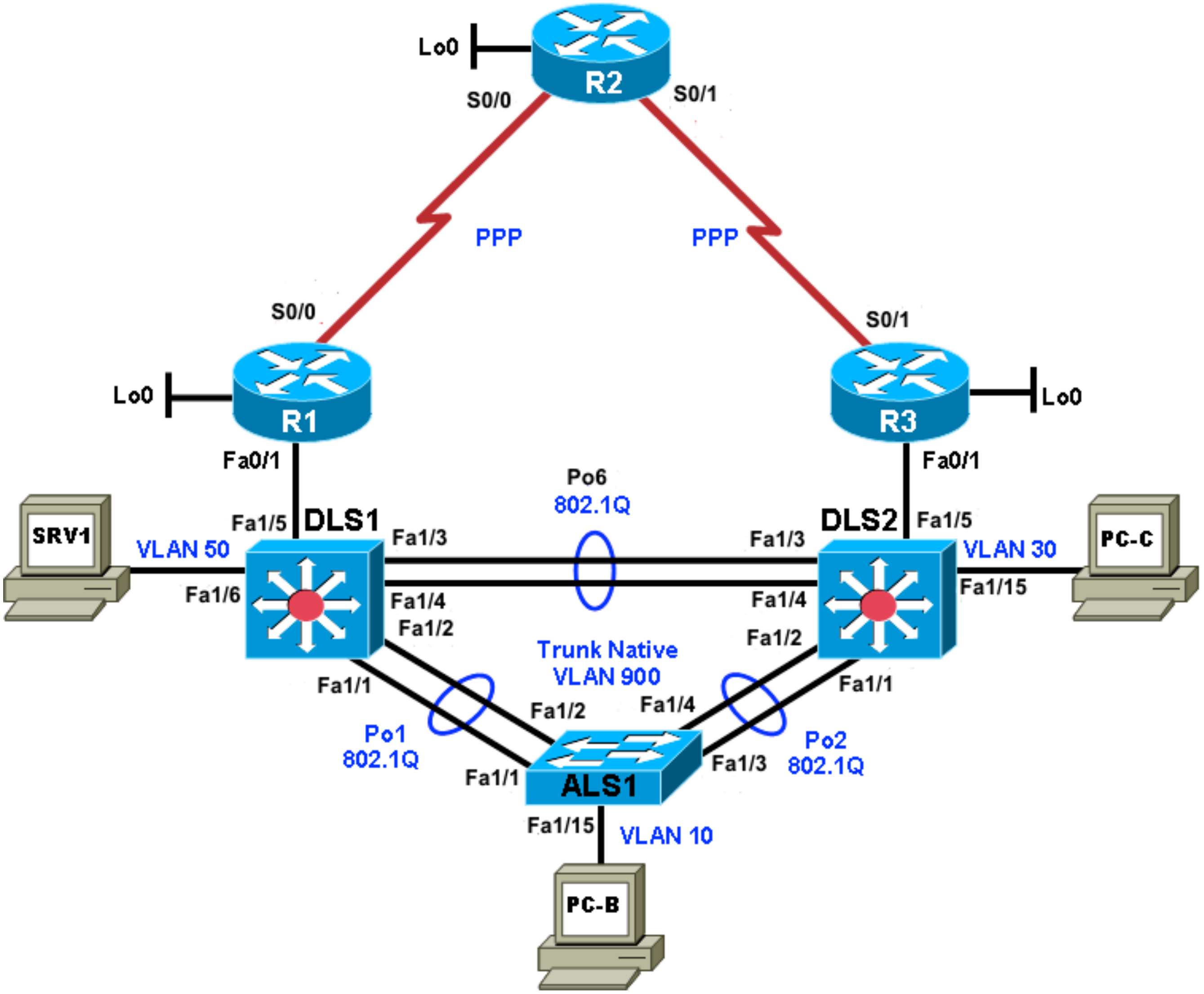
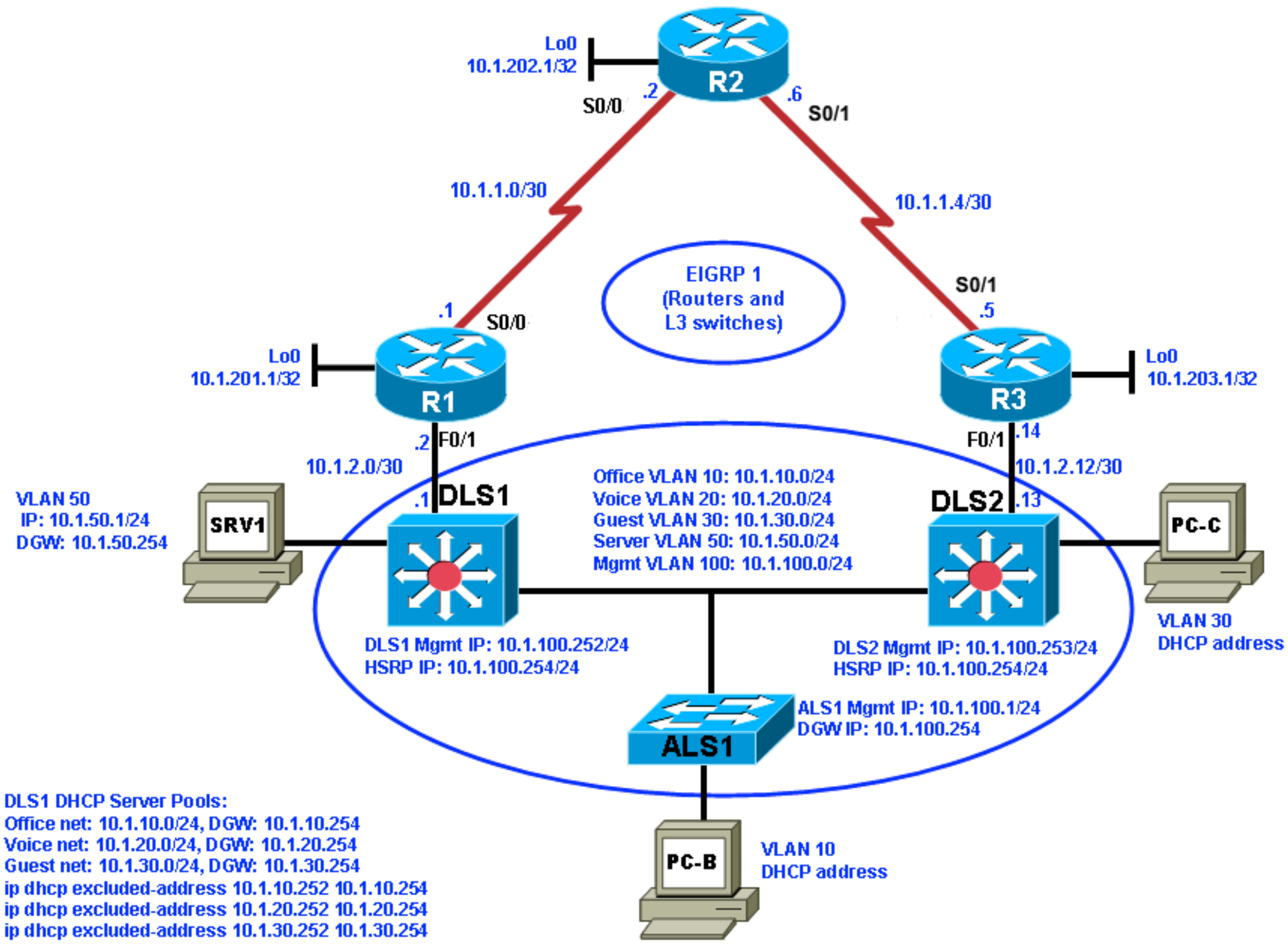
Lab 5-3, BGP

