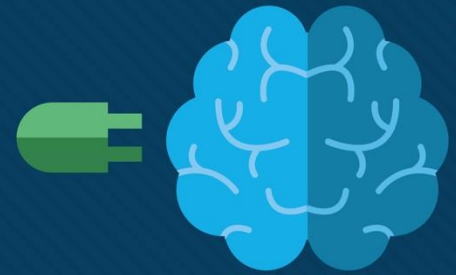

Chapter 4: Troubleshooting EIGRP for IPv4

Instructor Materials

CCNP Enterprise: Advanced Routing

Chapter 4 Content

This chapter covers the following content:

- **Troubleshooting EIGRP for IPv4 Neighbor Adjacencies -** This section covers the reasons EIGRP for IPv4 neighbor relationships might not be formed and how to identify them.
- **Troubleshooting EIGRP for IPv4 Routes -** This section explores the reasons EIGRP for IPv4 routes might be missing from a router's EIGRP table or routing table and how to determine why they are missing.
- **Troubleshooting Miscellaneous EIGRP for IPv4 Issues -** This section identifies some additional issues you might face while using EIGRP, how to identify them, and how to solve them.
- **EIGRP for IPv4 Trouble Tickets -** This section provides three trouble tickets that demonstrate how to use a structured troubleshooting process to solve a reported problem.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Troubleshooting EIGRP for IPv4 Neighbor Adjacencies

- EIGRP establishes neighbor relationships by sending hello packets to the multicast address 224.0.0.10, out interfaces participating in the EIGRP process.
- This section focuses on the reasons EIGRP neighbor relationships might not form and how you can identify them during the troubleshooting process.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

EIGRP Neighbors

The EIGRP process relies on the successful establishment of neighbor relationships with the other routers in the same autonomous system. Sometimes, for various reasons, neighbor relationships do not form successfully.

Use the **show ip eigrp neighbors** command to verify EIGRP neighbors. The output of the command lists the IPv4 address of the neighboring device's interface that sent the hello packet, the local interface on the router used to reach that neighbor, how long the local router will consider the neighboring router to be a neighbor, how long the routers have been neighbors, the amount of time it takes for the neighbors to communicate, on average, the number of EIGRP packets in a queue waiting to be sent to a neighbor, and a sequence number to keep track of the EIGRP packets to ensure that only newer packets from the neighbor are accepted and processed.

Example 4-1 *Verifying EIGRP Neighbors with show ip eigrp neighbors*

```
R2# show ip eigrp neighbors
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   10.1.23.3               Gi1/0            14  10:01:09  72    432  0   3
0   10.1.12.1               Gi0/0            11  10:32:14  75    450  0   8
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Foundation Topics

EIGRP neighbor relationships might not form for a variety of reasons, including the following:

- **Interface is down -** The interface must be up/up.
- **Mismatched autonomous system numbers -** Both routers need to be using the same autonomous system number.
- **Incorrect network statement -** The network statement must identify the IP address of the interface you want to include in the EIGRP process.
- **Mismatched K values -** Both routers must be using exactly the same K values.
- **Passive interface -** The passive interface feature suppresses the sending and receiving of hello packets while still allowing the interface's network to be advertised.
- **Different subnets -** The exchange of hello packets must be done on the same subnet;
- if it isn't, the hello packets are ignored.
- **Authentication -** If authentication is being used, the key ID and key string must match, and the key must be valid (if valid times have been configured).
- **ACLs -** An access control list (ACL) may be denying packets to the EIGRP multicast address 224.0.0.10.
- **Timers -** Timers do not have to match; however, if they are not configured correctly, neighbor adjacencies could flap.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Mismatched Autonomous System Numbers

Interface is Down

The interface must be up if you plan on forming an EIGRP neighbor adjacency. You can verify the status of an interface with the **show ip interface brief** command. The status should be listed as **up**, and the protocol should be listed as **up**.

Mismatched Autonomous System Numbers

For an EIGRP neighbor relationship to be formed, both routers need to be in the same autonomous system. You specify the autonomous system number when you issue the r**outer eigrp** *autonomous_system_number* command in global configuration mode. The best command to display the autonomous system number is **show ip protocols**, which displays an incredible amount of information for troubleshooting, as shown in Example 4-2.

Example 4-2 *Verifying the Autonomous System Number with show ip protocols*

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(100)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 10.1.12.1
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Mismatched AS Numbers (Cont.)

The output of the **debug eigrp packets** command shown in Example 4-3 indicates that the router is not receiving any hello packets from the neighbors with the mismatched autonomous system number.

In this example, R1 is sending hello packets out Gi0/0 and Gi1/0. However, it is not receiving any hello packets. This could be because of an autonomous system mismatch caused by either router having an incorrect autonomous system number configured.

Example 4-3 *Sample Output of debug eigrp packets When an Autonomous System Mismatch Exists*

```
R1# debug eigrp packets
 (UPDATE, REQUEST, QUERY, REPLY, HELLO, UNKNOWN, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)
EIGRP Packet debugging is on
R1#
EIGRP: Sending HELLO on Gi0/0 - paklen 20
   AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0
R1#
EIGRP: Sending HELLO on Gi1/0 - paklen 20
   AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0
R1#
EIGRP: Sending HELLO on Gi0/0 - paklen 20
   AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0
R1# l
EIGRP: Sending HELLO on Gi1/0 - paklen 20
   AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0
R1# l
EIGRP: Sending HELLO on Gi0/0 - paklen 20
   AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0
R1# u all
All possible debugging has been turned off
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Incorrect Network Statement

If the **network** command is misconfigured, EIGRP may not be enabled on the proper interfaces, and as a result, hello packets will not be sent and neighbor relationships will not be formed. The command **show ip eigrp interfaces** shows the interfaces participating in the EIGRP process . In Example 4-4, for instance, you can see that two interfaces are participating in the EIGRP process for autonomous system 100. Gi0/0 does not have an EIGRP peer, and Gi1/0 does have an EIGRP peer.

Example 4-4 *Verifying EIGRP Interfaces with show ip eigrp interfaces*

```
R2# show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(100)
                        Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface    Peers      Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Gi0/0          0            0/0       0         0/0           0          0
Gi1/0          1            0/0      78         0/0         300          0
```

Remember that EIGRP passive interfaces do not show up in this output. If an interface is missing, it is possible that it is configured as passive.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Incorrect Network Statement (Cont.)

