00              0x00000013   0xed58        929           0/0/0
R11.00-00             0x0000000d   0xbb18        568           0/0/0

 Total Level-2 LSP count: 3     Local Level-2 LSP count: 1
RP/0/0/CPU0:R7#


RP/0/0/CPU0:R7#sh isis adjacency-log first 100
Sun Mar 24 16:57:39.960 UTC

   IS-IS 20 Level 1 Adjacency log
When         System         Interface         State   Details
--- Sun Mar 24 2019 ---
14:33:30.973  R8            Gi0/0/0/0         d -> i
14:33:30.993  R8            Gi0/0/0/0         i -> u  New adjacency
                                               IPv4 Unicast Up
                                               IPv6 Unicast Up

   IS-IS 20 Level 2 Adjacency log
When         System         Interface         State   Details
--- Sun Mar 24 2019 ---
14:33:30.973  R8            Gi0/0/0/1         d -> i
14:33:30.973  R11           Gi0/0/0/3         d -> i
14:33:30.993  R8            Gi0/0/0/1         i -> u  New adjacency
                                               IPv4 Unicast Up
                                               IPv6 Unicast Up
14:33:31.003  R11           Gi0/0/0/3         i -> u  New adjacency
                                               IPv4 Unicast Up
                                               IPv6 Unicast Up
RP/0/0/CPU0:R7#
```

```
RP/0/0/CPU0:R7#sh isis topology summary
Sun Mar 24 17:00:14.080 UTC

IS-IS 20 IS Topology Summary IPv4 Unicast
                      L1                          L2
              Reach  UnReach   Total/All     Reach  UnReach  Total/All
                  In Top                      In Top
             ------- ------- -------------   ------- ------- -------------
Router nodes:       3       0      3/3             2       1      3/3
Pseudo nodes:       0       0      0/0             0       0      0/0

 Total nodes:       3       0      3/3             2       1      3/3
RP/0/0/CPU0:R7#



RP/0/0/CPU0:R7#sh isis error-log
Sun Mar 24 17:01:37.384 UTC

   IS-IS 20 Error Log
When          Log Level  Err String Err Code   Details
RP/0/0/CPU0:R7#



RP/0/0/CPU0:R7#sh isis afi-all safi-all fast-reroute
Sun Mar 24 17:06:34.244 UTC

IS-IS 20 IPv4 Unicast FRR backups

Codes: L1 - level 1, L2 - level 2, ia - interarea (leaked into level 1)
       df - level 1 default (closest attached router), su - summary null
       C - connected, S - static, R - RIP, B - BGP, O - OSPF
       E - EIGRP, A - access/subscriber, M - mobile, a - application
       i - IS-IS (redistributed from another instance)
       D - Downstream, LC - Line card disjoint, NP - Node protecting
       P - Primary path, SRLG - SRLG disjoint, TM - Total metric via backup
```

Maximum parallel path count: 8

C 20.0.0.7/32
    is directly connected, Loopback0
  L2 RIB backup [20/115]
    via 20.77.8.8, GigabitEthernet0/0/0/1, R8, Weight: 0
      No FRR backup
L1 20.0.0.8/32 [10/115]
    via 20.7.8.8, GigabitEthernet0/0/0/0, R8, Weight: 0
      No FRR backup
L1 20.0.0.12/32 [20/115]
    via 20.7.8.8, GigabitEthernet0/0/0/0, R8, Weight: 0
      No FRR backup
L1 20.7.8.0/24 [20/115]
    via 20.7.8.8, GigabitEthernet0/0/0/0, R8, Weight: 0
      No FRR backup
L1 20.8.12.0/24 [20/115]
    via 20.7.8.8, GigabitEthernet0/0/0/0, R8, Weight: 0
      No FRR backup
L2 20.77.8.0/24 [20/115]
    via 20.77.8.8, GigabitEthernet0/0/0/1, R8, Weight: 0
      No FRR backup

IS-IS 20 IPv6 Unicast FRR backups

Codes: L1 - level 1, L2 - level 2, ia - interarea (leaked into level 1)
       df - level 1 default (closest attached router), su - summary null
       C - connected, S - static, R - RIP, B - BGP, O - OSPF
       E - EIGRP, A - access/subscriber, M - mobile, a - application
       i - IS-IS (redistributed from another instance)
       D - Downstream, LC - Line card disjoint, NP - Node protecting
       P - Primary path, SRLG - SRLG disjoint, TM - Total metric via backup

Maximum parallel path count: 8

C 2012:20::7/128
    is directly connected, Loopback0
  L2 RIB backup [20/115]
    via fe80::8, GigabitEthernet0/0/0/1, R8, Weight: 0