Physical Topology (Baseline)



Logical Topology (Baseline)


Lo0
10.1.202.1/32
R2
S0/0
.2
.6
S0/1
10.1.1.0/30
10.1.1.4/30
EIGRP 1
(Routers and
L3 switches)
.1
S0/0
S0/1
.5
Lo0
10.1.201.1/32
R1
R3
Lo0
10.1.203.1/32
.2
F0/1
F0/1
.14
10.1.2.0/30
10.1.2.12/30
Office VLAN 10: 10.1.10.0/24
Voice VLAN 20: 10.1.20.0/24
Guest VLAN 30: 10.1.30.0/24
Server VLAN 50: 10.1.50.0/24
Mgmt VLAN 100: 10.1.100.0/24
VLAN 50
IP: 10.1.50.1/24
DGW: 10.1.50.254
SRV1
.1
DLS1
DLS2
.13
PC-C
VLAN 30
DHCP address
DLS1 Mgmt IP: 10.1.100.252/24
HSRP IP: 10.1.100.254/24
DLS2 Mgmt IP: 10.1.100.253/24
HSRP IP: 10.1.100.254/24
ALS1
ALS1 Mgmt IP: 10.1.100.1/24
DGW IP: 10.1.100.254
DLS1 DHCP Server Pools:
Office net: 10.1.10.0/24, DGW: 10.1.10.254
Voice net: 10.1.20.0/24, DGW: 10.1.20.254
Guest net: 10.1.30.0/24, DGW: 10.1.30.254
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254
PC-B
VLAN 10
DHCP address

Objectives

- Load the trouble ticket device configuration files for each trouble ticket.
- Diagnose and resolve problems related to the BGP exterior routing protocol.
- Document troubleshooting progress, configuration changes, and problem resolution.

Background

Border Gateway Protocol (BGP) is the most widely used exterior routing protocol on the Internet. It is the de facto standard for route (prefix) exchange between the autonomous systems (AS) of Internet service providers (ISPs). BGP can also be used between a customer network and one or more ISPs. In this lab, you will troubleshoot various problems related to BGP. For each task or trouble ticket, the trouble scenario and problem symptom are described. While troubleshooting, you will discover the cause of the problem, correct it, and then document the process and results.

Implementing BGP

Your company has decided to implement several new Internet-based services. The current web services that the company offers are hosted at an external data center. It has been decided to build an in-house data center from which the new services will be hosted. The servers that are currently externally hosted will also be moved to the new data center.

Your company currently has a single ISP for Internet access. You have obtained a registered AS number (65501) and address block 172.30.1.0/27, which will be used for the new services. After consulting with the ISP, it has been decided to use BGP between the network edge router R1 and the ISP (R2). Upon successful completion of the BGP implementation, your company is considering adding another ISP for redundancy, but not as part of the current project.

Your support team has been working closely together with the engineering team to prepare the implementation. You have received confirmation from the ISP that they have prepared their router for the BGP implementation.

Router R1 will advertise the 172.30.1.0/27 IP address block to the ISP (R2). No other prefixes are allowed to be advertised. This ensures that only the assigned network address block will be received by the ISP. ISPs typically place filters on their edge routers to prevent customers from accidently announcing routes that do not belong to them.

The ISP router will send a default route to router R1 via BGP. The default route will be redistributed into Enhanced Interior Gateway Routing Protocol (EIGRP) by router R1. No other routes will be redistributed.

It is Friday evening, and the engineering team has just configured router R1 for BGP. To facilitate testing, a new hosted services VLAN and the corresponding subnet 172.30.1.0/27 will be created. All other devices, which have IP addresses in the 10.1.0.0/16 range, are using Network Address Translation (NAT), and their Internet access should not be affected by the BGP configuration.

You are on standby to assist in troubleshooting and testing the solution.

Implementation Plan

The implementation plan is in two phases.

Phase 1

During Phase 1, the link between edge router R1 and the existing ISP will be upgraded to a T1 leased line and converted to BGP. The remainder of the network will continue to use EIGRP. The 10.1.1.0/30 addressing on the R1-to-R2 serial WAN link will be changed to a public address (209.165.200.224/30) provided by the ISP. NAT will be used to translate the 10.1.0.0/16 internal private addresses to public address 209.165.200.225 using Port Address Translation (PAT). The loopback 0 address on R1 is also changed to 192.168.1.1.

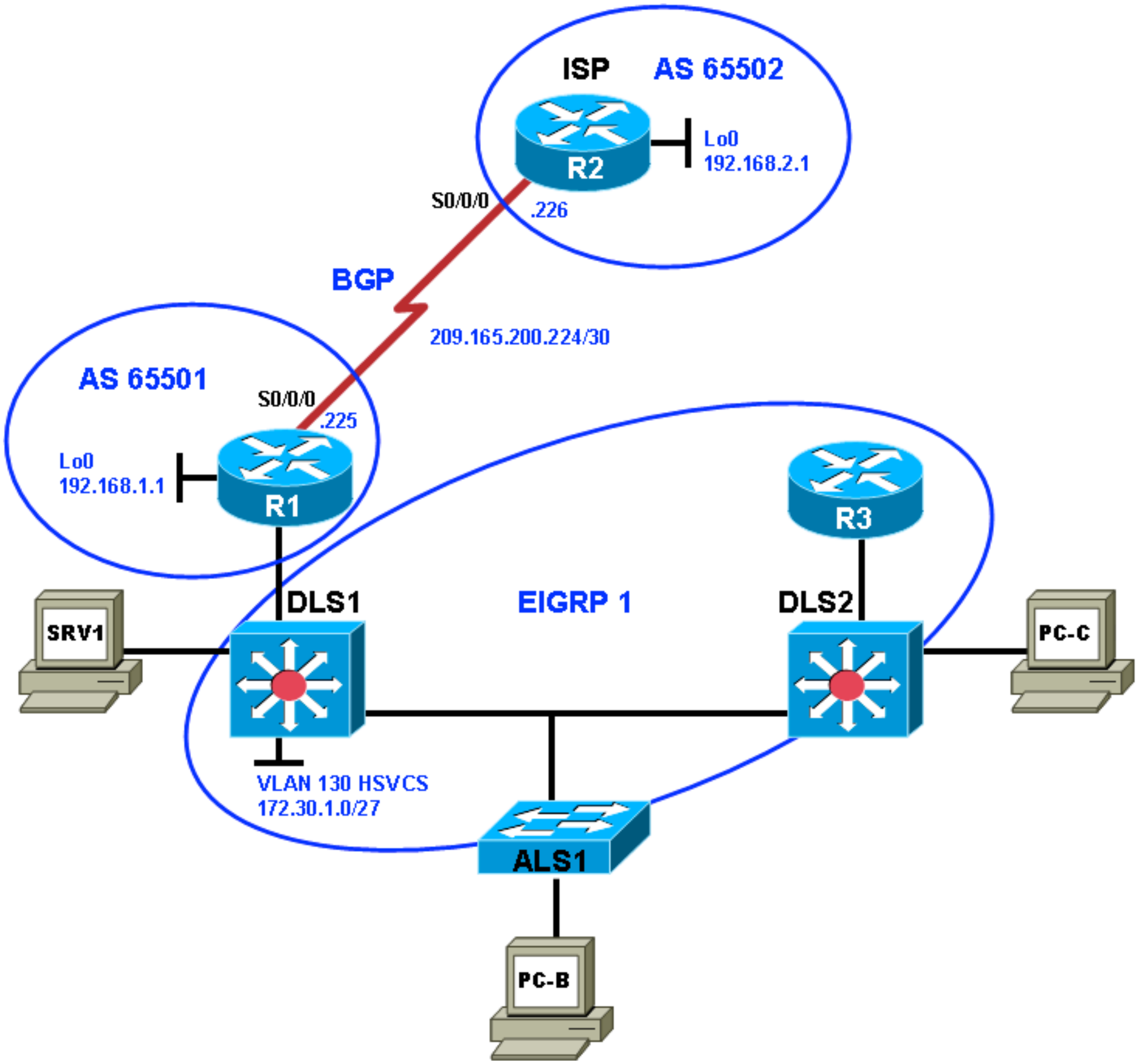
An external BGP peering will be established between router R1 and the ISP (R2). The ISP will advertise a default route to R1 via BGP. On router R1, redistribution of the default route will be configured between BGP and EIGRP to ensure connectivity between headquarters and the ISP.

