

TSHOOT

Troubleshooting and Maintaining Cisco IP Networks

Volume 2

Version 1.0

Student Guide

Text Part Number: 97-2819-01

<https://t.me/learningnets>



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco.Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLNNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED “AS IS.” CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

Table of Contents

Volume 2

<i>Maintaining and Troubleshooting Routing-Based Solutions</i>	5-1
Overview	5-1
Module Objectives	5-1
Troubleshooting Network Layer Connectivity	5-3
Overview	5-3
Objectives	5-3
Layer 3 Connectivity Overview	5-4
Layer 3 Data Structures	5-11
Layer 3 to Layer 2 Mapping	5-14
Summary	5-16
Troubleshooting EIGRP	5-17
Overview	5-17
Objectives	5-17
EIGRP Data Structures	5-18
EIGRP Information Flow	5-21
Cisco IOS EIGRP Commands	5-22
Summary	5-32
Lab 5-1 Debrief	5-33
Overview	5-33
Objectives	5-33
Review and Verification	5-34
Trouble Ticket I: Fire in the Server Room	5-37
Suggested Solution	5-45
Trouble Ticket H: Preparation for CCTV Pilot	5-48
Suggested Solution	5-53
Trouble Ticket J: User in Branch Cannot Access the Internet	5-54
Suggested Solution	5-59
Consolidation	5-60
Summary	5-61
Troubleshooting OSPF	5-63
Overview	5-63
Objectives	5-63
OSPF Data Structures	5-64
OSPF Information Flow Inside an Area	5-71
OSPF Information Flow from Area to Area	5-74
OSPF Cisco IOS Commands	5-76
Summary	5-86
Troubleshooting Route Redistribution	5-87
Overview	5-87
Objectives	5-87
The Route Redistribution Process	5-88
Verifying Redistribution	5-93
Summary	5-102

Lab 5-2 Debrief	5-103
Overview	5-103
Objectives	5-103
Review and Verification	5-104
Trouble Ticket K: No Connectivity from Client PC CLT2	5-109
Suggested Solution	5-116
Trouble Ticket L: No Connectivity from Client PC CLT3	5-117
Suggested Solution	5-123
Trouble Ticket M: Internet not Reachable from Client PC CLT1	5-124
Suggested Solution	5-129
Trouble Ticket N: OSPF Authentication not Working	5-130
Suggested Solution	5-136
Consolidation	5-137
Summary	5-138
Troubleshooting BGP	5-139
Overview	5-139
Objectives	5-139
BGP Data Structures	5-140
BGP Routing Information Flow	5-143
BGP Cisco IOS Commands	5-145
Summary	5-157
Lab 5-3 Debrief	5-159
Overview	5-159
Objectives	5-159
Review and Verification	5-160
Trouble Ticket O: BGP Peering to Router ISP1 Not Established	5-164
Suggested Solution	5-172
Trouble Ticket P: Client CLT1 Cannot Reach the Internet	5-173
Suggested Solution	5-179
Consolidation	5-180
Summary	5-181
Troubleshooting Performance Problems on Routers	5-183
Overview	5-183
Objectives	5-183
Troubleshooting High CPU on Routers	5-184
Understanding Cisco IOS Switching Paths	5-194
Process Switching	5-196
Fast Switching	5-197
Cisco Express Forwarding	5-198
Troubleshooting Process and Fast Switching	5-199
Troubleshooting Cisco Express Forwarding	5-202
Cisco IOS Tools to Analyze Packet Forwarding	5-206
Troubleshooting Router Memory Issues	5-209
Summary	5-218
Lab 5-4 Debrief	5-219
Overview	5-219
Objectives	5-219
Review and Verification	5-220
Trouble Ticket Q: Problems with Connectivity	5-221
Suggested Solutions	5-228
Consolidation	5-231
Summary	5-232

References to Additional Troubleshooting on NAT, DHCP, and Other Protocols in E-Learning	5-233
Overview	5-233
Objectives	5-233
Preview of E-Learning on Additional Routing Technologies	5-234
Summary	5-240
Module Summary	5-241
References	5-242
Module Self-Check	5-243
Module Self-Check Answer Key	5-254
<i>Maintaining and Troubleshooting Network Security Solutions</i>	6-1
Overview	6-1
Module Objectives	6-1
Troubleshooting Security Features	6-3
Overview	6-3
Objectives	6-3
Network and Device Security	6-4
Summary	6-16
Lab 6-1 Debrief	6-17
Overview	6-17
Objectives	6-17
Review and Verification	6-18
Trouble Ticket R: Internet not Reachable from Client PC CLT1	6-20
Suggested Solution	6-25
Trouble Ticket S: Internet Not Reachable from Client PC CLT3	6-26
Suggested Solution	6-33
Trouble Ticket T: Client PC CLT2 Has No Network Connectivity	6-34
Suggested Solution	6-39
Consolidation	6-40
Summary	6-41
Security Features Review	6-43
Overview	6-43
Objectives	6-43
Troubleshooting Transport Layer Problems	6-44
Cisco IOS Firewall	6-49
Authentication, Authorization, and Accounting	6-59
Summary	6-68
Lab 6-2 Debrief	6-69
Overview	6-69
Objectives	6-69
Review and Verification	6-70
Trouble Ticket W: No Connectivity to Server SRV1	6-73
Suggested Solution	6-77
Trouble Ticket U: No Connectivity from Client PCs CLT2 and CLT3	6-78
Suggested Solution	6-84
Trouble Ticket V: No Connectivity from Client PC CLT1	6-85
Suggested Solution	6-91
Trouble Ticket X: Lost Remote Connectivity to All Routers	6-92
Suggested Solution	6-96
Trouble Ticket Y: Port Security Problems on Switch BSW1	6-97
Suggested Solution	6-102
Consolidation	6-103
Summary	6-104

References to Additional Security Troubleshooting in E-Learning **6-105**

Overview	6-105
Objectives	6-105
Preview of E-Learning on Additional Security Troubleshooting	6-106
Summary	6-111
Module Summary	6-113
References	6-114
Module Self-Check	6-115
Module Self-Check Answer Key	6-118

Maintaining and Troubleshooting Integrated, Complex Enterprise Networks **7-1**

Overview	7-1
Module Objectives	7-1

Troubleshooting Complex Environments **7-3**

Overview	7-3
Objectives	7-3
Troubleshooting Complex Networks	7-4
Summary of Lab 2-1	7-6
Summary of Lab 3-1	7-8
Summary of Lab 4-1	7-10
Summary of Lab 4-2	7-12
Summary of Lab 5-1	7-14
Summary of Lab 5-2	7-16
Summary of Lab 5-3	7-17
Summary of Lab 5-4	7-19
Summary of Lab 6-1	7-20
Summary of Lab 6-2	7-21
Introduction to Lab 7-1	7-22
Summary	7-28

Lab 7-1 Debrief **7-29**

Overview	7-29
Objectives	7-29
Review and Verification	7-30
Trouble Ticket A: No Connectivity from CLT1 to SRV1	7-33
Suggested Solution	7-38
Trouble Ticket B: No Internet Access from CLT1	7-39
Suggested Solution	7-47
Trouble Ticket C: No Connectivity Between Headquarters and Branch Office	7-48
Suggested Solution	7-55
Trouble Ticket D: No Internet Access for Guest Users	7-56
Suggested Solution	7-61
Network Maintenance: Verify Network Operation	7-62
Suggested Solution	7-68
Consolidation	7-69
Summary	7-70
Module Summary	7-71
References	7-71

Maintaining and Troubleshooting Routing-Based Solutions

Overview

IP routing is the core technology deployed in all current enterprise networks. It is used in all areas of the network: the campus LAN, the data center, the WAN, and remote access networks.

A good understanding of routing protocols such as Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP), route redistribution mechanisms, network layer connectivity in general, and the ability to diagnose and resolve problems associated with these technologies is therefore essential to any network engineer.

This module reviews routing technologies and protocols deployed in enterprise IP networks and focuses on the resolution of problems related to these technologies and protocols.

Module Objectives

Upon completing this module, you will be able to diagnose and correct problems found in a network infrastructure consisting of routers. This ability includes being able to meet these objectives:

- Diagnose and resolve network layer connectivity problems using the Cisco IOS command line interface
- Diagnose and resolve problems related to EIGRP
- Diagnose and resolve problems related to the OSPF routing protocol
- Diagnose and resolve problems related to route redistribution
- Diagnose and resolve problems related to BGP
- Diagnose and resolve performance problems on routers

Troubleshooting Network Layer Connectivity

Overview

For most connectivity problems in IP networks, the network layer is the point where troubleshooting processes start. By first establishing whether there is network layer connectivity between two hosts, a quick separation can be made between problems on the higher layers of the Open Systems Interconnection (OSI) model and the lower three layers. If you can confirm network layer connectivity between two hosts, the problem is more likely to be caused by application issues or security related problems. On the other hand, if you cannot establish end-to-end network layer connectivity, the problem is clearly network related, and a network engineer should have the skills and knowledge to diagnose and resolve these problems in an efficient manner.

This lesson reviews the processes and data structures that are used by routers to forward IP packets and the Cisco IOS tools that can be used to diagnose problems related to IP packet forwarding, to provide you with the essential skills and knowledge that are necessary to resolve network layer problems successfully.

Objectives

Upon completing this lesson, you will be able to diagnose network layer connectivity problems using the Cisco IOS command-line interface. This ability includes being able to meet these objectives:

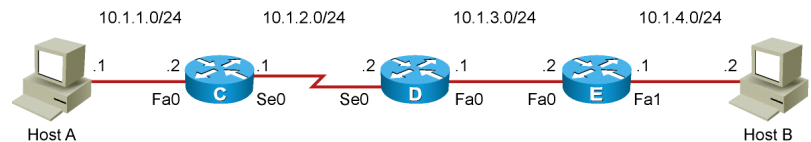
- Describe the processes involved in routing packets across multiple router hops from one host to another host in a different subnet
- Analyze information gathered from a router's routing table and FIB to verify the IP packet forwarding process
- Verify the mapping of Layer 3 information to Layer 2 information to ensure that routed packets are correctly encapsulated and transmitted using the data-link protocol of the egress interface

Layer 3 Connectivity Overview

This topic describes the processes involved in routing a packet from a host to another across multiple routed hops.

IP Routing Review

Troubleshooting Layer 3 connectivity requires detailed knowledge of routing processes.



Discuss

- Which processes are involved in sending packets from Host A to Host B and back?
- Which data structures are used to route the packets?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--6-2

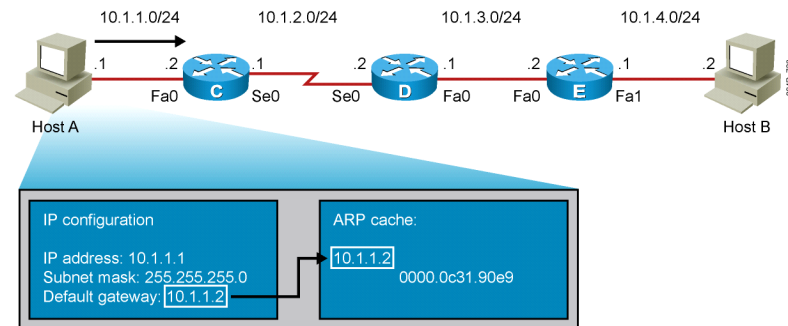
To troubleshoot Layer 3 connectivity, you need to have a good understanding of the processes that are involved in routing a packet from a host across multiple routers to the final destination.

Look at the network in the figure and ask yourself the following questions:

1. Which decisions will host A make, which information does it need, and which actions will it perform to successfully send a packet destined for host B to first hop router C?
2. Which decisions will router C make, which information does it need, and which actions will it perform to successfully send the packet from host A destined for B on to router D?
3. Which decisions will router D make, which information does it need, and which actions will it perform to successfully send the packet from host A destined for B on to router E? Is this answer the same as the answer to previous question or are there any differences?
4. Which decisions will router E make, which information does it need, and which actions will it perform to successfully send the packet from host A destined for B to its final destination, host B?
5. Are there any differences in the processes and information required in order to successfully transmit return packets from host B to host A?

Case Study: Routing a Packet

- Host A verifies that the destination is not on the local subnet and forwards the packet to the default gateway.
- The packet is encapsulated in an Ethernet frame, and the ARP cache is consulted to find the MAC address of the default gateway router C.



Understanding this process and knowing it from memory is fundamental to troubleshooting IP routing. If the source host or any of the routers in the chain are not capable of forwarding packets, because the host or routers are missing the required information, the packets will be dropped and Layer 3 connectivity is lost.

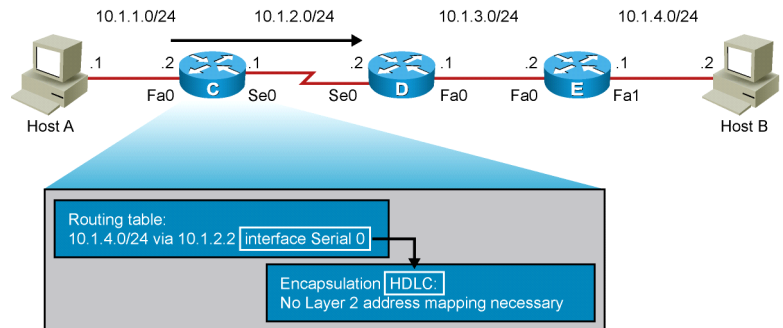
To verify your answers to the questions a sequence of the major processes, decisions, and actions is presented in this topic.

The answers to the previous questions are listed here:

1. When host A needs to send a packet to host B it will start by comparing the destination IP address (10.1.4.2) to its own IP address and subnet mask (10.1.1.1/24) to determine if the destination is on its local subnet or not. It concludes that the destination is not local and therefore it will attempt to forward the packet to its default gateway, which can be manually configured or learned via DHCP. In order to encapsulate the packet in an Ethernet frame, it will need the MAC address of the default gateway. This can be resolved via the Address Resolution Protocol (ARP). The host will either already have an entry in its ARP cache for the default gateway IP address, or alternatively, it will send out an ARP request to obtain the information and populate the cache.

Case Study: Routing a Packet (Cont.)

- Router C decapsulates the packet and performs a routing table lookup on the destination address to find the outbound interface and next-hop IP address.
- Router C encapsulates the packet in a HDLC frame. No Layer 3 to Layer 2 address mapping is required.



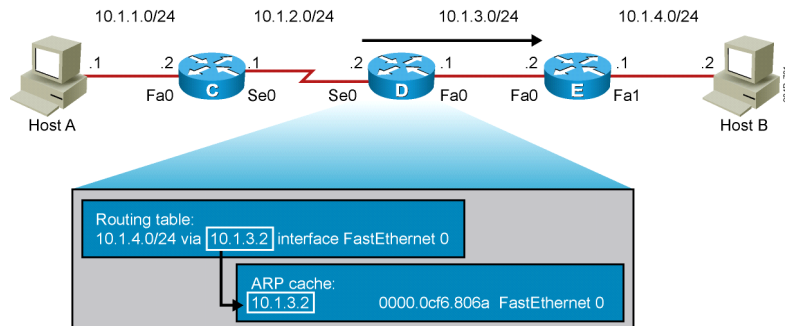
© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-4

- Router C decapsulates the received Ethernet frame and examines the IP header of the packet contained in the frame. It decrements the Time to Live (TTL) field in the IP header of the packet by one. If this causes the TTL field to be set to zero, it will discard the packet and send an Internet Control Message Protocol (ICMP) "time exceeded" message back to the source. If the TTL of the packet is not reduced to zero the router performs a routing table lookup to find the longest prefix that matches the destination IP address contained in the packet header. In this example, router C finds the entry 10.1.4.0/24 as the best match for the destination address of the packet (10.1.4.2). Two important parameters are associated with this entry: The next hop IP address 10.1.2.2 and the egress interface Serial 0. This serial interface uses the High-Level Data Link Control (HDLC) protocol on Layer 2. Because this protocol does not require a MAC address or other form of Layer 2 address for the next hop IP address, no further lookups are necessary. Router C encapsulates the frame in a HDLC frame and transmits it on interface Serial 0.

Case Study: Routing a Packet (Cont.)

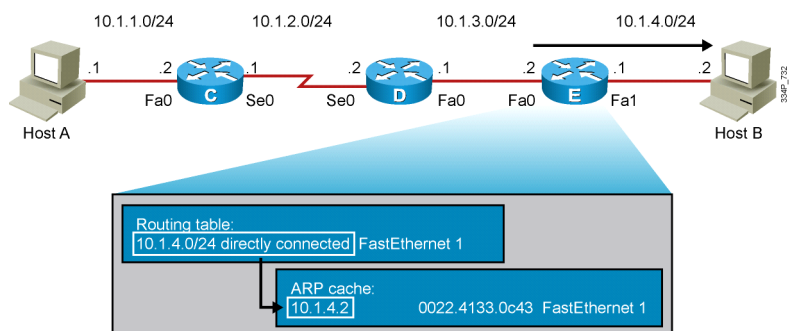
- Router D decapsulates the frame and performs a routing table lookup to find the outbound interface and next-hop IP address.
- The packet is encapsulated in an Ethernet Frame, and the ARP cache is consulted to find the MAC address of next-hop router E.



3. Router D will go through the same general process as router C. It also finds an entry for prefix 10.1.4.0/24 in its routing table. In this case, the next hop is 10.1.3.2 and the egress interface is FastEthernet 0. The biggest difference with the previous step is the Layer 2 protocol of the interface. Because this is a Fast Ethernet interface, the router performs an ARP cache lookup to find the MAC address of the next hop router 10.1.3.2. If it finds an entry in the cache it will encapsulate the packet in an Ethernet frame and forward it to next hop router E. Similar to the process on a host, it will send out an ARP request if no entry in the cache is found. However, the packet that triggers this ARP request will be dropped. The router will not keep the packet in a buffer until an ARP reply is received. For any subsequent packets that need to be forwarded to router E, router D will have an entry in the ARP cache after it processes the ARP reply and these packets will be forwarded correctly.

Case Study: Routing a Packet (Cont.)

- Router E decapsulates the frame and performs a routing table lookup to find the outbound interface and next-hop IP address.
- The packet is encapsulated in an Ethernet Frame, and the ARP cache is consulted to find the MAC address of Host B.



4. The process on router E is similar to the process on routers C and D. The most important difference is that the entry for prefix 10.1.4.0/24, which router D finds in the routing table, is listed as being directly connected to interface FastEthernet 1. This means that instead of forwarding the packets to a next-hop router, this router will forward them directly to the destination host on that interface. Because the Layer 2 protocol in this example is again Ethernet, router E will consult its ARP cache to find the MAC address for host B (10.1.4.2) and encapsulate the packet in an Ethernet frame destined for host B. When host B receives the packet, this concludes the transmission of a packet from host A to host B.
5. The process in sending return packets from host B to host A is similar. However, the information used in the lookups in the routing table and Layer 3 to Layer 2 mapping tables, such as the ARP cache, is different. For the return packets, the destination IP address is 10.1.1.1, so instead of entries for subnet 10.1.4.0/24, entries for subnet 10.1.1.0/24 will need to be present in all routers. These entries will have different associated egress interfaces and next-hop IP addresses. As a result, the corresponding ARP cache entries for those next hops will need to be present and these are different from the entries that were used on the path from host A to host B. Consequently, you cannot conclude that if packets are successfully forwarded from host A to host B, return packets from host B to host A will automatically be successful as well.

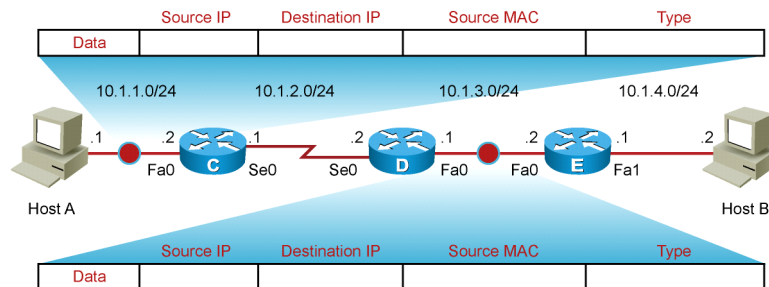
So what does this mean from a troubleshooting standpoint?

When you find that there is no network layer connectivity between two hosts, a good method to troubleshoot the problem is to track the path of the packet from router to router, similar to the method of tracking the path of a frame from switch to switch to diagnose Layer 2 problems. Along the way, you need to verify the availability of a matching route in the routing table for the destination of the packet and, subsequently, the availability of a Layer 3 to Layer 2 address mapping for the next hop for those technologies that require a Layer 2 address, such as Ethernet.

For any type of application that requires two-way communication, you need to track the packets in both directions. Availability of the correct routing information and Layer 3 to Layer 2 mappings for packets traveling in one direction does not imply that the correct information is available for packets traveling in the other direction as well.

Quiz: Packet and Frame Headers

What are the values in the frame and packet headers of the packets sent from Host A to Host B, while they are in transit at the highlighted points?



Based on your knowledge of the processes that take place when packets are forwarded across multiple router hops, fill in the correct values for the fields in the packet and frame headers of the packets that were traced in the example.

What are the source IP address, destination IP address, source MAC address, and destination MAC address contained in the frame as it is in transit between host A and router C?

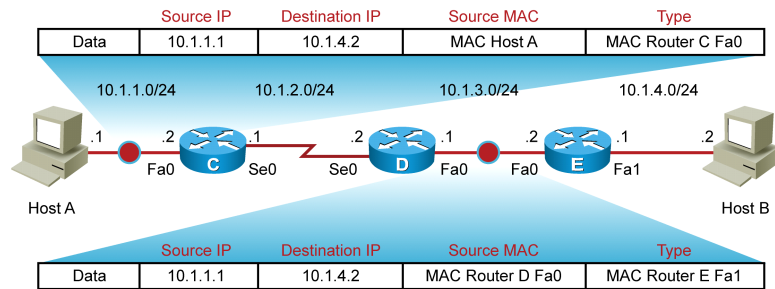
1. Source IP address: _____
2. Destination IP address: _____
3. Source MAC address: _____
4. Destination MAC address: _____

What are the source IP address, destination IP address, source MAC address, and destination MAC address contained in the frame as it is in transit between router D and router E?

1. Source IP address: _____
2. Destination IP address: _____
3. Source MAC address: _____
4. Destination MAC address: _____

Answers: Packet and Frame Headers

What are the values in the frame and packet headers of the packets sent from Host A to Host B, while they are in transit at the highlighted points?



The headers fields of the frame as it is in transit between host A and router C are as follows:

1. Source IP address: 10.1.1.1 (IP address of host A)
2. Destination IP address: 10.1.4.2 (IP address of host B)
3. Source MAC address: MAC address of host A
4. Destination MAC address: MAC address of interface FastEthernet 0 on router C (0000.0c31.90e9)

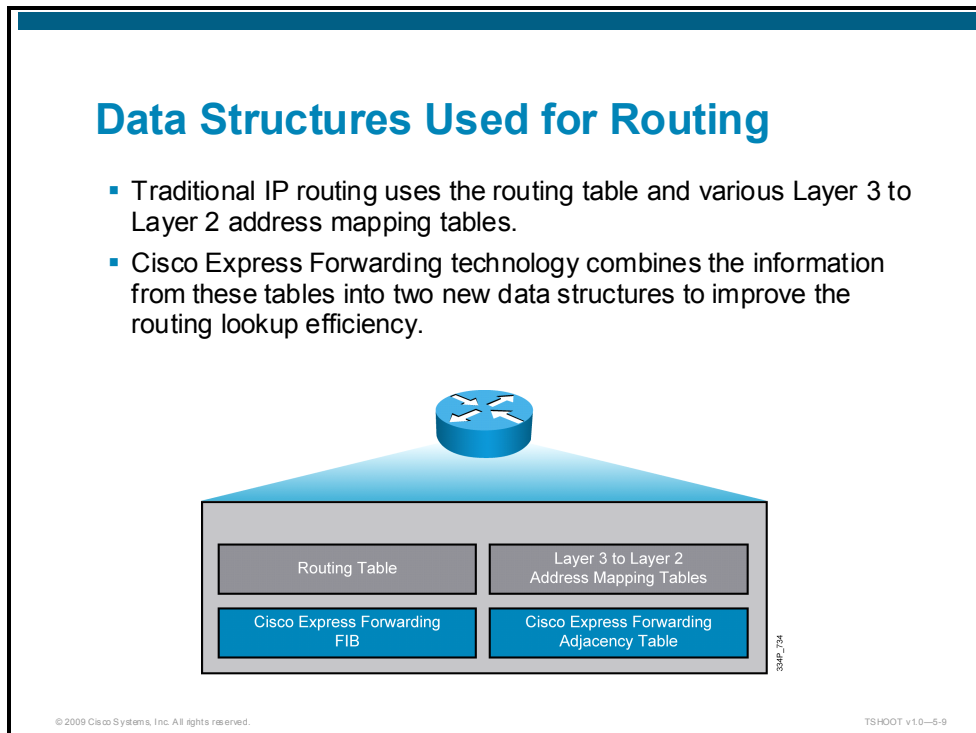
The headers fields of the frame as it is in transit between router D and router E are as follows:

1. Source IP address: 10.1.1.1 (IP address of host A)
2. Destination IP address: 10.1.4.2 (IP address of host B)
3. Source MAC address: MAC address of interface FastEthernet 0 on router D
4. Destination MAC address: MAC address of interface FastEthernet 1 on router E (0000.0cf6.806a)

Being able to quickly predict and interpret packet headers is an essential skill when you are troubleshooting. It will help you to switch quickly between tracing Layer 3 paths across routers and Layer 2 paths in the switched networks between routers or multilayer switches.

Layer 3 Data Structures

This topic describes the data structures that a router uses to forward Layer 3 packets.



To route packets, a router combines information from various control plane data structures. The most important of these data structures is the routing table. Unlike switches, which flood frames on all ports if they cannot find an entry in their MAC address table, routers will drop any packet for which they cannot find a matching route in the routing table.

When a packet needs to be routed, the routing table is searched for the longest possible prefix that matches the destination IP address of the packet. Associated with this entry is an egress interface and, in most cases, a next-hop IP address.

For point-to-point egress interfaces, such as a serial interface running PPP or HDLC, a point-to-point Frame Relay or point-to-point Asynchronous Transfer Mode (ATM) subinterface, a next-hop IP address is not mandatory, because all the information that is necessary to construct the frame and encapsulate the packet can be derived from the egress interface itself. For example, in the case of Frame Relay, a point-to-point subinterface has a single associated Data Link Connection Identifier (DLCI), so there is no need to map the next-hop IP address to a DLCI to be able to construct the Frame Relay frame header and encapsulate the packet.

For multipoint egress interfaces, such as Ethernet interfaces or multipoint Frame Relay or ATM subinterfaces, the next-hop IP address is a mandatory element, because this next hop is necessary to find the correct Layer 2 destination address or other Layer 2 identifier to construct the frame and encapsulate the packet. The mapping between the next hop-IP address and the Layer 2 address or identifier is stored in a data structure that is specific for that Layer 2 protocol. For example, in the case of Ethernet, this information is stored in the ARP cache and for Frame Relay multipoint interfaces, the information is stored in the Frame Relay map table.

Consequently, a routing table lookup might need to be followed up by a lookup in a Layer 3 to Layer 2 mapping table to gather all the necessary information that is required to construct a frame, encapsulate the packet, and transmit it.

Executing all these different table lookups and combining the information to construct a frame every time a packet needs to be routed is an inefficient approach to forwarding IP packets. To improve this process and increase the performance of IP packet switching operations on routers, Cisco has developed Cisco Express Forwarding. This advanced Layer 3 IP switching mechanism can be used on all routers and is at the core of the Layer 3 switching technology used in Cisco Catalyst multilayer switches. On most platforms, the Cisco Express Forwarding switching method is enabled by default.

In essence, Cisco Express Forwarding combines the information from the routing table and various Layer 3 to Layer 2 tables into two new data structures, the Forwarding Information Base (FIB) and the adjacency table. The FIB mostly reflects the routing table, supplemented with entries for directly connected hosts and multicast entries. A lookup in the FIB results in a pointer to an adjacency entry in the adjacency table. Similar to what we have seen in the routing table, an adjacency entry can consist of an egress interface only for point-to-point interfaces or an egress interface and next-hop IP address for a multipoint interface. The adjacency entry contains the exact frame header that is necessary to encapsulate packets destined for that adjacency.

Verifying Routing Information

How do you verify the information that is used to route packets?

- To display the content of the routing table for specific IP addresses or networks, use:
 - **show ip route** *ip-address*
 - **show ip route** *network mask*
 - **show ip route** *network mask longer-prefixes*
- To display the content of the Cisco Express Forwarding FIB for specific IP addresses or networks, use:
 - **show ip cef** *ip-address*
 - **show ip cef** *network mask*
 - **show ip cef exact-route** *source destination*

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0–5-10

To verify the information that is used to route packets you can verify the availability of specific routes in the routing table or the Cisco Express Forwarding FIB. The choice whether to check the routing table or FIB is dependent on what you are exactly trying to diagnose. To diagnose control plane problems, such as the exchange of routing information by routing protocols using the **show ip route** command is a clear choice, because it contains all the control plane details for a route, such as the advertising routing protocol, routing source, administrative distance, and routing protocol metrics. To diagnose problems that are more closely related to the data plane, for example by tracking the exact traffic flow between two hosts through the network, the FIB

is often the best choice, because it contains all the details that are necessary to make packet switching decisions.

To display the content of the routing table you can use the following commands:

- **show ip route *ip-address***: Supplying the destination IP address as an option to the **show ip route** command will cause the router to perform a routing table lookup for that IP address and display the best route that matches the address and all associated control plane details. (Note that the default route will never be displayed as a match for an IP address.)
- **show ip route *network mask***: By supplying the network and mask as an option to the **show ip route** command, the routing table will be searched for an exact match for that network and mask, and if it is found, this entry is displayed with all of its associated control plane details.
- **show ip route *network mask longer-prefixes***: Using the **longer-prefixes** option will cause the router to display all prefixes in the routing table that fall within the prefix specified by the *network* and *mask* parameters. This command can be very useful to diagnose problems related to route summarization.