The output of **show ip protocols** displays the interfaces that are running EIGRP as a result of the **network** commands. Focus on the highlighted text in Example 4-5. The output in the *Routing for Networks* section indicates the interface addresses on which EIGRP will be enabled, based on the **network** commands. In this case, **10.1.1.1/32** really means **network 10.1.1.1 0.0.0.0**, and **10.1.12.1/32** really means **network 10.1.12.1 0.0.0.0**. Therefore, a better option is to use the **show run | section router eigrp** command, as displayed in Example 4-6. You can also use **debug eigrp packets** to identify interfaces that are not sending out hello packets because of misconfigured network statements.

Example 4-6 *Verifying network Statements with* show run | section router eigrp

```
R1# show run | section router eigrp
router eigrp 100
 network 10.1.1.1 0.0.0.0
 network 10.1.12.1 0.0.0.0
```

Example 4-5 *Verifying Network Statements with show ip protocols*

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(100)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 10.1.12.1
    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:
    10.1.1.1/32
    10.1.12.1/32
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.12.2            90      09:54:36
  Distance: internal 90 external 170
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Mismatched K Values

The K values that are used for metric calculation must match between neighbors in order for an adjacency to form. Usually there is no need to change the K values. If they are changed, you must verify that they are the same on every router in the autonomous system. You can verify whether K values match by using **show ip protocols**, as shown in Example 4-7. The default K values are highlighted.

Mismatched K values generate a syslog message with severity level 5, if logging is enabled.

```
%DUAL-5-NBRCHANGE: EIGRP-IPv4 100:Neighbor
10.1.12.2
(GigabitEthernet1/0) is down: K-value mismatch
```

Example 4-7 *Verifying K Values with show ip protocols*

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(100)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 10.1.12.1
    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:
   10.1.1.1/32
   10.1.12.1/32
 Routing Information Sources:
   Gateway         Distance      Last Update
   10.1.12.2            90      09:54:36
 Distance: internal 90 external 170
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Passive Interface

The passive interface feature is a must have for all organizations. It does two things:

- Reduces the EIGRP-related traffic on a network
- Improves EIGRP security

The passive interface feature turns off the sending and receiving of EIGRP packets on an interface while still allowing the interface's network ID to be injected into the EIGRP process and advertised to other EIGRP neighbors. If you configure the wrong interface as passive, a legitimate EIGRP neighbor relationship will not be formed. As shown in the **show ip protocols** output in Example 4-8, Gigabit Ethernet 0/0 is a passive interface.

Example 4-8 *Verifying Passive Interfaces with show ip protocols*

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(100)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 10.1.12.1
    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:
    10.1.1.1/32
    10.1.12.1/32
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.12.2             90      11:00:14
  Distance: internal 90 external 170
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Different Subnets

To form an EIGRP neighbor adjacency, the router interfaces must be on the same subnet. The simplest way to verify the subnets is to look at the interface configuration in the running configuration with the **show run interface** *interface_type interface_number* command. You can also use the **show ip interface** *interface_type interface_number* command or the **show interface** *interface_type interface_number* command. Example 4-9 shows the configuration of Gig1/0 on R1 and Gig0/0 on R2. Both IP addresses are in the same subnet.

Example 4-9 *Verifying IPv4 Addresses and Masks on Router Interfaces*

```
R1# show running-config interface gigabitEthernet 1/0
Building configuration...

Current configuration : 90 bytes
!
interface GigabitEthernet1/0
 ip address 10.1.12.1 255.255.255.0
 negotiation auto
end

R2# show running-config interface gigabitEthernet 0/0
Building configuration...

Current configuration : 132 bytes
!
interface GigabitEthernet0/0
 ip address 10.1.12.2 255.255.255.0
 negotiation auto
end
```

If they are not in the same subnet, and syslog is set up for a severity level of 6, a syslog message is generated.

```
%DUAL-6-NBRINFO: EIGRP-IPv4 100: Neighbor 10.1.21.2 (GigabitEthernet1/0)
is blocked: not on common subnet (10.1.12.1/24)
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Authentication

Authentication is used to ensure that EIGRP routers form neighbor relationships only with legitimate routers and that they only accept EIGRP packets from legitimate routers.

Example 4-10 shows the output of the commands **show run interface** *interface_type interface_number* and **show ip eigrp interfaces detail** *interface_type interface_number*, which identify whether EIGRP authentication is enabled on the interface. Note that the authentication must be configured on the correct interface and that it must be tied to the correct autonomous system number.

Make sure that you specify the correct keychain that will be used for the Message Digest 5 (MD5) authentication hash. You can verify the keychain with the command **show key chain**, as shown in Example 4-11.

Example 4-10 *Verifying EIGRP Authentication on an Interface*

```
R1# show run interface gig 1/0
Building configuration...

Current configuration : 178 bytes
!
interface GigabitEthernet1/0
 ip address 10.1.12.1 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 EIGRP_AUTH
 negotiation auto
end

R1# show ip eigrp interfaces detail gigabitEthernet 1/0
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
Gi1/0        1        0/0          0/0        87       0/0           376           0
  Hello-interval is 5, Hold-time is 15
  Split-horizon is enabled
  Next xmit serial <none>
  Packetized sent/expedited: 2/0
  Hello's sent/expedited: 17/2
  Un/reliable mcasts: 0/3 Un/reliable ucasts: 2/2
  Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 0
  Retransmissions sent: 1 Out-of-sequence rcvd: 1
  Topology-ids on interface - 0
  Authentication mode is md5, key-chain is "EIGRP_AUTH"
```

Example 4-11 *Verifying the Keychain Used for EIGRP Authentication*

```
R1# show key chain
Key-chain EIGRP_AUTH:
    key 1 -- text "ENARSI"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Authentication (Cont.)

It is mandatory that the key ID in use and the key string in use between neighbors match. Therefore, if you have multiple keys and key strings in a chain, the same key and string must be used at the same time by both routers (meaning they must be valid and in use); otherwise, authentication will fail.

When using the **debug eigrp packets** command for troubleshooting authentication, you receive output based on the authentication issue. Example 4-12 shows the message that is generated when the neighbor is not configured for authentication.