```
      No FRR backup
L1 2012:20::8/128 [10/115]
    via fe80::8, GigabitEthernet0/0/0/0, R8, Weight: 0
      No FRR backup
L1 2012:20::12/128 [20/115]
    via fe80::8, GigabitEthernet0/0/0/0, R8, Weight: 0
      No FRR backup
RP/0/0/CPU0:R7#


RP/0/0/CPU0:R7#sh isis protocol
Sun Mar 24 17:12:23.040 UTC

IS-IS Router: 20
  System Id: 0020.2000.0007
  IS Levels: level-1-2
  Manual area address(es):
    49
  Routing for area address(es):
    49
  Non-stop forwarding: Disabled
  Most recent startup mode: Cold Restart
  Topologies supported by IS-IS:
    IPv4 Unicast
      Level-1
        Metric style (generate/accept): Wide/Wide
        Metric: 10
        ISPF status: Disabled
      Level-2
        Metric style (generate/accept): Wide/Wide
        Metric: 10
        ISPF status: Disabled
      No protocols redistributed
      Distance: 115
      Advertise Passive Interface Prefixes Only: Yes
    IPv6 Unicast
      Level-1
        Metric: 10
```

```
    ISPF status: Disabled
  Level-2
    Metric: 10
    ISPF status: Disabled
  No protocols redistributed
  Distance: 115
  Advertise Passive Interface Prefixes Only: Yes
 Interfaces supported by IS-IS:
  Loopback0 is running passively (passive in configuration)
  GigabitEthernet0/0/0/0 is running suppressed (active in configuration)
  GigabitEthernet0/0/0/1 is running suppressed (active in configuration)
  GigabitEthernet0/0/0/3 is running suppressed (active in configuration)
RP/0/0/CPU0:R7#


R11#sh isis * topology

Tag 20:

IS-IS TID 0 paths to level-2 routers
System Id          Metric     Next-Hop           Interface   SNPA
R7                 10         R7                 Et0/0       5000.0007.0004
R8                 20         R7                 Et0/0       5000.0007.0004
R11                --


IS-IS TID 2 paths to level-2 routers
System Id          Metric     Next-Hop           Interface   SNPA
R7                 10         R7                 Et0/0       5000.0007.0004
R8                 20         R7                 Et0/0       5000.0007.0004
R11                --
R11#

R11#sh isis * rib


IPv4 local RIB for IS-IS process 20

IPV4 unicast topology base (TID 0, TOPOID 0x0) ================
```

20.0.0.7/32
[115/L2/10] via 20.7.11.7(Ethernet0/0), from 20.0.0.7, tag 0, LSP[2/17]
(installed)
[115/L2/30] via 20.7.11.7(Ethernet0/0), from 20.0.0.8, tag 0, LSP[4/2]

20.0.0.8/32
[115/L2/20] via 20.7.11.7(Ethernet0/0), from 20.0.0.7, tag 0, LSP[2/17]
(installed)
[115/L2/20] via 20.7.11.7(Ethernet0/0), from 20.0.0.8, tag 0, LSP[4/2]

20.0.0.12/32
[115/L2/30] via 20.7.11.7(Ethernet0/0), from 20.0.0.7, tag 0, LSP[2/17]
(installed)
[115/L2/30] via 20.7.11.7(Ethernet0/0), from 20.0.0.8, tag 0, LSP[4/2]

20.7.8.0/24
[115/L2/30] via 20.7.11.7(Ethernet0/0), from 20.0.0.7, tag 0, LSP[2/17]
(installed)
[115/L2/30] via 20.7.11.7(Ethernet0/0), from 20.0.0.8, tag 0, LSP[4/2]

20.8.12.0/24
[115/L2/30] via 20.7.11.7(Ethernet0/0), from 20.0.0.7, tag 0, LSP[2/17]
(installed)
[115/L2/30] via 20.7.11.7(Ethernet0/0), from 20.0.0.8, tag 0, LSP[4/2]

20.77.8.0/24
[115/L2/30] via 20.7.11.7(Ethernet0/0), from 20.0.0.8, tag 0, LSP[4/2]
(installed)
IS-IS IPv6 process 20, local RIB
* 2012:20::7/128
via FE80::7/Ethernet0/0, type L2 metric 10 tag 0 LSP [2/11]
via FE80::7/Ethernet0/0, type L2 metric 30 tag 0 LSP [4/2]
* 2012:20::8/128
via FE80::7/Ethernet0/0, type L2 metric 20 tag 0 LSP [2/11]
via FE80::7/Ethernet0/0, type L2 metric 20 tag 0 LSP [4/2]
* 2012:20::12/128
via FE80::7/Ethernet0/0, type L2 metric 30 tag 0 LSP [2/11]
via FE80::7/Ethernet0/0, type L2 metric 30 tag 0 LSP [4/2]