To display the content of the Cisco Express Forwarding FIB you can use the following commands:

- **show ip cef *ip-address***: This command is very similar to the **show ip route *ip-address*** command, but it searches the FIB instead of the routing table. Therefore, the displayed results do not include any routing protocol-related information, but only the information that is necessary to forward packets. (Note that this command will display the default route if it is the best match for a particular IP address.)
- **show ip cef *network mask***: This is similar to the **show ip route *network mask*** command, but displays information from the FIB instead of the routing table.
- **show ip cef exact-route *source destination***: This command will display the exact adjacency that will be used to forward a packet with source and destination IP addresses, as specified by the *source* and *destination* parameters. The main reason to use this command is in a situation when you are tracking a packet flow across the routed network, but the routing table and FIB contain two or more equal routes for a particular prefix. In this case, the Cisco Express Forwarding mechanisms will balance the traffic load across the multiple adjacencies associated with that prefix. By use of this command, you can determine which of the possible adjacencies is used to forward packets for a specific source and destination IP address pair.

For sample output of these commands and guidelines regarding their use, see the “Sample Troubleshooting Flows” section in the course lab guide.

To review the complete syntax and a description of all command options, see the command reference sections of the Cisco Product Support pages on <http://www.cisco.com>.

Layer 3 to Layer 2 Mapping

This topic describes the relation between Layer 3 and Layer 2 protocol tables as they are used in the forwarding of IP packets.

Verifying Layer 2 Encapsulation

The commands to verify Layer 3 to Layer 2 address mapping are protocol dependent.

Some examples are:

- For Ethernet: **show ip arp**
- For Frame Relay: **show frame-relay map**

To display the content of the Cisco Express Forwarding adjacency table, use the command:

- **show adjacency detail**

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0-5-11

After a an egress interface and, in case of multipoint interfaces, a next-hop IP address for the destination of a packet has been determined by the routing table or FIB, the router needs to construct a frame for the data link layer protocol associated with the egress interface in order to be able to encapsulate and transmit the packet. Depending on the data link layer that is used on the interface, the header of this frame will require some connection specific parameters, such as source and destination MAC addresses for Ethernet, Data Link Connection Identifiers (DLCI) for Frame Relay, or virtual path identifier/virtual circuit identifier (VPI/VCI) pairs for ATM.

These data link layer parameters are stored in various different places. For point-to-point interfaces and subinterfaces, the relation between the interface and data link identifier or address is usually statically configured. For multipoint interfaces and subinterfaces, the relation between the next-hop IP address and the data link identifier and address can be manually configured or dynamically resolved through some form of an address resolution protocol. The commands to display the statically configured or dynamically obtained mappings are unique for each data link layer technology. Research the command references for the data link layer protocol that you are troubleshooting to find the appropriate commands for that protocol.

Some examples of commands that can be used to verify the Layer 3 to Layer 2 mappings are the following:

- **show ip arp:** This command can be used to verify the dynamic IP address to Ethernet MAC address mappings that were resolved by the Address Resolution Protocol. Routers cache this information for four hours by default, so if a change is made to a host or other router that would require this information to be refreshed, you may need to issue the **clear ip arp** command to clear a particular entry from the cache in order to allow it to be refreshed.
- **show frame relay map:** This command lists all the mappings of next-hop IP addresses on multipoint interfaces (subinterfaces) to the DLCI of the corresponding permanent virtual circuit (PVC). These mappings might have been manually configured or dynamically resolved via the Frame Relay inverse ARP protocol. In addition, the command also lists any DLCIs that were manually associated to specific point-to-point subinterfaces.

When Cisco Express Forwarding is used as the switching method, the information from the various Layer 2 data structures is used to construct a frame header for each adjacency that is listed in the adjacency table. The full frame header that will be used to encapsulate the packet can be displayed by use of the **show adjacency detail** command. In addition, this command displays packet and byte counters for all traffic that was forwarded via this adjacency.

When do you typically resort to verifying the Layer 3 to Layer 2 mappings during a troubleshooting process? When you have verified that the routing table, or even better the FIB, lists the correct next hop-IP address and egress interface for a particular destination, but packets do not arrive at that next hop, you should verify the Layer 3 to Layer 2 mappings for the data link protocol that is used on the egress interface. Specifically, you should verify that a correct frame header is constructed to encapsulate the packets and forward them to the next hop.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- You have reviewed and analyzed the process involved in forwarding packets between hosts across multiple router hops.
- You have learned how to gather information from the key data structures that are used in the IP packet forwarding process using Cisco IOS commands.
- You have learned how to confirm the correct operation of the process of encapsulation of Layer 3 packets in Layer 2 frames using Cisco IOS commands.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-12

Troubleshooting EIGRP

Overview

Enhanced Interior Gateway Routing Protocol (EIGRP) is one of the routing protocols that are commonly used in large enterprise networks. Troubleshooting problems related to the exchange of routing information is one of the most essential skills for a network engineer that is involved in the implementation and maintenance of large routed enterprise networks that use EIGRP as the interior gateway protocol (IGP).

This lesson reviews the data structures used by EIGRP and the flow of routing information between routers running EIGRP, as well as the processing of routing information inside the router. In addition, the Cisco IOS commands that you can use to gather information from the EIGRP data structures and routing processes are reviewed and a case study is presented to illustrate the use of the commands as part of a structured troubleshooting process.

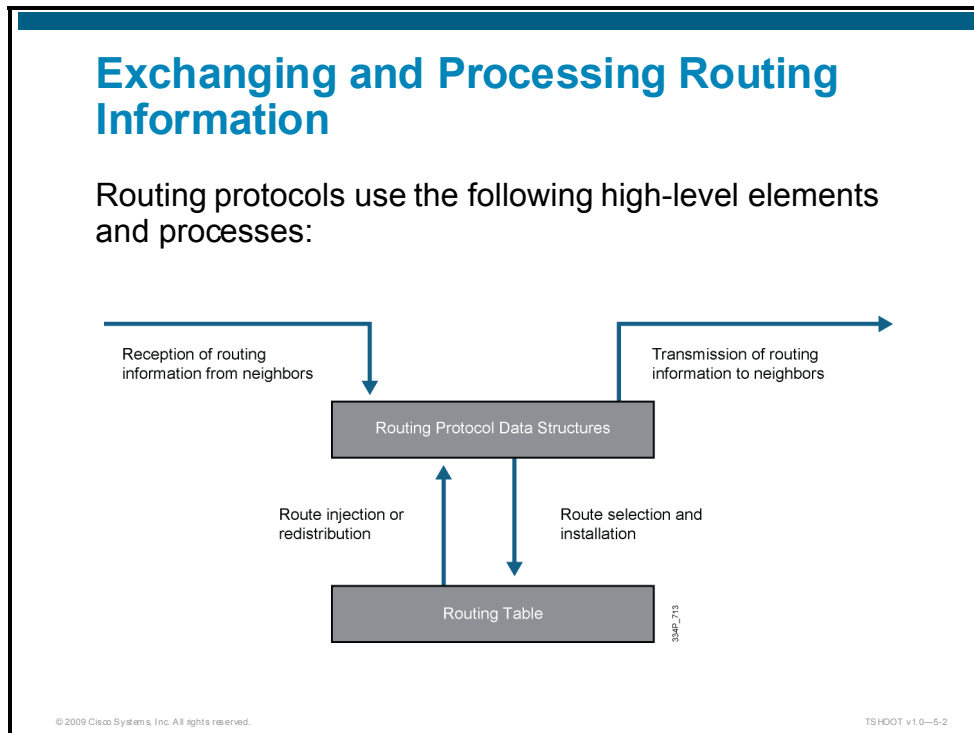
Objectives

Upon completing this lesson, you will be able to diagnose and resolve problems related to the exchange of routing information by use of EIGRP. This ability includes being able to meet these objectives:

- Apply your knowledge of EIGRP data structures to plan the gathering of necessary information as part of a structured approach to troubleshooting EIGRP routing problems
- Apply your knowledge of the processes that EIGRP uses to exchange routing information to interpret and analyze the information that is gathered during an EIGRP troubleshooting process
- Use Cisco IOS commands to gather information from the EIGRP data structures and track the flow of EIGRP routing information to troubleshoot EIGRP operation

EIGRP Data Structures

This topic describes the data structures that EIGRP uses to store information.



Network layer connectivity is dependent on having correct, consistent, and up-to-date routing information available in all routers.

To forward packets correctly between hosts across a routed network, all routing tables in the path between the source and the destination need to have an entry for the destination network in their routing tables. The information used to select the best path needs to be consistent, to ensure that no routing loops occur. The information also needs to be up-to-date, to ensure that traffic will not be forwarded toward a broken link or failed neighbor.

Static routing can be efficiently deployed in relatively small environments or in networks that do not incorporate a lot of redundant elements at the network layer. However, many large routed enterprise networks deploy a routing protocol to exchange routing information in a highly scalable manner and to ensure that routing information accurately reflects changes in the state of the network.

At a high level, each routing protocol consists of the following elements and processes:

- **Reception of routing information from neighbors:** Through routing protocol updates, each router learns about the availability of paths to other prefixes in the routed network. All interior gateway protocols (IGPs) receive their updates from routers that are Layer 2 adjacent, commonly called neighbors. Some protocols, such as EIGRP, the Open Shortest Path First (OSPF) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol, have a process to establish a neighbor relationship before exchanging routing information. Other protocols, such as the Routing Information Protocol (RIP) simply accept routes that they receive.

- **Routing protocol data structures:** Most modern routing protocols have their own data structures that they use to store the routing update information that they receive from their neighbors, or that is locally injected or redistributed into the routing protocol. Some older routing protocols, such as RIP, do not have data structures of their own, but install and store their routing information directly in the routing table.
- **Route injection or redistribution:** All routing information needs to originate at a certain point in the network. All interior gateway protocols inject directly connected routes, which are associated with interfaces that the protocol is activated for, into their data structures and advertise them out to their neighbors. Routes from other sources can also be specifically redistributed into the protocol's data structures and advertised out to the protocol's neighbors.
- **Route selection and installation:** For each prefix stored in its data structures, a routing protocol selects one or more routes as the best route for that prefix from all the available routes. Different routing protocols use different algorithms to calculate the best route. Route selection is based on the routing protocol's metric, and multiple routes will only be selected as best routes for the same prefix if their metrics are identical. (This is the case unless the protocol supports unequal cost load balancing, in which case multiple routes can be selected for installation in the routing table, even if their metrics are not identical.) The routing protocol will attempt to install the routes it selected as best for each prefix in the routing table. If multiple routing protocols attempt to install a route for the same prefix in the routing table, the administrative distance of the routing protocols involved will determine which routing protocol succeeds in installing its route.
- **Transmission of routing information to neighbors:** Routing information that was learned from other routers or that was injected or redistributed into the routing protocol data structures will be forwarded to neighboring routers that run the same protocol. Similar to the mechanisms used in the reception of routing information, some routing protocols, such as EIGRP, OSPF, or IS-IS require a neighbor relationship to be established before they forward routing information to another router, while other protocols, such as RIP, will simply broadcast or multicast their information to any adjacent router that is listening.

How can knowledge of these generic processes and elements be applied to the troubleshooting of routing protocols, such as EIGRP?

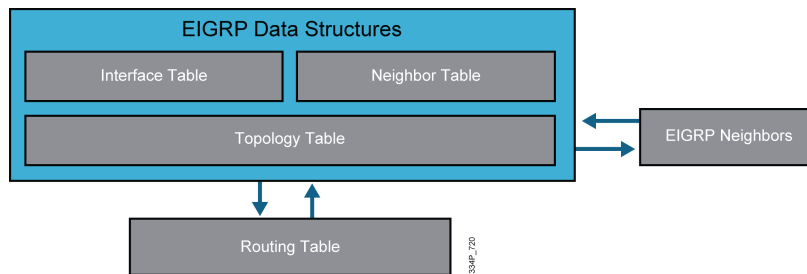
These generic elements and processes help you understand the flow of information between neighboring routers and, inside the router, between the routing protocol data structures and the routing table. The trigger to start troubleshooting routing protocol operation is usually when you find a router that is missing routing information or that has incorrect information in the routing table, causing it to drop packets or send traffic out to the wrong egress interface or next hop. Understanding these generic processes will help you to establish a troubleshooting plan and help you track the flow of routing information as it is propagated by the routing protocol.

In addition, when you recognize these principles in routing protocols that you are familiar with, it will become easier to apply the knowledge and experience that you have gained while troubleshooting a particular protocol to new and unfamiliar protocols.

EIGRP Data Structures

EIGRP tracks information using these data structures:

- Interface table: Active interfaces.
- Neighbor table: Discovered neighbors.
- Topology table: All routes received from neighbors or injected locally.



© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-3

EIGRP stores its operational data, configured parameters, and statistics in three main data structures:

- **Interface table:** This table lists all interfaces that have been enabled for the processing of EIGRP packets, such as hellos, updates, queries, replies, and acknowledgments. Passive interfaces are not listed in this table.
- **Neighbor table:** This table is used to keep track of all active EIGRP neighbors. Neighbors are added to this table based on the reception of hello packets, and they are removed when a neighbors hold-time expires or when the associated interface goes down or is removed from the interface table. This table is also used to keep track of the status of any routing information exchanges between the router and its neighbors.
- **Topology table:** This table holds all the routes that were received from neighboring routers, locally injected, or redistributed into EIGRP. For each prefix, EIGRP selects the best route from the available possible routes stored in this table to be installed in the routing table. If multiple routes have the exact same metric, all entries that share that same metric are selected for installation in the routing table. Routes with a higher metric are not selected for installation in the routing table, unless unequal cost load balancing has been enabled.

EIGRP Information Flow

This topic describes the flow of routing information as it is passed from neighbor to neighbor and installed in the EIGRP topology tables.

EIGRP Routing Update Process

- EIGRP neighbors discover and maintain adjacencies through use of hello packets.
- On the initial discovery of a neighbor, full routing updates are exchanged.
- After the initial exchange, only triggered incremental updates are exchanged as long as the adjacency is not lost or reset.
- All received routes are stored in the topology table.
- Only successors are advertised to neighbors.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-5-4

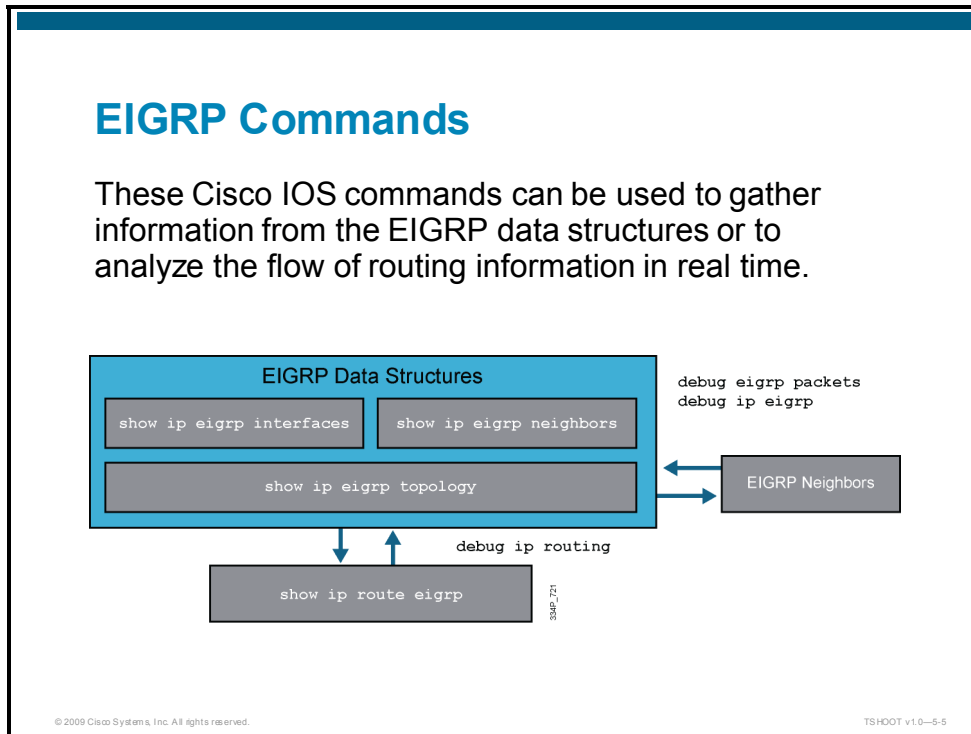
EIGRP uses an incremental update process. When the adjacency is first established, each router sends a full update to the other router, sending all prefixes that it has a successor for in the topology table. (Note that only the successor route entries will be sent, not feasible successors or possible successors.)

After the initial updates have been exchanged, routing updates will only be exchanged as a result of changes on the networks. Changes can be caused by changes in connectivity, such as loss of a link or neighbor, or they can be caused by configuration events, such as the addition of new interfaces to EIGRP, implementation of route summarization, or implementation of route filtering.

All routes received from neighbors are stored in the topology table. From the routes in the topology table, the router will select the best route or routes for each prefix and attempt to install these entries in the routing table. If it succeeds in installing a route in the routing table, it is marked as a successor in the topology table, and this route is advertised to neighbors.

Cisco IOS EIGRP Commands

This topic describes the Cisco IOS commands that you can use to gather information from the EIGRP data structures and track the flow of routing information.



You can use the following commands to gather information from the EIGRP data structures:

- **show ip eigrp interface:** This command is used to display the interfaces that have been activated for EIGRP processing. This list contains all the interfaces that have an IP address that is covered by one of the network statements under the EIGRP configuration and have not been marked as a passive interface.
- **show ip eigrp neighbors:** This command lists all neighbors that have been discovered by this router on its active EIGRP interfaces.
- **show ip eigrp topology:** This command displays the content of the EIGRP topology table. To select a specific entry from the table, the network and mask of the selected prefix can be provided as an option to the command.

The following debugs can be used to observe the transmission and reception of packets and the exchange of routing information:

- **debug ip routing:** This command is not specific to the EIGRP protocol, but displays any changes that are made to the routing table, such as installation or removal of routes. This can be useful to diagnose routing protocol instabilities.
- **debug eigrp packets:** This command displays the transmission and reception of EIGRP packets. Either all packets can be displayed, or packets of a particular type, such as hellos, updates, queries, and replies can be selected.

- **debug ip eigrp:** This command displays EIGRP routing events, such as updates, queries, and replies sent to or received from neighbors. While the **debug eigrp packets** command shows the transmission and reception of the packets themselves, this command focuses on the routing information contained in the packets and the actions that EIGRP takes as a result of the information received.

These **debug** commands can generate a large amount of output, and proper care needs to be taken to prevent this from affecting the router's performance. Logging debug output to buffers on the router instead of to the console can limit the impact of these commands.

The output of the **debug eigrp packets** and **debug ip eigrp** commands can be further limited by use of two additional debug commands:

- **debug ip eigrp neighbor *as-number ip-address*:** By imposing this extra condition, you limit the output of the **debug eigrp packets** and **debug ip eigrp** commands to information that is associated with the specified neighbor.
- **debug ip eigrp *as-number network mask*:** By imposing this extra condition, you limit the output of the **debug eigrp packets** and **debug ip eigrp** commands to information that is associated with the network specified by the *network* and *mask* options.

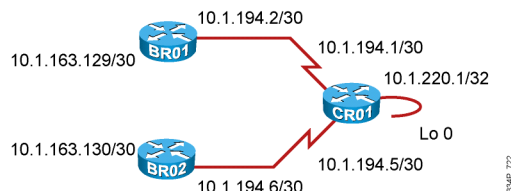
For sample output of these commands and guidelines regarding their use, see the “Sample Troubleshooting Flows” section in the course lab guide.

To review the complete syntax and a description of all command options, see the command reference sections of the Cisco Product Support pages on <http://www.cisco.com>.

Case Study: Troubleshooting EIGRP

Consider the following situation:

- A **traceroute** command from router BRO1 to the loopback IP address of router CRO1 reveals that packets to that loopback are routed via router BRO2 instead of being routed directly to CRO1 via the WAN connection.
- A **ping** command from router BRO1 to the 10.1.194.1 address is successful, proving that there is IP connectivity across the WAN.



© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-5-6

This small case study illustrates how knowledge of EIGRP data structures, update processes, and Cisco IOS commands can be leveraged to troubleshoot a routing problem.

The network depicted in the figure is using EIGRP as its routing protocol. When a **traceroute** command is executed to determine the path that is used to reach the loopback of router CRO1, it turns out that the traffic path goes through BRO2:

```
BRO1#traceroute 10.1.220.1
```

Type escape sequence to abort.

```
Tracing the route to crol.mgmt.tshoot.local (10.1.220.1)
```

```
 1 10.1.163.130 0 msec 0 msec 0 msec
 2 10.1.194.5 12 msec 12 msec *
```

This is not the expected behavior because the path across the WAN link is the better path (both, WAN links have the same bandwidth). To verify whether this problem is caused by an underlying Layer 1, Layer 2, or Layer 3 problem, a **ping** command is used to test the Layer 3 connectivity to the other side of the WAN link:

```
BRO1#ping 10.1.194.1
```

Type escape sequence to abort.

```
Sending 5, 100-byte ICMP Echos to 10.1.194.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
```


From the fact that this ping succeeds, you can conclude that the WAN link is operational at Layers 3 and below. Given that the link is functional, but is not used to route the packets across, this is by its nature a routing problem and calls for investigation of the operation of EIGRP.

There are various different methods to troubleshoot this problem. The method presented is just one possible approach and was selected to show the role of the EIGRP data structures in the troubleshooting process. Other methods to approach this problem might be valid as well.

Case Study: Troubleshooting EIGRP (Cont.)

Displaying the topology table on router BRO1 for network 10.1.220.1/32 yields the following result:

- The topology table contains only a single entry for the prefix.
- The route across the WAN is not listed.
- **Conclusion:** Routing information is not exchanged correctly between routers BRO1 and CRO1.

```
BRO1#show ip eigrp topology 10.1.220.1 255.255.255.255
IP-EIGRP (AS 1): Topology entry for 10.1.220.1/32
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 40642560
  Routing Descriptor Blocks:
    10.1.163.130 (FastEthernet0/1.30), from 10.1.163.130, Send flag is 0x0
      Composite metric is (40642560/40640000), Route is Internal
      Vector metric:
        Minimum bandwidth is 64 Kbit
        Total delay is 25100 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 2
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-5-7

The objective is to find out why the direct route across the WAN is not used to route packets to the loopback interface of router CRO1, but the packets are routed via router BRO2 instead.

There are two likely reasons why the traffic is routed via router BRO2 instead of directly across the WAN to router CRO1. The first reason could be that router BRO1 has not learned about the direct route to router CRO1. The second reason could be that the router has learned about the route, but incorrectly selects the route via router BRO2 as the best route.

To help you find out which of these two possible scenarios fits the situation, the EIGRP topology table can yield some clues. The topology table lists all routes that were received, so if the direct route to CRO1 is missing you should be able to see that in the topology table. On the other hand, if both routes were learned, but the wrong route was selected, you will see both routes listed in the topology table together with their metrics, and this might yield a clue as to why the wrong route was selected.

From the output in the figure, you can see that only one entry is listed in the topology table, and therefore you can conclude that the direct route via router CRO1 was not learned by router BRO1.

Case Study: Troubleshooting EIGRP (Cont.)

Displaying the neighbor table on router BRO1 yields the following result:

- There is only one entry in the neighbor table: Router BRO2.
- CRO1 is not listed as a neighbor.
- **Conclusion:** A neighbor relationship between routers BRO1 and CRO1 has not been established.

```
BRO1#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address                Interface    Hold Uptime   SRTT   RTO   Q   Seq
                               (sec)         (ms)          Cnt  Num
0   10.1.163.130            Fa0/1.30    12 00:09:56   4     200   0   585
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-8

Because EIGRP learns all its routes from neighbors that were first discovered via hello packets, you now need to determine whether the route was not learned because a neighbor relationship with CRO1 was never established or if the relationship was established but the specific route was not exchanged.

Therefore, a good next step is to display the neighbor table to find out if a neighbor relationship was established between router BRO1 and router CRO1, and if so, to determine what the status is.

As you can see from the output in the figure, router CRO1 is not listed as a neighbor on router BRO1.

Case Study: Troubleshooting EIGRP (Cont.)

Displaying the interface table on router BRO1 yields the following result:

- There is only one entry in the neighbor table: The Fast Ethernet interface that leads to router BRO2.
- The serial interface that leads to router CRO1 is not listed
- **Conclusion:** Either there is no network statement that matches the IP address of the serial interface, or the serial interface has been configured as a passive interface.

```
BRO1#show ip eigrp interfaces
IP-EIGRP interfaces for process 1
```

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Fa0/1.30	1	0/0	4	0/1	50	0

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-5-9

There can be two different reasons why router BRO1 does not list router CRO1 in its neighbor table. The trigger to add a neighbor to the neighbor list is the reception of hello packets from that neighbor. So one reason why router CRO1 is not listed could be that router BRO1 has not received any hello packets from router CRO1. Another explanation could be that the packets were received but ignored, because router BRO1 is not processing EIGRP packets on that interface.

The interface table allows you to see which interfaces are enabled for EIGRP processing. As you can see from the output in the figure, the serial interface is not listed. Consequently, even if hello packets are received on the serial interface, router BRO1 will not process them.

Case Study: Troubleshooting EIGRP (Cont.)

Displaying the EIGRP configuration on router BRO1 yields the following result:

```
BRO1#show running-config | section router eigrp
router eigrp 1
 network 10.1.163.129 0.0.0.0
 network 10.1.194.1 0.0.0.0
 no auto-summary
```

The network statements do not match the IP address of BRO1 (10.1.194.2).

The network statement is changed to match the correct IP address:

```
BRO1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BRO1(config)#router eigrp 1
BRO1(config-router)#no network 10.1.194.1 0.0.0.0
BRO1(config-router)#network 10.1.194.2 0.0.0.0
```

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0-6-10

Two conditions need to be met for an interface to be added to the EIGRP interface table. The IP address of the interface needs to be matched by one of the configured network statements, and the interface should not be configured as a passive interface.

These two conditions are both controlled by configuration commands, so at this point the configuration needs to be checked to see if one of these two conditions is not met.

As can be seen in the figure, there is a problem with one of the network statements. The network statement **network 10.1.194.1 0.0.0.0** matches IP address 10.1.194.1, which is not one of router BRO1's IP addresses, but an IP address of router CRO1. This is clearly a configuration mistake, and the network statement needs to be replaced with the statement **network 10.1.194.2 0.0.0.0** or some other network statement that matches IP address 10.1.194.2, which is the IP address of router BRO1 for the WAN link.

The network statement is replaced to test the hypothesis that the misconfigured network statement was the cause of the problem. Now the results of the change need to be verified, to confirm that the problem was solved. Strictly speaking, the only test that needs to be performed to confirm that the problem was solved is to execute the **tracert** command again to confirm that packets traveling to the loopback IP address of router CRO1 are now sent directly across the WAN instead of making a detour via router BRO2.

However, to show the effect of the change on all the EIGRP data structures, the changes in the output of the **show** commands that were used to diagnose the problem are shown in the following figures.

Case Study: Troubleshooting EIGRP (Cont.)

The interface table and neighbor tables now show the WAN connection as expected.

```
BR01#show ip eigrp interfaces
IP-EIGRP interfaces for process 1
```

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Fa0/1.30	1	0/0	1	0/1	50	0
Se0/0/0.111	1	0/0	707	10/380	4592	0

```
BR01#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
```

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
1	10.1.194.1	Se0/0/0.111	14	00:10:10	707	4242	0	783
0	10.1.163.130	Fa0/1.30	12	01:34:49	1	200	0	587

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--5-11

After making the change to the network statements, the interface table now lists subinterface Serial 0/0/0.111 in addition to subinterface FastEthernet 0/1.30. This means that EIGRP packets are now processed on interface Serial 0/0/0.111.

The IP address of router CRO1 (10.1.194.2) is now listed in the neighbor table on the WAN interface.

Case Study: Troubleshooting EIGRP (Cont.)

The topology table now shows both routes and has selected the route via the serial as the best route.

```
BRO1#show ip eigrp topology 10.1.220.1 255.255.255.255
IP-EIGRP (AS 1): Topology entry for 10.1.220.1/32
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 40640000
Routing Descriptor Blocks:
 10.1.194.1 (Serial0/0/0.111), from 10.1.194.1, Send flag is 0x0
   Composite metric is (40640000/128256), Route is Internal
   Vector metric:
     Minimum bandwidth is 64 Kbit
     Total delay is 25000 microseconds
     Reliability is 255/255
     Load is 1/255
     Minimum MTU is 1500
     Hop count is 1
 10.1.163.130 (FastEthernet0/1.30), from 10.1.163.130, Send flag is 0x0
   Composite metric is (40642560/40640000), Route is Internal
   Vector metric:
     Minimum bandwidth is 64 Kbit
     Total delay is 25100 microseconds
     Reliability is 255/255
     Load is 1/255
     Minimum MTU is 1500
     Hop count is 2
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-12

The EIGRP topology table now lists two entries for network 10.1.220.1/32: It lists the entry via router BRO2 (10.1.163.130), which was present before the change was made, but it also lists an entry via router CRO1 (10.1.194.2). The entry via router CRO1 was selected as the best route, because its metric of 40640000 is better than the metric via router BRO1, which equals 40642560.

The second conclusion that we can draw from the output in the figure is that the route via router CRO1 must have been successfully installed in the routing table, because it is listed as a successor for the prefix 10.1.220.1/32.

Case Study: Troubleshooting EIGRP (Cont.)

The route via the serial interface has been successfully installed in the routing table, and the **traceroute** shows that packets are not routed via BRO2 any longer.

```
BR01#show ip route 10.1.220.1 255.255.255.255
Routing entry for 10.1.220.1/32
  Known via "eigrp 1", distance 90, metric 40640000, type internal
  Redistributing via eigrp 1
  Last update from 10.1.194.1 on Serial0/0/0.111, 00:20:55 ago
  Routing Descriptor Blocks:
    * 10.1.194.1, from 10.1.194.1, 00:20:55 ago, via Serial0/0/0.111
      Route metric is 40640000, traffic share count is 1
      Total delay is 25000 microseconds, minimum bandwidth is 64 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1

BR01#traceroute 10.1.220.1

Type escape sequence to abort.
Tracing the route to crol.mgmt.tshoot.local (10.1.220.1)

 1 10.1.194.1 16 msec 12 msec *
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--5-13

The output in the figure confirms that the route via router CRO1 has been installed in the routing table, and the result of the **traceroute** command confirms that this route is now used to route packets to the loopback of router CRO1.