Example 4-12 *Debug Output When Authentication Is Missing on the Neighbor*

```
R1# debug eigrp packets
 (UPDATE, REQUEST, QUERY, REPLY, HELLO, UNKNOWN, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)
EIGRP Packet debugging is on
R1#
EIGRP: Sending HELLO on Gi1/0 - paklen 60
 AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0
EIGRP: Gi1/0: ignored packet from 10.1.12.2, opcode = 5 (missing authentication)
EIGRP: Sending HELLO on Gi0/0 - paklen 20
 AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0
R1# u all
All possible debugging has been turned off
```

Example 4-13 *Debug Output When Key IDs or Key Strings Do Not Match*

```
R1# debug eigrp packets
 (UPDATE, REQUEST, QUERY, REPLY, HELLO, UNKNOWN, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)
EIGRP Packet debugging is on
R1#
EIGRP: pkt authentication key id = 2, key not defined
EIGRP: Gi1/0: ignored packet from 10.1.12.2, opcode = 5 (invalid authentication)
EIGRP: Sending HELLO on Gi0/0 - paklen 20
 AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0
EIGRP: Sending HELLO on Gi1/0 - paklen 60
 AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0
R1# u all
All possible debugging has been turned off
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

ACLs

Access control lists (ACLs) are extremely powerful. How they are implemented determines what they are controlling in a network. If there is an ACL applied to an interface and the ACL is denying EIGRP packets, or if an EIGRP packet falls victim to the implicit deny all at the end of the ACL, a neighbor relationship does not form.

To determine whether an ACL is applied to an interface, use the **show ip interface** *interface_type interface_number* command, as shown in Example 4-14. Notice that ACL 100 is applied inbound on interface Gig1/0. To verify the ACL 100 entries, issue the command **show access-lists 100**, as shown in Example 4-15. In this case, you can see that ACL 100 is denying EIGRP traffic; this prevents a neighbor relationship from forming.

Example 4-14 *Verifying ACLs Applied to Interfaces*

```
R1# show ip interface gig 1/0
GigabitEthernet1/0 is up, line protocol is up
  Internet address is 10.1.12.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound access list is 100
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
```

Example 4-15 *Verifying ACL Entries*

```
R1# show access-lists 100
Extended IP access list 100
    10 deny eigrp any any (62 matches)
    20 permit ip any any
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Timers

Although EIGRP timers do not have to match, if the timers are skewed enough, an adjacency will flap.

It is important that routers send hello packets at a rate that is faster than the hold timer. You verify the configured timers with the **show ip eigrp interfaces detail** command, as shown in Example 4-10.

Example 4-10 *Verifying EIGRP Authentication on an Interface*

```
R1# show run interface gig 1/0
Building configuration...

Current configuration : 178 bytes
!
interface GigabitEthernet1/0
 ip address 10.1.12.1 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 EIGRP_AUTH
 negotiation auto
end

R1# show ip eigrp interfaces detail gigabitEthernet 1/0
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
Gi1/0        1         0/0         0/0         87       0/0           376           0
  Hello-interval is 5, Hold-time is 15
  Split-horizon is enabled
  Next xmit serial <none>
  Packetized sent/expedited: 2/0
  Hello's sent/expedited: 17/2
  Un/reliable mcasts: 0/3 Un/reliable ucasts: 2/2
  Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 0
  Retransmissions sent: 1 Out-of-sequence rcvd: 1
  Topology-ids on interface - 0
  Authentication mode is md5, key-chain is "EIGRP_AUTH"
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Troubleshooting EIGRP for IPv4 Routes

- After establishing a neighbor relationship, an EIGRP router performs a full exchange of routing information with the newly established neighbor. After the full exchange, only updates to route information are exchanged with that neighbor.
- There are various reasons EIGRP routes might be missing from either the topology table or the routing table, and you need to be aware of them if you plan on successfully troubleshooting EIGRP route-related problems.
- This section examines the reasons EIGRP routes might be missing and how to determine why they are missing.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Missing EIGRP Routes

The following are some common reasons EIGRP routes might be missing either from the topology table or the routing table:

- **Bad or missing network command -** The **network** command enables the EIGRP process on an interface and injects the prefix of the network the interface is part of into the EIGRP process.
- **Better source of information -** If exactly the same network prefix is learned from a more reliable source, it is used instead of the EIGRP learned information.
- **Route filtering -** A filter might be preventing a network prefix from being advertised or learned.
- **Stub configuration -** If the wrong setting is chosen during the stub router configuration, or if the wrong router is chosen as the stub router, it might prevent a network prefix from being advertised.
- **Interface is shut down -** The EIGRP-enabled interface must be up/up for the network associated with the interface to be advertised.
- **Split horizon -** Split horizon is a loop-prevention feature that prevents a router from advertising routes out the same interface on which they were learned.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Bad or Missing Network Command

- When you use the **network** command, the EIGRP process is enabled on the interfaces that fall within the range of IP addresses identified by the command. EIGRP then takes the network/subnet the interface is part of and injects it into the topology table so that it can be advertised to other routers in the autonomous system.
- If the **network** statement is missing or configured incorrectly, EIGRP is not enabled on the interface, and the network the interface belongs to is never advertised and is therefore unreachable by other routers.
- You can confirm which interfaces are participating in the EIGRP process by using the **show ip eigrp interfaces** command, as shown in Example 4-4.

Example 4-4 *Verifying EIGRP Interfaces with show ip eigrp interfaces*

```
R2# show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(100)
                        Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface      Peers    Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Gi0/0            0          0/0       0         0/0           0          0
Gi1/0            1          0/0      78         0/0         300          0
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Better Source of Information

- For an EIGRP-learned route to be installed in the routing table, it must be the most trusted routing source. Trustworthiness is based upon administrative distance (AD). EIGRP's AD is 90 for internally learned routes (networks inside the autonomous system) and 170 for externally learned routes (networks outside the autonomous system).
- If another source with a better AD is advertising the exact same network, that source wins and its information is installed in the routing table.
- Example 4-20, which displays the output of the **show ip route 172.16.33.16 255.255.255.252** command, identifies that this network is directly connected and has an AD of 0. Because a directly connected network has an AD of 0, and an internal EIGRP route has an AD of 90, the directly connected source is installed in the routing table.