Phase 2

During Phase 2, the hosted services VLAN 130 named HSVCS and the corresponding subnet 172.30.1.0/27 will be created on switch DLS1. A test server for the hosted services subnet will be installed, simulated by switch virtual interface (SVI) VLAN 130 172.30.1.1/27 on DLS1. A static route will be provided from R1 to DLS1 VLAN 130. Some services will be migrated to the new IP address block before moving them to the newly built datacenter.

BGP Network Design

The BGP design is outlined in the following figure. BGP AS 65501 is the company’s newly acquired AS number. The ISP AS is 65502.



Test Plan

In Phase 1, edge router R1 must become a BGP peer with the ISP, and the internal office clients must be able to access the Internet through the ISP. In Phase 2, the Internet clients must be able to access the hosted services network.

Note: Trouble ticket A is related to the verification and acceptance of BGP Phase 1. Trouble tickets B and C are related to the second phase of BGP conversion. Any interfaces that have been shut down on routers R2 and R3 should remain shut down for the duration of this lab exercise.

Physical and Logical Topology Diagrams

The physical and logical topologies for the existing EIGRP-based network are provided in this lab to assist the troubleshooting effort.

Section 1—Trouble Tickets and Troubleshooting Logs

Task 1: Trouble Ticket Lab 53-A (2 Issues)

Step 1: Review trouble ticket Lab 53-A.

After your colleague finished configuring BGP on edge router R1, you tested connectivity from PC-B in VLAN 10 to the ISP router to verify the configuration and peering between R1 and R2. This test failed. When you asked your colleague, he said he did not actually test the configuration from a client PC on the internal network. He suspected there was a problem with the ISP and contacted them to find out if there was an issue at their end. They stated that everything was correctly configured on router R2.

Your task is to diagnose the problem and verify that BGP is properly configured to enable BGP peering between router R1 and the ISP.

Step 2: Load the device trouble ticket configuration files for 53-A.

a. On each device issue the command **53-A**

b. In GNS3, go to **File**, select **Save Project As,** click Yes to Message and give it name **TSHOOT-53A**

c. Shut down GNS3, restart this new project. Restart all the devices.

Step 3: Clear mac address table on DSL1 and DSL2

```
a.  DLS1#clear mac

b.  DLS2#clear mac
```

Step 4: Check DHCP addresses on PC-B and PC-C.

Ensure that PC-B and PC-C are configured as DHCP clients and have the expected IP addresses.

Note: Problems introduced into the network by the trouble ticket might prevent one or both of these PCs from acquiring an IP address. Do not assign either PC a static address.

Step 5: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions and methods, and procedure and communication improvements.

____

____

____

____

____

____

____

Task 2: Trouble Ticket Lab 53-B (2 Issues)

Step 1: Review trouble ticket Lab 53-B.

The next step after the peering has been established is to test the new hosted services subnet, which has been created using VLAN 130. This subnet uses the 172.30.1.0/27 IP address block that was assigned to your company by the ISP. The subnet has been configured, and a test server has been installed (simulated by DLS1 SVI VLAN 130 - 172.30.1.1). Internet clients must be able to access the subnet from ISP router R2 (simulated by Lo0 192.168.2.1). Other hosts in the EIGRP 10.1.0.0/16 domain do not require access to the hosted services subnet.

Your task is to verify VLAN configuration and routing functionality. Also, verify that traffic from the Internet can be sent to the hosted network test server in VLAN 130 via R1 and that the return traffic can be received via ISP router R2.

Step 2: Load the device trouble ticket configuration files for 53-B.

d. On each device issue the command **53-B**

e. In GNS3, go to **File**, select **Save Project As,** click Yes to Message and give it name **TSHOOT-53B**

f. Shut down GNS3, restart this new project. Restart all the devices.

Step 3: Clear mac address table on DSL1 and DSL2

```
c.  DLS1#clear mac

d.  DLS2#clear mac
```

Step 4: Check DHCP addresses on PC-B and PC-C.

Ensure that PC-B and PC-C are configured as DHCP clients and have the expected IP addresses.

Note: Problems introduced into the network by the trouble ticket might prevent one or both of these PCs from acquiring an IP address. Do not assign either PC a static address.

Step 7: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions and methods, and procedure and communication improvements.

____

____

____

____

____

____

____

Section 2—Troubleshooting Reference Information

General Troubleshooting Process

As a general guideline, you can use the following general troubleshooting process described in the course.

1. Define the problem (symptoms).
2. Gather information.
3. Analyze the information.
4. Propose a hypothesis (possible cause).
5. Test the hypothesis.
6. Eliminate or accept the hypothesis.
7. Solve the problem.
8. Document the problem.

Command Summary

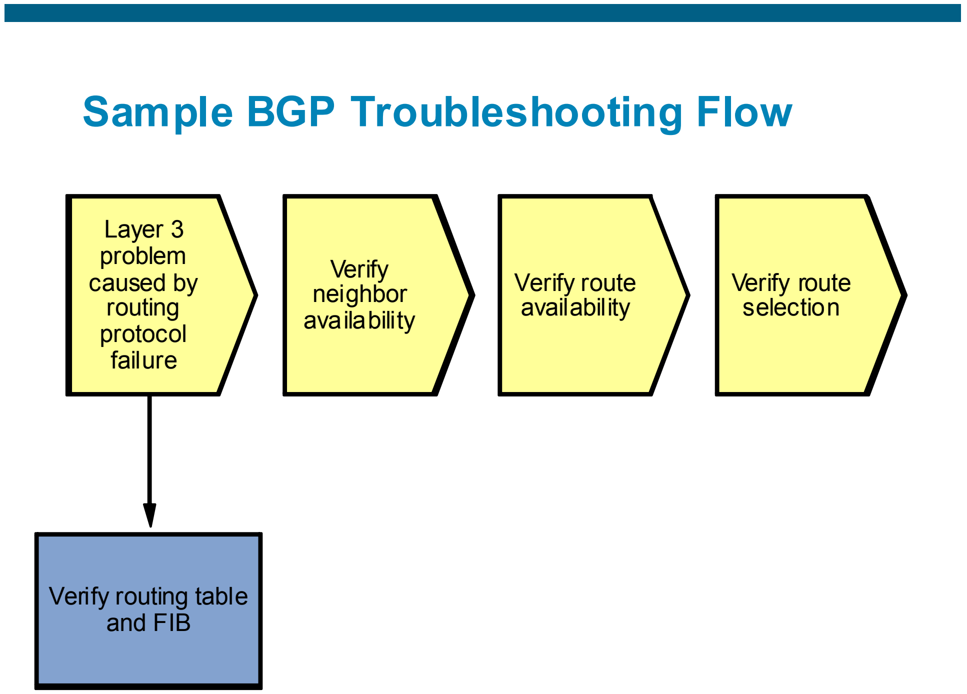
The table lists useful commands. Sample output is shown on the following pages.