This short case study illustrates the use of the Cisco IOS **show** commands to display the content of the EIGRP data structures. It also illustrates how knowledge of these data structures and the flow of EIGRP routing information can be leveraged to diagnose and resolve EIGRP routing problems.

For more examples of EIGRP troubleshooting methods and the output of key EIGRP troubleshooting commands, see the “Sample Troubleshooting Flows” section in the course lab guide.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- You have reviewed the main data structures used by the EIGRP routing protocol.
- You have reviewed the processes that EIGRP uses to exchange and process routing information.
- You have learned how to use the EIGRP Cisco IOS commands to gather information about EIGRP operation as part of a troubleshooting process.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-14

Lab 5-1 Debrief

Overview

In this lab, you have practiced troubleshooting generic Layer 3 connectivity problems and specific problems related to Enhanced Interior Gateway Routing Protocol (EIGRP). You have created a troubleshooting plan to coordinate the work between the team members. You have methodically researched the problems, kept a log of your actions and findings, and resolved the problems and documented your solutions.

During the lab debrief, the instructor will lead a group discussion during which you can present your solutions. You will get an opportunity to verify your solution against a number of checkpoints provided by the instructor and compare your solution to other students' solutions. The instructor will discuss alternate solutions and their advantages and disadvantages.

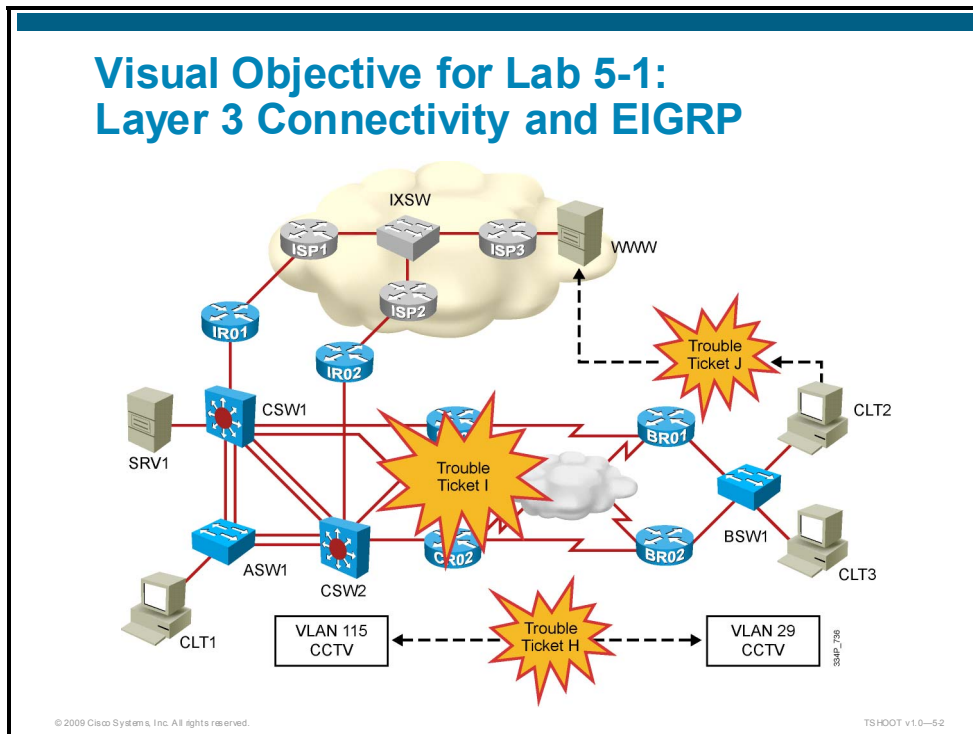
Objectives

Upon completing this lesson, you will be able to diagnose and resolve IP routing and EIGRP-related problems using a structured, methodical approach. This ability includes being able to meet these objectives:

- Compare your solution, findings, and action log against a set of checkpoints provided by the instructor and identify common and alternate solutions
- Consolidate the lessons learned during the review discussions into a set of best-practice methods and commands to aid you in future troubleshooting procedures

Review and Verification

This topic describes the problems that were introduced in Lab 5-1, asks how you can verify that you have solved the problems, and gives an example of a troubleshooting process that will allow you to find and resolve the issues.



This lab consists of three trouble tickets: Trouble Ticket H, which concerns verification of connectivity between two newly implemented VLANs, Trouble Ticket I, which revolves around a major WAN outage, and Trouble Ticket J, which deals with an internet connectivity problem via Internet service provider ISP2.

The problem introduced in Trouble Ticket I disrupts all communications between the branch and the headquarters networks. Therefore, Trouble Tickets H and J cannot be resolved until the WAN connectivity between the headquarters and branch has been restored.

Planning Troubleshooting

How did your team approach the three trouble tickets?

- Did you troubleshoot all tickets in parallel, in sequence, or did you use a combination of methods?
- How did you decide on the order that you chose to address the tickets in?
- How long did you take to restore the connectivity between the headquarters and branch?
- Did you use available resources in an efficient manner?
- How did you coordinate device access between your team members?
- How did you communicate with your team members?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—53

Note This lesson provides sample answers and solutions to the questions posed during the debrief discussions. Keep in mind that alternate solutions and methods might be just as valid and that the solutions provided here only highlight a sample approach and solution.

After assessing the criticality and urgency of the trouble tickets in this lab it is clear that ticket I has the highest priority. The problem described in ticket I causes the entire WAN connectivity to be lost and, given the fact that tickets H and J also deal with connectivity problems between the headquarters and branch, it is not possible to resolve tickets H and J without resolving ticket I first.

However, no more than one team member can work on each of the routers CRO1 and CRO2 at the same time. If your team consists of more members, you will need to decide how to use these resources most efficiently. They can watch over the shoulder of the team members that are at the console and offer advice when needed. They can take actions or gather information in support of the troubleshooting process. Alternatively, they can start doing some preliminary verification and information gathering for tickets H and J, while they wait for ticket I to be resolved.

When Trouble Ticket I has been resolved, Trouble Tickets H and J can be worked on in parallel. If you decide to work on these tickets in sequence, you must weigh the priorities of these two tickets. You will need to balance the impact on the closed-circuit television (CCTV) pilot if the network is not ready tomorrow against the impact of one or more users that cannot connect to the Internet. However, without more background information, you cannot properly assess these consequences, and any order to resolve these two tickets is acceptable.

Assigning device access during this lab is best done based on the role assignment of each of the team members during the exercise. Communication is an important factor during this lab. Make sure that time and resources are used efficiently.

The consoles of switch BSW1 and routers BRO1 and BRO2 are not accessible during this lab, but the devices can be accessed by use of Telnet or Secure Shell (SSH). Initially this is only possible from client PC CLT2, but after the WAN connectivity has been restored, they can also be accessed from other network devices.

In accordance with the fact that Trouble Ticket I is the first ticket that needs to be resolved, this lesson will follow the same order. First, Trouble Ticket I will be reviewed, followed by tickets H and J.

Trouble Ticket I: Fire in the Server Room

The text introducing this trouble ticket was the following:

Before starting to work on your assigned tasks, you first have to drive to one of the nearby branch offices to pick up some equipment that was delivered to the wrong office and is needed this afternoon. After fifteen minutes, you get an urgent phone call: You should return to the office immediately. A short circuit has caused a small fire in the server room and both routers CRO1 and CRO2, which were mounted in the same rack, were damaged. Luckily, you had two cold spares in storage. When you arrive at the office, two of your colleagues have already installed the two replacement routers, cabled them, and tried to configure the routers. However, the routers are not operational yet when you come in.

You receive a number of phone calls from network administrators that work in the branch offices asking about the loss of the WAN. Some of them have started to troubleshoot by themselves. You tell them what happened and ask them not to do anything until you have resolved the problem at the central site.

Your task is to work together with your colleagues on restoring routers CRO1 and CRO2 and regaining connectivity across the WAN.

Trouble Ticket I: Review and Discuss

How did your team approach Trouble Ticket I?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you accomplish the goal of restoring the WAN connectivity between headquarters and the branch?
- How long did it take to restore the connectivity?
- How did you verify that full connectivity had been restored?
- Which additional actions have you taken as part of the resolution of this ticket after connectivity had been restored?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--54

The main problem in this ticket is that the configuration of router CRO1 has been loaded in router CRO2 and vice versa. Because of the difference in IP addresses and subnets, none of the links between routers CRO1 and CRO2 and the campus core switches CSW1 and CSW2 are functional. They are operational at the physical and data link layer, but not at the network layer. In a similar way, the links between the headquarters routers CRO1 and CRO2 and the branch routers BRO1 and BRO2 should not be functional. However, it turns out that the Frame Relay links between the headquarters routers CRO1 and CRO2 and the branch router BRO1 are functional. Someone at the branch must have swapped the IP addresses on the Frame Relay links in an attempt to solve the problem. This same person has shut down the direct serial connection between routers BRO1 and CRO1.

This causes a second problem: The connectivity across these links will be lost as soon as the correct configurations on routers CRO1 and CRO2 have been restored.

There are various different methods of approaching this problem. After you have recognized the fact that the configurations of routers CRO1 and CRO2 have been swapped, a good approach is to focus on restoring the connectivity to the server SRV1 first and then load the backup configurations from that server via TFTP. If you have saved the baseline configurations on your PC during a previous lab, you can also paste the correct configurations to the routers via the console.

A second possibility is to rebuild the configurations of routers CRO1 and CRO2 based on the available network documentation. This is a more time-consuming method. Therefore, if you select this method, you should focus on restoring the WAN connectivity as soon as possible by reconfiguring a single LAN connection and a single WAN connection on one of the two routers. After restoring the connectivity, you can take more time to reconfigure the redundant LAN and WAN connections carefully.

Although there are many possible methods that you could use to solve this problem, the following example of a troubleshooting log shows you a methodical approach to resolve this problem. The method in this example follows the first approach that was mentioned earlier—it focuses on restoring connectivity to the server first and then copying the correct configurations to the routers.

Trouble Ticket	Actions and results
Ticket I	CRO1: Prompt on console displays CRO2. All interfaces are up except Serial 0/0/1.
	CRO2: Prompt on console displays CRO1. All interfaces are up.
	CRO1: Branch routes are available via Serial 0/0/0.121. No routes via Fast Ethernet interfaces.
	CRO2: Branch routes are available via Serial 0/0/0.121. No routes via Fast Ethernet interfaces.
	CRO1 & CRO2: EIGRP is enabled on all interfaces.
	CRO1: Pings to directly connected neighbor routers are not successful. Except to neighbor 10.1.194.10 (BRO1) on Serial 0/0.121.
	CRO2: Pings to directly connected neighbor routers are not successful. Except to neighbor 10.1.194.2 (BRO1) on Serial 0/0.121.
	Check baseline: Verify network diagrams and documentation.
	CRO1 & CRO2: Verify Cisco Discovery Protocol neighbors and compare against diagrams.
	Conclusion: It looks like CRO1 and CRO2 were swapped. However, this does not fit with the fact that there is a connection to BRO1.
	BRO1: Reached via Telnet from CRO1. Configuration of Serial 0/0/0.111 and Serial 0/0/0.112 does not match diagrams. Interface Serial 0/0/1 is shutdown.
	Conclusion: It looks like somebody changed the configuration of Serial 0/0/0.111 and Serial 0/0/0.112 on BRO1 to match the current situation.
	BRO2: Reached via Telnet from CRO1. Configuration conforms to baseline. Confirms the hypothesis that configurations of CRO1 and CRO2 were loaded incorrectly.
	Action plan: Restore LAN connectivity on CRO1 FastEthernet 0/0. This will restore connectivity between headquarters and branch. Next, restore LAN configuration on CRO2 and load the correct configuration. After CRO2 has been fully restored, the WAN connection will be switched to CRO2. Then the correct configuration will be loaded on CRO1. Finally, BRO1 will be reconfigured to match the original configuration.
	Communicated this with team members. One team member will prepare the LAN connectivity on CRO2, while another works on the LAN connectivity on CRO1.
	CRO1: Saved configuration in flash. Shut interface FastEthernet 0/1. Reconfigured IP address on FastEthernet 0/0. Added network statement under EIGRP for changed IP address.
	CRO1: Connectivity to SRV1 and to branch has been restored.
	CRO2: Saved configuration in flash. Shut interface FastEthernet 0/1, Serial 0/0/0 and Serial 0/0/1. Reconfigured IP address on FastEthernet 0/0. Added network statement under EIGRP for changed IP address.

Trouble Ticket	Actions and results
	CRO2: Connectivity to SRV1 has been restored. Copy archived backup to NVRAM. Communicate to team members: Reload CRO2.
	CRO2: Router has reloaded with correct configuration. Verified routing operation.
	CRO1: Communicate to team members: Shutdown interface Serial 0/0/0 and Serial 0/0/1. Confirmed with team members: WAN connectivity still available via CRO2.
	CRO1: Copy archived backup to NVRAM. Communicate to team members: Reload CRO1.
	CRO1: Router has reloaded with correct configuration. Verified routing operation.
	BRO1: Saved configuration in flash. Enabled interface Serial 0/0/1. Shut interface Serial 0/0/0. Confirmed with team members: WAN connectivity still available via CRO2.
	BRO1: Reconfigured interfaces Serial 0/0/0.111 and Serial 0/0/0.112 to match baseline. Enabled interface Serial 0/0/0. Verified routing operation.
	CRO1, CRO2 & BRO1: Saved backups of configurations to NVRAM, flash and SRV1.
	Communicated to team members: Problem solved. Documented changes. Closed ticket.

Key Clue: EIGRP Log Messages

EIGRP displays log messages stating that the neighbor is not on a common subnet for the interface.

```
*Apr 10 08:03:45.616 PDT: IP-EIGRP(Default-IP-Routing-Table:1): Neighbor
10.1.192.13 not on common subnet for FastEthernet0/1
*Apr 10 08:04:08.852 PDT: IP-EIGRP(Default-IP-Routing-Table:1): Neighbor
10.1.193.6 not on common subnet for Serial0/0/1
*Apr 10 08:04:19.095 PDT: IP-EIGRP(Default-IP-Routing-Table:1): Neighbor
10.1.194.14 not on common subnet for Serial0/0/0.122
*Apr 10 08:04:29.531 PDT: IP-EIGRP(Default-IP-Routing-Table:1): Neighbor
10.1.192.5 not on common subnet for FastEthernet0/0
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-56

The first clue that might give an indication of what is going on here is the fact that the prompt of the console of router CRO1 displays CRO2 as its hostname, and vice versa.

Several other clues indicate that the configurations of routers CRO1 and CRO2 might have been swapped. One of the clues is that the log messages that are stored in buffers on the router contain messages from the EIGRP routing protocol stating that its neighbor is not on a common subnet for a particular interface. This message indicates that EIGRP has detected that the source IP address of the received hellos from that neighbor does not match the subnet that is configured for that interface. If you receive this message for a single interface only, it usually indicates a configuration error in the IP address or mask for one of the two neighbors.

Another common reason for this error message is in cases where multiple IP addresses are configured on an interface by use of the **ip address address mask secondary** command and the primary (nonsecondary) IP address of the neighbors has not been selected from the same subnet.

In this case, however, the error message is received for all interfaces except interface Serial 0/0/0.121. This is a clue that this problem is caused by something more severe than a simple configuration error for a single interface.

Key Clue: cdp neighbor IP Address Does Not Match Subnet on Interface

Output of the **show cdp neighbor interface-id detail** command displays an IP address that does not match the locally configured IP address and subnet for that same interface.

```
CRO1#show cdp neighbor FastEthernet 0/0 detail | include address|Device
Device ID: CSW1.mgmt.tshoot.local
Entry address(es):
  IP address: 10.1.192.5
```

```
CRO1#show ip interface brief | include FastEthernet0/0
FastEthernet0/0      10.1.192.2      YES NVRAM  up
```

```
CRO1#show ip route connected | include FastEthernet0/0
C      10.1.192.0/30 is directly connected, FastEthernet0/0
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--5.6

Taking a cue from the log messages, it is a good idea to verify that the IP address of the neighbor is indeed on a different subnet. Cisco Discovery Protocol contains the IP address of the neighbor in its messages. By comparing the neighbor IP address to the locally configured IP address and subnet, you can see that there is indeed a mismatch between the IP configuration on neighbor CSW2 and the configuration on the FastEthernet 0/0 interface.

After repeating this procedure for several of the interfaces on routers CRO1 and CRO2 and comparing this to the network documentation, you can confirm that the configuration of router CRO1 was loaded on router CRO2, and vice versa.

Trouble Ticket I Checkpoints

Minimum checkpoints to prove that you have resolved this trouble ticket:

- You have restored routers CRO1 and CRO2 as fully functional routers.
- You have regained full IP connectivity between the headquarters subnets and branch subnets across the WAN.
- You have documented your process, your solution, and any changes that you have made to the device configurations.

What else should you have checked?

Are there any unresolved issues?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-57

The figure shows a list of minimum requirements that should be met to consider this trouble ticket to be resolved.

Because of the pressure to repair the WAN connectivity as soon as possible and because of the major configuration changes that are necessary on routers CRO1 and CRO2, it is possible that not all configurations are resolved at the end of the process. The WAN is highly redundant; therefore, if you forget to adapt the configuration on BRO1, it may go unnoticed.

To properly verify the results of the configuration changes after you have restored routers CRO1 and CRO2, you should at least execute the following tests:

- Verify that you can ping the neighbor IP address for each active interface from routers CRO1 and CRO2.
- Verify that you see the correct number of operational EIGRP neighbors for each active interface on router CRO1 and CRO2.

For comparison, the output of the **show ip eigrp neighbors** command on routers CRO1 and CRO2 is listed here:

```
CRO1#sh ip eigrp neighbors
```

```
IP-EIGRP neighbors for process 1
```

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
4	10.1.194.2	Se0/0/0.121	12	02:11:21	1084	5000	0	382
3	10.1.194.6	Se0/0/0.122	14	02:11:22	146	2280	0	536
2	10.1.193.2	Se0/0/1	12	02:12:21	14	1140	0	378
1	10.1.192.9	Fa0/1	12	02:12:21	29	200	0	1977
0	10.1.192.1	Fa0/0	11	02:12:21	37	222	0	719

```
CRO2#sh ip eigrp neighbors
```

```
IP-EIGRP neighbors for process 1
```

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
4	10.1.194.10	Se0/0/0.121	12	02:13:25	103	2280	0	377
3	10.1.194.14	Se0/0/0.122	13	02:13:25	401	2406	0	532
2	10.1.193.6	Se0/0/1	12	02:14:21	11	1140	0	529
1	10.1.192.13	Fa0/1	14	02:14:21	8	200	0	1978
0	10.1.192.5	Fa0/0	14	02:14:21	8	200	0	720

Suggested Solution

Correcting the configurations of routers CRO1 and CRO2 as follows can restore their connectivity to server SRV1.

Suggested Configuration Changes

- On router CRO1, change the IP address on interface FastEthernet 0/0 and activate EIGRP on it by using the network command that matches the changed IP address.

```
CRO2(config)#interface FastEthernet 0/0
CRO2(config-if)#ip address 10.1.192.2
255.255.255.252
CRO2(config-if)#router eigrp 1
CRO2(config-router)#network 10.1.192.2 0.0.0.0
```

- On router CRO2, change the configuration for interface FastEthernet 0/0 in a similar manner.

```
CRO1(config)#interface FastEthernet 0/0
CRO1(config-if)#ip address 10.1.192.6 255.255.255.252
CRO1(config-if)#router eigrp 1
CRO1(config-router)#network 10.1.192.6 0.0.0.0
```

- **Note:** Due to the swapped configurations, router CRO1 displays “CRO2” as its prompt and router CRO2 displays “CRO1.”

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0-68

After reestablishing the connection between routers CRO1 and CRO2 and the server SRV1, you can copy the latest archived configuration via TFTP or FTP to the NVRAM of the routers.

This exercise clearly shows why it is important to establish a baseline and have a good up-to-date configuration archive. Rebuilding the configurations based on the documentation and diagrams only is a tough exercise that could extend the outage for longer than necessary.

It is worth noting that after the FastEthernet 0/0 has been reconfigured and EIGRP has been enabled, not only connectivity to the headquarters LAN from routers CRO1 and CRO2 is restored, but due to the changed configuration on BRO1, the connectivity between the branch and headquarters is also restored.

This means that even before you load the configurations from server SRV1, you have reestablished the connectivity between the headquarters and branch sites. As far as the users are concerned, the problem has now been resolved. As a result, you will now have to plan the subsequent steps to restore routers CRO1, CRO2, and BRO1 to their original state very carefully. Unnecessary disruptions will not be tolerated.

Suggested Configuration Changes (Cont.)

- An archived copy of the configuration can now be loaded into the NVRAM of the devices as follows:

```
CRO2#copy tftp://srv1/CRO1-archive-config-3 startup-config
Accessing tftp://srv1/CRO1-archive-config-3...
Loading CRO1-archive-config-3 from 10.1.152.1 (via FastEthernet0/0): !
[OK - 5811 bytes]
[OK]
5811 bytes copied in 3.416 secs (1701 bytes/sec)
```

- After copying the configuration to NVRAM, the router can be reloaded to boot from the saved configuration.
- As an alternative, the running configuration can be replaced with the configuration in NVRAM by issuing the command:

```
CRO2#configure replace nvram:startup-config
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: yes
Total number of passes: 1
Rollback Done
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-59

Therefore, you need to be careful if you plan to reload after copying the archived configurations to the routers. In this particular case, you can plan reloads in such a way that there is hardly any disruption. However, it might be even better to use the **configure replace** command to restore the routers to the archived configurations. This command allows you to replace the current configuration with a different configuration without the need to reload.

How did you make sure that no unnecessary disruptions were caused by the reconfiguration of routers CRO1, CRO2, and BRO1?

Suggested Configuration Changes (Cont.)

- On router BRO1, re-enable the direct serial interface that connects router BRO1 to router CRO1:

```
BRO1(config-if)#interface Serial 0/0/1  
BRO1(config-subif)#no shutdown
```

- Also, swap the IP addresses on the Frame Relay subinterfaces:

```
BRO1(config-if)#interface Serial 0/0/0.111  
BRO1(config-subif)#description PVC to CRO1  
BRO1(config-subif)#ip address 10.1.194.2 255.255.255.252  
BRO1(config-subif)#  
BRO1(config-subif)#interface Serial 0/0/0.112  
BRO1(config-subif)#description PVC to CRO2  
BRO1(config-subif)#ip address 10.1.194.10 255.255.255.252
```

After the configurations on routers CRO1 and CRO2 are changed, there is a mismatch between the configurations of the Frame Relay subinterfaces on router BRO1 on one side and the changed configurations of routers CRO1 and CRO2 on the other side that needs to be repaired. Also, the direct serial connection between router CRO1 and BRO1 is shut down and should be re-enabled.

Trouble Ticket H: Preparation for CCTV Pilot

The text introducing this trouble ticket was the following:

Your company is interested in implementing an IP based closed circuit television (CCTV) solution. Currently, different solutions and vendors are being evaluated and one of the vendors has offered to implement a small pilot to show the capabilities of their solution. Although most of the video will be stored locally, there needs to be some communication between the central server at headquarters and the servers at the branch locations. To keep the traffic associated with the CCTV solution separate from the rest of the traffic, it will be implemented using two new VLANs, one at headquarters (VLAN 115 and subnet 10.1.155.0/24) and one at the branch office (VLAN 29 and subnet 10.1.163.64/26). Tomorrow the vendor will come in to install his systems and the network team has been asked to make sure that the new VLANs have been implemented and that there is IP connectivity between the headquarters CCTV VLAN and the branch CCTV VLAN. Your team has been very busy lately, so this was not done until yesterday. Yesterday afternoon, one of your colleagues implemented this while handling various other tasks, but did not have time to test the implementation. You were asked to verify his implementation.

Your task is to verify your colleague's implementation and ensure that there is IP connectivity between the two CCTV VLANs when the vendor comes in to implement the CCTV solution tomorrow.

Trouble Ticket H: Review and Discuss

How did your team approach Trouble Ticket H?

- How did you verify the implementation?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you accomplish the goal of establishing IP connectivity between the CCTV VLANs at the headquarters and branch sites?
- How did you verify that you accomplished your goal?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOTv1.0—5-11

After the successful resolution of Trouble Ticket I, only a minor issue remains: The IP address of router BRO1 on the subinterface FastEthernet 0/1.29, which belongs to CCTV VLAN 29, has a misconfigured IP address. It has been configured in subnet 10.1.164.64/26 instead of subnet 10.1.163.64/26. After changing the IP address to reflect the correct subnet, it will automatically be advertised by EIGRP because subnet 10.1.163.64/26 is covered under the EIGRP network statement **network 10.1.160.0 0.0.3.255**, while subnet 10.1.164.64/26 is not.

Although there are many possible methods that you could use to solve this problem, the following example of a troubleshooting log shows you a methodical approach to resolve this problem.

Trouble Ticket	Actions and results
Ticket H	ASW1: Change interface Fa 0/7, which connects to client PC CLT1, from VLAN 17 to VLAN 115. Notified team members that CLT1 will be used for testing.
	CSW1: Verified configuration of interface VLAN 115 on CSW1. Configured with IP address 10.1.155.252/24. HSRP is not enabled for this interface.
	CSW2: Interface VLAN 115 does not exist. Note: Need to implement VLAN 115 on CSW2 and enable HSRP when the network goes to production.
	CLT1: Configure IP address 10.1.155.1/24 and default gateway 10.1.155.252 (CSW1).
	CLT1: Ping to default gateway (10.1.155.252): Ping succeeds.
	BSW1: Change interface Fa 0/8, which connects to client PC CLT3, from VLAN 19 to VLAN 29. Notified team members that CLT3 will be used for testing.
	BRO1: Verified configuration of interface Fa 0/1.29 on BRO1. Configured with IP address 10.1.164.126/26. No GLBP configured.
	BRO2: No configuration for VLAN 29 exists. Note: Need to implement VLAN 29 on BRO2 and enable GLBP when the network goes to production.
	CLT3: Configure IP address 10.1.163.65/26 and default gateway 10.1.163.126.
	CLT3: Ping to default gateway 10.1.163.126: Ping does not succeed.
	BSW1: MAC address of CLT3 is learned on interface Fa 0/8 in vlan 29.
	BRO1: Ping to CLT3 (10.1.163.65): Ping does not succeed. Received unreachable (?!).
	BRO1: Traceroute to 10.1.163.65: Trace leads to router IRO1, which sends unreachable. Conclusion: Problem with local interface. Packets should not follow the default route.
	BRO1: Verified interface Fa 0/1.129. Interface is up, but IP address is misconfigured.
	BRO1: Changed IP address of interface Fa 0/1.29 to 10.1.163.126/26.
	CLT3: Ping to default gateway (10.1.163.126) succeeds.
	CLT3: Ping to CLT1 (10.1.155.1) succeeds.
	Conclusion: Test successful. CCTV VLANs are operational.
	Saved configuration on BRO1 to flash and TFTP server. Documented changes.
	BSW1: Changed interface Fa 0/8 back to VLAN 19.
	CLT3: Changed IP address assignment back to DHCP. Address is assigned. Ping to SRV1 succeeds.
	ASW1: Changed interface Fa 0/7 back to VLAN 17.
	CLT1: Changed IP address assignment back to DHCP. Address is assigned. Ping to SRV1 succeeds.
	Verified availability of subnets 10.1.155.0/24 and 10.1.163.64/26 on all routers.
	Problem solved. Communicated to team members. Notified colleague of test results. Closed ticket.

Key Clue: Traceroute Leads to Router IRO1

- A **ping** to IP address 10.1.163.65 of client CLT3 shows the reception of ICMP unreachable messages:

```
BR01#ping 10.1.163.65

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.163.65, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
```

- A traceroute reveals that packets follow the default route to routers IRO1 and ISP1:

```
BR01#trace 10.1.163.65

Type escape sequence to abort.
Tracing the route to 10.1.163.65

 0 10.1.163.130 0 msec 0 msec 4 msec
 1 10.1.193.5 16 msec 12 msec 8 msec
 2 10.1.192.13 8 msec 12 msec 12 msec
 3 10.1.192.19 12 msec 12 msec 12 msec
 4 192.168.224.254 12 msec 12 msec 12 msec
 5 192.168.224.254 !H !H *
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-5-2

No obvious clues in any of the **show** commands indicate the cause of this problem, other than the fact that the IP address configured on the interface FastEthernet 0/1.29 does not match the subnet specified in the trouble ticket text. The clues that you pick up while gathering information about this problem are dependent on the method that you used.

One of the things that you might have noticed is that a ping to the IP address of client CLT3 in subnet 10.1.163.64/26 from router BR01 displays a number of 'U's in the output. This indicates that an Internet Control Message Protocol (ICMP) unreachable message has been received from a router in the path. This is an unexpected result, because client CLT3 should be directly connected and therefore packets sent to it should not go through any other router.

However, the output of a traceroute command to client CLT3 confirms that the traffic is routed via router IRO1 and router ISP1, which discards the packets. This behavior is caused by the fact that the packets to IP address 10.1.163.65 are routed via the default route because they do not find a matching more-specific route in the routing table.

Trouble Ticket H Checkpoints

Minimum checkpoints to prove that you have resolved this trouble ticket:

- Subnet 10.1.155.0/24 and 10.1.163.64/26 are visible in all routing tables on the network.
- A host assigned to VLAN 115 at headquarters (for example, client PC CLT1) can successfully ping a host assigned to VLAN 29 in the branch (for example, client PC CLT3).
- You have documented your process, your solution, and any changes that you have made to the device configurations.

What else should you have checked?

Are there any unresolved issues?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-13

The figure shows a list of minimum requirements that should be met to consider this trouble ticket to be resolved.

The implementation of your colleague did not include any First Hop Redundancy Protocol (FHRP) configuration. It could be argued that this would be necessary configuration to stay consistent with the configuration used for other VLANs. The configuration of the Hot Standby Router Protocol (HSRP) at headquarters or the Gateway Load Balancing Protocol (GLBP) at the branch site is not considered a mandatory component of this ticket's solution, but at least you should have made a note of the fact that it is missing.