Example 4-20 *Sample show ip route 172.16.33.16 255.255.255.252 Command Output*

```
Router# show ip route 172.16.33.16 255.255.255.252
Routing entry for 172.16.33.16/30
  Known via "connected", distance 0, metric 0 (connected, via interface)
...output omitted...
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Better Source of Information (Cont.)

- Using a suboptimal source of routing information can cause suboptimal routing in the network.
- Figure 4-1 shows a network running two different routing protocols. Even though it is quicker to use the Open Shortest Path First (OSPF) path, EIGRP wins by default because it has the lower AD, and suboptimal routing occurs. In this case, you might want to consider increasing the AD of EIGRP or lowering the AD of OSPF to optimize routing.

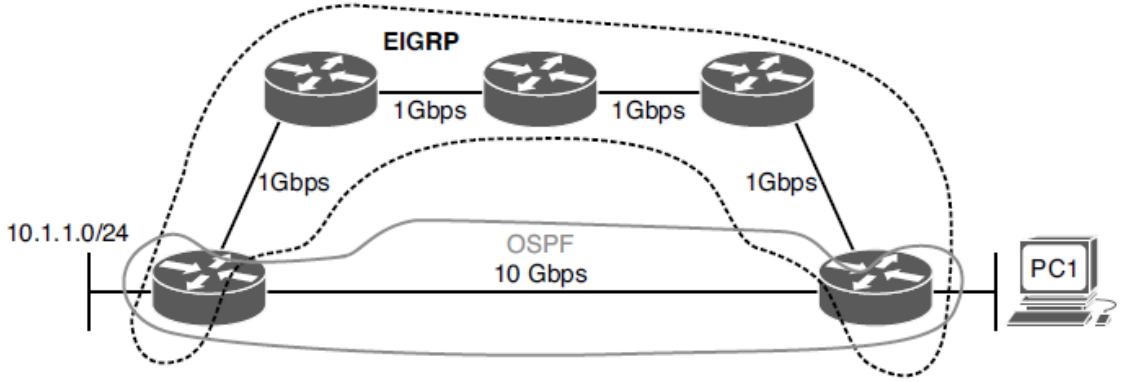

Figure 4-1 *Using the Suboptimal EIGRP Path*

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Route Filtering

- A distribute list applied to an EIGRP process controls which routes are advertised to neighbors and which routes are received from neighbors. The distribute list is applied in EIGRP configuration mode either inbound or outbound, and the routes sent or received are controlled by ACLs, prefix lists, or route maps.
- When troubleshooting route filtering, consider the following:
  - Is the distribute list applied in the correct direction?
  - Is the distribute list applied to the correct interface?
  - If the distribute list is using an ACL, is the ACL correct?
  - If the distribute list is using a prefix list, is the prefix list correct?
  - If the distribute list is using a route map, is the route map correct?

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Route Filtering (Cont.)

The **show ip protocols** command identifies whether a distribute list is applied to all interfaces or to an individual interface, as shown in Example 4-21. This example indicates that there are no outbound filters and that there is an inbound filter on Gig1/0.

- The inbound filter in Example 4-21 on Gig1/0 is filtering with ACL 10. To verify the entries in the ACL, you must issue the **show access-lists 10** command. If a prefix list was applied, you issue the **show ip prefix-list** command. If a route map was applied, you issue the **show route-map** command.
- As shown in Example 4-22, you verify the command that was used to apply the distribute list in the running configuration by reviewing the EIGRP configuration section.

Example 4-21 *Verifying Route Filters with show ip protocols*

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 100"
 Outgoing update filter list for all interfaces is not set
 Incoming update filter list for all interfaces is not set
      GigabitEthernet1/0 filtered by 10 (per-user), default is not set
 Default networks flagged in outgoing updates
 Default networks accepted from incoming updates
 EIGRP-IPv4 Protocol for AS(100)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 10.1.12.1
...output omitted...
```

Example 4-22 *Verifying EIGRP distribute-list Command*

```
R1# show run | section router eigrp
router eigrp 100
 distribute-list 10 in GigabitEthernet1/0
 network 10.1.1.1 0.0.0.0
 network 10.1.12.1 0.0.0.0
 passive-interface GigabitEthernet0/0
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Stub Configuration

- The EIGRP stub feature allows you to control the scope of EIGRP queries in the network.
- Figure 4-2 shows normal query scope for EIGRP, router R3 receives the query even though it will never have alternate information about the 192.168.1.0/24 network.
- As shown in Figure 4-3, configuring the EIGRP stub feature on R3 with the **eigrp stub** command ensures that R2 never sends a query to R3.

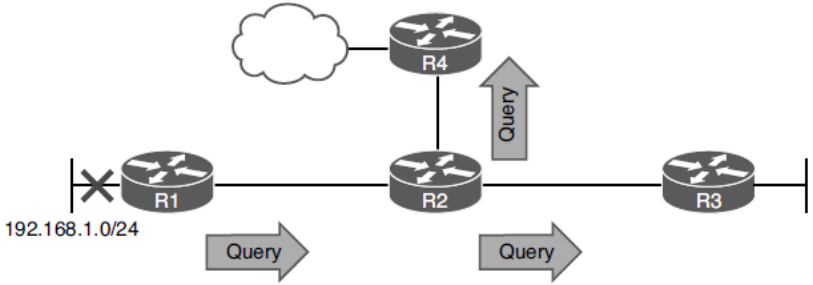

Figure 4-2 *Query Scope Without the EIGRP Stub Feature*

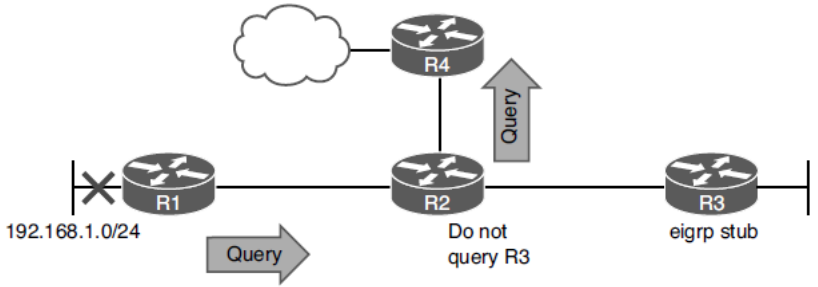

Figure 4-3 *Query Scope with the EIGRP Stub Feature*

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Stub Configuration (Cont.)

- The EIGRP stub feature comes in handy over slow hub-and-spoke WAN links, as shown in Figure 4-4.
- Configuring stub networks reduces the amount of EIGRP traffic being sent over the WAN links. In addition, it reduces the chance of a route being stuck in active (SIA) due to congestion on the WAN.
- By default an EIGRP stub router advertises connected and summary routes. You have the option of advertising connected, summary, redistributed, or static—or a combination of these. The other option is to send no routes (called receive only). If the wrong option is chosen, the stub routers do not advertise the correct routes to their neighbors, resulting in missing routes on the hub and other routers in the topology.

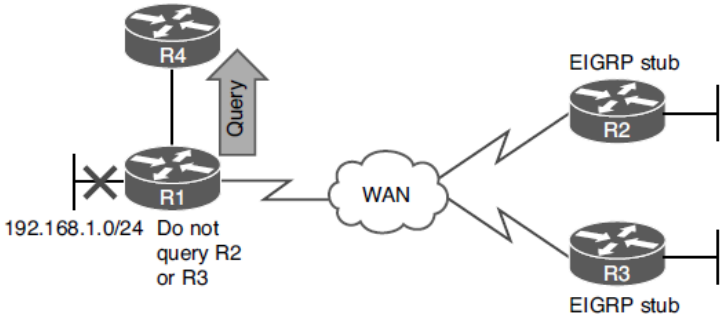

Figure 4-4 *EIGRP Stub Feature over WAN Links*

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Stub Configuration (Cont.)

- To verify whether a router is a stub router and determine the routes it will advertise, issue the **show ip protocols** command, as shown in Example 4-23.
- To determine whether a neighbor is a stub router and the types of routes it is advertising, issue the command **show ip eigrp neighbors detail**. Example 4-24 shows the output of **show ip eigrp neighbors detail** on R1, which indicates that the neighbor is a stub router advertising connected and summary routes and suppressing queries.

Example 4-23 *show ip protocols Command Output on R2*