Command	**Key Information Displayed**
show ip route or **show ip route** *ip-addr*	Displays the entire routing table or information for a particular destination address.
show ip bgp	Displays local and learned network entries in the BGP table with next hop, metric, local preference, weight, and AS path.
show ip bgp summary	Displays a summary of the BGP neighbor table. This command lists important BGP parameters, such as the AS number and router ID, statistics about the memory consumption of the various BGP data structures, and a brief overview of the configured neighbors and their state.
show ip bgp neighbors or **show ip bgp neighbor** *ip-address*	Displays parameters and extensive statistics about the peering session for all neighbors or for a particular neighbor address.
show ip bgp *network mask*	Displays the contents of the BGP table for a specific prefix. The information is organized in the following manner: The entry for each available path in the table starts with the AS path attribute of the path, using the word “Local” to represent the empty AS path string.
debug ip tcp transactions	Displays TCP connection activity between peers. Can be used to investigate whether the TCP session is refused, established, and subsequently torn down again, or no response is received at all from the neighbor.
debug ip bgp	Displays the successive state transitions during the

	establishment of the BGP peering. If one of the peers decides to close the session because of a parameter problem, such as a mismatched AS number or an invalid router ID, the debug also displays information about the cause.
`clear ip bgp *`	Clears the contents of the BGP table.
`show ip bgp` *`network mask`* **`longer prefixes`**	Displays more specific prefixes present in the BGP table (including the prefix itself) that are contained in the prefix specified by the *`network`* and *`mask`* options.
`show ip bgp neighbor` *`ip-address`* **`routes`**	Displays all routes in the BGP table that were received from the neighbor specified by the *`ip-address`* option.
`show ip bgp neighbor` *`ip-address`* **`advertised-routes`**	Displays all routes in the BGP table that will be advertised to the neighbor specified by the *`ip-address`* option.
`show ip bgp regexp` *`regular-expression`*	Displays all routes from the BGP table that have an AS path string that is matched by the specified regular expression.

Lab 5-3: Sample Troubleshooting Flows

The figure illustrates an example of a method that you could follow to diagnose and resolve problems related to BGP.



Sample BGP Troubleshooting Flow

Layer 3 problem caused by routing protocol failure

Verify neighbor availability

Verify route availability

Verify route selection

Verify routing table and FIB

The typical trigger to start investigating BGP operation is when you are using BGP as an exterior gateway protocol to connect to other autonomous systems and you are troubleshooting IP connectivity to a destination in a different AS. Some reasons to start investigating BGP are if a route to the destination network is missing from the routing table of one of the routers, a different route than expected was selected to forward the packets to that destination, or return traffic from the other AS is not making it back to the source.

Troubleshooting problems with missing return traffic usually requires coordination with those responsible for the routing in the destination AS and possibly even intermediate autonomous systems. The only thing you can verify from within your own AS is if your routing information is correctly passed to the neighbor AS. Propagation of your routes beyond your direct peers cannot be verified without access to routers in other autonomous systems.

Therefore, this flow focuses mainly on troubleshooting traffic to a destination network in a different AS. However, commands that are helpful in troubleshooting route advertisement to a different AS are also highlighted, if appropriate.

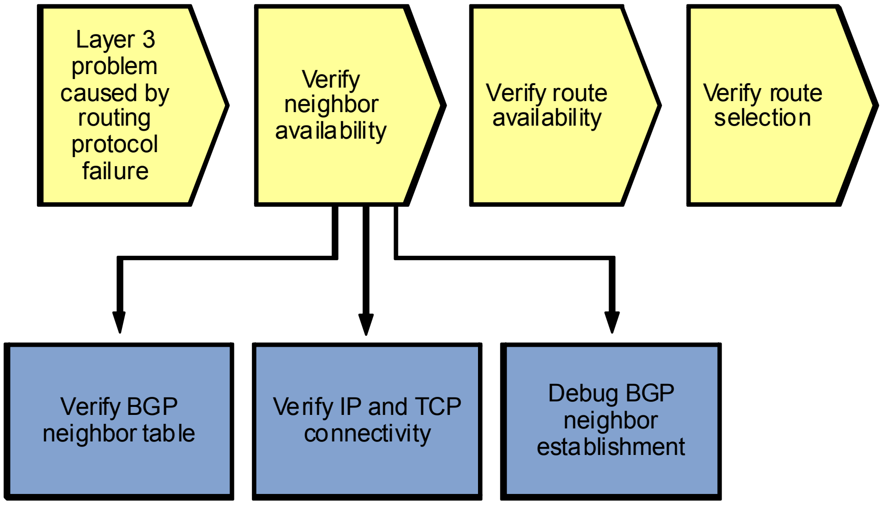
To install a route into the routing table, each router that uses BGP goes through several stages:

1. Establish neighbor relationships with its configured neighbors.
2. Exchange routing information with neighbors and store the received information in the BGP table.
3. Select the best route from the available routes and install it in the routing table.

Errors during any of these stages can cause routing information to be missed or incorrect routing information to be installed in the routing table.

The order in which the different stages are verified is not important, as long as a structured approach is used.

Sample BGP Troubleshooting Flow


Layer 3 problem caused by routing protocol failure
Verify neighbor availability
Verify route availability
Verify route selection
Verify BGP neighbor table
Verify IP and TCP connectivity
Debug BGP neighbor establishment

BGP does not discover neighbors. Neighbor relationships are established based on an explicit configuration on both routers that participate in the peering session.

BGP uses TCP as a transport protocol. Establishing a peering relationship always starts with the establishment of a TCP session on port 179 between the configured neighbor IP addresses. By default, both neighbors attempt to initiate the TCP session to the configured IP address of the neighbor. When a router receives an incoming session request, it compares the source IP address of the session to its list of configured neighbors. It only accepts the session if the source IP address matches one of the IP addresses of its configured neighbors. Therefore, it is important that a router always sources the BGP packets that it sends to a specific neighbor from the IP address that has been configured as the neighbor IP address on the peer router. For neighbors that are directly connected on an interface, the correct source address is automatically used. For neighbors that are not directly connected, the appropriate source IP address for the session to a neighbor might need to be selected with the **neighbor** *ip-address* **update-source** *interface-id* command.