Do not forget to reassign the client PCs CLT1 and CLT3 to their original VLANs after you have completed your testing.

Suggested Solution

Correcting the configurations of routers CRO1 and CRO2 as follows can restore their connectivity to server SRV1.

Suggested Configuration Change

On router BRO1, change the IP address on interface FastEthernet 0/1.29 to an IP address in VLAN 10.1.163.64/26.

```
BRO1(config)#interface FastEthernet 0/1.29  
BRO1(config-subif)#ip address 10.1.163.126 255.255.255.192
```

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0—5-14

If, instead of changing the IP address of router BRO1 to match subnet 10.1.163.64/26, you changed the EIGRP and the IP configuration of client CLT3 to use subnet 10.1.164.64/26, this is not considered a valid solution. The implementation guidelines for the CCTV VLANs specified the subnets 10.1.155.0/24 and 10.1.163.64/26 to be used. Therefore, any solution that uses different subnets does not comply with the implementation plan for the CCTV pilot project.

Concerning the implementation of an FHRP at a later moment, it is interesting to note that on router BRO1 the last host in the subnet is configured as the IP address. By convention, this host address is used as the FHRP virtual IP address on this network. As a result, if the CCTV systems are installed using this IP address as their default gateway, it will only require a network side change. The default gateway IP address on the host will not need to be changed.

This choice has not been made in a consistent manner on switch CSW1. There the IP address configured on interface VLAN 115 is 10.1.155.252, which is not the last IP address in the subnet. Therefore, the implementation of an FHRP at a later moment will require the default gateway configuration on the CCTV host to be changed.

Technically these are not major problems, but a consistent implementation choice at both sites is the preferred solution.

Trouble Ticket J: User in Branch Cannot Access the Internet

The text introducing this trouble ticket was the following:

While you were on the road, just before the fire started, a user in the office LAN in Branch 1 (who uses client PC CLT2) complained that he did not have Internet access. When he tries to open the website <http://www.isp3.local> (which corresponds to IP address 172.34.224.1), he receives an error message from his browser saying that it cannot display the web page. He can reach the internal server SRV1 without any problems. You know that there were some problems with Internet access yesterday evening, but your colleague who worked on the problem has called in sick today and the logs do not show any useful information.

Your task is to diagnose and solve this problem and make sure that the user regains connectivity to the Internet.

Trouble Ticket J: Review and Discuss

How did your team approach Trouble Ticket J?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you accomplish the goal of restoring Internet connectivity from client PC CLT2?
- How did you verify that you accomplished your goal?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOTv1.0--5-55

After a successful resolution of Trouble Ticket I, you can begin to troubleshoot the loss of connectivity reported in this ticket. The problem in this ticket is caused by a wrongly configured next-hop IP address for the default route configured on router IRO2.

Which clients actually lose their connectivity to the Internet is dependent on the load balancing hashing algorithms that are integrated in the Cisco Express Forwarding technology that the routers and multilayer switches use to forward the packets. The clients that have their traffic routed via router IRO1 are unaffected, while the clients that have their traffic routed via router IRO2 will lose their connection.

However, the behavior observed in the lab was that not only the connectivity from client CLT2 to server <http://www.isp3.local> fails, but also other clients cannot connect to the ISP3 web server either. The underlying root cause is that the traffic of server SRV1, which is the Domain Name System (DNS) server for the network, to the outside DNS service is routed via router IRO2 and it therefore can no longer resolve the name of server <http://www.isp3.local>.

After any cached DNS entries expire on the clients they will therefore lose the ability to browse to server <http://www.isp3.local> when connecting by name, even if they would still be able to reach the server on its IP address.

The IP address of server <http://www.isp3.local> (172.34.224.1) was listed in the ticket description; therefore, it is possible to diagnose and resolve this problem without detailed knowledge of the DNS configuration of the network.

Although there are many possible methods that you could use to diagnose this problem, the following example of a troubleshooting log shows you a methodical approach to resolve this problem.

Trouble Ticket	Actions and results
Ticket J	CLT2: Verified problem: Cannot browse to http://www.isp3.local. A ping to www.isp3.local also fails, due to DNS problems.
	CLT2: Ping to SRV1 succeeds. Local DNS is operational. Note: Diagnose external DNS problems later. Troubleshoot based on IP address first.
	CLT2: Ping to 172.34.224.1 fails. Traceroute to 172.34.224.1 displays the following partial path: BRO2, CRO2, CSW2, IRO2. After that the requests time out.
	IRO2: Verified default route: Points to interface Fa 0/1 and next-hop IP address 172.24.244.85.
	IRO2: Verified ARP cache: No ARP entry found for 172.24.244.85.
	IRO2: Ping broadcast address for subnet to ISP2 (172.24.244.87). Received response from 172.24.244.86, not 172.24.244.85.
	Verify baseline: IP address of ISP2 router should be 172.24.244.86.
	IRO2: Configuration changed: Changed next-hop IP address for default route to 172.24.244.86. Both pre- and post-change configurations were saved in flash on the switch. Communicated this information to team members.
	IRO2: Ping to 172.34.224.1 succeeds.
	CLT2: Ping to 172.34.224.1 succeeds.
	CLT2: Browsing to http://www.isp3.local succeeds.
	Note: The change seems to have solved the external DNS problem as well.
	Problem fixed. Documented changes. Backed up configurations. Closed ticket.

Key Clue: ARP Cache Shows Different IP Address

- The ARP cache displays IP address 172.24.244.86, while 172.24.244.85 is listed as incomplete.

```
IRO2#show ip arp FastEthernet 0/1
Protocol Address      Age (min)  Hardware Addr  Type   Interface
Internet 172.24.244.81    -         0019.562c.2db1 ARPA   FastEthernet0/1
Internet 172.24.244.82    -         0019.562c.2db1 ARPA   FastEthernet0/1
Internet 172.24.244.85    0         Incomplete     ARPA   FastEthernet0/1
Internet 172.24.244.86    64        0019.5592.a464 ARPA   FastEthernet0/1
```

- A ping to IP address 172.24.244.87, which is the broadcast address for subnet 172.24.244.80/29, shows responses from address 172.24.244.86, but not from 172.24.244.85:

```
IRO2#ping 172.24.244.87
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.24.244.87, timeout is 2 seconds:

Reply to request 0 from 172.24.244.86, 1 ms
Reply to request 1 from 172.24.244.86, 1 ms
Reply to request 2 from 172.24.244.86, 1 ms
Reply to request 3 from 172.24.244.86, 1 ms
Reply to request 4 from 172.24.244.86, 1 ms
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--5-8

Various methods could eventually lead you to the fact that the next-hop IP address of the static default route on IRO2 is incorrectly configured. On the affected clients, a traceroute to IP address 172.34.224.1 (<http://www.isp3.local>) will display the path to router IRO2 and then fail. This should cause you to focus your troubleshooting on router IRO2. Verification of the default route shows IP address 172.24.244.85 as the next-hop IP address and interface FastEthernet 0/1 as the egress interface.

When you verify the ARP cache, you notice that IP address 172.24.244.85 is listed as Incomplete, while IP address 172.24.244.86 is listed also, which is not expected. The reason that IP address 172.24.244.86 is listed in the ARP cache is because the IP service level agreement (SLA) probe configured on router IRO2 (which is tracked by the default route) polls this IP address every 10 seconds.

Even if no IP SLA had been configured, it is often possible to discover the IP addresses in use on a particular subnet by issuing a **ping** command to the subnet broadcast address. Many devices respond to a ping that is directed to the broadcast IP address for their subnet. On some systems, this may have been disabled for security reasons and therefore it may not always work. However, it is a method that is worth trying in situations where you are unsure of the exact IP addresses that are being used on a subnet. In this case, the broadcast ping reveals the IP address of router ISP2.

Trouble Ticket J Checkpoints

Minimum checkpoints to prove that you have resolved this trouble ticket:

- Client PC CLT2 can use a web browser to connect to <http://www.isp3.local>.
- You have documented your process, your solution, and any changes that you have made to the device configurations.

What else should you have checked?

Are there any unresolved issues?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-17

The figure shows a list of minimum requirements that should be met to consider this trouble ticket to be resolved.

Suggested Solution

Correcting the configuration of router IRO2 as follows will restore the connectivity to server <http://www.isp3.local>.

Suggested Configuration Change

On router IRO2, change the next-hop IP address for the static default route to 172.24.244.86.

```
IRO2(config)#no ip route 0.0.0.0 0.0.0.0 172.24.244.85 track 1
IRO2(config)#ip route 0.0.0.0 0.0.0.0 172.24.244.86 track 1
```

Note: Do not forget to remove the route that points to the incorrect next-hop address 172.24.244.85.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-18

To resolve the problem introduced in this trouble ticket, the next-hop IP address of the default route on router IRO2 needs to be changed. To do this, you should remove the incorrectly configured static default route, and a correct static default route should be added.

Do not forget to remove the incorrect static route. Otherwise, traffic will be load-balanced over the two entries and 50 percent of the traffic will be dropped.

Consolidation

This topic describes the key lessons that could be learned from the lab exercise.

Discussion: Lessons Learned

Method and process:

- How could you improve your troubleshooting methods?
- What alternative methods did you discover?

Communication and procedures:

- How could the troubleshooting process be made more effective?
- What kind of procedures would be useful and why?

Technology and tools:

- Which tools were most useful during troubleshooting?
- Which tools could have improved the effectiveness of your process?
- Which useful Cisco IOS commands did you discover?

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0—5-19

In addition to thinking of the methods, processes, and tools as they were used in the lab, reflect on how these would apply to your own organization. Think about all the things that you learned during the lab itself and during the debrief discussions. There is room to write down key learning points in the Lab Debrief Notes section of the lab guide.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- You have reviewed and verified your lab results.
- You have consolidated the experiences and discoveries that all students got from the lab and have derived a number of key learning points from these experiences.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-20

Troubleshooting OSPF

Overview

The Open Shortest Path First (OSPF) protocol is one of the routing protocols commonly used in large enterprise networks. Troubleshooting problems related to the exchange of routing information is one of the most essential skills for a network engineer that is involved in the implementation and maintenance of large routed enterprise networks that use OSPF as the interior gateway protocol.

This lesson reviews the data structures used by OSPF and the flow of routing information between routers running the OSPF protocol, as well as the processing of routing information inside the router. In addition, the Cisco IOS commands that can be used to gather information from the OSPF data structures and routing processes are reviewed and a case study is presented to illustrate the use of the commands as part of a structured troubleshooting process.

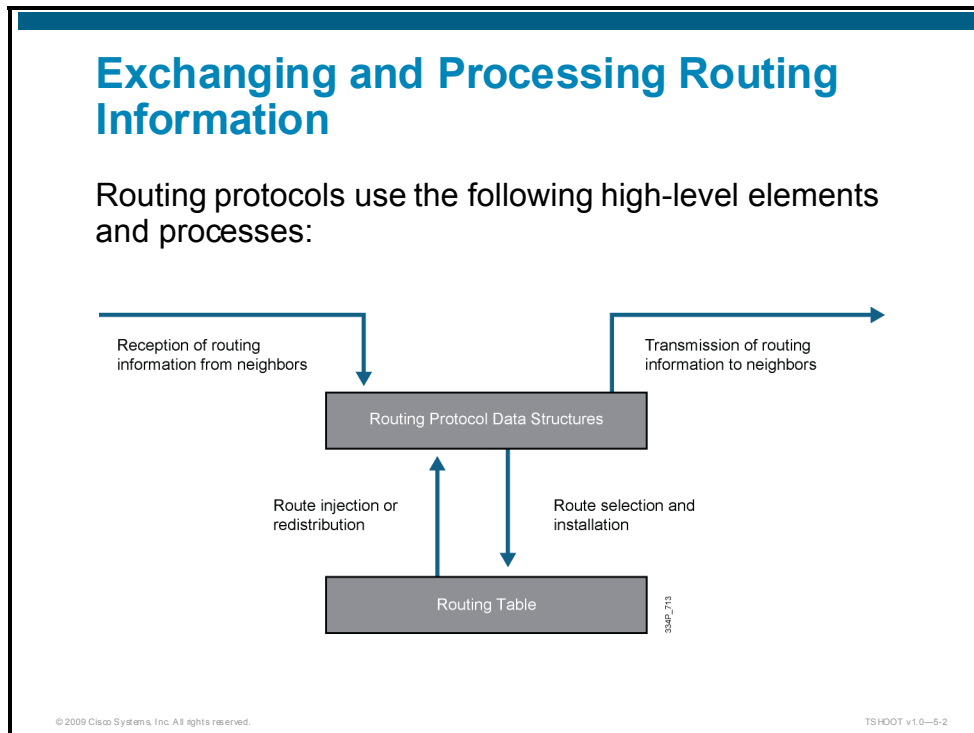
Objectives

Upon completing this lesson, you will be able to diagnose and resolve problems related to the exchange of routing information by use of the OSPF routing protocol. This ability includes being able to meet these objectives:

- Apply your knowledge of OSPF data structures to plan the gathering of necessary information as part of a structured approach to troubleshooting OSPF routing problems
- Apply your knowledge of the processes that OSPF uses to exchange network topology information within an area, to interpret and analyze the information that is gathered during an OSPF troubleshooting process
- Apply your knowledge of the processes that OSPF uses to exchange network topology information between areas to interpret and analyze the information that is gathered during an OSPF troubleshooting process
- Use Cisco IOS commands to gather information from the OSPF data structures and track the flow of OSPF routing information to troubleshoot OSPF operation

OSPF Data Structures

This topic describes the data structures that OSPF uses to store routing information.



To troubleshoot IP connectivity problems caused by missing or incorrect routes in a network that uses OSPF as the routing protocol, you need to have a good understanding of the processes and data structures that OSPF uses to distribute, store, and select routing information.

For any routing protocol, the following high-level elements and processes can be discerned:

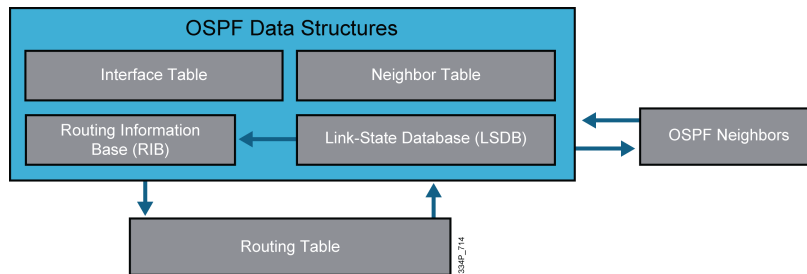
- **Reception of routing information from neighbors:** With OSPF, routing information is not exchanged in the form of routes, but in the form of link-state advertisements (LSAs), which contain information about elements of the network topology, such as routers, neighbor relationships, connected subnets, subnets available in different areas, redistributing routers, and redistributed subnets.
- **Routing protocol data structures:** OSPF stores the LSAs that it receives in a link-state database. Dijkstra's Shortest Path First (SPF) algorithm is used to compute the shortest path in terms of cost, which is the OSPF metric, to each network, based on the information in the link-state database. In addition, several other data structures, such as an interface table, a neighbor table, and a routing information base (RIB) are maintained.
- **Route injection or redistribution:** Directly connected networks that are enabled for OSPF are advertised in the router's LSA. Routes from other sources, such as other routing protocols or static routes, can also be imported into the link-state database and advertised by use of special LSAs.

- **Route selection and installation.** OSPF will attempt to install the best routes that are computed using the SPF algorithm in the routing table. OSPF discerns three different types of routes: intra-area routes, inter-area routes, and external routes. If two routes of different types for the same prefix are available for installation in the routing table, OSPF will prefer intra-area routes over interarea routes, and both these types will be preferred over external routes, regardless of the cost of the paths. If two equal cost routes of the same type are available, they will both be selected for installation in the routing table.
- **Transmission of routing information to neighbors.** Routing information is flooded to all routers in an area by passing LSAs from neighbor to neighbor using a reliable transport mechanism. Area Border Routers (ABRs) inject routing information from an area into the backbone area or, conversely, from the backbone area into the other areas that it is connected to.

OSPF Data Structures

OSPF tracks information using these data structures:

- Interface table: Active interfaces
- Neighbor table: Discovered neighbors
- Link-state database: Network topology information
- Routing information base: Results of the SPF calculation



© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-3

OSPF stores its operational data, configured parameters, and statistics in four main data structures:

- **Interface table:** This table lists all interfaces that have been enabled for OSPF. The directly connected subnets, that are associated with these interfaces, are included in the type 1 router LSA that the router injects into the OSPF link-state database for its area. When an interface is configured as a passive interface, it is still listed in the OSPF interface table, but no neighbor relationships are established on this interface.
- **Neighbor table:** This table is used to keep track of all active OSPF neighbors. Neighbors are added to this table based on the reception of hello packets, and they are removed when the OSPF dead time for a neighbor expires or when the associated interface goes down. OSPF goes through a number of states while establishing a neighbor relationship (also known as adjacency), and the neighbor table lists the current state for each individual neighbor.
- **Link-state database:** This is the main data structure that OSPF uses to store all its network topology information. This database contains full topology information for the areas that a router participates in and condensed information about the paths that are available to reach networks and subnets in other areas or other autonomous systems. Because this database contains a wealth of network topology information, it is one of the most important data structures to gather information from when troubleshooting OSPF problems.
- **Routing information base:** After executing the SPF algorithm, the results of this calculation are stored in the routing information base (RIB). This information includes the best routes to each individual prefix in the OSPF network with their associated path costs. When the information in the link-state database changes, only a partial recalculation might be necessary (depending on the nature of the change), and routes might be added to or deleted from the RIB without the need for a full SPF recalculation. From the RIB, OSPF will attempt to install its routes into the routing table.

The OSPF Link-State Database

- The OSPF link-state database contains all OSPF topology information available inside an area.
- OSPF network topology information is stored and exchanged using link-state advertisements.
- There are various different types of LSAs, and each type is used for a particular purpose and contains information elements specific to that purpose.

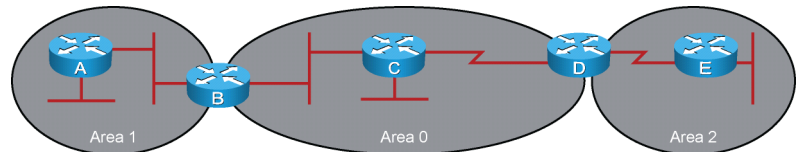
© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-4

The OSPF link-state database is used to store all the network topology information that is received by a router. There are separate databases for each OSPF area. In a stable situation, the database for each area will be identical on all routers in that area. An ABR has a database for each of the areas that it participates in, and it is responsible for exchanging network topology information between the databases of its connected areas and the backbone area. External routing information that was redistributed into OSPF from a different source is maintained in a separate section of the database that is not specific to any area.

OSPF Quiz: LSA Type Review

- Which LSA types are present in the database of each of the routers in the diagram and how many are there of each type?
- No redistribution or summarization has been configured, and each link represents a single subnet.



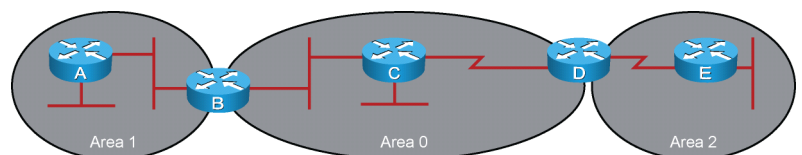
© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-5

Given the network diagram depicted in the figure, which LSA types are present in the database of each of the routers in the diagram and how many are there of each type?

OSPF Quiz: Answers

Router	Type 1	Type 2	Type 3
Router A			
Router B			
Router C			
Router D			
Router E			



© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-6

In a multiarea OSPF network without any redistribution, only LSA type 1, type 2, and type 3 are used. They serve the following purposes:

- Each router in an area generates a type-1 LSA that describes that router's link state including its directly connected subnets, connection types, and neighbors. Type-1 LSAs are not passed between areas.

- For each broadcast- or nonbroadcast-type network, OSPF elects a designated router. If the network is a transit network (that is, more than one router is connected to it) the designated router generates a type-2 LSA that describes the link state for that link including its subnet and connected routers. Type-2 LSAs are not passed between areas.
- For each subnet that an area border router can reach in a connected area, it will generate a type-3 LSA in the database of the backbone area 0, listing the subnet and its associated cost. For each subnet that it can reach in the backbone area, either directly or via another ABR, it will generate a type-3 LSA in the database of each connected area listing the subnet and its cost.

Based on these rules you can calculate the number of elements in each area's database:

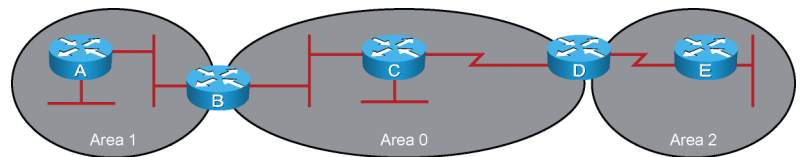
- **Type 1:** Area 1 contains two routers (A and B), and therefore its database will contain two type-1 entries. Area 0 contains three routers (B, C, and D), and therefore its database will contain three type-1 entries. Area 2 contains two routers, and its database will therefore contain two type-1 entries.
- **Type 2:** Area 1 contains one transit Ethernet (broadcast) network, and therefore its database will contain one type-2 entry (there is a second Ethernet network in area 1, but this is a stub network and not a transit network). Area 0 also contains one transit Ethernet link, and therefore it will also contain one type-2 entry. (A designated router is not elected for a point-to-point link). Area 2 has no transit broadcast or nonbroadcast type networks, and therefore no type-2 entries are generated.
- **Type 3:** Area 1 contains two subnets. For each of these subnets, a type-3 entry will be generated in the area 0 database by router B. Subsequently, router C will generate a type-3 entry for each of these subnets in the area 2 database. Area 0 contains three subnets. Router B will generate a type-3 entry for each of those subnets in the area 1 database, and router D will also generate three entries in the area 2 database. Area 2 contains two subnets; therefore, router D will generate two type-3 entries in the area 0 database, and router B will generate two type-3 entries in the area 1 database. In total, this means that the area 1 database contains $3 + 2 = 5$ type-3 entries, the area 0 database contains $2 + 2 = 4$ type-3 entries, and the area 2 database contains $2 + 3 = 5$ type-3 entries. For each area database, the total equals the number of subnets available outside its area.

Therefore, the totals for each area database are the following:

- **Area 1:** Two type-1, one type-2, and five type-3 entries
- **Area 0:** Three type-1, one type-2, and four type-3 entries
- **Area 2:** Two type-1, zero type-2, and five type-3 entries

OSPF Quiz: Answers (Cont.)

Router	Type 1	Type 2	Type 3
Router A	2	1	5
Router B	5	2	9
Router C	3	1	4
Router D	5	1	9
Router E	2	0	5



© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-7

The final step is to add the numbers for each individual router:

- **Router A:** Router A carries only the area 1 database and as a result, it has two type-1, one type-2, and five type-3 entries.
- **Router B:** Router B is an ABR and carries the databases for both area 1 and area 0. Therefore, it has $2 + 3 = 5$ type-1 entries, $1 + 1 = 2$ type-2 entries, and $5 + 4 = 9$ type-3 entries.
- **Router C:** Router C carries only the area 0 database, which contains three type-1, one type-2, and four type-3 entries.
- **Router D:** Router D is an ABR and carries the databases for area 0 and area 2. Therefore, it has $3 + 2 = 5$ type-1, $1 + 0 = 1$ type-2, and $4 + 5 = 9$ type-3 entries.
- **Router E:** Router E carries only the area 2 database that contains two type-1, zero type-2, and five type-3 entries.

What is the relevance of this exercise in troubleshooting?

To troubleshoot you often need to compare observed behavior against expected behavior, and when troubleshooting OSPF this means that you will need to be able to predict which different types of LSAs you can expect each router to generate. Understanding the role and content of the most fundamental OSPF LSA types (type 1, type 2, and type 3) is essential to troubleshoot OSPF effectively.

OSPF Information Flow Inside an Area

This topic describes the exchange of OSPF network topology information inside an OSPF area.

Requirement to Become OSPF Neighbors

Two OSPF routers will become neighbors only if the following parameters in the hello packets match:

- Hello and dead timers
- Area number
- Area type (normal, stub, NSSA)
- IP subnet and mask
- Authentication (type and data)

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-8

OSPF discovers neighbors through the transmission of periodic hello packets.

Two routers become neighbors only if these parameters match in the hello packets:

- **Hello and dead timers:** Two routers will become neighbors only if they use the same hello and dead time. The default values for broadcast and point-to-point type networks are 10-second hello and 40-second dead time. If these timers are changed on an interface of a router, the timers should be configured to match on all neighboring routers on that interface.
- **OSPF area number:** Two routers will become neighbors on a link only if they both consider that link to be in the same area.
- **OSPF area type:** Two routers will become neighbors only if they both consider the area to be the same type of area (normal, stub, or not-so-stubby area [NSSA]).
- **IP subnet and subnet mask:** Two routers will not become neighbors if they are not on the same subnet. The exception to this rule is that for point-to-point links the subnet mask is not verified. However, even if the subnet mask does not match, they still need to consider each other to be on the subnet associated with their respective interfaces.
- **Authentication type and authentication data:** Two routers will become neighbors only if they both use the same authentication type (null, clear text, or MD5). If they use authentication, the authentication data (password or hash value) also needs to match.

If two routers do not list each other as neighbors on a link and the interfaces have been activated for OSPF on both sides, it is worthwhile to verify the preceding parameters. A mismatch in any of these parameters will also show in the output of the **debug ip ospf event** command.

Establishing OSPF Adjacencies

OSPF goes through several states while establishing a neighbor relationship:

- Attempt
- Init
- 2-way
- Exstart
- Exchange
- Loading
- Full

All states except 2-way and full are transitory, and routers should not remain in these states for extended periods of time.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--6-9

After a router has received a hello packet and registered the neighbor in its neighbor table, it will attempt to build a neighbor relationship or adjacency with the neighboring router and exchange topology information to synchronize their link state databases. This process consists of several stages:

- **Attempt:** This state is encountered only when unicast hellos are used and a neighbor has been explicitly configured. When the router has sent a hello to the configured neighbor, but not received any hello from the neighbor yet, the neighbor relationship is in the attempt state. This state is not used on point-to-point or broadcast type networks, which use multicast hellos instead of unicast hellos.
- **Init:** This is the state that a neighbor is in if a hello has been received from the neighbor, but the neighbor is not listing this router in its neighbor list yet. This is a transitory state, and if a router is stuck in this state, this usually indicates that the neighbor is not receiving this router's hello packets correctly.
- **2-Way:** This is the state that a neighbor relationship is in when the router sees its own router ID listed in the active neighbor list in the hello packets received from that neighbor. This is usually a transitory state. The only time when this is considered the normal state is on broadcast or nonbroadcast networks, between two routers that both are neither the designated router (DR) nor the backup designated router (BDR) for the segment.
- **Exstart:** This stage indicates that the routers are starting the database exchange state by establishing a master and slave relationship and determining the initial sequence number for the database description (DBD) packets.
- **Exchange:** During the exchange stage, neighboring routers exchange database description packets to list the content of their link-state database in order to discover which entries each neighbor is missing. Exstart and exchange are transitory states, and if a neighbor is stuck in exstart or exchange state, this could indicate a mismatch in the maximum transmission unit (MTU) between the neighbors or a duplicate router ID.

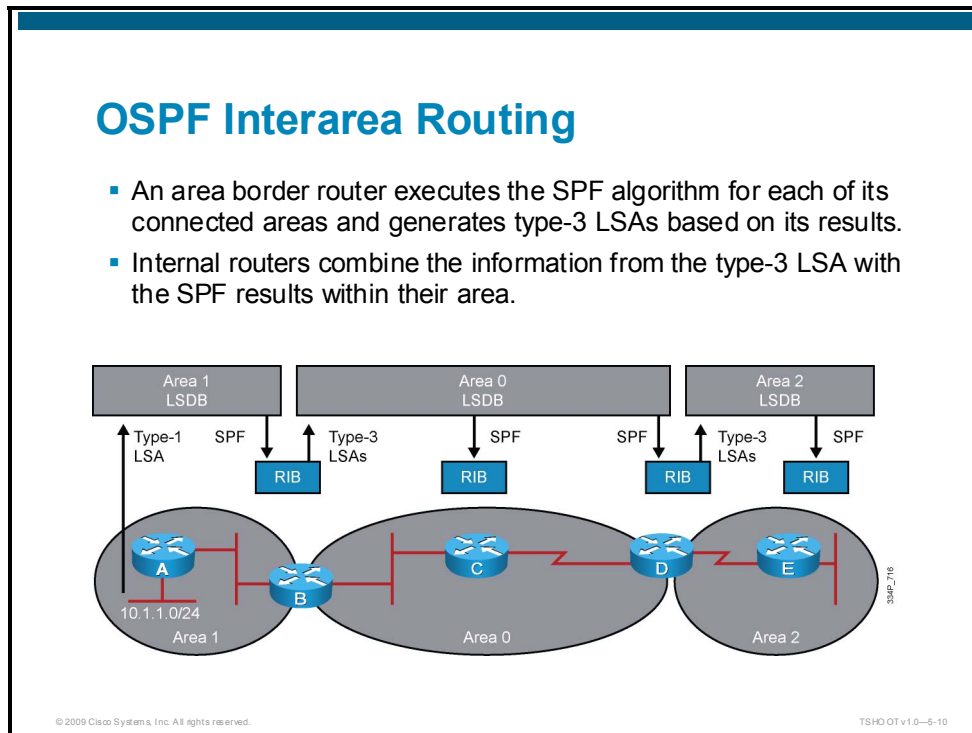
- **Loading:** During this stage, each of the two routers can request missing LSAs from the other router. This is a transitory state. If routers are stuck in this state, this could indicate packet or memory corruption, or in certain scenarios, an MTU mismatch between the neighbors.
- **Full:** This is the normal final stage of OSPF adjacency establishment. This state indicates that the router and its neighbor have successfully synchronized their link-state databases.

Full is the normal state after establishing a neighbor relationship and indicates that the routers have synchronized their databases; 2-way is an acceptable final state for certain types of neighbor relationships (two non-DR, non-BDR routers on a broadcast or nonbroadcast network). Any other state is a transitory state, and if a router is stuck in one of these states for an extended period of time this calls for further investigation.

During this adjacency building process, two routers in the same area synchronize their link-state databases for that area, and after they have reached the “full” state, their databases for the area are identical.

OSPF Information Flow from Area to Area

This topic describes the exchange of OSPF network topology information between areas.



ABRs play a key role in exchanging routing information between OSPF areas. Two routers can only become neighbors on a link if they are in the same area. When they exchange their databases during the initial database exchange, LSAs that belong to different areas are not exchanged.

To distribute information about subnets that are available in a particular area to other areas, the ABR generates type-3 LSA to inject the information into the area 0 database. Other ABRs use these type-3 LSAs to compute the best path to these subnets and then in turn inject the information into their connected areas by use of type-3 LSAs.

The diagram in the figure illustrates the following process:

Router B, which is an ABR, executes the SPF algorithm using the area 1 database to compute the best path for each subnet that is available in area 1. Based on this computation, router B will generate a type-3 LSA, which is then injected into the area 0 database. These type-3 LSAs include the cost that router B has computed for each of these prefixes.

Any other router in area 0, such as routers C and D, executes its own SPF algorithm based on the area 0 database. They will then add the cost in the type-3 LSAs to their computed cost to router B to find their total cost to the prefixes in area 1.

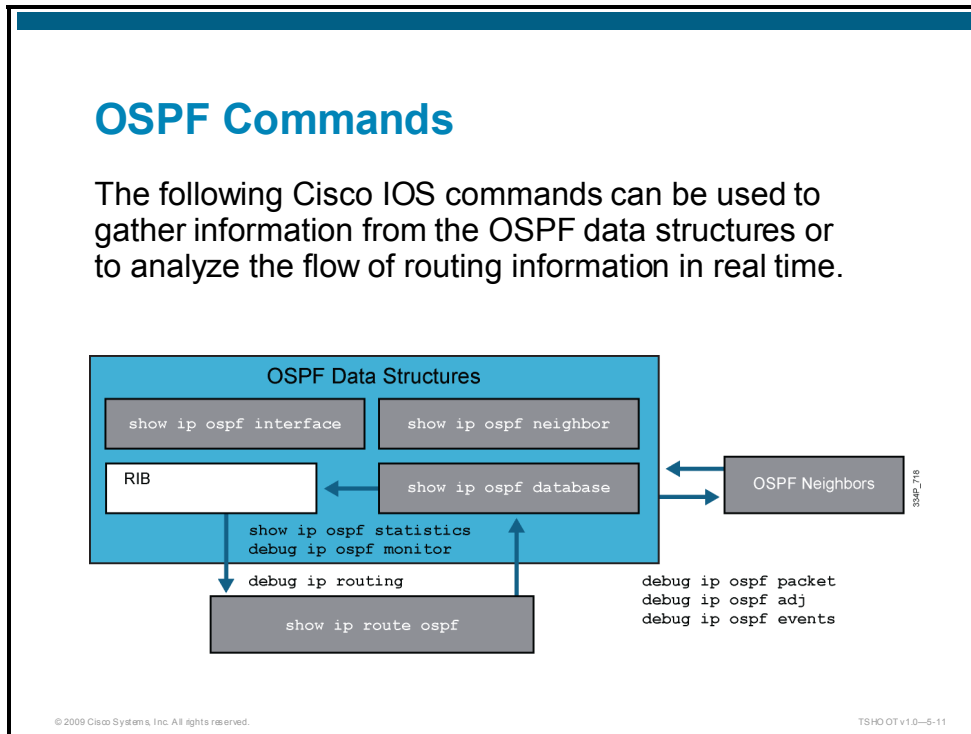
After router D has computed these costs, it will then generate type-3 LSAs for the prefixes from area 1 and inject these into the area 2 database.

Any router in area 2, such as router E, can now compute its own best path to router D and add this cost to the cost advertised by router D in the type-3 LSAs to find the total path cost to each prefix in area 1.

When you are troubleshooting OSPF and tracking the advertisement of routes and their associated costs, it is important to understand this process. It will enable you to know which routers are expected to generate the necessary type-3 LSAs and how the cost of the total path is calculated. Understanding this process helps you to track the flow of routing information from a router in one area to routers in different areas.

OSPF Cisco IOS Commands

This topic describes Cisco IOS commands that can be used to gather information from the OSPF data structures and track the flow of routing information.



The following commands can be used to gather information from the OSPF data structures:

- **show ip ospf interface:** This command is used to display the interfaces that have been activated for OSPF. This list contains all the interfaces that have an IP address that is covered by one of the network statements under the OSPF configuration. This command displays a lot of detailed information for each interface. For a brief overview, issue the command **show ip ospf interface brief**.
- **show ip ospf neighbor:** This command lists all neighbors that have been discovered by this router on its active OSPF interfaces and shows their current state.
- **show ip ospf database:** This command displays the content of the OSPF link-state database. When the command is issued without any additional options, it will display a summary of the database, listing only the LSA headers. Using additional command options, specific LSAs can be selected and the actual LSA content can be inspected.
- **show ip ospf statistics:** This command can be used to view how often and when the SPF algorithm was last executed. This command can be helpful when diagnosing routing instability.

The following debugs can be used to observe the transmission and reception of packets and the exchange of routing information:

- **debug ip routing:** This command is not specific to the OSPF protocol, but displays any changes that are made to the routing table, such as installation or removal of routes. This can be useful to diagnose routing protocol instabilities.

- **debug ip ospf packet:** This command displays the transmission and reception of OSPF packets. Only the packet headers are displayed, not the content of the packets. This command is useful to verify whether hellos are sent and received as expected.
- **debug ip ospf events:** This command displays OSPF events. This includes reception and transmission of hellos, and also the establishment of neighbor relationships and the reception or transmission of LSAs. This command can also provide clues as to why neighbor hellos might be ignored.
- **debug ip ospf adj:** This command displays events that are related to the adjacency building process and allows you to see a neighbor relationship transition from one state to the next.
- **debug ip ospf monitor:** This command monitors when the SPF algorithm is scheduled to run and displays the triggering LSA and a summary of the results after the SPF algorithm has completed.

These **debug** commands can generate a large amount of output, and proper care needs to be taken to prevent this from affecting the router's performance. Logging debug output to buffers on the router instead of to the console can limit the impact of these commands.

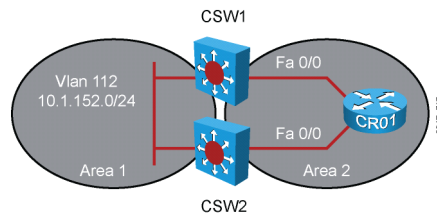
For sample output of these commands and guidelines regarding their use, see the "Sample Troubleshooting Flows" section in the course lab guide.

To review the complete syntax and a description of all command options, see the command reference sections of the Cisco Product Support pages on <http://www.cisco.com>.

Case Study: Troubleshooting OSPF

Consider the following situation:

- The routing table in router CRO1 shows only a single entry to reach network 10.1.152.0/24, the path via next-hop router CSW1 and interface FastEthernet 0/0.
- A ping confirms that neighbor router CSW2 is reachable on interface FastEthernet 0/1.
- You need to find out why the second, equal-cost path via router CSW2 is not used.



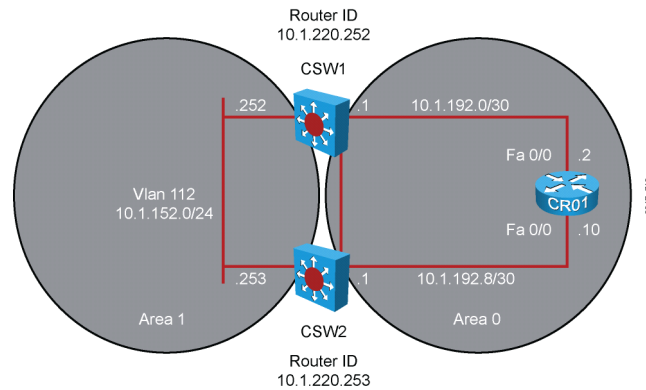
© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-12

The following case study illustrates how knowledge of OSPF data structures, update processes, and Cisco IOS commands can be leveraged to troubleshoot a routing problem.

Case Study: Troubleshooting OSPF (Cont.)

All relevant IP addresses for this case study are listed in the following diagram:



The network shown in the figure is using OSPF as the routing protocol and is configured for multiple areas. When you examine the routing table on router CRO1, you find only a single entry, the route via router CSW1:

```
Routing entry for 10.1.152.0/24
  Known via "ospf 100", distance 110, metric 2, type inter area
  Last update from 10.1.192.1 on FastEthernet0/0, 00:00:11 ago
  Routing Descriptor Blocks:
    * 10.1.192.1, from 10.1.220.252, 00:00:11 ago, via FastEthernet0/0
      Route metric is 2, traffic share count is 1
```

This result is unexpected because the diagram shows that two equal cost paths should be available. To verify if this problem is caused by an underlying Layer 1, Layer 2, or Layer 3 problem, a **ping** command is executed to test the Layer 3 connectivity to router CSW2 on the FastEthernet 0/1 interface:

```
CRO1#ping 10.1.192.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.192.9, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Because this ping succeeds, one can conclude that the Fast Ethernet link between router CRO1 and router CSW2 is operational at Layers 3 and below. Given that the link is functional but is not used to route the packets across, this is a routing problem and calls for an investigation of the operation of OSPF.

There are various different methods to troubleshoot this problem. The method presented is just one possible approach and was selected to show the role of the OSPF data structures in the troubleshooting process. Other methods to approach this problem might be valid as well.

Case Study: Troubleshooting OSPF (Cont.)

Displaying the type 3 summary LSA entries for subnet 10.1.152.0/24 yields the following result:

```
CRO1#show ip ospf database summary 10.1.152.0

      OSPF Router with ID (10.1.220.1) (Process ID 100)

      Summary Net Link States (Area 0)

Routing Bit Set on this LSA
LS age: 201
Options: (No TOS-capability, DC, Upward)
LS Type: Summary Links(Network)
Link State ID: 10.1.152.0 (summary Network Number)
Advertising Router: 10.1.220.252
LS Seq Number: 80000001
Checksum: 0x1C97
Length: 28
Network Mask: /24
      TOS: 0 Metric: 1

<... to be continued ...>
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-14

The objective is to find out why the second, equal-cost path via router CSW2 is not installed in the routing table in addition to the entry via router CSW1.

There are two main reasons why this could be happening: maybe router CSW2 is not advertising subnet 10.1.152.0/24 to area 0, or alternatively, CSW2 might be advertising the route, but the cost to reach subnet 10.1.152.0/24 via router CSW2 from router CRO1 is considered to be worse than the cost via router CSW1.

To find out if router CSW2 is advertising subnet 10.1.152.0/24 to area 0, you can consult the OSPF database in router CRO1. It is expected that both routers CSW1 and CSW2 will advertise a type-3 summary LSA for subnet 10.1.152.0/24.

The command **show ip ospf database summary lsa-id** can be used to display the content type-3 summary LSAs that have a specific link-state identifier. For type-3 LSAs, the link-state identifier is the subnet part of the associated prefix.

This command shows two entries. One entry was generated by the router with router ID 10.1.220.252 (CSW1).

Case Study: Troubleshooting OSPF (Cont.)

- Both routers CSW1 (router-id 10.1.220.252) and CSW2 (router-id 10.1.220.253) injected a type-3 LSA for subnet 10.1.152.0/24
- Both routers advertise a cost of 1 to reach 10.1.152.0/24.
- **Conclusion:** The difference must be caused by the path to router CSW2 inside area 0.

```
<... continuation ...>
LS age: 136
Options: (No TOS-capability, DC, Upward)
LS Type: Summary Links(Network)
Link State ID: 10.1.152.0 (summary Network Number)
Advertising Router: 10.1.220.253
LS Seq Number: 80000001
Checksum: 0x169C
Length: 28
Network Mask: /24
TOS: 0 Metric: 1
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--5-15

The command also displays a second entry that was generated by the router with router ID 10.1.220.253 (CSW2).

Both entries are advertised with an OSPF cost of 1. Therefore, the preference for the path to 10.1.152.0/24 via CSW1 must be based on the topology within area 0.

Given that router CRO1 has a direct connection in area 0 to both router CSW1 and CSW2, there are only two plausible explanations for the fact that router CRO1 is not using the path via router CSW2. Either the direct path to router CSW2 is not used because routers CSW2 and CRO1 have not become neighbors, or the path is not used because the cost for interface FastEthernet 0/1 is higher than the cost for interface FastEthernet 0/0. The second option is less likely because the interfaces are of the same type, and by default the OSPF cost is related to the interface bandwidth.

Case Study: Troubleshooting OSPF (Cont.)

Displaying the neighbor table on router CRO1 yields the following result:

```
CRO1#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.1.220.252	1	FULL/DR	00:00:33	10.1.192.1	FastEthernet0/0

- There is only one entry in the neighbor table: Router CSW1.
- Router CSW2 is not listed as a neighbor.
- **Conclusion:** A neighbor relationship between CRO1 and CSW2 has not been established.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-16

To verify whether router CRO1 has established a proper neighbor relationship with router CSW1, you can use the **show ip ospf neighbor** command.

In the example, only one neighbor is listed: Router CSW1.

Note that in the output of the command the first address is the router ID of the neighbor, while the second IP address in the “address” column is the interface IP address of the neighbor.

There can be several reasons that router CSW2 is not listed as a neighbor. One reason could be that it is not sending hellos. Another reason could be that the hellos are received, but ignored due to mismatched hello parameters. A third explanation could be that the hellos are sent but not received, because interface FastEthernet 0/1 has not been activated for OSPF and therefore does not listen to the OSPF multicast group 224.0.0.5.

Case Study: Troubleshooting OSPF (Cont.)

Displaying the interface table on router CRO1 yields the following result:

CRO1#show ospf interface brief						
Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs F/C
Lo0	100	0	10.1.220.1/32	1	LOOP	0/0
Fa0/0	100	0	10.1.192.2/30	1	BDR	1/1

- Interface FastEthernet 0/1, which leads to CSW2 is not listed in the interface table.
- **Conclusion:** Interface FastEthernet 0/1 has not been activated for OSPF.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-17

To verify whether interface FastEthernet 0/1 has been enabled for OSPF, the **show ip ospf interface brief** command is issued. Because the interface is not listed, you can conclude that the interface most not have been activated for OSPF. Unlike the **show ip eigrp interfaces** command, the **show ip ospf interface** command will display interfaces that are enabled for OSPF, but configured as passive interfaces. Therefore, the only possible explanation is that the interface has not been enabled.

Case Study: Troubleshooting OSPF (Cont.)

- Displaying the OSPF configuration on router CRO1 yields the following result:

```
CRO1#show running-config | section router ospf
router ospf 100
log-adjacency-changes
network 10.1.192.2 0.0.0.0 area 0
network 10.1.192.9 0.0.0.0 area 0
network 10.1.220.1 0.0.0.0 area 0
```

- The network statements do not match the IP address of CRO1 (10.1.192.10).
- The network statement is changed to match the correct IP address:

```
CRO1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CRO1(config)#router ospf 100
CRO1(config-router)#no network 10.1.192.9 0.0.0.0 area 0
CRO1(config-router)#network 10.1.192.10 0.0.0.0 area 0
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-18

Whether an interface is enabled for OSPF is controlled by configuration commands. Therefore, the configuration needs to be checked now to see why interface FastEthernet 0/1 has not been enabled.

As can be seen in the figure, there is a problem with one of the network statements. The network statement **network 10.1.192.9 0.0.0.0 area 0** matches IP address 10.1.192.9, which is not one of router CRO1's IP addresses, but an IP address of router CSW2. This is clearly a configuration mistake, and the network statement needs to be replaced with the statement **network 10.1.192.10 0.0.0.0 area 0** or some other network statement that matches IP address 10.1.192.10 (which is the IP address of router CRO1 on interface FastEthernet 0/1).

The network statement is replaced to test the hypothesis that the misconfigured network statement was the cause of the problem. Now the results of the change need to be verified, to confirm that the problem was solved. Strictly speaking, the only test that needs to be performed to confirm that the problem was solved is to execute the **show ip route 10.1.152.0 255.255.255.0** command again to confirm that both the routes via routers CSW1 and CSW2 now show in the routing table.

However, to show the impact of the change on the OSPF data structures, the changes in the interface table and neighbor table are displayed in the figure.

Case Study: Troubleshooting OSPF (Cont.)

The interface table and neighbor table now show the connection to router CSW2 as expected.

```
CRO1#show ip ospf interface brief
```

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Lo0	100	0	10.1.220.1/32	1	LOOP	0/0	
Fa0/1	100	0	10.1.192.10/30	1	BDR	1/1	
Fa0/0	100	0	10.1.192.2/30	1	BDR	1/1	

```
CRO1#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.1.220.253	1	FULL/DR	00:00:39	10.1.192.9	FastEthernet0/1
10.1.220.252	1	FULL/DR	00:00:31	10.1.192.1	FastEthernet0/0

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-19

After making the change to the network statements, the interface table now lists interface FastEthernet 0/1. This means that OSPF has now been enabled for the interface and OSPF packets are processed on interface FastEthernet 0/1.

The router ID (10.1.220.253) and interface IP address (10.1.192.9) of router CSW2 are now listed in the neighbor table on the FastEthernet 0/1 interface.

Case Study: Troubleshooting OSPF (Cont.)

The route via router CSW2 has been successfully added to the routing table and the traffic is balanced over the two available paths.

```
CRO1#show ip route 10.1.152.0 255.255.255.0
Routing entry for 10.1.152.0/24
  Known via "ospf 100", distance 110, metric 2, type inter area
  Last update from 10.1.192.9 on FastEthernet0/1, 00:00:29 ago
  Routing Descriptor Blocks:
    10.1.192.9, from 10.1.220.253, 00:00:29 ago, via FastEthernet0/1
      Route metric is 2, traffic share count is 1
    * 10.1.192.1, from 10.1.220.252, 00:00:29 ago, via FastEthernet0/0
      Route metric is 2, traffic share count is 1
```

The output shown in the figure confirms that the route via router CSW2 has been installed in the routing table in addition to the route via router CSW1.

Note that the routing source for the entries (the address behind the word “from”) in the routing table lists the router IDs of routers CSW2 (10.1.220.253) and CSW1 (10.1.220.252) respectively. These routers are listed as the source of the route, because they generated the type-3 LSA entries from which these routes were calculated.

This short case study illustrates the use of the Cisco IOS **show** commands to display the content of the OSPF data structures and how to leverage knowledge of these data structures and OSPF routing information flow to diagnose and resolve OSPF routing problems.

For more examples of OSPF troubleshooting methods and the output of key OSPF troubleshooting commands, see the “Sample Troubleshooting Flows” section in the course lab guide.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- You have reviewed the main data structures used by the OSPF routing protocol.
- You have reviewed the processes that OSPF uses to exchange and process the network topology information within a single area.
- You have reviewed the processes that OSPF uses to exchange and process the network topology information between areas.
- You have learned how to use the OSPF Cisco IOS commands to gather information about OSPF operation as part of a troubleshooting process.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-21

Troubleshooting Route Redistribution

Overview

Ideally, a single routing protocol is used to exchange routing information in an enterprise network. However, organizational requirements such as partnerships, mergers, technology migrations, and changes in policy can make it necessary to support the use of multiple routing protocols in the same enterprise network. In such situations, route redistribution between the different routing protocols is often necessary to achieve IP connectivity between the different parts of the network.

Route redistribution adds an extra layer of complexity to a routed network. In addition to understanding each of the routing protocols involved, it is also important to understand the interactions between them. This understanding is vital in order to be able to diagnose and resolve problems such as suboptimal routing and routing feedback that can occur when route redistribution is implemented.

This lesson will review the data structures and processes that play a part in the exchange of routing information between different routing protocols. Additionally, you can use the Cisco IOS commands to gather information about the operation of a route redistribution process, and a case study is presented to illustrate the use of these commands.

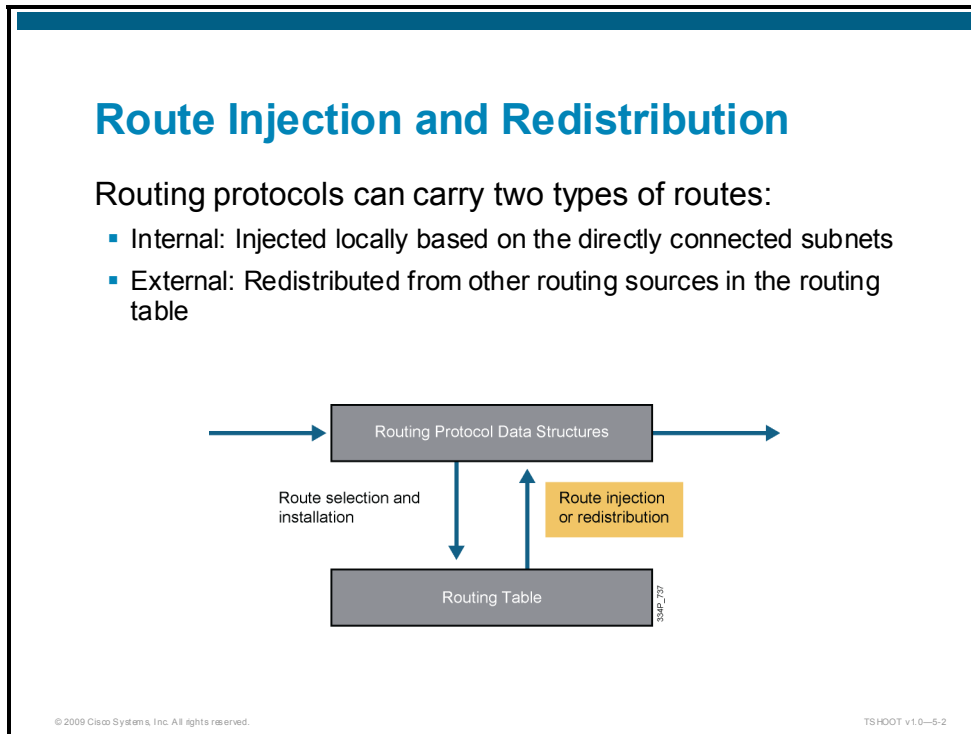
Objectives

Upon completing this lesson, you will be able to diagnose problems related to route redistribution. This ability includes being able to meet these objectives:

- Describe the data structures and processes involved in route redistribution
- Verify the correct operation of a route redistribution process

The Route Redistribution Process

This topic describes the processes that are used by routers to take routing information from a particular source and distribute the information by means of a different routing protocol.



The most common way to distribute routing information is to select a single routing protocol and use this throughout the network. On each of the participating routers, interfaces are activated for the routing protocol, and the directly connected subnets associated with these interfaces are injected into the routing protocol data structures and distributed via the routing protocol update mechanisms.

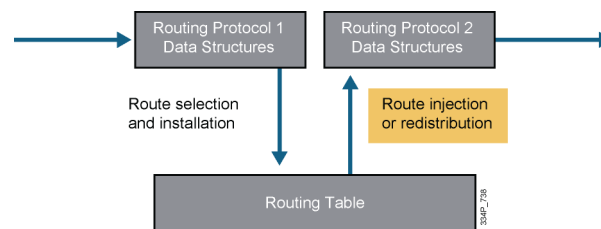
However, there might be situations where you have routes that are not local to the part of the network where the routing protocol operates, and you want to distribute these routes using the routing protocol. For example, you have a number of static routes that point to routers that are not using the same routing protocol, and you want to distribute the information about these subnets via your routing protocol. Alternatively, you might have a situation where two different routing protocols are used for two different parts of the network and you want to take the routes from the part of the network that are learned via one routing protocol and distribute that information by means of the other protocol to all routers that participate in the second routing protocol.

You can implement these scenarios by use of redistribution. There are two ways for routes to be injected in a routing protocol: Directly connected subnets can be injected by enabling the routing protocol on an interface. These routes are considered internal by the routing protocol. Alternatively, subnets from a different source that are present in the routing table can be taken from the table and redistributed by using the routing protocol's update mechanisms. Because these routes were not originated by the routing protocol, they are considered external. Older routing protocols, such as the Routing Information Protocol (RIP) do not have the ability to mark routes as external in their routing update messages. Newer routing protocols, such as Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) and

Intermediate System-to-Intermediate System (IS-IS), have the capability to mark routes as external and prefer internal routes over external routes. This is an important mechanism in the prevention of routing loops caused by route feedback.

Redistribution and the Routing Table

- Redistributed routes are taken from the routing table.
- Routes are not transferred directly between the routing protocol data structures of different protocols.
- Route redistribution is configured under the “destination” protocol.



© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-5-3

The redistribution process takes routes from the routing table. As a result, only routes that are installed in the routing table can be redistributed. Routes are not transferred directly between the data structures of different routing protocols.

As an example of this process, consider a router that is running two routing protocols, OSPF and EIGRP. EIGRP has been configured to redistribute the routes learned from OSPF. OSPF receives network topology information in the form of link-state advertisements from its neighbor OSPF routers, places these in its link-state database, and executes the Shortest Path First (SPF) algorithm to calculate the best routes to the subnets in the OSPF network. After calculating the best path for each prefix, it will attempt to install these prefixes in the routing table. If no competing routes with a lower administrative distance are present for a prefix, the OSPF route will be installed in the routing table.

EIGRP, which is configured to redistribute OSPF, scans the routing table and will take any route that was installed in the routing table by OSPF, import these routes in its topology table, marking them as external, and advertise them via its own update mechanisms. In addition to routes that are marked as OSPF routes in the routing table, EIGRP will also take any connected routes from the routing table that are enabled for OSPF (either by use of a **network** statement under the **router ospf** configuration or by use of the **ip ospf process-id area area-id** command on the interface. Although these routes are not marked as OSPF routes, but as directly connected routes in the routing table, EIGRP treats these routes as OSPF routes.

It must be noted that the redistribution process is the process that takes the routes from the routing table, not the process that installs the routes in the routing table. Therefore, redistribution is always configured under the “destination” protocol for the routing information. For example, when OSPF routes are redistributed into EIGRP, this is configured under the EIGRP process.

Seed Metrics

- All routes exchanged via a routing protocol need to have an associated metric for that protocol.
- There are no formulas to transform the metric for one protocol to a metric for a different protocol.
- The starting metric or seed metric for a protocol can be configured.
- If no seed metric is configured, a default is used.
 - Note: For RIP and EIGRP the default seed metric is “unreachable.”

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0–6-4

When the route is taken from the routing table and imported into the other protocol’s data structures, a metric for the redistributing protocol needs to be attached to that route. This metric is not computed from the metric of the original protocol through the use of some formula. A starting metric, or seed metric, should be configured, which will then be attached to all redistributed routes by the router. If no seed metric is configured, a default value for the redistributing protocol is used. For some protocols, such as RIP and EIGRP, the default metric is the maximum possible value, which represents “infinity” or “unreachable.” This is important to know when troubleshooting redistribution issues, because redistribution into these protocols will fail without explicit configuration of a seed metric.

Looking at this chain of events, there are two important conditions that need to be met for a route that is learned via one protocol to be successfully advertised via another protocol:

- The route needs to be installed in the routing table. The route needs to be selected as the best route by the source protocol and, if routes from competing sources are present, the route will need to have a lower administrative distance than the competing routes.
- The route needs to be redistributed in the destination protocol data structures with a valid metric for the destination protocol.

Access lists and route maps can be used to influence this process further by filtering routes, manipulating the seed metric, or setting additional parameters, such as route-type or tags for specific routes.

Troubleshooting Redistribution

Troubleshooting route propagation problems in a network that uses redistribution consists of:

- Troubleshooting routing exchange for the source protocol.
- Troubleshooting route selection and installation.
- Troubleshooting the redistribution process.
- Troubleshooting routing exchange for the destination protocol.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-5

When troubleshooting problems in a network that uses route redistribution, troubleshooting the actual redistribution process itself is often only a small part of the process.

Troubleshooting IP connectivity problems caused by redistribution involves the following elements:

- **Troubleshooting the source routing protocol:** Routes can be redistributed only if they are present in the routing table of the redistributing router. If routes are not redistributed as expected, you first need to confirm that they are learned on the redistributing router via the source protocol.
- **Troubleshooting route selection and installation:** To redistribute a route it needs to be selected and successfully installed in the routing table by the source protocol. When routes are redistributed between routing protocols in two directions, it is possible that routing information that originates in one of the routing domains is redistributed into the other routing domain and loops back to a router that is also connected to the source domain. If that route is subsequently accepted as a better route than the original source route, this will not only cause suboptimal routing, but if that route is subsequently redistributed back into the source protocol, it might also cause routing loops and routing instability. After diagnosing a suboptimal routing problem or routing loop, changing the administrative distance or filtering routes to influence the route selection and installation process can often solve the problem.
- **Troubleshooting the redistribution process:** If routes are learned and installed in the routing table of the redistributing router, but not inserted into the data structures and advertisements of the redistributing protocol, you should verify the configuration of the redistribution process. Bad seed metrics, route filtering, or misconfigured routing protocol process or autonomous system numbers are common causes for the redistribution process to fail.

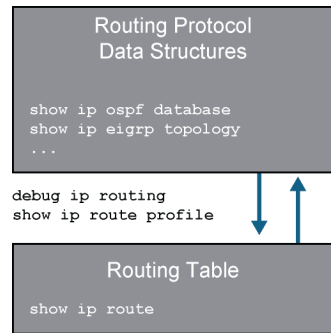
- **Troubleshooting the destination routing protocol:** After the routing information is inserted into the destination protocol's data structures, the routing information is propagated using that protocol's routing update mechanisms. If the routing information is not properly distributed to all routers in the destination routing domain, you should troubleshoot the routing exchange mechanisms for the destination protocol. Each routing protocol has its own methods of exchanging routing information, including external routing information. Research the specific protocol that you are working with to find out if external routes are handled differently from internal routes.

Verifying Redistribution

This topic describes how to verify the redistribution process using Cisco IOS commands.

Commands to Verify Redistribution

The following commands can be used to verify the route redistribution process:



As mentioned in the previous topic, diagnosing route redistribution problems mostly involves troubleshooting routing protocols and routing information exchange in general. To troubleshoot redistribution from one routing protocol to another, you need to be proficient with the troubleshooting toolkit for both the source and destination protocols.

The redistribution process itself consists of interaction between the data structures of the involved routing protocols and the routing table. To troubleshoot, you will need to use the commands to gather information from the routing protocol data structures, such as **show ip ospf database** to display the content of OSPF link-state database or **show ip eigrp topology** to display the content of the EIGRP topology table. Detailed information about specific routes installed in the routing table can be gathered by use of the **show ip route network mask** command.

The **debug ip routing** command displays routes being installed or removed from the routing table in real time. This command can be very powerful when you are troubleshooting routing loops or flapping routes caused by route redistribution.

Another feature that can be helpful in diagnosing suspected route instability is the route-profiling feature. Using the **ip route profile** command in global configuration mode enables this feature. After enabling this feature, the router tracks the number of routing table changes that occurred over 5-second sampling intervals. This can give you an indication of the overall stability of the routing table, without the need to enable a **debug** command. However, to find out which particular route or routes are causing the instability, enabling the **debug ip routing** command might be necessary.

The output of the **show ip route profile** command might not be self-explanatory without researching the command references. The following is an example of the output of the command after the feature has been enabled in global configuration mode:

```
CRO1#show ip route profile
```

```
IP routing table change statistics:
```

```
Frequency of changes in a 5 second sampling interval
```

Change/ interval	Fwd-path change	Prefix add	Nexthop change	Pathcount change	Prefix refresh
0	8	8	11	8	11
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
10	0	0	0	0	0
15	0	0	0	0	0
20	0	1	0	1	0
25	0	0	0	2	0
30	1	2	0	0	0
55	2	0	0	0	0
80	0	0	0	0	0
105	0	0	0	0	0
130	0	0	0	0	0
155	0	0	0	0	0
280	0	0	0	0	0
405	0	0	0	0	0
Change/ interval	Fwd-path change	Prefix add	Nexthop change	Pathcount change	Prefix refresh
530	0	0	0	0	0
655	0	0	0	0	0
780	0	0	0	0	0
1405	0	0	0	0	0
2030	0	0	0	0	0
2655	0	0	0	0	0
3280	0	0	0	0	0
3905	0	0	0	0	0

7030	0	0	0	0	0
10155	0	0	0	0	0
13280	0	0	0	0	0
Overflow	0	0	0	0	0

The way that this feature works is that it samples the number of routing table changes and the type of change during 5-second intervals. The first column in the output of the command represents the number of changes per sampling interval. So for example the row that has value 20 in the first column counts the number of sampling intervals during which 20 to 24 changes routing table changes of a particular type were recorded during the a 5-second sampling interval. The value of one in the column that represents “Prefix adds” in this row means that during one 5-second sampling interval between 20 and 24 prefixes were added to the routing table.

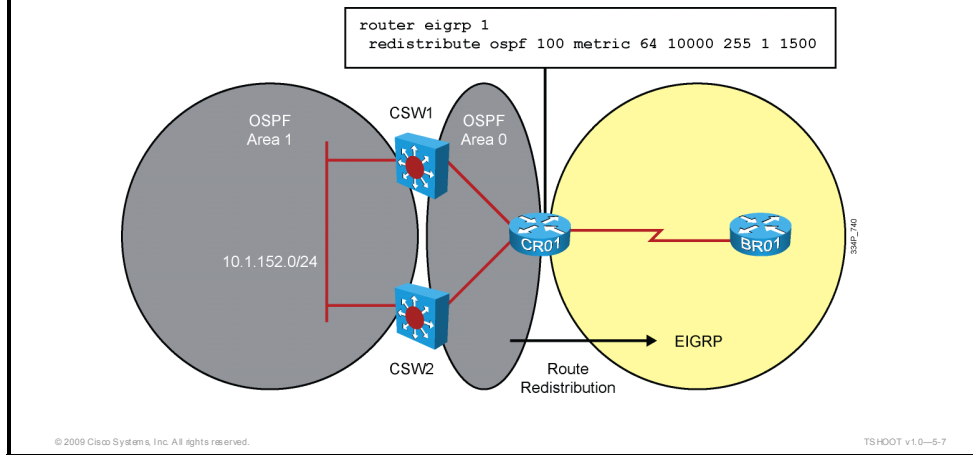
When the network is stable, only the counters in the first row should increase, because this row represents the number of intervals during which no changes to the routing occurred. When other rows than the first row increase in a situation that you thought to be stable, this could indicate a routing loop.

For more information, refer to the IP Routing Protocol command references at:

https://www.cisco.com/en/US/docs/ios/iproute/command/reference/irp_pi2.html#wp1016059

Case Study: Redistribution from OSPF to EIGRP

In this case study, a route from the OSPF network 10.1.152.0/24 is tracked as it is redistributed into the EIGRP network.



The following short case study illustrates the redistribution process and the commands that you can use to verify this process. The case study does not revolve around a problem that needs to be diagnosed and resolved, but tracks a route coming from an OSPF network that is being redistributed into EIGRP. The output of various **show** commands is presented as an example of how a route can be tracked in a situation where redistribution is working correctly. To troubleshoot effectively, it is important to know the behavior of processes and protocols when everything is working correctly, so this behavior can be compared and contrasted against the behavior when it is malfunctioning.

The figure shows the process. The network 10.1.152.0/24 resides in area 1 of the OSPF network and is connected to the multilayer switches CSW1 and CSW2. Router CRO1 is participating in OSPF in area 0 to communicate with switches CSW1 and CSW2. Router CRO1 is also connected to router BR01, and these two routers use EIGRP to exchange routing information.

Redistribution has been configured as listed in the figure.

Case Study: Redistribution from OSPF to EIGRP (Cont.)

Displaying the OSPF database shows that two type-3 summary entries for network 10.1.152.0/24 are present on router CRO1.

```
CRO1#show ip ospf database | begin Summary
Summary Net Link States (Area 0)

Link ID          ADV Router      Age      Seq#           Checksum
10.1.152.0       10.1.220.252   472      0x8000 003B   0x00A7D1
10.1.152.0       10.1.220.253   558      0x8000 003B   0x00A1D6
<... further output omitted ...>
```

To follow the routing information as it is passed between the various routing protocol data structures, first the main data structure of the source protocol, the OSPF database, is displayed. Two type-3 summary LSAs have been received and stored in the database for network 10.1.152.0/24, one from switch CSW1 and one from switch CSW2.

OSPF executes its SPF algorithm, calculates the cost of the path to switches CSW1 and CSW2, and adds these costs to the costs advertised in the respective LSAs. From these results, the lowest-cost path is selected for installation into the routing table if no competing routes with a lower administrative distance are present.

Case Study: Redistribution from OSPF to EIGRP (Cont.)

- Because the paths have an equal cost, both routes have been installed into the routing table on router CRO1.
- The fact that this route is being redistributed into EIGRP is marked in the routing table.

```
CRO1#show ip route 10.1.152.0 255.255.255.0
Routing entry for 10.1.152.0/24
  Known via "ospf 100", distance 110, metric 2, type inter area
  Redistributing via eigrp 1
  Advertised by eigrp 1 metric 64 10000 255 1 1500
  Last update from 10.1.192.9 on FastEthernet0/1, 00:28:24 ago
  Routing Descriptor Blocks:
    10.1.192.9, from 10.1.220.253, 00:28:24 ago, via FastEthernet0/1
      Route metric is 2, traffic share count is 1
    * 10.1.192.1, from 10.1.220.252, 00:28:24 ago, via FastEthernet0/0
      Route metric is 2, traffic share count is 1
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-9

The figure shows the routing table for network 10.1.152.0/24 on router CRO1. Both paths via switch CSW1 and switch CSW2 have been installed in the routing table because their costs are the same.

You can see in the routing table that this route has been marked for redistribution by EIGRP, and the configured EIGRP seed metric is also listed.

Case Study: Redistribution from OSPF to EIGRP (Cont.)

- The route has been entered into the EIGRP topology table on router CRO1 and marked as external.
- Source protocol and originating router are recorded.

```
CRO1#show ip eigrp topology 10.1.152.0 255.255.255.0
IP-EIGRP (AS 1): Topology entry for 10.1.152.0/24
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 42560000
Routing Descriptor Blocks:
  10.1.192.9, from Redistributed, Send flag is 0x0
    Composite metric is (42560000/0), Route is External
      Vector metric:
        Minimum bandwidth is 64 Kbit
        Total delay is 100000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 0
      External data:
        Originating router is 10.1.220.1 (this system)
        AS number of route is 100
        External protocol is OSPF, external metric is 2
        Administrator tag is 0 (0x00000000)
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--5-10

To verify that the route is being redistributed, the EIGRP topology table for network 10.1.152.0/24 on router CRO1 is displayed. You can clearly see in the figure that the route was taken from the routing table and inserted into the topology table as an external route. The five components of the configured seed metric are listed. In addition, some extra parameters were attached to the route to mark that the route was originated by the OSPF protocol with process number 100 and was injected into EIGRP by the router with EIGRP router-id 10.1.220.1 (which is this router, CRO1).

Case Study: Redistribution from OSPF to EIGRP (Cont.)

- The route has been exchanged with router BRO1 and entered into the EIGRP topology table.
- External data was exchanged together with the route.

```
BRO1#show ip eigrp topology 10.1.152.0 255.255.255.0
IP-EIGRP (AS 1): Topology entry for 10.1.152.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 43072000
Routing Descriptor Blocks:
  10.1.193.1 (Serial0/0/1), from 10.1.193.1, Send flag is 0x0
    Composite metric is (43072000/42560000), Route is External
      Vector metric:
        Minimum bandwidth is 64 Kbit
        Total delay is 120000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
      External data:
        Originating router is 10.1.220.1
        AS number of route is 100
        External protocol is OSPF, external metric is 2
        Administrator tag is 0 (0x00000000)
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-11

The external data that was attached to the route is passed along to router BRO1 within the EIGRP routing updates. When the EIGRP topology table is displayed on router BRO1, the originating router and routing protocol are still visible. Clearly, this information can be very useful when you are troubleshooting redistribution into EIGRP, because it makes it easy to see which router is the source when you are seeing unexpected routes. The information that is attached to and exchanged with external routes is different for each routing protocol.

Case Study: Redistribution from OSPF to EIGRP (Cont.)

- The route has been selected as the best route and installed in the routing table on router BRO1.
- The route is marked as an EIGRP external route and has a corresponding administrative distance of 170.

```
BRO1#show ip route 10.1.152.0 255.255.255.0
Routing entry for 10.1.152.0/24
  Known via "eigrp 1", distance 170, metric 43072000, type external
  Redistributing via eigrp 1
  Last update from 10.1.193.1 on Serial0/0/1, 00:00:35 ago
  Routing Descriptor Blocks:
  * 10.1.193.1, from 10.1.193.1, 00:00:35 ago, via Serial0/0/1
    Route metric is 43072000, traffic share count is 1
    Total delay is 120000 microseconds, minimum bandwidth is 64 Kbit
    Reliability 255/255, minimum MTU 1500 bytes
    Loading 3/255, Hops 1
```

Finally, you can see in the figure that the route has been selected as the best route and installed in the routing table. In the routing table, it is marked as an external EIGRP route and has been installed with a corresponding administrative distance of 170. However, the external information that was present in the EIGRP topology table, such as the originating router and protocol, is not carried into the routing table.

This short case study illustrates the process that you can use to verify the various data structures that play a role in redistribution processes. It also shows that it is important to practice the use of these commands as part of the creation of a baseline of your network in order to know what the expected results are in a working situation.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- You have reviewed the processes and data structures that are used when routing information from an external source is redistributed into a routing protocol.
- You have learned how to use Cisco IOS commands to verify the operation of a route redistribution process.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-13

Lab 5-2 Debrief

Overview

In this lab, you have practiced troubleshooting problems related to the Open Shortest Path First (OSPF) routing protocol and problems related to route redistribution between OSPF and the Enhanced Interior Gateway Routing Protocol (EIGRP). You have created a troubleshooting plan to coordinate the work between the team members. You have methodically researched the problems, kept a log of your actions and findings, and resolved the problems and documented your solutions.

During the lab debrief, the instructor will lead a group discussion during which you can present your solutions. You will get an opportunity to verify your solution against a number of checkpoints provided by the instructor and compare your solution to other students' solutions. The instructor will discuss alternate solutions and their advantages and disadvantages.

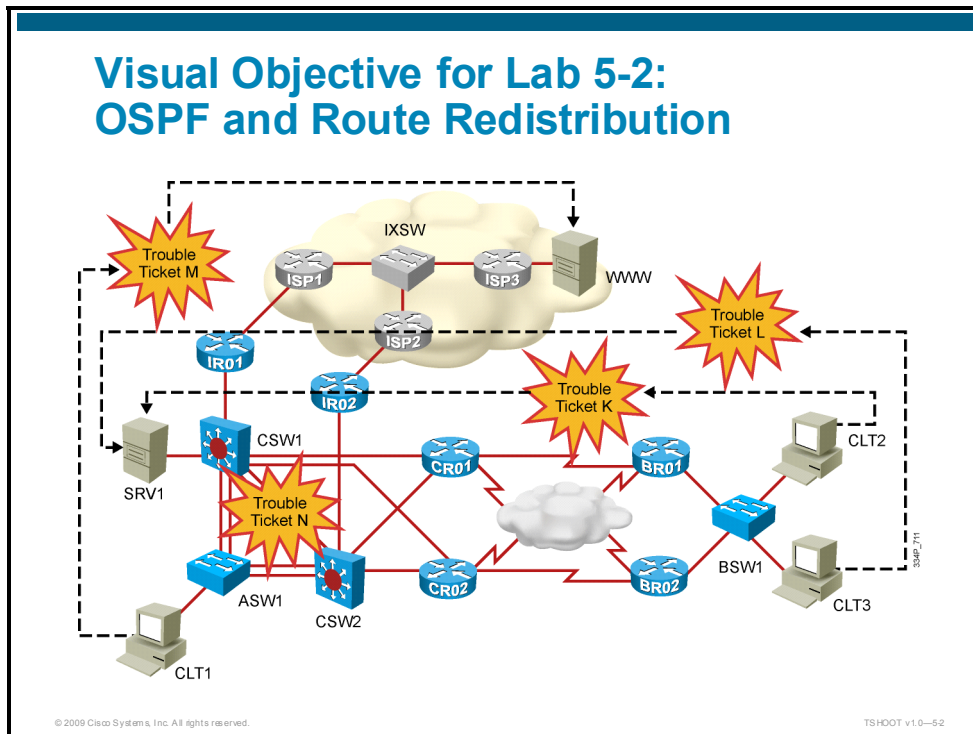
Objectives

Upon completing this lesson, you will be able to diagnose and resolve problems related to OSPF and route redistribution using a structured, methodical approach. This ability includes being able to meet these objectives:

- Compare your solution, findings, and action log against a set of checkpoints provided by the instructor and identify common and alternate solutions
- Consolidate the lessons learned during the review discussions into a set of best-practice methods and commands to aid you in future troubleshooting procedures

Review and Verification

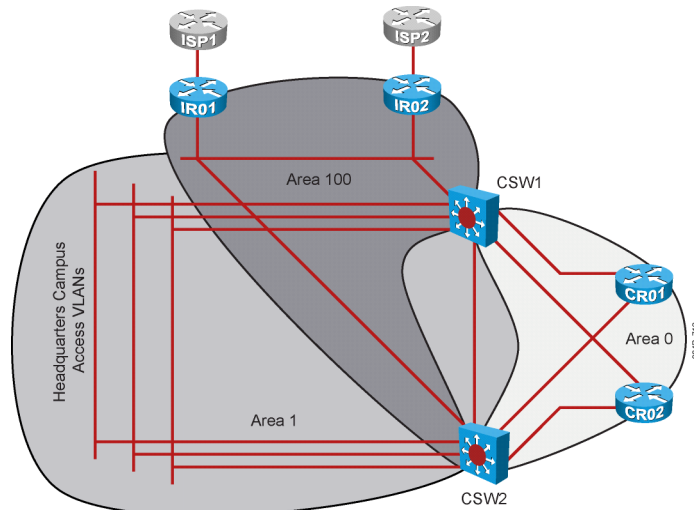
This topic describes the problems that were introduced in Lab 5-2, asks how you can verify that you have solved the problems, and provides an example of a troubleshooting process that will allow you to find and resolve the issues.



This lab consists of four trouble tickets: Trouble Ticket K involves the connectivity from the client PC CLT2 at the branch site to the headquarters site and the Internet. Trouble Ticket L involves the connectivity from client PC CLT3 to the headquarters and the Internet. Trouble Ticket M involves the Internet connectivity from the headquarters campus; and Trouble Ticket N involves a test of OSPF authentication.

It must be noted that Trouble Tickets K and L can be fully resolved only after a solution for Trouble Ticket M has been implemented. The connectivity to the Internet from client PCs CLT2 and CLT3 is dependent on the connectivity from the headquarters network to the Internet.

Lab 5-2: OSPF Area Design



All four of the trouble tickets are embedded in a larger scenario: the migration of the network from using OSPF as the routing protocol to using EIGRP. The text introducing the scenario was the following:

“Your company has decided to migrate from using EIGRP to using OSPF as the routing protocol. This migration is going to be executed in two phases. During the first phase, the headquarters campus is migrated to OSPF. During this phase, EIGRP will still be used on the WAN toward the branch offices. On routers CR01 and CR02, redistribution will be configured between OSPF and EIGRP to ensure connectivity between headquarters and the branches. During the second phase, the branch offices will be migrated one by one until OSPF is used in the entire network.

The migration has been planned and designed by the engineering team, but the support team will need to support the new network and will be involved in migrating most of the branches during the second phase.

Today is Saturday, and the engineering team has been busy implementing OSPF and removing EIGRP at the headquarters site. Although you have not taken part in the actual implementation, some of the senior engineers in the support team are on standby to assist during the verification and troubleshooting phase. Together with the engineering team, you will have to make the decision on Sunday to either accept the implementation or if major issues are uncovered that would threaten the stability of the network, roll back to the original configurations.”

The OSPF design is outlined in the diagram presented in the figure, and some further design and implementation guidelines were given in the introduction to the trouble ticket:

The branch sites will be in separate areas that are configured as totally stubby areas.

To test both the branch connectivity using redistribution between EIGRP and OSPF and the eventual situation of only using OSPF, branch routers BRO1 and BRO2 have been specifically prepared for both these scenarios. The access VLANs at the branch 1 site have been divided between routers BRO1 and BRO2 by disabling the corresponding interface on the other router. As a result, router BRO1 will function as the default gateway for VLANs 16 and 17, while router BRO2 will be the default gateway for VLANs 18, 19 and 128. Router BRO1 will run EIGRP as usual, while router BRO2 has been converted to run OSPF in area 11. This allows testing of the EIGRP redistribution from client PC CLT2 and testing of OSPF from client PC CLT3.

All following trouble tickets are related to the verification and acceptance of the first phase of the OSPF migration.

Further, a note is provided stating that all interfaces that are configured to be shut down on routers BRO1 and BRO2 should remain shut down for the duration of the exercise.

Planning Troubleshooting

How did your team approach the four trouble tickets?

- Did you troubleshoot all tickets in parallel, in sequence, or did you use a combination of methods?
- How did you decide on the order that you chose to address the tickets in?
- How did you coordinate device access between your team members?
- How did you communicate with your team members?
- Did you meet the criteria to successfully go through with the migration or would you need to roll back?
- Which choice did you make regarding the resolution of ticket N? Did you manage to make the authentication work or did you remove the authentication?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-54

Note This lesson provides sample answers and solutions to the questions posed during the debrief discussions. Keep in mind that alternate solutions and methods might be just as valid and that the solutions provided here only highlight a sample approach and solution.

After assessing the four trouble tickets, it is clear that Trouble Tickets K, L, and M have equal priority. All the issues in these tickets need to be successfully addressed to complete the migration. If any of these issues remain, the migration is considered unsuccessful, and a rollback procedure needs to be initiated.

It is not mandatory to resolve the authentication problem in Trouble Ticket N. However, the neighbor relationship between switches CSW1 and CSW2 on VLAN 111 should be successfully established. This means that at some point before the end of the lab, a decision needs to be made on how to handle this ticket. If the neighbor relationship between the switches CSW1 and CSW2 has not been successfully established at the end of the lab, the migration is also considered unsuccessful and a rollback procedure needs to be initiated.

Based on these assessments, a possible work plan for a team consisting of three members would be the following:

- Team member 1 will first focus on Trouble Ticket K. This team member is considered to be in control of router BRO1. If any other team member needs to make changes or perform disruptive actions such as reloading or debugging on router BRO1, they should ask for permission of team member 1 first.
- Team member 2 will first focus on Trouble Ticket L. This team member is considered to be in control of router BRO2. If any other team member needs to make changes or perform disruptive actions such as reloading or debugging on router BRO2, they should ask for permission of team member 2 first.

- Control of switch BSW1 and routers CRO1 and CRO2 will be shared and coordinated between team members 1 and 2. If team member 3 needs to make changes or perform disruptive actions on any of these devices, permission from both team members 1 and 2 is necessary.
- Team member 3 will first focus on Trouble Ticket M. This team member is considered to be in control of routers IRO1 and IRO2. If any other team member needs to make changes or perform disruptive actions on these routers, they should ask for permission of team member 3 first.
- Control of switches ASW1, CSW1, and CSW2 is assigned and coordinated between all team members based on need.
- The team member that first completes the initially assigned ticket will notify the other team members and start work on Trouble Ticket N. Device control is reassigned as necessary at this point in time.
- Half an hour before the set completion time of the lab, the team will reassess the priorities and decide how to move forward to maximize the chances of successfully completing the migration.

Trouble Ticket K: No Connectivity from Client PC CLT2

The text introducing this trouble ticket was the following:

After the implementation of OSPF and the implementation of redistribution between EIGRP and OSPF, the connectivity from client PC CLT2, which uses router BRO1 as its default gateway to server SRV1 at headquarters, is tested. A ping from client PC CLT2 to server SRV1 fails. The connectivity problem is not limited to SRV1. An attempt to browse to <http://www.isp3.local> also fails.

Your task is to diagnose this problem and if possible, resolve it. Connectivity from PC CLT2 to server SRV1 and to server <http://www.isp3.local> on the Internet is mandatory for this phase of the migration to be considered successful.

Trouble Ticket K: Review and Discuss

How did your team approach Trouble Ticket K?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you accomplish the goal of restoring the connectivity from client PC CLT2 to the headquarters network and the Internet?
- How did you verify that you accomplished your goal?
- Were there any implementation choices that you made and if so, what were those choices?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--5.6

The problem in this ticket revolves around the redistribution of routes from OSPF into EIGRP and from EIGRP into OSPF. There are two separate issues in this ticket. The redistribution of OSPF routes into EIGRP on routers CRO1 and CRO2 is not working because a seed metric has not been specified for the redistribution. The redistribution from OSPF into EIGRP on routers CRO1 and CRO2 is not working because the **subnets** keyword is missing on the redistribution from EIGRP into OSPF. As a result, only classful routes are redistributed.

One of the implementation choices you need to make during the resolution of this ticket regards the seed metric that is used to redistribute the OSPF routes into OSPF. The exact value that you choose for this seed metric is not very important as long as it is consistently applied.

Although there are many possible methods that you could use to solve this problem, the following example of a troubleshooting log shows you a methodical approach to resolve this problem.

Trouble Ticket	Actions and results
Ticket K	CLT2: Verified problem: Cannot ping to SRV1. Cannot browse to http://www.isp3.local.
	CLT2: Ping to default gateway (10.1.160.126) succeeds. Traceroute to SRV1 (10.1.152.1) stops at router BRO1.
	BRO1: Routing table shows no route to 10.1.152.0/24. Default route is missing. Only four EIGRP learned routes are shown (corresponding to the WAN routes).
	BRO1: All expected EIGRP neighbor relationships between BRO1 and routers CRO1 and CRO2 have been established.
	CRO1: A route to 10.1.152.0/24 is present in the routing table, learned via OSPF. The default route is not available.
	Missing default route may be related to ticket M. Verified with team member 3. Decision: Troubleshoot connectivity to SRV1 first. Check back with team member 3 after connectivity to SRV1 has been established.
	CRO1: Redistribution from OSPF to EIGRP has been configured. No additional parameters or filters have been configured.
	CRO1: Network 10.1.152.0/24 is marked in the routing table as "Redistributing via eigrp 1", but there is no line that says "Advertised..."
	CRO1: Network 10.1.152.0/24 is not present in the EIGRP topology table.
	CRO1: Enabled debug ip routing and debug ip eigrp . Cleared route to 10.1.152.0/24 from the routing table. Result: route is deleted and installed in the routing table. EIGRP shows no activity. Disabled debug.
	Research EIGRP redistribution: EIGRP needs a default metric to be specified.
	CRO1: Configuration changed: Added metrics to redistribution from OSPF to EIGRP (bandwidth 10 Mb/s, delay 1 msec, reliability 255, load 1, MTU 1500). Both pre- and post-change configurations were saved in flash on the switch. Communicated this information to team members.
	CRO1: Network 10.1.152.0/24 shows in routing table as "Advertised by eigrp 1 metric 10000 100 255 1 1500." Network 10.1.152.0/24 is now also displayed in EIGRP topology table as an external route.
	BRO1: Routing table now shows a route to 10.1.152.0/24. Ping to SRV1 from BRO1 succeeds.
	CLT2: Ping to SRV1 still fails. Traceroute now reaches CRO1 and times out after that.
	BRO1: Ping to SRV1 sourced from interface Fa 0/1.17 fails. Conclusion: Problem may be caused by return path from SRV1 to subnet 10.1.160.64/26.
	CSW2: Subnet 10.1.160.64/26 is not present in the routing table on CSW2.
	CRO1: Subnet 10.1.160.64/26 is present in the routing table as an EIGRP route. The route is marked as "Redistributing via ospf 100", but there is no line that says "Advertised..."
	CRO1: Redistribution from EIGRP to OSPF has been configured without any additional parameters.
	Hypothesis: Problem is similar to the redistribution from EIGRP to OSPF. Seed metric needs to be specified.
	CRO1: Configuration changed: Added metric to redistribution from EIGRP to OSPF (cost 100). Both prechange and postchange configurations were saved in flash on the switch. Communicated this information to team members. Note: After issuing the redistribution command the router responded with "% Only classful networks will be redistributed."
	CRO1: Output of show ip route did not change.

Trouble Ticket	Actions and results
	Research OSPF redistribution: subnets option is necessary to redistribute non-classful networks.
	CRO1: Configuration changed: Added subnets option to the redistribution from EIGRP to OSPF. Kept configured metric of 100 for clarity and consistency. Both pre- and post-change configurations were saved in flash on the switch. Communicated this information to team members.
	CRO1: Network 10.1.160.64/26 shows in routing table as "Advertised by ospf 100 metric 100 subnets". An external LSA for 10.1.160.64 is now also present in the OSPF database.
	CLT2: Ping to SRV1 succeeds. Browsing to http://www.isp3.local succeeds.
	Check with team member 3 who works on Trouble Ticket M: Ticket M was resolved.
	CRO2: Verify configuration. Redistribution configuration is identical to the original configuration of CRO1.
	CRO2: Configuration changed: Added metrics to redistribution from OSPF to EIGRP (bandwidth 10 Mb/s, delay 1 msec, reliability 255, load 1, MTU 1500). Added subnets option and metric of 100 to the redistribution from EIGRP to OSPF. Both pre- and post-change configurations were saved in flash on the switch. Communicated this information to team members.
	BRO1: EIGRP topology table shows three possible routes to 10.1.152.0/24 as expected.
	CSW2: The routing table of CSW2 shows two routes to subnet 10.1.160.64/26 as expected.
	Problem fixed. Documented changes. Backed up configurations. Communicated to team members. Closed ticket.

Key Clue: Route Not Advertised

- On router CRO1, which redistributes from OSPF to EIGRP, the route is:
 - Marked as “Redistributing via eigrp 1”
 - Not marked as “Advertised by eigrp 1”
- This shows that redistribution is configured, but not redistributing the route.

```
CRO1#show ip route 10.1.152.0 255.255.255.0
Routing entry for 10.1.152.0/24
  Known via "ospf 100", distance 110, metric 2, type inter area
  Redistributing via eigrp 1
  Last update from 10.1.192.1 on FastEthernet0/0, 03:37:17 ago
  Routing Descriptor Blocks:
    10.1.192.9, from 10.1.220.253, 03:37:17 ago, via FastEthernet0/1
      Route metric is 2, traffic share count is 1
    * 10.1.192.1, from 10.1.220.252, 03:37:17 ago, via FastEthernet0/0
      Route metric is 2, traffic share count is 1
```

There are no obvious clues that show that the missing metric on the **redistribute ospf 100** command under the **router eigrp 1** configuration is what causes network 10.1.152.0/24 (and all other OSPF learned routes) not to be redistributed into EIGRP. The diagnosis itself, however, is supported by the output of the **show ip route 10.1.152.0 255.255.255.0** command on router CRO1.

The output of this command includes a line that states “Redistributing via eigrp1,” which indicates that the route has been selected for redistribution via EIGRP. However, if the route would actually be redistributed, there would also be a line stating “Advertised by eigrp 1.” Because that line is missing, you can conclude that the redistribution has been configured but the route is not actually being redistributed.

Researching the documentation of redistribution should eventually lead to the hypothesis that configuring a seed metric is a mandatory step for EIGRP redistribution to work.