```
R2# show ip protocols
...output omitted...
  EIGRP-IPv4 Protocol for AS(100)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 192.1.1.1
    Stub, connected, summary
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
...output omitted...
```

Example 4-24 *Verifying Whether an EIGRP Neighbor Is a Stub Router*

```
R1# show ip eigrp neighbors detail
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   10.1.13.1               Se1/0             14 00:00:18  99    594  0   11
   Version 11.0/2.0, Retrans: 0, Retries: 0, Prefixes: 2
   Topology-ids from peer - 0
   Stub Peer Advertising (CONNECTED SUMMARY ) Routes
   Suppressing queries
...output omitted...
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Interface is Shut Down

- The **network** command enables the routing process on an interface.
- Once the EIGRP process is enabled on the interface, the network that the interface IP address is part of is injected into the EIGRP process.
- If the interface is shut down, there is no directly connected entry for the network in the routing table.
- The interface must be up/up for routes to be advertised or for neighbor relationships to be formed.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Split Horizon

- The EIGRP split-horizon rule states that any routes learned inbound on an interface will not be advertised out the same interface. This rule is designed to prevent routing loops. However, this rule presents an issue in certain topologies, such as a Dynamic Multipoint Virtual Private Network (DMVPN) network or non-broadcast, multi-access Frame Relay hub-and-spoke topologies. Figure 4-5 shows a network using multipoint interfaces that is experiencing a split horizon issue.
- A multipoint interface provides connectivity to multiple routers on the same subnet out a single interface, as does Ethernet.
- To verify whether split horizon is enabled on an interface, issue the **show ip interface** *interface_type interface_number* command, as shown in Example 4-25

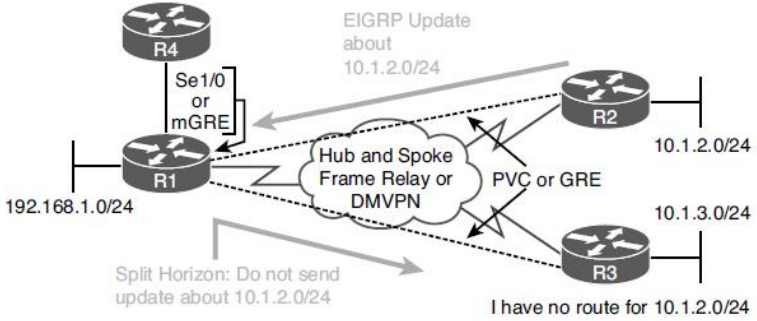

Figure 4-5 *EIGRP Split Horizon Issue*

Example 4-25 *Verifying Whether Split Horizon Is Enabled on an Interface*

```
R1# show ip interface tunnel 0
Tunnel0 is up, line protocol is up
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1476 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are never sent
...output omitted...
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Split Horizon (Cont.)

- To completely disable split horizon on an interface, issue the **no ip split-horizon** command in interface configuration mode. If you only want to disable it for the EIGRP process running on the interface, issue the command **no ip split-horizon eigrp** *autonomous_system_number*.
- If you disable split horizon for the EIGRP process, it still shows as enabled in the output of **show ip interface** (refer to Example 4-25). To verify whether split horizon is enabled or disabled for the EIGRP process on an interface, issue the command **show ip eigrp interfaces detail** *interface_type interface_number*. Example 4-26 shows that it is disabled for EIGRP on interface tunnel 0.

Example 4-26 *Verifying Whether Split Horizon Is Enabled for EIGRP on an Interface*

```
R1# show ip eigrp interfaces detail tunnel 0
EIGRP-IPv4 Interfaces for AS(100)
                      Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Tu0                0      0/0         0        6/6            0           0
  Hello-interval is 5, Hold-time is 15
  Split-horizon is disabled
  Next xmit serial <none>
  Packetized sent/expedited: 0/0
  Hello's sent/expedited: 17/1
  Un/reliable mcasts: 0/0 Un/reliable ucasts: 0/0
  Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 0
  Retransmissions sent: 0 Out-of-sequence rcvd: 0
  Topology-ids on interface - 0
  Authentication mode is not set
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Troubleshooting Miscellaneous EIGRP for IPv4 Issues

- The focus of this section is on troubleshooting issues related to feasible successors, discontiguous networks and autosummarization, route summarization, and equal-unequal metric load balancing.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Feasible Successors

- The best route (based on the lowest feasible distance [FD] metric) for a specific network in the EIGRP topology table becomes a candidate to be injected into the router's routing table.
- The term candidate is used because even though it is the best EIGRP route, a better source of the same information might be used.
- If that route is indeed injected into the routing table, that route becomes known as the *successor* (best) route.
- The successor route is then advertised to neighboring routers.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Feasible Successors (Cont.)