Verify the BGP Neighbor Table

```
R1#show ip bgp
BGP table version is 2, local router ID is 192.168.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 0.0.0.0          192.168.2.1              0             0 65502 i

R1#show ip bgp summary
BGP router identifier 192.168.1.1, local AS number 65501
BGP table version is 3, main routing table version 3
2 network entries using 264 bytes of memory
2 path entries using 104 bytes of memory
3/2 BGP path/bestpath attribute entries using 504 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 928 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.2.1     4 65502      36      36        3    0    0 00:33:01        1
```

To verify that all expected neighbor relationships are operational, you can display a summary of the BGP neighbor table using the **show ip bgp summary** command. This command lists important BGP parameters, such as the AS number and router ID, statistics about the memory consumption of the various BGP data structures, and a brief overview of the configured neighbors and their state.

For each neighbor, the configured IP address and AS of the neighbor are listed. The Up/Down column lists the time that has elapsed since the last state change. For a neighbor that is currently up, it lists the time elapsed since the session was established. For a neighbor that is down, it lists the time elapsed since the session was lost.

The most important column to verify the operational state of the neighbor is State/PfxRcd. This column can display the following values:

- **Idle** – Indicates that there is no session with the peer, and the router is not currently attempting to establish a session with the peer. The router is ready to accept incoming sessions.
- **Idle (Admin)** – Indicates that the session has been administratively shut down with the **neighbor** *ip-address* **shutdown** command.
- **Active** – The router is actively trying to open a TCP session with the neighbor. If it does not succeed in establishing the session, the router toggles between the Idle and Active states
- **Open Sent** – An Open message has been sent to the neighboring router containing the router ID, AS number, BGP version, hold timer, and capabilities.
- **Open Confirm** – An Open message from the neighbor has been received, the parameters in the message have been processed and accepted, and a hello message has been sent to acknowledge the acceptance of the neighbor's Open message.

- **Number of received prefixes** – After an acknowledgment from the neighbor confirming the reception of this router's Open message, the state of the session moves to the Established state. At this point, the State/PfxRcd column does not list the state. It shows the number of prefixes that have been received from that neighbor and installed in the BGP table. The desired result is to see a number listed in this column, because that indicates that the session with the peer has been successfully established.

The Open Sent and Open Confirm states are transitory states. When the state for a neighbor toggles between Active and Idle, this indicates that the router is not successful in establishing a session with the neighbor.

You can use the `show ip bgp neighbor` *`ip-address`* command to display additional parameters and extensive statistics about the peering session. For more information about these parameters and statistics, see the BGP command references on www.cisco.com.

Verify IP and TCP Connectivity

```
R1#debug ip tcp transactions
TCP special event debugging is on

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#no router bgp 65501
R1(config)#
*Nov 16 17:21:35.102: %BGP-5-ADJCHANGE: neighbor 192.168.2.1 Down BGP protocol i
nitialization
R1(config)#
*Nov 16 17:21:35.102: TCP0: state was ESTAB -> FINWAIT1 [179 -> 192.168.2.1(1188
9)]
*Nov 16 17:21:35.102: TCP0: sending FIN
*Nov 16 17:21:35.126: Released port 179 in Transport Port Agent for TCP IP type
0 delay 240000
*Nov 16 17:21:35.126: TCP0: state was LISTEN -> CLOSED [179 -> 192.168.2.1(0)]
*Nov 16 17:21:35.126: TCB 0x66EE8F34 destroyed
*Nov 16 17:21:35.138: TCP0: state was FINWAIT1 -> FINWAIT2 [179 -> 192.168.2.1(1
1889)]
*Nov 16 17:21:35.138: TCP0: FIN processed
*Nov 16 17:21:35.138: TCP0: state was FINWAIT2 -> TIMEWAIT [179 -> 192.168.2.1(1
1889)]
R1(config)#
*Nov 16 17:21:50.286: Reserved port 0 in Transport Port Agent for TCP IP type 0
*Nov 16 17:21:50.286: TCP: sending RST, seq 0, ack 2752306274
*Nov 16 17:21:50.286: TCP: sent RST to 192.168.2.1:41738 from 192.168.1.1:179
*Nov 16 17:21:50.290: Released port 0 in Transport Port Agent for TCP IP type 0
delay 240000
*Nov 16 17:21:50.290: TCP0: state was LISTEN -> CLOSED [0 -> UNKNOWN(0)]
*Nov 16 17:21:50.290: TCB 0x66F17E40 destroyed
R1(config)#
*Nov 16 17:21:55.006: Reserved port 0 in Transport Port Agent for TCP IP type 0
*Nov 16 17:21:55.006: TCP: sending RST, seq 0, ack 3974493125
*Nov 16 17:21:55.006: TCP: sent RST to 192.168.2.1:47416 from 192.168.1.1:179
*Nov 16 17:21:55.006: Released port 0 in Transport Port Agent for TCP IP type 0
delay 240000


R1(config)#router bgp 65501
R1(config-router)#no synchronization
R1(config-router)#bgp log-neighbor-changes
R1(config-router)#neighbor 192.168.2.1 remote-as 65502
R1(config-router)#neighbor 192.168.2.1 ebgp-multihop 2
```

```
R1(config-router)#neighbor 192.168.2.1 update-source Loopback0
*Nov 16 17:28:46.549: TCB65950C34 created
*Nov 16 17:28:46.549: TCB65950C34 setting property TCP_PMTU (38) 66A7C214
*Nov 16 17:28:46.549: TCB65950C34 setting property TCP_TOS (11) 66A7C220
*Nov 16 17:28:46.549: TCB65950C34 setting property TCP_VRFTABLEID (20) 66F233F8
*Nov 16 17:28:46.549: TCB65950C34 setting property TCP_IN_TTL (29) 66A7C200
*Nov 16 17:28:46.553: TCB65950C34 setting property TCP_OUT_TTL (30) 66A7C200
*Nov 16 17:28:46.553: TCB65950C34 setting property TCP_OUT_TTL (30) 66F2359A
*Nov 16 17:28:46.553: TCB65950C34 bound to UNKNOWN.179
*Nov 16 17:28:46.553: TCB65950C34 setting property TCP_ACCESS_CHECK (5) 60B47108

*Nov 16 17:28:46.553: TCB65950C34 setting property TCP_MD5KEY (4) 0
*Nov 16 17:28:46.553: Reserved port 179 in Transport Port Agent for TCP IP type
0
*Nov 16 17:28:46.553: TCB65950C34 listening with queue 1
*Nov 16 17:28:46.585: TCB65950C34 setting property TCP_IN_TTL (29) 66A7C278
*Nov 16 17:28:46.585: TCB65950C34 setting property TCP_OUT_TTL (30) 66A7C278
*Nov 16 17:28:46.585: TCB65950C34 setting property TCP_OUT_TTL (30) 66F2359A
R1(config-router)#
*Nov 16 17:28:50.581: TCB67096718 created
*Nov 16 17:28:50.581: TCB67096718 setting property TCP_VRFTABLEID (20) 66F233F8
*Nov 16 17:28:50.581: TCB67096718 setting property TCP_MD5KEY (4) 0
*Nov 16 17:28:50.581: TCB67096718 setting property TCP_ACK_RATE (32) 66F1B4D4
*Nov 16 17:28:50.581: TCB67096718 setting property TCP_TOS (11) 66F1B4C0
*Nov 16 17:28:50.581: TCB67096718 setting property TCP_PMTU (38) 66F1B48C
*Nov 16 17:28:50.581: TCB67096718 setting property TCP_IN_TTL (29) 66F1B478
*Nov 16 17:28:50.581: TCB67096718 setting property TCP_OUT_TTL (30) 66F1B478
*Nov 16 17:28:50.581: TCB67096718 setting property TCP_OUT_TTL (30) 66F2359A
*Nov 16 17:28:50.581: TCP: Random local port generated 30517, network 1
*Nov 16 17:28:50.581: TCB67096718 bound to 192.168.1.1.30517
*Nov 16 17:28:50.581: TCB67096718 setting property TCP_RTRANSTMO (31) 66F1B4D8
*Nov 16 17:28:50.581: Reserved port 30517 in Transport Port Agent for TCP IP typ
e 1
*Nov 16 17:28:50.581: TCP: sending SYN, seq 3632881552, ack 0
*Nov 16 17:28:50.581: TCP0: Connection to 192.168.2.1:179, advertising MSS 536
*Nov 16 17:28:50.585: TCP0: state was CLOSED -> SYNSENT [30517 -> 192.168.2.1(17
9)]
*Nov 16 17:28:50.593: TCP0: state was SYNSENT -> ESTAB [30517 -> 192.168.2.1(179
)]
*Nov 16 17:28:50.593: TCP: tcb 67096718 connection to 192.168.2.1:179, peer MSS
536, MSS is 536
*Nov 16 17:28:50.593: TCB67096718 connected to 192.168.2.1.179
*Nov 16 17:28:50.593: TCB67096718 setting property TCP_NO_DELAY (0) 66F1B4D8
*Nov 16 17:28:50.593: TCB67096718 setting property TCP_RTRANSTMO (31) 66F1B4D8
*Nov 16 17:28:50.621: %BGP-5-ADJCHANGE: neighbor 192.168.2.1 Up
R1(config-router)#
*Nov 16 17:28:50.821: TCP0: ACK timeout timer expired
R1(config-router)#do u all
All possible debugging has been turned off
```