Key Clue: Only Classful Networks Will Be Redistributed

- When you configure redistribution from any source into OSPF and do not add the **subnets** option to the **redistribute** command, the router responds with “% Only classful networks will be redistributed.”
- Without the **subnets** option, only classful networks will be redistributed, and other prefixes will not be advertised.

```
CRO1(config-router)#redistribute eigrp 1 metric 100  
% Only classful networks will be redistributed
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--57

After you have resolved the OSPF to EIGRP redistribution problem by adding a seed metric to the redistribution, a likely approach is to try to resolve the EIGRP to OSPF redistribution in the same manner and configure a metric as an option to the **redistribute** command.

When you configure redistribution from any source into OSPF and forget to add the **subnets** option to the **redistribute** command, the router responds with “% Only classful networks will be redistributed.” This serves as a reminder that without the **subnets** option, only classful networks will be redistributed and other prefixes will not be advertised.

This message might serve as a hint that causes you to research OSPF redistribution and find the function of the **subnets** keyword.

Trouble Ticket K Checkpoints

Minimum checkpoints to prove that you have resolved this trouble ticket:

- Client PC CLT2 can ping server SRV1.
- Client PC CLT2 can use a web browser to connect to <http://www.isp3.local>.
- You have documented your process, your solution, and any changes that you have made to the device configurations.

What else should you have checked?

Are there any unresolved issues?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-58

The figure shows a list of minimum requirements that should be met to consider this trouble ticket to be resolved.

Note that the second point, the connectivity to <http://www.isp3.local>, is dependent on the successful resolution of Trouble Ticket M. Depending on the order in which your team addressed the tickets, Trouble Ticket M might have been resolved by the time you have resolved the redistribution problems. If this was not the case, you need to wait for ticket M to be completed before this ticket can be closed.

Suggested Solution

Correcting the configurations of routers CRO1 and CRO2 as follows can restore the connectivity from client PC CLT2 to server SRV1.

Suggested Configuration Changes

- On router CRO1, add metrics to the redistribution from OSPF to EIGRP and add the subnets keyword on the redistribution from EIGRP to OSPF.

```
CRO1(config)#router eigrp 1
CRO1(config-router)#redistribute ospf 100 metric 100000 10 255 1 1500
CRO1(config-router)#router ospf 100
CRO1(config-router)#redistribute eigrp 1 metric 100 subnets
```

- On router CRO2, change the configuration in a similar manner.

```
CRO2(config)#router eigrp 1
CRO2(config-router)#redistribute ospf 100 metric 100000 10 255 1 1500
CRO2(config-router)#router ospf 100
CRO2(config-router)#redistribute eigrp 1 metric 100 subnets
```

- In the example, a metric is configured on the redistribution from EIGRP to OSPF. This is not strictly required, but good practice.
- The exact value of the chosen EIGRP metrics is irrelevant as long as they are consistently applied on CRO1 and CRO2.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-59

As an alternative to specifying the EIGRP metrics as an option on the **redistribute** command, you can also use the **default-metric** command under the **router eigrp 1** configuration to specify the seed metrics to be used for redistribution.

The actual choice of metric values is largely irrelevant, as long as the configuration is consistent between routers CRO1 and CRO2. The values chosen here are the metric values that are typical for a directly connected Fast Ethernet interface.

In this example, a metric is also specified for the redistribution from EIGRP to OSPF. Although it is not strictly necessary, it is good habit to specify a seed metric when configuring redistribution.

Trouble Ticket L: No Connectivity from Client PC CLT3

The text introducing this trouble ticket was the following:

After the implementation of OSPF, the connectivity from client PC CLT3, which uses router BRO2 as its default gateway, to server SRV1 at headquarters is tested. A ping from client PC CLT3 to server SRV1 fails. The connectivity problem is not limited to SRV1. An attempt to browse to <http://www.isp3.local> also fails.

Your task is to diagnose this problem and, if possible, resolve it. Connectivity from PC CLT3 to server SRV1 and to server <http://www.isp3.local> on the Internet is mandatory for this phase of the migration to be considered successful.

Trouble Ticket L: Review and Discuss

How did your team approach Trouble Ticket L?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you accomplish the goal of restoring the connectivity from client PC CLT3 to the headquarters network and the Internet?
- How did you verify that you accomplished your goal?
- Were there any implementation choices that you made and if so, what were those choices?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-10

The connectivity problem in this ticket is caused by two mismatches between the OSPF configuration on router BRO2 and the OSPF configuration on routers CRO1 and CRO2.

On routers CRO1 and CRO2, the WAN links leading to router BRO2 have been configured to be part of area 11, in accordance with the specifications in the introduction of the trouble ticket. On router BRO2, all interfaces have been added to area 111. This prevents router BRO2 from becoming neighbors with routers CRO1 and CRO2.

The second issue that prevents the proper establishment of a neighbor relationship between router BRO2 and routers CRO1 and CRO2 is a mismatch in the area type. Area 11 has been defined as a totally stubby area on routers CRO1 and CRO2 (in accordance with the specifications), while on router BRO2 the area has not been defined as a stub area.

Although many possible approaches can be used to solve this problem, the following example of a troubleshooting log shows you a method that could have been used to come to a resolution in a structured manner.

Trouble Ticket	Actions and results
Ticket L	CLT3: Verified problem: Cannot ping to SRV1. Cannot browse to http://www.isp3.local.
	CLT3: Ping to default gateway (10.1.160.254) succeeds. Traceroute to SRV1 (10.1.152.1) stops at router BRO2.
	BRO2: Routing table shows no route to 10.1.152.0/24. Routing table only shows connected routes.
	BRO2: No OSPF neighbors have been established. All relevant interfaces have been enabled for OSPF. WAN interfaces are not configured as passive interfaces.
	BRO2: Pings to directly connected WAN IP addresses of CRO1 and CRO2 succeed.
	BRO2: debug ip ospf adj reveals an area mismatch. Received hellos have area 11. Router BRO2 is configured for area 111. Disabled debug.
	Verify implementation guidelines: Area should be area 11.
	BRO2: Configuration changed: All references to area 111 were changed to area 11. Both pre- and post-change configurations were saved in flash on the switch. Communicated this information to team members.
	BRO2: All interfaces are now enabled in area 11. Neighbors still have not been established.
	BRO2: debug ip ospf packet reveals that hellos are received from CRO1 and CRO2. debug ip ospf adj does not yield any clues. Disabled debugs.
	CRO2: debug ip ospf packet reveals that hellos are received from BRO2. debug ip ospf adj does not yield any clues. Disabled debugs.
	BRO2: debug ip ospf event reveals a "mismatched Stub/Transit area option bit". Area 11 on router BRO2 is not configured as a stub area. Disabled debugs.
	CRO1 & CRO2: Area 11 is configured as a totally stubby area.
	Verify implementation guidelines: Area 11 should be a totally stubby area.
	BRO2: Configuration changed: Area 11 is configured as a stub area. Both pre- and post-change configurations were saved in flash on the switch. Communicated this information to team members.
	BRO2: OSPF neighbors have been established. Route to 10.1.152.0/24 is not visible in the routing table, but a default route is present. This is the expected result for a totally stubby area.
	CLT3: Ping to SRV1 succeeds. Browsing to http://www.isp3.local succeeds.
	Problem fixed. Documented changes. Backed up configurations. Communicated to team members. Closed ticket.

Key Clue: Area Mismatch in Debug

- Enabling **debug ip ospf adj** on router BRO2 reveals the following:
 - Router BRO2 receives hellos on its serial interfaces, which it considers to be in area 111.
 - The sending routers (CRO1 and CRO2) advertise area 11 in their hellos.

```
BRO2#debug ip ospf adj
OSPF adjacency events debugging is on
BRO2#show logging | begin OSPF
*Apr 24 02:00:13.226 PDT: OSPF: Rcv pkt from 10.1.194.13,
Serial0/0/0.112, area 0.0.0.111
      mismatch area 0.0.0.11 in the header
*Apr 24 02:00:16.858 PDT: OSPF: Rcv pkt from 10.1.193.5,
Serial0/0/1, area 0.0.0.111
      mismatch area 0.0.0.11 in the header
*Apr 24 02:00:21.658 PDT: OSPF: Rcv pkt from 10.1.194.5,
Serial0/0/0.111, area 0.0.0.111
      mismatch area 0.0.0.11 in the header
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-11

The only way to solve this problem without resorting to the use of **debug** commands, but by using **show** commands only, is the careful comparison of configurations between router BRO2 and routers CRO1 and CRO2. Area mismatches or flag mismatches, such as a stub area mismatch, are not revealed by any of the **show** commands.

Enabling the **debug ip ospf adj** command can reveal the area mismatch. This command reveals mismatches in the parameters contained in the OSPF packet headers, such as a mismatched area number, but not the other parameters contained in the hello packets, such as hello timers,

In this case, the output reveals that the area in the hello packets received on router BRO2's serial interfaces is area 11, while router BRO2 considers those interfaces to be in area 111.

Key Clue: Stub Flag Mismatch in Debug

- Enabling **debug ip ospf event** on router BRO2 reveals that it is receiving hellos with a mismatched stub/transit area option bit from routers CRO1 and CRO2 on its serial interfaces.
- This issue is not revealed by the **debug ip ospf adj** command.

```
BRO2#debug ip ospf event
OSPF adjacency events debugging is on
BRO2#clear logging
Clear logging buffer [confirm]
BRO2#show logging | begin OSPF
*Apr 24 02:23:01.567 PDT: OSPF: Rcv hello from 10.1.220.1 area 11
from Serial0/0/0.111 10.1.194.5
*Apr 24 02:23:01.567 PDT: OSPF: Hello from 10.1.194.5 with
mismatched Stub/Transit area option bit
*Apr 24 02:23:03.151 PDT: OSPF: Rcv hello from 10.1.220.2 area 11
from Serial0/0/0.112 10.1.194.13
*Apr 24 02:23:03.151 PDT: OSPF: Hello from 10.1.194.13 with
mismatched Stub/Transit area option bit
*Apr 24 02:23:06.823 PDT: OSPF: Rcv hello from 10.1.220.2 area 11
from Serial0/0/1 10.1.193.5
*Apr 24 02:23:06.823 PDT: OSPF: Hello from 10.1.193.5 with
mismatched Stub/Transit area option bit
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOTv1.0-5-2

Unfortunately, the same debug does not reveal the mismatched stub area configuration between router BRO2 and routers CRO1 and CRO2. To reveal this, the **debug ip ospf event** command can be used.

This command reveals that there is a mismatch in the stub/transit area option bit. This is a bit set in the OSPF hello packets that indicates whether the router considers this area to be a stub area or not. The debug reveals that this setting is mismatched between router BRO2 and routers CRO1 and CRO2. Verifying the OSPF configuration on these routers subsequently reveals that routers CRO1 and CRO2 have been configured with the **area 11 stub no-summary** command, while router BRO2 does not have a corresponding **area 11 stub** command in its configuration.

Trouble Ticket L Checkpoints

Minimum checkpoints to prove that you have resolved this trouble ticket:

- Client PC CLT3 can ping server SRV1.
- Client PC CLT3 can use a web browser to connect to <http://www.isp3.local>.
- You have documented your process, your solution, and any changes that you have made to the device configurations.

What else should you have checked?

Are there any unresolved issues?

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0-6-B

The figure shows a list of minimum requirements that should be met to consider this trouble ticket to be resolved.

Note that the second point, the connectivity to <http://www.isp3.local>, is again dependent on the successful resolution of Trouble Ticket M. Depending on the order in which your team addressed the tickets, Trouble Ticket M might have been resolved by the time you have resolved the redistribution problems. If this was not the case, you need to wait for ticket M to be completed before this ticket can be closed.

Another point to consider is which minimum extra verification steps you should take before deciding whether the OSPF migration was successful and the OSPF network is ready to be taken into production. At the very least, you should verify if all the relevant branch office subnets are available on all routers at the headquarters location and, vice versa, if all headquarters subnets are available at both branch routers. More rigorous testing would include connectivity tests from subnet to subnet based on a matrix that specifies which subnets should be able to connect to which other subnets. Finally, failover tests should be executed to ensure that connectivity is also guaranteed when links or devices fail.

A test plan including these elements should be created before the actual migration takes place. At the same time, one should determine which parts of the test plan need to be successfully completed in order to go through with the migration and which elements would be a cause to roll back if they cannot be successfully completed.

Suggested Solution

Correcting the configuration of router BRO2 as follows restores the connectivity from client PC CLT3 to server SRV1.

Suggested Configuration Changes

- On router BRO2 change all **network** statements under the **router ospf** process to assign the interfaces that are enabled for OSPF to area 11 instead of area 111.

```
BRO2(config)#router ospf 100
BRO2(config-router)# no network 10.1.160.0 0.0.3.255 area 111
BRO2(config-router)# no network 10.1.193.6 0.0.0.0 area 111
BRO2(config-router)# no network 10.1.194.6 0.0.0.0 area 111
BRO2(config-router)# no network 10.1.194.14 0.0.0.0 area 111
BRO2(config-router)# no network 10.1.221.2 0.0.0.0 area 111
BRO2(config-router)# network 10.1.160.0 0.0.3.255 area 11
BRO2(config-router)# network 10.1.193.6 0.0.0.0 area 11
BRO2(config-router)# network 10.1.194.6 0.0.0.0 area 11
BRO2(config-router)# network 10.1.194.14 0.0.0.0 area 11
BRO2(config-router)# network 10.1.221.2 0.0.0.0 area 11
```

- In addition, area 11 should be configured as a stub area.

```
BRO2(config)#router ospf 100
BRO2(config-router)#area 11 stub
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-14

Network statements using different wildcard masks from those in the figure can be used as well, as long as they match the same interfaces.

Technically, the problem could also be solved by changing the configuration on routers CRO1 and CRO2 to area 111 instead of changing the configuration on router BRO2 to area 11 as the example shows. However, because the text that introduces the trouble tickets clearly states that area 11 is the assigned area for the branch, this is not considered a valid solution.

In the same way, removing the **area 11 stub no-summary** command from routers CRO1 and CRO2 is not considered a valid solution either, because the implementation guidelines specify that the area used in the branch should be a totally stubby area.

Trouble Ticket M: Internet not Reachable from Client PC CLT1

The text introducing this trouble ticket was the following:

After the implementation of OSPF, the connectivity from client PC CLT1 to the Internet does not seem to be working. A ping from client PC CLT1 to server SRV1 succeeds, but an attempt to browse to <http://www.isp3.local> fails.

Your task is to diagnose this problem and, if possible, resolve it. Connectivity from PC CLT1 to server <http://www.isp3.local> on the Internet is mandatory for this phase of the migration to be considered successful.

Trouble Ticket M: Review and Discuss

How did your team approach Trouble Ticket M?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you accomplish the goal of restoring the connectivity from client PC CLT1 to the Internet?
- How did you verify that you accomplished your goal?
- Were there any implementation choices that you made and if so, what were those choices?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--5-5

The problem in this ticket is caused by a mismatch in the OSPF hello and dead timers. Routers IRO1 and IRO2 have been configured to use 5-second hellos and a 15-second dead timer on the transit VLAN 129, while routers CSW1 and CSW2 use the default 10-second hello and 40-second dead timer. An OSPF router will not become neighbors with another router on the same segment if they are not using the same timers.

To resolve this problem, the timers need to be matched on all routers on VLAN 129. Therefore, one of the implementation choices you need to make during the resolution of this ticket is the value of the hello and dead timer. What the best value is for the timers depends on the convergence times that are required. This requirement is unknown, so it is not possible to establish an exact best value for these timers.

Many possible methods could be used to solve this problem. The following example of a troubleshooting log shows a methodical approach to resolve this problem.

Trouble Ticket	Actions and results
Ticket M	CLT1: Verified problem: Cannot browse to http://www.isp3.local. Ping to SRV1 succeeds.
	CLT1: DNS cannot resolve address for the name www.isp3.local.
	CSW1: No default route is present in the routing table.
	IRO1: Static default route is present in the routing table. Ping to next hop for default route (ISP1) succeeds.
	IRO1: Verify OSPF configuration: Static routes are not redistributed, but a default-information originate command is present under the router ospf configuration.
	IRO1: External LSA 0.0.0.0 is present in the OSPF database for area 100 generated by IRO1. A second entry generated by router IRO2 is also present.
	IRO1: Only router IRO2 is an OSPF neighbor on interface FastEthernet 0/1. Expected three neighbors: IRO2, CSW1 and CSW2.
	IRO1: Pings to CSW1 (10.1.192.17) and CSW2 (10.1.192.18) succeed.
	IRO1: debug ip ospf packet reveals that hellos are received from CSW1 and CSW2.
	IRO1: debug ip ospf event reveals mismatched hello parameters "Dead R 40 C 15, Hello R 10 C 5 Mask R 255.255.255.248 C 255.255.255.248"
	IRO1: Verify configuration: Hello timer is set to 5 seconds and dead timer to 15 seconds on interface Fa 0/1.
	IRO2: Verify configuration: Hello timer is set to 5 seconds and dead timer to 15 seconds on interface Fa 0/0.
	CSW1 & CSW2: Verify configuration: Timer values are set to default on interface Vlan 129.
	Verify implementation guidelines: Timer values are not mentioned.
	Discuss with team members: IRO1 and IRO2 are the only routers on which timer values have been changed. Decision: Revert back to default values on IRO1 and IRO2. Timer tuning may be done later as a separate project.
	IRO1 & IRO2: Configuration changed: Set hello and dead timer back to default values. Both pre- and post-change configurations were saved in flash on the switch. Communicated this information to team members.
	IRO1: CSW1, CSW2 and IRO2 are now all listed as neighbors on interface Fa 0/1.
	CSW1: Two default routes are now present in the routing table: One via IRO1 and one via IRO2.
	CLT1: Browsing to http://www.isp3.local succeeds.
	Problem fixed. Documented changes. Backed up configurations. Communicated to team members. Closed ticket.

Key Clue: Parameter Mismatch in Debug

- Enabling **debug ip ospf event** on router IRO1 reveals that it is receiving hellos with mismatched parameters.

```
IRO1#debug ip ospf event
OSPF adjacency events debugging is on
IRO1#clear logging
Clear logging buffer [confirm]
IRO1#show logging | begin OSPF
Apr 24 06:03:43.509 PDT: OSPF: Rcv hello from 10.1.220.4 area 100 from
FastEthernet0/1 10.1.192.20
Apr 24 06:03:43.509 PDT: OSPF: End of hello processing
Apr 24 06:03:44.093 PDT: OSPF: Rcv hello from 10.1.220.253 area 100 from
FastEthernet0/1 10.1.192.18
Apr 24 06:03:44.093 PDT: OSPF: Mismatched hello parameters from 10.1.192.18
Apr 24 06:03:44.093 PDT: OSPF: Dead R 40 C 15, Hello R 10 C 5 Mask R
255.255.255.248 C 255.255.255.248
Apr 24 06:03:43.509 PDT: OSPF: Rcv hello from 10.1.220.4 area 100 from
FastEthernet0/1 10.1.192.20
Apr 24 06:03:43.509 PDT: OSPF: End of hello processing
Apr 24 06:03:44.093 PDT: OSPF: Rcv hello from 10.1.220.253 area 100 from
FastEthernet0/1 10.1.192.18
Apr 24 06:03:44.093 PDT: OSPF: Mismatched hello parameters from 10.1.192.18
Apr 24 06:03:44.093 PDT: OSPF: Dead R 40 C 15, Hello R 10 C 5 Mask R
255.255.255.248 C 255.255.255.248
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOTv1.0-5-98

Like Trouble Ticket L, this problem needs to be solved either through debugging or through configuration comparison. The mismatched hello and dead timers are easily overlooked in the configuration because they are configured on the interface, not under the **router ospf** process.

The **debug ip ospf event** command output shows the problem when it is enabled. It displays the message “Mismatched hello parameters from 10.1.192.18” that flags the source of the hello that contains the mismatched parameters, and in addition it displays the mismatched parameters as “Dead R 40 C 15, Hello R 10 C 5 Mask R 255.255.255.248 C 255.255.255.248.” The values marked with “R” represent the received values, while the values marked with “C” represent the configured values. From this, you can see that the received hello and dead timers are 10 and 40 seconds, respectively, while the locally configured values are 5 and 15 seconds, respectively.

Trouble Ticket M Checkpoints

Minimum checkpoints to prove that you have resolved this trouble ticket:

- Client PC CLT1 can use a web browser to connect to `http://www.isp3.local`.
- You have documented your process, your solution, and any changes that you have made to the device configurations.
What else should you have checked?

Are there any unresolved issues?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-17

The figure shows a list of minimum requirements that should be met to consider this trouble ticket to be resolved.

Note that the successful resolution of this ticket is a prerequisite for the successful resolution of Trouble Tickets K and L, because the Internet connectivity of clients CLT2 and CLT3 is dependent on the correct propagation of a default route from routers IRO1 and IRO2 to routers CSW1 and CSW2 and further.

Suggested Solution

Correcting the configuration of routers IRO1 and IRO2 as follows restores the connectivity from client PC CLT1 to server www.isp3.local.

Suggested Configuration Changes

- On router IRO1 change the hello and dead timer back to the default values on interface FastEthernet 0/1.

```
IRO1(config)#interface FastEthernet 0/1
IRO1(config-if)#default ip ospf hello-interval
IRO1(config-if)#default ip ospf dead-interval
```

- On router IRO2 change the hello and dead timer back to the default values on interface FastEthernet 0/0.

```
IRO2(config)#interface FastEthernet 0/0
IRO2(config-if)#default ip ospf hello-interval
IRO2(config-if)#default ip ospf dead-interval
```

- As an alternative, the configuration on CSW1 and CSW2 could be changed to match IRO1 and IRO2.

```
CSW1(config)#interface Vlan 129
CSW1(config-if)#ip ospf hello-interval 5
CSW1(config-if)#ip ospf dead-interval 15
```

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOTv10--5-8

To solve the problem of the mismatched timers, either the timers on routers IRO1 and IRO2 need to be changed to match the default timers that are used by routers CSW1 and CSW2, or routers CSW1 and CSW2 need to be changed to match the configured timers of routers IRO1 and IRO2.

Technically, these two solutions are equal in the sense that they both accomplish the goal of restoring the OSPF adjacencies between the routers.

What are the advantages and disadvantages of each of these two solutions?

One of the factors to take into account is consistency between configurations. Changing the hello and dead timers only on the transit VLAN 129 between the routers CSW1, CSW2, IRO1, and IRO2 will create a situation where different timers are used for different links and configuration at the interface level is not consistent on all routers. This increases the chance of creating future failures similar to the failure experienced in this ticket. If you decide to tune the timers, it is recommended to tune the timers in a consistent manner throughout your network, document the recommended values, and include these values in your configuration templates.

Another factor is convergence speed. In the case of an indirect failure, the reduced dead timer will allow the discovery of a lost neighbor to be faster: 15 seconds as opposed to the default of 40 seconds. What the acceptable convergence time is for your network, and therefore the best timer values, depends on the requirements of your business applications. In this scenario, there is not enough information to know whether changing the hello and dead timers is needed for this network to meet the established requirements.

Trouble Ticket N: OSPF Authentication not Working

The text introducing this trouble ticket was the following:

Yesterday one of the engineers suggested that it might be a good idea to secure the OSPF implementation by using MD5 authentication between the routers. Because this could complicate the implementation, it was decided that it was too late to include this in the implementation for all areas now. However, to test the concept it was decided to enable the authentication for area 1 only to test the concept. If this test is successful, the authentication will be added to other areas during the second phase of the implementation. If the test is not successful, a separate project will be initiated to implement the authentication.

One of your colleagues has enabled MD5 authentication for area 1 on VLAN 111, which is used as a transit link between the core switches CSW1 and CSW2 in area 1. Unfortunately, the neighbor relationship between CSW1 and CSW2 on VLAN 111 is not established.

Your task is to diagnose this problem and, if possible, resolve it. The inability to resolve the authentication problem is not considered a reason to roll back the OSPF migration. You are allowed to remove the authentication for area 1 if necessary. However, in this case you still need to make sure that the neighbor relationship between switches CSW1 and CSW2 on VLAN 111 in area 1 is established correctly.

Trouble Ticket N: Review and Discuss

How did your team approach Trouble Ticket N?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you manage to establish the adjacency between CSW1 and CSW2 on VLAN 111 using MD5 authentication?
- How did you verify that you accomplished your goal?
- If you did not manage to make the authentication work, what did you do to establish the required adjacency on VLAN 111?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOTv1.0--5-9

The problem in this ticket is caused by two different issues.

One of the issues is not related to the authentication itself. On both routers CSW1 and CSW2, all interfaces are configured as passive interfaces by default. On router CSW1, interface Vlan 111 has been specifically enabled. On router CSW2, this was not configured and as a result, interface Vlan 111 is a passive interface.

The second issue is caused by a mismatch in the configured authentication-key between routers CSW1 and CSW2.

The following example of a troubleshooting log shows you a methodical approach to resolve this problem.

Trouble Ticket	Actions and results
Ticket N	CSW1: Verified problem: CSW2 is not listed as a neighbor on VLAN 111.
	CSW1: Interface Vlan111 has been enabled for OSPF in area 1. MD5 authentication has been enabled using key 1.
	CSW2: Interface Vlan111 has been enabled for OSPF in area 1. MD5 authentication has been enabled using key 1.
	CSW1: Interface Vlan111 is not passive.
	CSW2: Interface Vlan111 is listed as passive in the show ip ospf interface command.
	CSW2: Configuration changed: Configured interface Vlan111 not to be passive. Both pre- and post-change configurations were saved in flash on the switch. Communicated this information to team members.
	CSW2: CSW1 and CSW2 have not become neighbors on VLAN 111.
	CSW2: debug ip ospf adj reveals "Mismatch Authentication Key - Message Digest Key 1"
	CSW2: Verify key string: Using key 1 with string cisco
	CSW1: Verify key string: Using key 1 with string cisco. Keys look identical.
	Plan: Remove authentication first. Reconfigure after adjacency has been successfully established to rule out non-authentication-related problems.
	CSW1 & CSW2: Configuration changed: Removed authentication and keys. Both prechange and postchange configurations were saved in flash on the switch. Communicated this information to team members.
	CSW1: CSW1 and CSW2 are neighbors on VLAN 111 now.
	CSW1 & CSW2: Configuration changed: Reconfigured MD5 authentication using key 1 and key-string cisco. Both pre- and post-change configurations were saved in flash on the switch. Communicated this information to team members.
	CSW1: CSW1 and CSW2 are still neighbors.
	Problem fixed. Documented changes. Backed up configurations. Communicated to team members. Closed ticket.

Key Clue: Interface Marked as Passive

- The **show ip ospf interface** command shows that interface Vlan 111 is configured as a passive interface on CSW2.

```
CSW2#show ip ospf interface Vlan 111
Vlan111 is up, line protocol is up
Internet Address 10.1.151.194/30, Area 1
Process ID 100, Router ID 10.1.220.253, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 10.1.220.253, Interface address 10.1.151.194
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
No Hellos (Passive interface)
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 19/19, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
Youngest key id is 1
```

The first issue that prevents the adjacency between routers CSW1 and CSW2 to be established is the fact that interface Vlan 111 is configured as a passive interface on router CSW2. This is displayed in the output of the **show ip ospf interface Vlan 111** command. This cannot be seen in the output of the **show ip ospf interface brief** command.

A careful comparison between the **router ospf** configuration sections on routers CSW1 and CSW2 can also reveal that on router CSW1 there is an explicit **no passive-interface Vlan111** command under the **router ospf** configuration, which is missing on router CSW2.

Key Clue: Authentication Mismatch in Debug

- Enabling **debug ip ospf adj** on router CSW1 or CSW2 reveals that there is a mismatched authentication key.

```
CSW2#clear logging
Clear logging buffer [confirm]
CSW2#debug ip ospf adj
OSPF adjacency events debugging is on
CSW2#show logging | include OSPF
Apr 24 08:02:09.829 PDT: OSPF: Send with youngest Key 1
Apr 24 08:02:11.230 PDT: OSPF: Rcv pkt from 10.1.151.193, Vlan111 : Mismatch
Authentication Key - Message Digest Key 1
Apr 24 08:02:19.837 PDT: OSPF: Send with youngest Key 1
Apr 24 08:02:21.238 PDT: OSPF: Rcv pkt from 10.1.151.193, Vlan111 : Mismatch
Authentication Key - Message Digest Key 1
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-21

The second problem, the mismatched authentication password, is not very easily spotted in the configuration because the only difference is that on CSW2 the password has a space appended to the word “cisco,” while on CSW1, that trailing space is not present. Visually this is almost impossible to spot.

However, the **debug ip ospf adj** command clearly shows that a key mismatch is causing the adjacency not to be established. In cases like these, it is a good strategy to first remove the authentication and then reconfigure it. This serves two purposes. To begin with, it allows you to confirm that the neighbor relationship will be established without the complicating factor of authentication. Secondly, by reconfiguring, you eliminate potential typing errors that you might have been overlooking. However, to rule out typing errors, it is important that you do not simply paste back the original configuration.

Trouble Ticket N Checkpoints

Minimum checkpoints to prove that you have resolved this trouble ticket:

- Switch CSW1 and CSW2 have established a neighbor relationship in area 1 on VLAN 111.
- MD5 authentication is used between switch CSW1 and switch CSW2 for area 1.
- Or, if the authentication cannot be made to work, authentication is removed from the configurations of CSW1 and CSW2 entirely.
- You have documented your process, your solution, and any changes that you have made to the device configurations.

Are there any unresolved issues?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-2

The figure shows a list of minimum requirements that should be met to consider this trouble ticket to be resolved.

Note that it is not strictly required that you manage to make the OSPF authentication between routers CSW1 and CSW2 work, as long as routers CSW1 and CSW2 have successfully established an adjacency on VLAN 111.

To achieve this result, it is important to make a timely assessment whether you will be able to get the authentication to work and give up your attempts in time if you are not able. If you keep troubleshooting until the last minute, you might end up not accomplishing the main objective of establishing the adjacency in the end.

Suggested Solution

Correcting the configuration of routers CSW1 and CSW2 as follows enables the OSPF authentication and establishes the adjacency between routers CSW1 and CSW2.

Suggested Configuration Changes

- On router CSW2 exclude interface Vlan 111 from the **passive-interface default** configuration.

```
CSW2(config)#router ospf 100
CSW2(config-router)#no passive-interface Vlan111
```

- On router CSW1 change OSPF message digest key to “cisco”:

```
CSW1(config)#interface Vlan 111
CSW1(config-if)#no ip ospf message-digest-key 1
CSW1(config-if)#ip ospf message-digest-key 1 md5 cisco
```

- As an alternative, authentication can be removed entirely on routers CSW1 and CSW2.

```
CSW1(config)#router ospf 100
CSW1(config-router)#no area 1 authentication message-digest
CSW1(config-router)#interface Vlan 111
CSW1(config-if)#no ip ospf message-digest-key 1
```

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0-6-20

This ticket cannot be successfully resolved without enabling the transmission and reception of OSPF hello packets on interface Vlan 111 on router CSW2 by excluding it from the configured passive-interface default statement.