- Example 4-27 shows a sample EIGRP topology table, which you can view by issuing the **show ip eigrp topology** command.
- In the brackets after the next-hop IP address is the FD followed by the reported distance (RD):
  - **Feasible distance -** The RD plus the metric to reach the neighbor at the next-hop address that is advertising the RD.
  - **Reported distance -** The distance from the neighbor at the next-hop address to the destination network.
- The successor is the path with the lowest FD, however, EIGRP also pre-calculates paths that could be used if the successor disappeared. These routes are know as the *feasible successors.*
- To be a feasible successor, the RD of the path to become a feasible successor must be less than the FD of the successor.

Example 4-27 *Sample show ip eigrp topology Command Output*

```
R4# show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(192.4.4.4)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status

...output omitted...
P 10.1.13.0/24, 1 successors, FD is 3072
        via 10.1.34.3 (3072/2816), GigabitEthernet2/0
P 0.0.0.0/0, 1 successors, FD is 28160
        via Rstatic (28160/0)
P 192.1.1.1/32, 1 successors, FD is 131072
        via 10.1.34.3 (131072/130816), GigabitEthernet2/0
P 172.16.32.192/29, 1 successors, FD is 2174976
        via 172.16.33.5 (2174976/30720), Serial1/0
        via 172.16.33.6 (2684416/2172416), Serial1/0
        via 172.16.33.18 (2684416/2172416), Serial1/2
P 198.51.100.0/30, 1 successors, FD is 28416
        via 10.1.34.3 (28416/28160), GigabitEthernet2/0
P 172.16.33.12/30, 1 successors, FD is 2172416
        via 172.16.33.5 (2172416/28160), Serial1/0
...output omitted...
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Feasible Successors (Cont.)

- For troubleshooting, it is important to note that the output of **show ip eigrp topology** only displays the successors and feasible successors. If you need to verify the FD or RD of other paths to the same destination that are not feasible successors, you can use the **show ip eigrp topology all-links** command.
- Example 4-28 displays the output of **show ip eigrp topology** and **show ip eigrp topology all-links**.
- In the output of **show ip eigrp topology**, notice that there is only one path listed. In the output of **show ip eigrp topology all-links**, notice that there are two paths listed. This is because the next hop 172.16.33.13 has an RD greater than the FD of the successor and therefore cannot be a feasible successor.

Example 4-28 *Sample show ip eigrp topology Comparison*

```
Router# show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(172.16.33.14)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 172.16.33.8/30, 1 successors, FD is 2169856
        via Connected, Serial1/0
P 10.1.34.0/24, 1 successors, FD is 2682112
        via 172.16.33.9 (2682112/2170112), Serial1/0
P 203.0.113.0/30, 1 successors, FD is 2684416
        via 172.16.33.9 (2684416/2172416), Serial1/0
P 172.16.32.192/29, 1 successors, FD is 28160
        via Connected, FastEthernet2/0
P 172.16.33.12/30, 1 successors, FD is 5511936
        via Connected, Serial1/1
P 172.16.33.0/29, 1 successors, FD is 2681856
        via 172.16.33.9 (2681856/2169856), Serial1/0

Router# show ip eigrp topology all-links
EIGRP-IPv4 Topology Table for AS(100)/ID(172.16.33.14)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 172.16.33.8/30, 1 successors, FD is 2169856, serno 1
        via Connected, Serial1/0
P 10.1.34.0/24, 1 successors, FD is 2682112, serno 8
        via 172.16.33.9 (2682112/2170112), Serial1/0
        via 172.16.33.13 (6024192/3072256), Serial1/1
P 203.0.113.0/30, 1 successors, FD is 2684416, serno 9
        via 172.16.33.9 (2684416/2172416), Serial1/0
        via 172.16.33.13 (6026496/3074560), Serial1/1
P 172.16.32.192/29, 1 successors, FD is 28160, serno 3
        via Connected, FastEthernet2/0
P 172.16.33.12/30, 1 successors, FD is 5511936, serno 2
        via Connected, Serial1/1
P 172.16.33.0/29, 1 successors, FD is 2681856, serno 5
        via 172.16.33.9 (2681856/2169856), Serial1/0
        via 172.16.33.13 (6023936/3072000), Serial1/1
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Feasible Successors (Cont.)

- The EIGRP topology table contains not only the routes learned from other routers but also routes that have been redistributed into the EIGRP process and the local connected networks whose interfaces are participating in the EIGRP process, as highlighted in Example 4-29.