```
R11#


R11#sh isis database

Tag 20:
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R7.00-00              0x00000017   0xC524        1092              0/0/0
R8.00-00              0x00000016   0xE75B        1051              0/0/0
R11.00-00           * 0x00000011   0xB31C        1092              0/0/0
R11#


R11#sh isis neighbors

Tag 20:
System Id      Type Interface   IP Address      State Holdtime Circuit Id
R7             L2   Et0/0       20.7.11.7       UP    24       00
R11
```

Authentication:

3 Types:

Interface Authentication =====> configured only on interface.

Area Authentication =======> When area authentication is configured, the password is carried in the L1 LSPs, CSNPs and PSNPS. All of the routers are in the same IS-IS area, ex: 49.1234.

Domain Authentication =====> All of the routers are in the same IS-IS Domain (ex: 49.) and are configured with the domain password.

>>>
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Authentication Type	XE/IOS	XRv

Interface	interface Ethernet0/0
	 isis authentication mode md5
	 isis authentication key-chain isis_int_md5
	!
	key chain isis_int_md5
	 key 1
	  key-string 12345678910
	!
	
	OR
	
	interface Ethernet0/0
	isis password 12345678910
	!
		router isis 20
		 interface GigabitEthernet0/0/0/0
		  hello-password hmac-md5 12345678910
		!

Area	area-password 12345678910	router isis 20 lsp-password hmac-md5 12345678910
Domain	domain-password 12345678910	Option not available

Dual Algorithm
- Reliable (unicast updates every 60sec)
- Unreliable (unicast updates every 5sec)

K values for Metric Calculations:
K1 = 1 == Bandwidth in kbits
K2 = 0 == Bandwidth in kbits
K3 = 1 == Delay in microseconds
K4 = 0 == Load ===>more load more traffic ===> lower is preffered
K5 = 0 == Reliabilty ===>deals with no. of errors ==> less errors more reliabilty

MTU is a tie-breaker but does not take part in Metric Calculations

Successor Node:
Neighbor connected to Subject Node having lowest neighbor-path metric.

Feasible Node:(Node having the met feasible condition)
In case of multiple paths towards the destination route, the neighboring node having a path-metric lower than the lowest metric in towards destination is considered as feasible node

Basic Config, Diagnosis and Troubleshoot

Diagnosis :

*Apr 14 17:19:31.600: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 100.1.2.1 (GigabitEthernet2) is down: retry limit exceeded

====>*Solution:* https://community.cisco.com/t5/routing/eigrp-retry-limit-exceeded/td-p/1925586

Configuration guide