If a session to one of the neighbors is not established correctly, you can take several steps to diagnose the issue. The first step is to test IP connectivity to the IP address of the neighbor by using the **`ping`** command. Make sure that you specify the same source interface that is used as the source interface for the BGP session. If the ping fails, initiate a troubleshooting process to first restore IP connectivity to the neighbor.

If the ping is successful, the next step is to determine whether the TCP session with the neighbor is established and successively torn down again, or if the TCP session is never established.

You can use the **debug ip tcp transactions** command to investigate whether the TCP session is refused (indicated by the reception of a TCP RST), established and subsequently torn down again (indicated by the normal TCP initiation and termination handshakes), or no response is received at all from the neighbor.

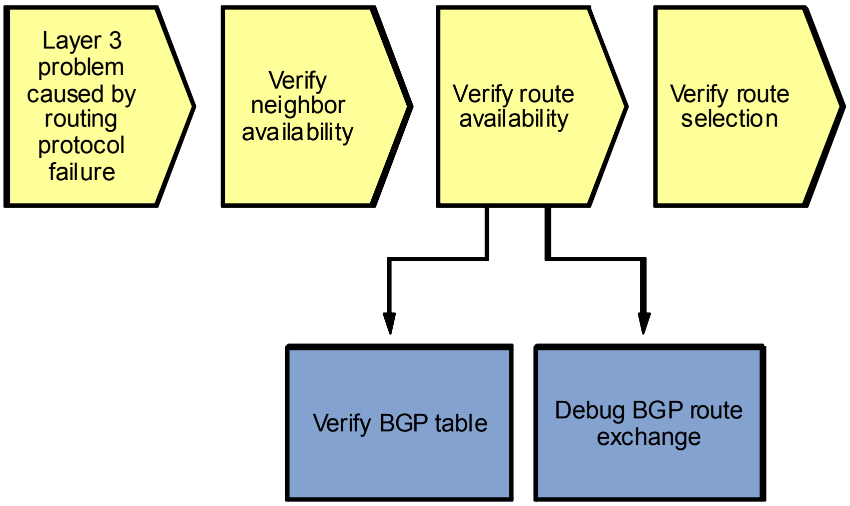
In the example output above, you can see that the TCP session to IP address 192.168.2.1 and TCP port 179 is refused by the peer, as indicated by the reception of the TCP RST from the peer. Clues like these can help eliminate possible problem causes. For instance, in this particular example, the output rules out an access list as the cause of the problem, because a TCP RST has been successfully received from the neighbor in response to the transmitted TCP SYN. In general, the fact that the peer refuses the session indicates that it does not recognize the session as coming from one of its configured neighbors. Possible causes are a missing neighbor statement or a mismatch between the configured IP address on the neighbor and the source IP address used by this router. Note that the source IP address and TCP port of the session are also displayed in the output of the debug as “bound to 192.168.1.1.30517.” You must work together with the party that manages the peer router to determine the exact cause of the problem.

Debug BGP Neighbor Establishment

```
R1#debug ip bgp
BGP debugging is on for address family: IPv4 Unicast

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface s0/0/0
R1(config-if)#shutdown
R1(config-if)#
*Nov 16 17:38:51.181: %LINK-5-CHANGED: Interface Serial0/0/0, changed state to a
dministratively down
*Nov 16 17:38:52.181: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/
0, changed state to down

R1(config-if)#do clear ip bgp 192.168.2.1
R1(config-if)#
*Nov 16 17:40:21.093: BGPNSF state: 192.168.2.1 went from nsf_not_active to nsf_
not_active
*Nov 16 17:40:21.093: BGP: 192.168.2.1 went from Established to Idle
*Nov 16 17:40:21.093: %BGP-5-ADJCHANGE: neighbor 192.168.2.1 Down User reset
R1(config-if)#
*Nov 16 17:40:21.093: BGP: 192.168.2.1 closing
R1(config-if)#
*Nov 16 17:40:22.973: BGP: 192.168.2.1 went from Idle to Active
*Nov 16 17:40:22.973: BGP: 192.168.2.1 active open failed - route to peer is inv
alid, open active delayed 26762ms (35000ms max, 60% jitter)


R1(config-if)#interface s0/0/0
R1(config-if)#no shutdown
R1(config-if)#
*Nov 16 17:40:51.041: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up

R1(config-if)#
*Nov 16 17:40:52.045: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/
0, changed state to up
R1(config-if)#
*Nov 16 17:41:11.365: BGP: 192.168.2.1 open active, local address 192.168.1.1
*Nov 16 17:41:11.373: BGP: 192.168.2.1 read request no-op
*Nov 16 17:41:11.377: BGP: 192.168.2.1 went from Active to OpenSent
*Nov 16 17:41:11.377: BGP: 192.168.2.1 sending OPEN, version 4, my as: 65501, ho
ldtime 180 seconds
*Nov 16 17:41:11.377: BGP: 192.168.2.1 send message type 1, length (incl. header
) 53
*Nov 16 17:41:11.397: BGP: 192.168.2.1 rcv message type 1, length (excl. header)
 34
*Nov 16 17:41:11.397: BGP: 192.168.2.1 rcv OPEN, version 4, holdtime 180 seconds

*Nov 16 17:41:11.397: BGP: 192.168.2.1 rcv OPEN w/ OPTION parameter len: 24
*Nov 16 17:41:11.397: BGP: 192.168.2.1 rcvd OPEN w/ optional parameter type 2 (C
apability) len 6
*Nov 16 17:41:11.397: BGP: 192.168.2.1 OPEN has CAPABILITY code: 1, length 4
*Nov 16 17:41:11.397: BGP: 192.168.2.1 OPEN has MP_EXT CAP for afi/safi: 1/1
*Nov 16 17:41:11.397: BGP: 192.168.2.1 rcvd OPEN w/ optional parameter type 2 (C
apability) len 2
*Nov 16 17:41:11.397: BGP: 192.168.2.1 OPEN has CAPABILITY code: 128, length 0
*Nov 16 17:41:11.397: BGP: 192.168.2.1 OPEN has ROUTE-REFRESH capability(old) fo
r all address-families
*Nov 16 17:41:11.397: BGP: 192.168.2.1 rcvd OPEN w/ optional parameter type 2 (C
apability) len 2
*Nov 16 17:41:11.397: BGP: 192.168.2.1 OPEN has CAPABILITY code: 2, length 0
*Nov 16 17:41:11.397: BGP: 192.168.2.1 OPEN has ROUTE-REFRESH capability(new) fo
r all address-families
*Nov 16 17:41:11.397: BGP: 192.168.2.1 rcvd OPEN w/ optional parameter type 2 (C
apability) len 6
*Nov 16 17:41:11.397: BGP: 192.168.2.1 OPEN has CAPABILITY code: 65, length 4
*Nov 16 17:41:11.397: BGP: 192.168.2.1 OPEN has 4-byte ASN CAP for: 65502
BGP: 192.168.2.1 rcvd OPEN w/ remote AS 65502, 4-byte remote AS 65502
*Nov 16 17:41:11.401: BGP: 192.168.2.1 went from OpenSent to OpenConfirm
*Nov 16 17:41:11.405: BGP: 192.168.2.1 went from OpenConfirm to Established
*Nov 16 17:41:11.405: %BGP-5-ADJCHANGE: neighbor 192.168.2.1 Up
R1(config-if)#
*Nov 16 17:41:11.433: BGP_Router: unhandled major event code 128, minor 0
R1(config-if)#do u all
All possible debugging has been turned off
```