Example 4-29 *Verifying Connected and Redistributed Entries in the Topology Table*

```
R4# show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(192.4.4.4)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

...output omitted...
P 192.2.2.2/32, 1 successors, FD is 131072
        via 10.1.34.3 (131072/130816), GigabitEthernet2/0
P 10.1.13.0/24, 1 successors, FD is 3072
        via 10.1.34.3 (3072/2816), GigabitEthernet2/0
P 0.0.0.0/0, 1 successors, FD is 28160
        via Rstatic (28160/0)
P 192.1.1.1/32, 1 successors, FD is 131072
        via 10.1.34.3 (131072/130816), GigabitEthernet2/0
P 172.16.32.192/29, 1 successors, FD is 2174976
        via 172.16.33.5 (2174976/30720), Serial1/0
        via 172.16.33.6 (2684416/2172416), Serial1/0
        via 172.16.33.18 (2684416/2172416), Serial1/2
P 198.51.100.0/30, 1 successors, FD is 28416
        via 10.1.34.3 (28416/28160), GigabitEthernet2/0
P 172.16.33.12/30, 1 successors, FD is 2172416
        via 172.16.33.5 (2172416/28160), Serial1/0
P 192.6.6.6/32, 2 successors, FD is 2297856
        via 172.16.33.6 (2297856/128256), Serial1/0
        via 172.16.33.18 (2297856/128256), Serial1/2
P 172.16.33.0/29, 1 successors, FD is 2169856
        via Connected, Serial1/0
...output omitted...
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Discontiguous Networks and Autosummarization

- EIGRP supports variable-length subnet masking (VLSM). In Cisco IOS versions before 15.0, EIGRP automatically performed route summarization on classful network boundaries.
- In Cisco IOS version 15.0 and newer, auto summarization is turned off by default. You no longer need to configure the **no auto-summary command**.
- Although it is turned off by default, the command can be manually enabled and can cause routing issues if the network contains discontiguous networks. Figure 4-6 provides and example of discontiguous subnets of the Class B network 172.16.0.0/16.

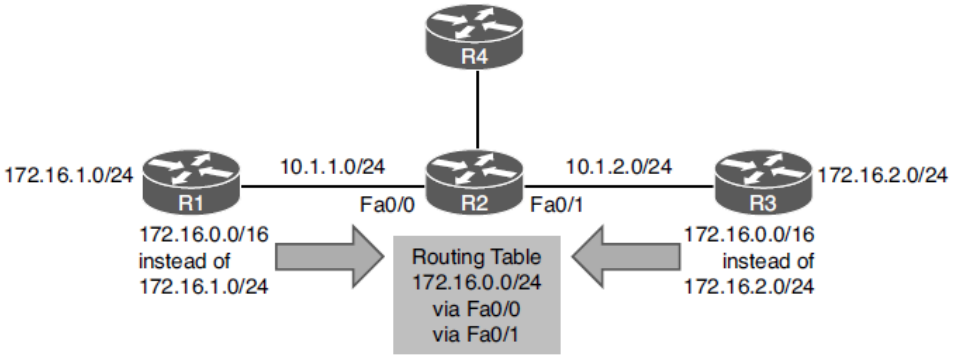

Figure 4-6 *Discontiguous Network Example*

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Discontiguous Networks and Autosummarization

- If you have a discontiguous network, auto summarization has to be off, and you must take care when performing manual summarization.
- To verify whether automatic summarization is enabled or disabled, use the **show ip protocols** command, as shown in Example 4-30.

Example 4-30 *Verifying Route Summarization with show ip protocols*

```
Router# show ip protocols
...output omitted...
  EIGRP-IPv4 Protocol for AS(100)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 10.1.13.1
    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
  Address Summarization:
    10.1.0.0/20 for Gi2/0
      Summarizing 2 components with metric 2816
  Maximum path: 4
  Routing for Networks:
...output omitted...
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Route Summarization

- By default with IOS 15.0 and later, autosummary is off. Therefore, you can either turn it on (which is not recommended) or perform manual route summarization (which is recommended).
- With EIGRP, manual route summarization is enabled on an interface-by-interface basis.
- It is important that you create accurate summary routes to ensure that your router is not advertising networks in the summary route that it does not truly know how to reach.
- When troubleshooting EIGRP route summarization, keep in mind the following:
  - Did you enable route summarization on the correct interface?
  - Did you associate the summary route with the correct EIGRP autonomous system?
  - Did you create the appropriate summary route?
- You determine the answers to these questions by using the show ip protocols command, as shown in Example 4-30.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Route Summarization (Cont.)

- When a summary route is created on a router, so is a summary route to null 0, as shown in the following snippet:

```
Router# show ip route | include Null
D 10.1.0.0/20 is a summary, 00:12:03, Null0
```

- This route to null 0 is created to prevent routing loops. It is imperative that this route exists in the table. It ensures that when a packet is received by the router with an unknown destination network address that falls within the summary, the packet will be dropped. If the route to null 0 did not exist, and there was a default route on the router, the router would forward the packet using the default route. The next-hop router would then end up forwarding the packet back to this router because it is using the summary route and the process would repeat. This is a routing loop.
- The route to null 0 has an AD of 5, to ensure that it is more trustworthy than most of the other sources of routing information. The only way this route would not be in the routing table is if you had a source with a lower AD (for example, if someone created a static route for the same summary network and pointed it to a next-hop IP address instead of null 0).

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Load Balancing

- By default, EIGRP load balances on four equal-metric paths. You can change this with the **maximum-paths** command in router configuration mode for EIGRP.
- EIGRP also supports load balancing across unequal-metric paths, using the *variance* feature. By default, the variance value for an EIGRP routing process is 1, which means the load balancing will occur only over equal-metric paths. Increasing the multiplier increases the range of metrics over which load balancing will occur.
- Even with unequal-metric load balancing, you are still governed by the **maximum-paths** command. Therefore, if you have five unequal-metric paths that you want to use, and you configure the correct variance multiplier, but maximum-paths is set to 2, you use only two of the five paths.
- If the path is not a feasible successor, it cannot be used for unequal-path load balancing. There is no exception to this rule.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Load Balancing (Cont.)

To verify the configured maximum paths and variance, you use the **show ip protocols** command, as shown in Example 4-31.

Example 4-31 *Verifying Variance and Maximum Paths*

```
Router# show ip protocols
Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(100)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 10.1.12.1
    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:
    0.0.0.0
  Routing Information Sources:
    Gateway    Distance    Last Update
    10.1.12.2         90    10:26:36
  Distance: internal 90 external 170
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

EIGRP for IPv4 Trouble Tickets

This section presents various trouble tickets related to the topics discussed earlier in the chapter. The purpose of these trouble tickets is to show a process that you can follow when troubleshooting in the real world or in an exam environment.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Trouble Ticket Topology

All trouble tickets in the section are based on the topology shown in Figure 4-7.

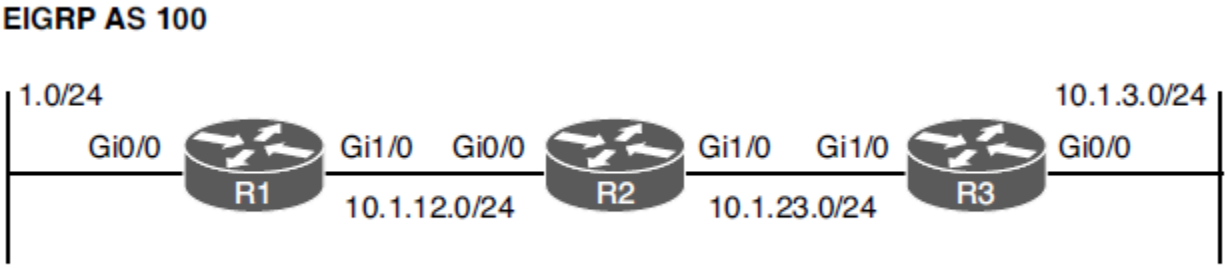

Figure 4-7 *EIGRP for IPv4 Trouble Tickets Topology*

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Trouble Ticket 4-1

Problem: Users in the 10.1.1.0/24 network indicate that they are not able to access resources in the 10.1.3.0/24 network.

Verify the problem by accessing a PC in the 10.1.1.0/24 network and ping an IP address in the 10.1.3.0/24 network. The resulting ping response is shown in Example 4-32. Notice that the reply is from the default gateway at 10.1.1.1, and it states Destination host unreachable. The ping is technically not successful.

Refer to your text for next steps and examples to troubleshoot and resolve this trouble ticket.

Example 4-32 *Destination Unreachable Result from the ping Command on a PC*