```
ipv6 unicast-routing
!
router eigrp 100
 network 100.0.0.0 0.7.255.255
 eigrp router-id 2.2.2.2
!
ipv6 router eigrp 100
 eigrp router-id 2.2.2.2
 default-metric 1 0 1 1 1400
!
interface GigabitEthernet1
 ipv6 eigrp 100
!
interface GigabitEthernet2
 ipv6 eigrp 100
!
interface GigabitEthernet5
 ipv6 eigrp 100
!
interface Loopback0
 ipv6 eigrp 100
!
```

Show commands EIGRP

check interfaces---

sh eigrp address-family ipv6 interfaces

check events and updates between neighbors---
sh eigrp address-family ipv6 events

check traffic flow between neighbors---
sh eigrp address-family ipv6 traffic

check eigrp topology / database---
sh eigrp address-family ipv6 topology

PASSIVE ==> Good
ACTIVE ===> Something is Wrong

Diagnosis and Tshoot

R2#sh eigrp address-family ipv4 events | s 100.0.0.3
32 18:19:25.197 **Metric set:** 100.0.0.3/32 **metric(130816)**
34 18:19:25.197 Update sent, RD: 100.0.0.3/32 metric(Infinity)
36 18:19:25.197 Update sent, RD: 100.0.0.3/32 metric(Infinity)
37 18:19:25.197 **Route installed:** 100.0.0.3/32 100.2.3.3
38 18:19:25.197 Route installing: 100.0.0.3/32 100.2.3.3
39 18:19:25.197 Find **FS**: 100.0.0.3/32 metric(Infinity)
41 18:19:25.197 **Rcv update dest/nh:** 100.0.0.3/32 100.2.3.3
42 18:19:25.197 Metric set: 100.0.0.3/32 **metric(Infinity)**

R2#sh eigrp address-family ipv4 interfaces
EIGRP-IPv4 Interfaces for AS(100)

		Xmit Queue	PeerQ	Mean	Pacing Time	**Multicast**	Pending
Interface	**Peers**	Un/Reliable	Un/Reliable	SRTT	Un/Reliable	Flow Timer	Routes
Gi1	**1**	0/0	0/0	7	0/0	50	0
Gi2	0	0/0	0/0	0	0/0	0	0
Gi4	0	0/0	0/0	0	0/0	0	0
Gi5	0	0/0	0/0	0	0/0	0	0
Lo0	0	0/0	0/0	0	0/0	0	0

R2#

R2#sh eigrp address-family ipv4 traffic
EIGRP-IPv4 Traffic Statistics for **AS(100)**
  Hellos sent/received: **594/150**
  Updates sent/received: **5/4**
  Queries sent/received: 0/0
  Replies sent/received: 0/0
  Acks sent/received: **2/4**
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 586
  PDM Process ID: 585
  Socket Queue: 0/10000/**2**/0 (current/max/highest/drops)
  Input Queue: 0/10000/**2**/0 (current/max/highest/drops)

R2#

R2#sh eigrp address-family ipv4 topology 100.0.0.3/32
EIGRP-IPv4 Topology Entry for **AS(100)/ID(2.2.2.2)** for 100.0.0.3/32
  State is **Passive**, Query origin flag is 1, **1 Successor(s), FD is 130816**
  Descriptor Blocks:
  100.2.3.3 (GigabitEthernet1), from 100.2.3.3, Send flag is 0x0
      Composite metric is **(130816/128256)**, route is **Internal**
      Vector metric:
        Minimum bandwidth is **1000000** Kbit
        Total delay is **5010** microseconds
        Reliability is **255/255**
        Load is **1/255**
        Minimum MTU is **1500**
        Hop count is 1
        Originating router is **3.3.3.3**
R2#

R2#sh ipv6 protocols | b EIGRP
EIGRP-IPv6 Protocol for AS(100)
  Metric weight **K1=1, K2=0, K3=1, K4=0, K5=0**
  Soft SIA disabled
  NSF-aware route hold timer is 240

EIGRP NSF disabled
NSF signal timer is 20s
NSF converge timer is 120s
Router-ID: 2.2.2.2
Topology : 0 (base)
Active Timer: 3 min
Distance: internal 90 external 170
Maximum path: 16
Maximum hopcount 100
Maximum metric variance 1
Default redistribution metric is 1 0 1 1 1400

Interfaces:
GigabitEthernet1
GigabitEthernet2
GigabitEthernet5
Redistribution:
None

R2#sh ip protocols | b EIGRP
EIGRP-IPv4 Protocol for AS(100)
Metric weight **K1=1, K2=0, K3=1, K4=0, K5=0**
Soft SIA disabled
NSF-aware route hold timer is 240
EIGRP NSF disabled
NSF signal timer is 20s
NSF converge timer is 120s
Router-ID: 2.2.2.2
Topology : 0 (base)
Active Timer: 3 min
Distance: internal 90 external 170
Maximum path: 4
Maximum hopcount 100
Maximum metric variance 1

Automatic Summarization: disabled
Maximum path: 4
Routing for Networks:
100.0.0.0/13

Routing Information Sources:

Gateway	Distance	Last Update
100.2.3.3	90	00:19:40

Authentication:

Eigrp Authenication is Per-Interface only.

Tunneling Modes:

MPLS labels include 3 bits that commonly are used for QoS marking, it is possible to “tunnel DiffServ”—that is, preserve Layer 3 DiffServ markings through a service provider’s MPLS VPN cloud while still performing re-marking (via MPLS EXP bits) within the cloud to indicate in- or out-of-contract traffic.

- Uniform Mode
- Short Pipe Mode
- Pipe Mode

Uniform Mode:

Figure 5-8 MPLS DiffServ Uniform Tunneling Mode Operation