If the TCP session is successfully established but consecutively torn down again, the likely cause is that one of the BGP peers is rejecting one of the parameters in the received Open message from the peer. The **debug ip bgp** command displays the successive state transitions during the establishment of the BGP peering. If one of the peers decides to close the session because of a parameter problem, such as a mismatched AS number or invalid router ID, the debug output displays information about the exact cause.

Sample BGP Troubleshooting Flow


Layer 3 problem caused by routing protocol failure
Verify neighbor availability
Verify route availability
Verify route selection
Verify BGP table
Debug BGP route exchange

After you have verified that neighbor relationships have been established as expected, verify that the route for the destination network that you are troubleshooting has been received correctly from all appropriate neighbors. BGP stores all routes that it receives from its neighbors in the BGP table and then selects the best route for each prefix to be installed in the routing table and advertised to other neighbors.

By investigating all available paths to the destination network in the BGP table, you can see if all the paths you expected to find are available. If multiple paths to the same prefix are listed, you can see which one was selected. In addition, you can see all the associated BGP attributes for the route, which can be useful to verify the path selection process and the results of the possible attribute manipulation by route maps that are used.

If routes are missing from the BGP table, you might need to debug the BGP route exchange process to see if they were not received or not entered into the BGP table.

Debug BGP Neighbor Establishment

```
R1#show ip bgp 0.0.0.0 0.0.0.0
BGP routing table entry for 0.0.0.0/0, version 4
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  65502
    192.168.2.1 from 192.168.2.1 (192.168.2.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
```

In the output above, the prefix is 0.0.0.0/0, the AS path is 65502, and the next hop is 192.168.2.1.

```
R1#show ip bgp 172.30.1.0 255.255.255.224
BGP routing table entry for 172.30.1.0/27, version 5
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Flag: 0x820
  Advertised to update-groups:
        1
  Local
    10.1.2.1 from 0.0.0.0 (192.168.1.1)
      Origin IGP, metric 0, localpref 100, weight 32768, valid, sourced, local,
R2>sh ip bgp 172.30.1.0/27
BGP routing table entry for 172.30.1.0/27, version 5
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Flag: 0x820
  Not advertised to any peer
  65501
    192.168.1.1 from 192.168.1.1 (192.168.1.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
```

The BGP table contains all routes that were received from all neighbors and were not denied by an incoming access list, prefix list, or route map. In the output for R2 above, the prefix is 172.30.1.0/27, the AS path is 65501 to the network, and the next hop is 192.168.1.1.

When you issue the **`show ip bgp`** *`network mask`* command to display the content of the BGP table for a specific prefix, the information is organized in the following manner. The entry for each available path in the table starts with the AS path attribute of the path (using the word “Local” to represent the empty AS path string). On the following lines, the other BGP attributes of the route, such as the next hop, origin code, and local preference, are listed. In addition, other information associated with the route is displayed. For example, the route is marked as internal if it was received from a BGP neighbor in the same AS. It is marked as external if it was received from a neighbor in a different AS. The path that was selected as the best path by the BGP path selection algorithm is marked as “best.”

Note: The following section uses some sample output not produced from the equipment in this lab to demonstrate how to interpret the output of this command. This output is interspersed with comments that explain the important fields and their interpretation.

```
IRO1#show ip bgp 172.34.224.0 255.255.224.0
BGP routing table entry for 172.34.224.0/19, version 98
Paths: (2 available, best #1, table Default-IP-Routing-Table)
```

Two paths are available to reach prefix 172.34.224.0/19. The first path listed has been selected as the best path.

```
Advertised to update-groups:
    2
```

The best path is advertised to all neighbors in update group 2. Use the **`show ip bgp update-group`** command to view the neighbors that are members of a specific update group.

```
65525 65486
```

The first path has 65525 65486 as its AS path attribute, which indicates that the route has originated in AS 65486 and then passed to AS 65525, which subsequently passed it to this AS.

```
  192.168.224.254 from 192.168.224.254 (192.168.100.1)
```

The BGP next hop for this route is 192.168.224.254. The route was received from neighbor 192.168.224.254. The router ID of that neighbor is 192.168.100.1.

```
    Origin IGP, localpref 100, valid, external, best
```

The origin attribute for this route is IGP, and the local preference attribute has a value of 100. This route is a valid route received from an external BGP peer, and it has been selected as the best path.

```
 64566 65486
```

The second path has 64566 65486 as its AS path attribute, which indicates that the route has originated in AS 65486 and then passed to AS 64566, which subsequently passed it to this AS.

```
            172.24.244.86 (metric 30720) from 10.1.220.4 (10.1.220.4)
```

The BGP next hop for this route is 172.24.244.86, and the IGP metric to reach this next-hop IP address is 30720 (which is the EIGRP metric listed in the routing table to reach 172.24.244.86). The route was received from neighbor 10.1.220.4, and the router ID of that neighbor is also 10.1.220.4.

```
             Origin IGP, metric 0, localpref 100, valid, internal
```

The origin attribute for this route is IGP, the multi-exit discriminator (MED) attribute has a value of 0, and the local preference attribute has a value of 100. The route is a valid route received from an internal BGP peer.

For troubleshooting purposes, the AS path, next hop, and best path indicator are the most important fields in the output of this command. For a full description of all possible fields, see the BGP command references on www.cisco.com.