```
C:\>ping 10.1.3.10

Pinging 10.1.3.10 with 32 bytes of data;

Reply from 10.1.1.1: Destination host unreachable.
Reply from 10.1.1.1: Destination host unreachable.
Reply from 10.1.1.1: Destination host unreachable.
Reply from 10.1.1.1: Destination host unreachable.

Ping statistics for 10.1.3.10:
    Packets: Sent = 4, Received = 4, lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Trouble Ticket 4-2

Problem: Users in the 10.1.1.0/24 network have indicated that they are not able to access resources in 10.1.3.0/24.

To begin, you verify the problem by pinging from a PC in the 10.1.1.0/24 network to a PC in the 10.1.3.0/24 network, as shown in Example 4-50, and it fails. Notice that the reply is from the default gateway at 10.1.1.1 and it states Destination host unreachable. Therefore, it is technically not successful.

Refer to your text for next steps and examples to troubleshoot and resolve this trouble ticket.

Example 4-50 *Destination Unreachable Result from the ping Command on a PC*

```
C:\>ping 10.1.3.10

Pinging 10.1.3.10 with 32 bytes of data;

Reply from 10.1.1.1: Destination host unreachable.
Reply from 10.1.1.1: Destination host unreachable.
Reply from 10.1.1.1: Destination host unreachable.
Reply from 10.1.1.1: Destination host unreachable.

Ping statistics for 10.1.3.10:
    Packets: Sent = 4, Received = 4, lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Trouble Ticket 4-3

Problem: Users in the 10.1.1.0/24 network have indicated that they are not able to access resources in 10.1.3.0/24.

To begin, you verify the problem by pinging from a PC in the 10.1.1.0/24 network to a PC in the 10.1.3.0/24 network. As shown in Example 4-59, it fails. Notice that the reply is from the default gateway at 10.1.1.1, and it states Destination host unreachable.

Refer to your text for next steps and examples to troubleshoot and resolve this trouble ticket.

Example 4-59 *Destination Unreachable Result from the ping Command on a PC*

```
C:\>ping 10.1.3.10

Pinging 10.1.3.10 with 32 bytes of data;

Reply from 10.1.1.1: Destination host unreachable.
Reply from 10.1.1.1: Destination host unreachable.
Reply from 10.1.1.1: Destination host unreachable.
Reply from 10.1.1.1: Destination host unreachable.

Ping statistics for 10.1.3.10:
    Packets: Sent = 4, Received = 4, lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Prepare for the Exam

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Prepare for the Exam

Key Topics for Chapter 4

Description	
Possible reasons an EIGRP neighbor relationship might not form	How a better source of routing information could cause suboptimal routing
Verifying the autonomous system number with **show ip protocols**	Considerations when troubleshooting route filters
Verifying EIGRP interfaces with **show ip eigrp interfaces**	Stub configuration
Verifying K values with **show ip protocols**	Split horizon
Verifying passive interfaces with **show ip protocols**	Considerations when troubleshooting route summarization
Authentication	Verifying variance and maximum paths
Possible reasons EIGRP for IPv4 routes missing from the routing table	

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Key Terms for Chapter 4

Term	Term	Term
Hello packet	Key string	Feasible distance
224.0.0.10	Keychain	Discontiguous network
Network command	Stub	Autosummarization
Autonomous system number	Split horizon	Classful
K value	Successor	Classless
Passive interface	Feasible successor	Maximum paths
Key ID	Reported distance	Variance

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Command Reference for Chapter 4

Task	Command Syntax
Display the IPv4 routing protocols enabled on the router; for EIGRP, display autonomous system number, outgoing and incoming filters, K values, router ID, maximum paths, variance, local stub configuration, routing for networks, routing information sources, administrative distance, and passive interfaces	**show ip protocols**
Show a router's EIGRP neighbors	**show ip eigrp neighbors**
Show detailed information about a router's EIGRP neighbors, including whether the neighbor is a stub router, along with the types of networks it is advertising as a stub	**show ip eigrp neighbors detail**
Display all of a router's interfaces that are configured to participate in an EIGRP routing process (with the exception of passive interfaces)	**show ip eigrp interfaces**

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Command Reference for Chapter 4 (Cont.)

Task	Command Syntax
Display the interfaces participating in the EIGRP for IPv4 routing process, along with EIGRP hello and hold timers, whether the split horizon rule is enabled, and whether authentication is being used	**show ip eigrp interfaces detail**
Display the EIGRP configuration in the running configuration	**show run | section router eigrp**
Display the configuration of a specific interface in the running configuration (This is valuable when you are trying to troubleshoot EIGRP interface commands.)	**show run interface** *interface_type interface_number*
Display the keychains and associated keys and key strings	**show key chain**
Display IPv4 interface parameters; for EIGRP, verify whether the interface has joined the correct multicast group (224.0.0.10) and whether any ACLs applied to the interface might be preventing an EIGRP adjacency from forming	**show ip interface** *interface_type interface_number*

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Command Reference for Chapter 4 (Cont.)

Task	Command Syntax
Display routes known to a router's EIGRP routing process, which are contained in the EIGRP topology table (The all-links keyword displays all routes learned for each network, and without the all-links keyword, only the successors and feasible successors are displayed for each network.)	**show ip eigrp topology [all-links]**
Show routes known to a router's IP routing table that were injected by the router's EIGRP routing process	**show ip route eigrp**
Display all EIGRP packets exchanged with a router's EIGRP neighbors or display only specific EIGRP packet types (for example, EIGRP hello packets)	**debug eigrp packets**

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


CISCO