Instead of viewing a specific entry in the BGP table, it can also be useful to select a set of routes from the BGP table based on certain criteria. The Cisco IOS BGP command toolkit includes the following options to select specific routes from the BGP table:

- **`show ip bgp`** *`network mask`* **`longer-prefixes`** – Lists more specific prefixes present in the BGP table (including the prefix itself) that are contained in the *`network`* and *`mask`* options.
- **`show ip bgp neighbor`** *`ip-address`* **`routes`** – Lists all routes in the BGP table that were received from the neighbor specified by the *`ip-address`* option.
- **`show ip bgp neighbor`** *`ip-address`* **`advertised-routes`** – Lists all routes in the BGP table that will be advertised to the neighbor specified by the *`ip-address`* option.
- **`show ip bgp regexp`** *`regular-expression`* – Selects all routes from the BGP table that have an AS path string that is matched by the specified regular expression.

For more information about how to match specific AS paths using regular expressions, see the "Understanding Regular Expressions" section in the *Cisco IOS Configuration Fundamentals Configuration Guide* at

http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics_ps6350_TSD_Products_Configuration_Guide_Chapter.html#wp1002051

Debug BGP Route Exchange

```
R1#debug ip bgp update
BGP updates debugging is on for address family: IPv4 Unicast

R1#clear ip bgp *
R1#
*Nov 16 18:14:11.508: %BGP-5-ADJCHANGE: neighbor 192.168.2.1 Down User reset
R1#
*Nov 16 18:14:13.844: %BGP-5-ADJCHANGE: neighbor 192.168.2.1 Up
R1#
*Nov 16 18:14:13.860: BGP(0): 192.168.2.1 rcvd UPDATE w/ attr: nexthop 192.168.2
.1, origin i, metric 0, merged path 65502, AS_PATH
*Nov 16 18:14:13.860: BGP(0): 192.168.2.1 rcvd 0.0.0.0/0
*Nov 16 18:14:14.832: BGP(0): Revise route installing 1 of 1 routes for 0.0.0.0/
0 -> 192.168.2.1(main) to main IP table
R1#
*Nov 16 18:14:47.264: BGP(0): nettable_walker 172.30.1.0/27 route sourced locall
y
*Nov 16 18:14:47.268: BGP(0): 192.168.2.1 send UPDATE (format) 172.30.1.0/27, ne
xt 192.168.1.1, metric 0
```

If you find expected route entries to be missing from the BGP table, or you doubt whether the router is sending specific routes to a neighbor, consider using the **`debug ip bgp updates`** command to display the processing of BGP updates by the router. However, this command can generate a large number of messages, especially if your BGP table carries many routes. Consequently, it has a high risk of disrupting the router's operation. In production networks, you should take extreme care when using this command, and you should use command options to limit the output to the prefixes and neighbor that you are troubleshooting.

Note: The following section uses sample output not produced from the equipment in this lab to demonstrate how to limit the output of the **`debug ip bgp updates`** command by specifying a neighbor and using an access list to select only certain prefixes.

The commands are interspersed with comments that explain the procedure and output.

```
IRO1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
IRO1(config)#access-list 37 permit 172.17.76.0 0.0.3.255
IRO1(config)#^Z
IRO1#
```

An access list with number 37 is created. When used to filter BGP routes, this access list matches any prefix in the 172.17.76.0–172.17.79.0 IP range.

```
IRO1#debug ip bgp 192.168.224.254 updates 37
BGP updates debugging is on for access list 37 for neighbor
192.168.224.254 for address family: IPv4 Unicast
```

The debug is enabled for neighbor 192.168.224.254 and access list 37. Only update messages transmitted to or received from neighbor 192.168.224.254 that are permitted by access list 37 will be displayed.

```
IRO1#clear ip bgp 192.168.224.254 soft
```

A “soft” clear of BGP neighbor 192.168.224.254 is issued. As opposed to a “hard” clear, a soft clear does not tear down and restart the session completely. It just forces the routes between this router and the neighbor to be retransmitted.

```
IRO1#
Apr 29 06:36:57.549 PDT: BGP(0): 192.168.224.254 send UPDATE (format)
172.17.76.0/22, next 192.168.224.241, metric 0, path Local
```

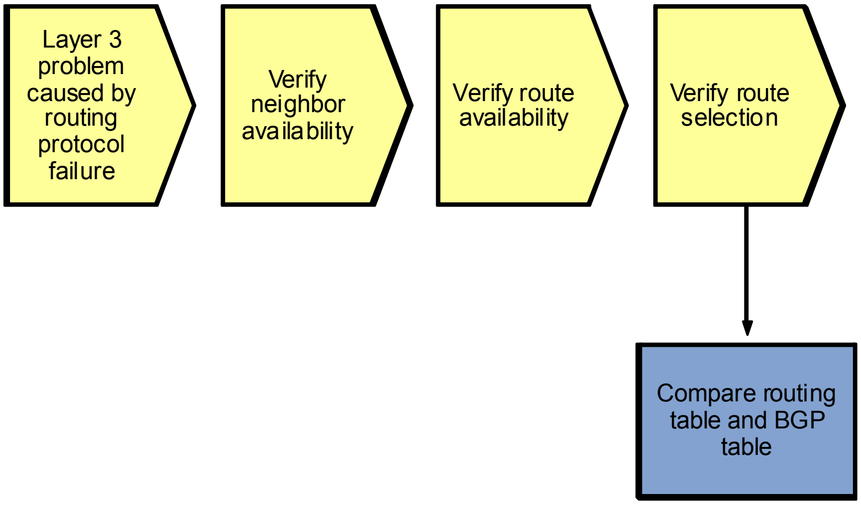
An update about prefix 172.17.76.0/22 is transmitted to neighbor 192.168.224.254. Note that both the neighbor and the prefix match the imposed restrictions.

```
Apr 29 06:36:57.553 PDT: BGP(0): 192.168.224.254 rcv UPDATE w/ attr:
nexthop 192.168.224.254, origin i, originator 0.0.0.0, path 65525 64568,
community , extended community
Apr 29 06:36:57.553 PDT: BGP(0): 192.168.224.254 rcv UPDATE about
172.17.76.0/22 -- DENIED due to: AS-PATH contains our own AS;
```

An update about prefix 172.17.76.0/22 is received but denied, because the AS path attribute contains this router's autonomous system (AS 64568).

Many more updates were sent between this router and its neighbor, but only updates that match the imposed restrictions were displayed, limiting the impact of the command.

Sample BGP Troubleshooting Flow


Layer 3 problem caused by routing protocol failure
Verify neighbor availability
Verify route availability
Verify route selection
Compare routing table and BGP table

If you find that a route is available in the BGP table but not in the routing table, there are two possible explanations. Either BGP has not been able to select any of the paths as the best path, or it has selected a best path, but a competing route from a different source with a better administrative distance is present and has been installed in the routing table.

If none of the paths has been selected as the best path, this will be clearly visible in the BGP table, and clues about the cause of the best path selection failure can be gathered from the BGP table. For example, if none of the paths has a next hop that can be resolved in the IP routing table, "Inaccessible" is displayed instead of the IGP metric to reach the next hop. If the BGP synchronization rule is causing a route not to be installed in the routing table, "not synchronized" is displayed behind the route.

If a best path has been selected for the prefix but not installed in the routing table due to the presence of a competing route with a better administrative presence, the route is marked as a "RIB-failure" in the BGP table. To list all BGP routes that have not been installed in the routing table due to a RIB failure, use the **`show ip bgp rib-failure`** command.