After that, you have a choice. The authentication could be made to work by changing the key-string to “cisco” on router CSW1 to match the configured key-string on router CSW2. Or, you could also replace the used key-strings with a different key-string. The description of the ticket did not prescribe a specific string to be used.

If you could not get the authentication to work, it was also a valid option to remove the authentication entirely. To achieve this, you should execute the commands listed as the third option in the figure on both routers CSW1 and CSW2.

It is important, however, that you make a timely and consistent choice regarding the final solution that you want to use.

Consolidation

This topic describes the primary lessons that could be learned from the lab exercise.

Discussion: Lessons Learned

Method and process:

- How could you improve your troubleshooting methods?
- What alternative methods did you discover?

Communication and procedures:

- How could the troubleshooting process be made more effective?
- What kind of procedures would be useful and why?

Technology and tools:

- Which tools were most useful during troubleshooting?
- Which tools could have improved the effectiveness of your process?
- Which useful Cisco IOS commands did you discover?

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0—5-38

Think about all the things that you learned during the lab itself and during the debrief discussions.

In addition to thinking of the methods, processes, and tools as they were used in the lab, reflect on how these would apply to your own organization. There is room to write down primary learning points in the Lab Debrief Notes section of the lab guide.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- You have reviewed and verified your lab results.
- You have consolidated the experiences and discoveries that all students got from the lab and you have derived a number of key learning points from these experiences.

Troubleshooting BGP

Overview

Enterprise networks might use Border Gateway Protocol (BGP) to exchange routing information in a controlled fashion with external parties such as Internet service providers or other providers of IP-based services. You can use BGP to exchange routing information between different regions within the enterprise network that are managed and administered by different organizational groups. BGP offers a toolkit to implement routing policies and control the flow of traffic to and from external parties such as service providers, or between the different regions of the network.

The exterior gateway protocol BGP is often used in combination with an interior gateway protocol such as Enhanced Interior Gateway Routing Protocol (EIGRP) or the Open Shortest Path First (OSPF) routing protocol. Understanding the mechanics of BGP and its interaction with interior gateway protocols is essential in order to troubleshoot complex routed networks that deploy BGP in an effective manner.

This lesson reviews the data structures used by BGP and the flow of routing information between routers running the BGP protocol, as well as the processing of routing information inside the router. In addition, you can use the Cisco IOS commands to gather information from the BGP data structures, and routing processes are reviewed and a case study is presented to illustrate the use of the commands as part of a structured troubleshooting process.

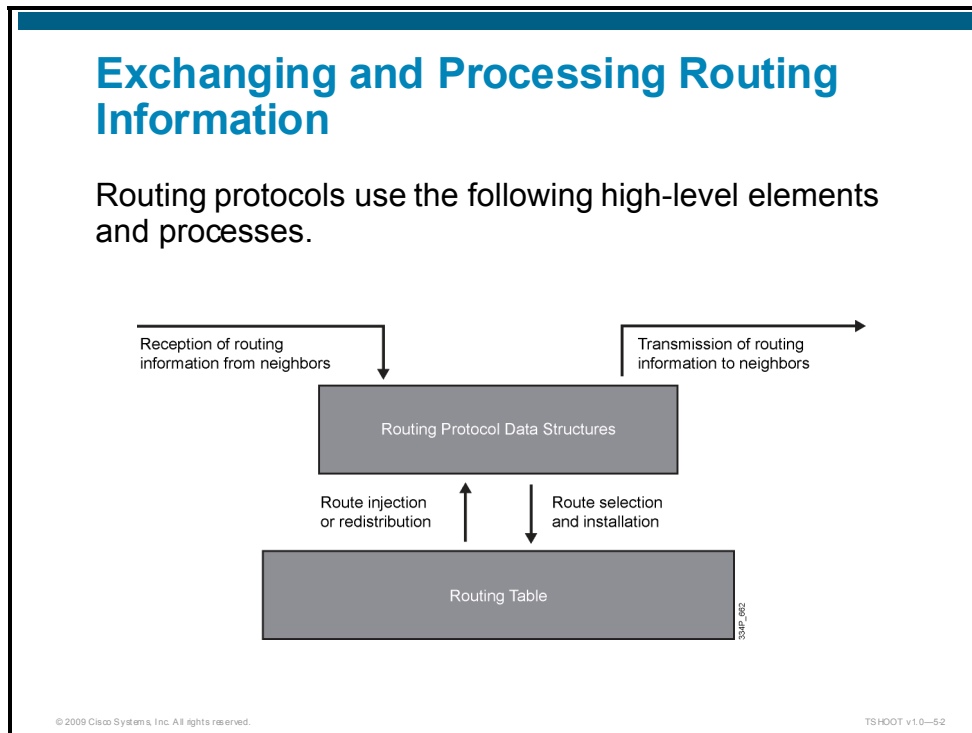
Objectives

Upon completing this lesson, you will be able to diagnose and resolve problems related to the exchange of routing information by use of BGP. This ability includes being able to meet these objectives:

- Apply your knowledge of BGP data structures to plan the gathering of necessary information as part of a structured approach to troubleshooting BGP routing problems
- Apply your knowledge of the processes that BGP uses to exchange routing information to interpret and analyze the information that is gathered during a BGP troubleshooting process
- Use Cisco IOS commands to gather information from the BGP data structures and track the flow of BGP routing information to troubleshoot BGP operation

BGP Data Structures

This topic describes the data structures that BGP uses to store routing information.



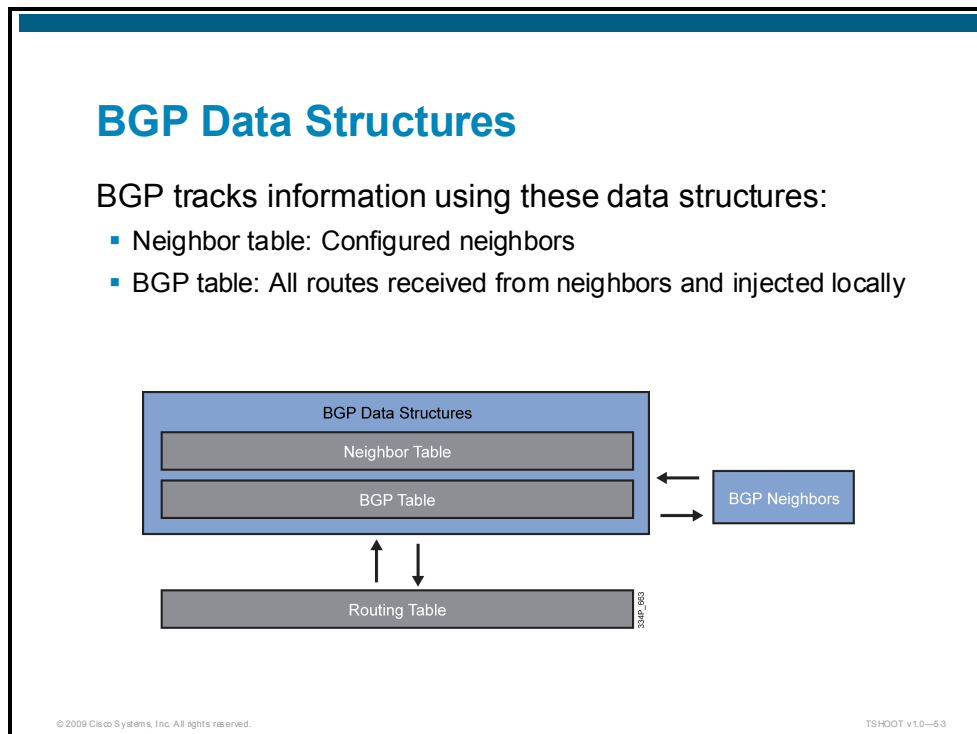
As an exterior gateway protocol (EGP), BGP fulfills a different role in enterprise networks when compared to interior gateway protocols (IGP), such as EIGRP or OSPF. BGP is not used to find the best paths within the enterprise network based on metrics such as bandwidth, delay, or path cost, but it is used to exchange routing information with external networks, such as Internet service providers, and to implement routing policies to control the flow of traffic to and from those external networks.

However, although its purpose is different, BGP is still a routing protocol in the sense that it exchanges information about the reachability of prefixes with other BGP routers, elects a best route for each of the prefixes that it has learned about, and installs those best routes in the routing table.

For any routing protocol, the following elements can be discerned:

- **Reception of routing information from neighbors:** One of the major differences with interior gateway protocols is that for BGP, its neighbors need not be directly connected. Neighbor relationships are predefined, not automatically discovered through a hello protocol. A TCP session is established between the predefined neighbors to exchange routing information, and this TCP session can span multiple router hops if necessary. Because the term “neighbor” inherently implies a sense of close proximity, an alternative commonly used term for two BGP routers that exchange information is “peer.” The terms “peer” and “neighbor” are used interchangeably when describing BGP. In the output of the Cisco IOS commands, the term “neighbor” is used.
- **Routing protocol data structures:** BGP has two main data structures: a neighbor table to keep track of the state of configured neighbors and its main data structure, and the BGP table, which it uses to store all the prefixes that it received from its neighbors.

- **Route injection or redistribution:** BGP does not automatically inject any routes into its BGP table. Routes learned from neighbors are placed in the BGP table and can be advertised out to other BGP neighbors. To inject prefixes into the BGP table locally and advertise them to BGP neighbors, these prefixes need to be specifically configured under the BGP routing process or redistributed. In either case, a prefix needs to be present in the routing table before it can be injected into the BGP table and advertised to BGP neighbors.
- **Route selection and installation:** BGP has a complex decision algorithm to compare routes received from its neighbors and select a best route for each prefix from the available options. Like any routing protocol, it will attempt to install the routes that it selected as best into the routing table.
- **Transmission of routing information to neighbors:** Routes that are selected as best routes in the BGP table can be advertised to other BGP routes. Several rules, such as the Internal Border Gateway Protocol (IBGP) split-horizon rule, govern the advertisement of BGP routes to neighbors. Also, access lists, prefix lists, and route maps are commonly applied to filter and manipulate the prefixes and their attributes before exchanging them with the neighbor. This type of filtering and manipulation can be performed either before transmitting the information to a neighbor or when receiving information from a neighbor.



BGP uses two main data structures to store its operational data, configured parameters, and statistics:

- **Neighbor table:** This table lists all neighbors that have been configured on this router by IP address. Among other things, this table stores the configured autonomous system (AS) number of the neighbor, whether the session is an internal or external session, the state of the session, the uptime of the neighbor, how many prefixes were exchanged with the neighbor, and many other statistics about the peer relationship.

- **BGP table:** This table, sometimes called the BGP Routing Information Base (RIB), stores all routes that were received from all the router's peers, together with all the BGP attributes that are associated with the route, such as the next hop, AS path, local preference, origin, multi-exit discriminator (MED) or metric, origin code, and community attributes. For each prefix, the BGP best path selection algorithm assesses the usability of the available paths and, if one or more usable paths exist, selects one of those paths as the best path. This path will subsequently be advertised to other BGP peers and BGP will attempt to install this route in the routing table. One of the checks that the BGP best path selection algorithm performs to assess whether a path is usable is to perform a routing table lookup on the IP address that is listed as the BGP next-hop attribute. If no match can be found in the routing table for the next-hop address, the route is not considered usable and will not be included as a best path candidate. By default, BGP will select only one best path for each prefix to be installed in the routing table. The BGP Multipath feature allows additional routes to be installed in the routing tables if they meet certain conditions.

For more details about the BGP best path selection algorithm, see the following document:

BGP Best Path Selection Algorithm:

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094431.shtml

BGP Routing Information Flow

This topic describes the flow of BGP routing information as it is passed from peer to peer and installed in the BGP tables.

BGP Routing Update Process

- BGP neighbors are explicitly configured.
- The configured IP addresses and AS numbers need to match between neighbors.
- On the initial discovery of a neighbor, full updates are exchanged.
- After the initial exchange, only triggered incremental updates are exchanged as long as the peering is not lost or reset.
- All received routes are stored in the BGP table (unless filtered).
- Only best routes are advertised to peers.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-54

BGP neighbors are explicitly configured, not automatically discovered based on a hello protocol. A BGP neighbor is configured by specifying its IP address and AS number. The router will attempt to establish a TCP session to the configured IP address on TCP port 179. Alternatively, it will accept incoming TCP sessions on port 179 if the source IP address matches one of its configured neighbor IP addresses.

After a TCP session has been successfully established, the routers send “OPEN” messages to exchange basic parameters and capabilities, such as autonomous system number, router ID, hold time, and supported address families. During this phase each router compares the received AS number to its configured AS number for the neighbor. If this does not match, the session is reset.

As a result of this process, the following issues are common causes for the successful establishment of a BGP peering to fail:

- There is no IP connectivity between the configured peer IP addresses. Because BGP peers are not necessarily directly connected, both routers need to have a route to the configured neighbor IP address in their routing table.
- The source IP address used by the router that initiates the session does not match the configured IP address on the receiving router.
- The advertised AS number of the peer does not match the locally configured AS number on one of the peers.

After the TCP session has been established and “OPEN” messages have been successfully exchange and accepted, BGP will start exchanging update messages on the TCP session.

BGP uses an incremental update process. When a BGP peer relationship is first established, each of the peers advertises its best route for each prefix that is present in its BGP table to its peer. Both peers subsequently install the received routes in the BGP table and execute the BGP best path selection algorithm to select the best path for each prefix based on the newly received information. Each time a new best path for a prefix is selected in the BGP table, an update for that prefix is sent to all relevant peers. When a prefix is removed from the BGP table, a “WITHDRAW” message for the prefix is sent to all relevant peers. To determine which peers need to be updated, the router applies several rules, such as the split-horizon rule and the IBGP split-horizon rule.

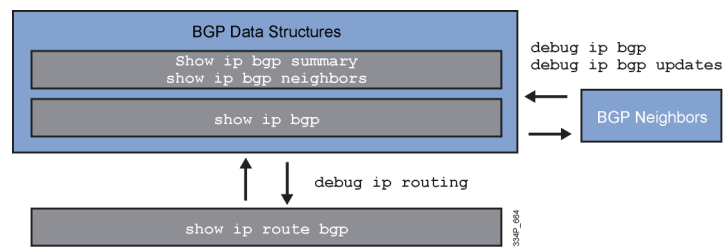
In addition, BGP updates are commonly filtered or manipulated by use of access lists, prefix lists, and route maps. These processes can be applied either upon reception of the updates, before the prefixes are installed in the BGP table, or upon transmission of the updates to a peer.

BGP Cisco IOS Commands

This topic describes the Cisco IOS commands that can be used to gather information from the BGP data structures and track the flow of routing information.

BGP Commands

The following Cisco IOS commands can be used to gather information from the BGP data structures or to analyze the flow of routing information in real time.



© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-56

The following commands can be used to gather information from the BGP data structures:

- **show ip bgp summary:** This command displays essential BGP parameters, such as the router ID and AS number of the router, statistics on the memory usage of the BGP process, and a brief overview of the configured neighbors and their state.
- **show ip bgp neighbors:** This command lists all configured neighbors and their current operational state, configured parameters, and extensive statistics for each neighbor. The output of this command can be limited to a specific neighbor by using the **show ip bgp neighbors ip-address** command.
- **show ip bgp:** This command displays the content of the BGP table. To select a specific entry from the table, the network and mask of the selected prefix can be provided as an option to the command.

The following debugs can be used to observe the transmission and reception of packets and the exchange of routing information:

- **debug ip bgp:** This debug displays significant BGP related events, most notably the subsequent phases of establishing a BGP peering relationship. This command does not display the content of the BGP updates and is relatively safe to enable.

- **debug ip bgp updates:** This debug displays the transmission and reception of BGP updates. The output of this debug can be limited to a specific neighbor and specific prefixes by use of extra options. Issuing the command **debug ip bgp *ip-address* updates *access-list*** limits the output of the command to only updates received from or sent to the neighbor specified by the *ip-address* option and only for those networks that are permitted by the access list specified by the *access-list* option. If no restrictions are imposed by use of the access-list or neighbor options, this command can generate a large amount of output and affect the router's performance.

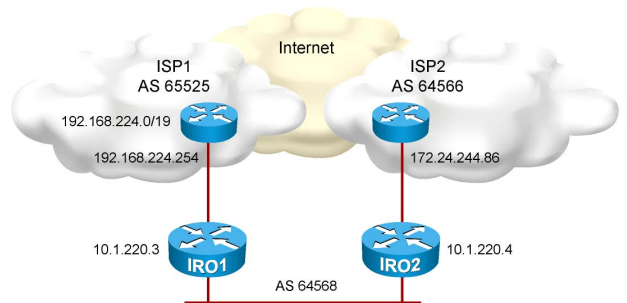
For sample output of these commands and guidelines regarding their use, see the “Sample Troubleshooting Flows” section in the course lab guide.

To review the complete syntax and a description of all command options, see the command reference sections of the Cisco Product Support pages on <http://www.cisco.com>.

Case Study: Troubleshooting BGP

Consider the following situation:

- A **traceroute** command from router IRO1 to IP address 192.168.224.1, which is owned by ISP1, indicates that traffic is routed via ISP2.
- A **ping** command from router IRO1 to the directly connected IP address 192.168.224.254 of the ISP1 access router succeeds.



The following short case study illustrates how knowledge of BGP data structures, update processes, and Cisco IOS commands can be leveraged to troubleshoot a routing problem.

The enterprise network shown in the figure uses BGP to exchange routing information with two different Internet service providers. When a **traceroute** command is executed on router IRO1 to determine the path that is used to reach IP address 192.168.224.1, which belongs to an IP address block that is owned by Internet Service Provider 1, it turns out that the traffic path goes through router IRO2:

```
IRO1#trace 192.168.224.1
```

Type escape sequence to abort.

Tracing the route to 192.168.224.1

```
 1 10.1.192.20 4 msec 0 msec 0 msec
 2 172.24.244.86 [AS 64566] 4 msec 0 msec 4 msec
 3 192.168.100.1 [AS 65486] 0 msec 4 msec 0 msec
 4 192.168.224.1 [AS 65525] 0 msec * 0 msec
```

This behavior is worth investigating, because it is expected that traffic destined for a network that is advertised by Internet Service Provider 1 would go directly to ISP 1 and not via Internet Service Provider 2. To verify whether this problem is caused by an underlying Layer 1, Layer 2, or Layer 3 problem, a **ping** command is executed to test the Layer 3 connectivity to the access router of Internet Service Provider 1:

```
IRO1#ping 192.168.224.254
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.224.254, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

From the fact that this ping succeeds, one can conclude that the link between router IRO1 and the Internet Service Provider 1 router is operational at Layers 3 and below. Given that the link is functional but is not used to route the packets across, this is by its nature a routing problem, and because BGP is used for external routing, this problem calls for investigation of the operation of BGP.

There are various different methods to troubleshoot this problem. The method presented is just one possible approach and was selected to show the role of the BGP data structures in the troubleshooting process. Other methods to approach this problem can be valid as well.

Case Study: Troubleshooting BGP (Cont.)

Displaying the routing table on router IRO1 for IP address 192.168.224.1 yields the following result:

```
IRO1#show ip route 192.168.224.1
Routing entry for 192.168.224.0/19, supernet
  Known via "bgp 64568", distance 200, metric 0
  Tag 64566, type internal
  Redistributing via eigrp 1
  Last update from 172.24.244.86 00:24:22 ago
  Routing Descriptor Blocks:
    * 172.24.244.86, from 10.1.220.4, 00:24:22 ago
      Route metric is 0, traffic share count is 1
      AS Hops 2
      Route tag 64566
```

- The routing table displays a BGP route sourced by router IRO2.
- The route to ISP1 is not the best route.
- **Conclusion:** The route via ISP1 is not present, or it is present but not selected as the best route.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v10-57

The objective is to find out why the direct route to Internet Service Provider 1 is not being used to route traffic to IP address 192.168.224.1.

There are two likely reasons why the traffic is routed via router IRO2 instead of directly to Internet Service Provider 1. The first reason could be that router IRO1 has not learned about the direct route to ISP1. The second reason could be that the router has learned about the route, but incorrectly selects the route via router BRO2 as the best route.

To start the investigation, a good first step is to confirm that the route used to route the traffic to 192.168.224.1 is indeed the BGP route learned from router IRO2 and not a route obtained from some other source.

From the output in the figure, you can see that the route to network 192.168.224.0/19 is the best match for destination IP address 192.168.224.1 and that this route was obtained via internal BGP and the source of the route is the router with IP address 10.1.220.4, which is router IRO2.

Case Study: Troubleshooting BGP (Cont.)

Displaying the BGP table on router IRO1 for IP address 192.168.224.1 yields the following result:

```
IRO1#show ip bgp 192.168.224.1
BGP routing table entry for 192.168.224.0/19, version 12
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Not advertised to any peer
 64566 65525
    172.24.244.86 (metric 30720) from 10.1.220.4 (10.1.220.4)
      Origin IGP, metric 0, localpref 100, valid, internal, best
```

- The BGP table displays only one available path, the path via router IRO2 and AS 64566 (ISP2) to AS 65525 (ISP1).
- The direct route via AS 65525 (ISP1) is not listed.
- **Conclusion:** The route to 192.168.224.0/19 is not exchanged as expected via BGP from ISP1 to router IRO1.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--5.8

After verifying the routing table, it has become clear that BGP is the protocol that is used to learn about prefix 192.168.224.0/19 and install the corresponding route in the routing table. However, the routing table does not show if the route via IRO2 is used because no other path is available, or because the path via IRO2 was selected as the best path. This information can be obtained from the BGP table.

From the output shown in the figure, you can see that only the path via router IRO2 is available. No other BGP learned paths are displayed.

Case Study: Troubleshooting BGP (Cont.)

Using the **show ip bgp summary** command to display an overview of the configured neighbors yields:

```
IR01#show ip bgp summary
BGP router identifier 10.1.220.3, local AS number 64568
BGP table version is 14, main routing table version 14
6 network entries using 702 bytes of memory
7 path entries using 364 bytes of memory
6/4 BGP path/bestpath attribute entries using 744 bytes of memory
3 BGP AS-PATH entries using 72 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
BGP using 1882 total bytes of memory
BGP activity 6/0 prefixes, 13/6 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.220.4      4 64568    82     80     14    0   0 01:12:02      6
192.168.224.244 4 65525     0      0      0    0   0 never    Active
```

- Configured neighbor 192.168.224.244 is in state Active.
- **Conclusion:** Router IR01 has not succeeded in establishing a neighbor relationship with router 192.168.224.244.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-58

The fact that the path via Internet Service Provider 1 is not present in the BGP table can have several different causes. ISP1 might not advertise the route; or ISP1 advertises it, but router IR01 rejects or ignores the advertisement; or possibly router IR01 and ISP1 have not successfully established a peering relationship and no routes have been exchanged at all.

At this point, a good next step is to start with the third option and investigate whether a neighbor relationship has been established between routers IR01 and the ISP1 router. The **show ip bgp summary** command displays the list of configured neighbors and their current state.

From the output shown in the figure, you can see that the peering to IP address 10.1.220.4 (IR02) has been established and six prefixes have been received from the neighbor, while the peering to IP address 192.168.224.244 is in the Active state. This means that this router is trying to establish a TCP session to neighbor 192.168.224.244, but has not succeeded yet.

Case Study: Troubleshooting BGP (Cont.)

- A ping to IP address 192.168.224.244 fails.
- Verification of the diagram shows that IP address 192.168.224.244 is not the correct peer address. The address should have been 192.168.224.254 instead.
- Displaying the BGP configuration on router IRO1 yields the following result:

```
IRO1#show running-config | section router bgp
router bgp 64568
  no synchronization
  bgp log-neighbor-changes
  neighbor 10.1.220.4 remote-as 64568
  neighbor 10.1.220.4 update-source Loopback0
  neighbor 192.168.224.244 remote-as 65525
```

- **Conclusion:** The peer IP address has been misconfigured in the BGP neighbor statement.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-10

Executing a ping to IP address 192.168.224.244 yields the following result:

```
IRO1#ping 192.168.224.244
```

Type escape sequence to abort.

```
Sending 5, 100-byte ICMP Echos to 192.168.224.244, timeout is 2
seconds:
```

```
.....
```

```
Success rate is 0 percent (0/5)
```

Compare this result to the earlier ping that was used to confirm the connectivity to Internet Service Provider 1 and also verify the IP address in the diagram. This comparison should lead to the conclusion that IP address 192.168.224.244 is not the correct IP address and IP address 192.168.224.254 should have been used for the peering to ISP1 instead.

Verification of the configuration, as shown in the figure, confirms that IP address 192.168.224.244 has mistakenly been used for the neighbor statement to AS 65525, which is the autonomous system number of Internet Service Provider 1.

Case Study: Troubleshooting BGP (Cont.)

The configuration of the neighbor statement is changed to the correct peer IP address:

```
IR01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
IR01(config)#router bgp 64568
IR01(config-router)#no neighbor 192.168.224.244 remote-as 65525
IR01(config-router)#neighbor 192.168.224.254 remote-as 65525
```

The neighbor relationship is now successfully established:

```
IR01#show ip bgp summary | begin Neighbor
Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.1.220.4    4  64568    146     146      19    0    0 02:15:17      5
192.168.224.254 4  65525     14     12      19    0    0 00:03:23      5
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-5-11

The IP address in the neighbor statement is changed to IP address 192.168.224.254 to test the hypothesis that the misconfigured IP address was the cause of the problem.

You now need to verify the results of the change, to confirm that the problem was solved. Strictly speaking, the only test that you need to perform to confirm you solved the problem is to use the **traceroute** command again to confirm that packets traveling to IP address 192.168.224.1 are now sent directly to Internet Service Provider 1, instead of making a detour via router IRO2 and Internet Service Provider 2.

However, to show the impact of the change on all the BGP data structures, the changes in the output of the **show** commands that were used to diagnose the problem are displayed in this figure and the following figures.

As you can see in the figure, the peering has now successfully been established, and five prefixes were received from neighbor 192.168.224.254.

Case Study: Troubleshooting BGP (Cont.)

The BGP table now shows the path via AS 65525 (ISP1), which has been selected as the best path:

```
IRO1#show ip bgp 192.168.224.1
BGP routing table entry for 192.168.224.0/19, version 17
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Advertised to update-groups:
    2
  65525
    192.168.224.254 from 192.168.224.254 (192.168.100.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
```

Question: Why is the path via router IRO2 not displayed as an alternative path?

Verification of the BGP table on router IRO1 shows that the path to prefix 192.168.224.0/19 via neighbor 192.168.224.254 to AS 65525 has now been selected as the best path. It is interesting to note that the path via router IRO2 is no longer displayed in the BGP table. One might expect to see this route displayed as an alternative path to reach prefix 192.168.224.0/19.

Why is the path to prefix 192.168.224.0/19 via router IRO2 not displayed in the BGP table on router IRO1?

Case Study: Troubleshooting BGP (Cont.)

Displaying the BGP table on router IRO2 yields the following result:

```
IRO2#show ip bgp 192.168.224.1
BGP routing table entry for 192.168.224.0/19, version 24
Paths: (2 available, best #1, table Default-IP-Routing-Table)
  Advertised to update-groups:
    1
  65525
    192.168.224.254 (metric 30720) from 10.1.220.3 (10.1.220.3)
      Origin IGP, metric 0, localpref 100, valid, internal, best
  64566 65525
    172.24.244.86 from 172.24.244.86 (172.24.240.1)
      Origin IGP, localpref 100, valid, external
```

Answer:

- Router IRO2 selects the path via router IRO1 as the best path and only the best path is advertised to neighbors.
- Split-horizon prevents the path via router IRO1 to be advertised back to router IRO1.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--5-3

To answer this question you need to consult the BGP table on router IRO2.

Router IRO2 has received an update about the path via router IRO1 and installed it in its BGP table. After executing the BGP best path selection algorithm for prefix 192.168.224.0/19, it selects this newly learned path via IRO1 as the best path to prefix 192.168.22.0/19 in AS 65525.

Because BGP has changed its best path to this prefix, it now withdraws the prefix and subsequently advertises its new best path to the prefix to all relevant neighbors. However, the split-horizon rule excludes router IRO1 from this update, because it is listed in the BGP table of router IRO2 as the original source of the update.

Case Study: Troubleshooting BGP (Cont.)

The route via neighbor 192.168.224.254 has been successfully installed in the routing table, and the **traceroute** shows that packets are not routed via router IRO2 and AS 64566 any longer.

```
IR01#show ip route 192.168.224.1
Routing entry for 192.168.224.0/19, supernet
  Known via "bgp 64568", distance 20, metric 0
  Tag 65525, type external
  Redistributing via eigrp 1
  Last update from 192.168.224.254 00:49:55 ago
  Routing Descriptor Blocks:
  * 192.168.224.254, from 192.168.224.254, 00:49:55 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
    Route tag 65525
IR01#traceroute 192.168.224.1

Type escape sequence to abort.
Tracing the route to 192.168.224.1

 1 192.168.224.254 [AS 65525] 0 msec 0 msec 4 msec
 2 192.168.224.1 [AS 65525] 0 msec 0 msec *
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-14

The output in the figure confirms that the route via neighbor 192.168.224.254 has been installed in the routing table, and the result of the **traceroute** command confirms that this route is now used to route packets to IP address 192.168.224.1.

This short case study illustrates the use of the Cisco IOS **show** commands to display the content of the BGP data structures. It also illustrates how knowledge of these data structures and the flow of BGP routing information can be leveraged to diagnose and resolve BGP routing problems.

For more examples of BGP troubleshooting methods and the output of key BGP troubleshooting commands, see the “Sample Troubleshooting Flows” section in the course lab guide.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- You have reviewed the main data structures used by the BGP routing protocol.
- You have reviewed the processes that BGP uses to exchange and process routing information.
- You have learned how to use the BGP Cisco IOS commands to gather information about BGP operation as part of a troubleshooting process.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-15

Lab 5-3 Debrief

Overview

In this lab, you have practiced troubleshooting problems related to the Border Gateway Protocol (BGP). You have created a troubleshooting plan to coordinate the work between the team members. You have methodically researched the problems, kept a log of your actions and findings, and resolved the problems and documented your solutions.

During the lab debrief, the instructor will lead a group discussion during which you can present your solutions. You will get an opportunity to verify your solution against a number of checkpoints provided by the instructor and compare your solution to other students' solutions. The instructor will discuss alternate solutions and their advantages and disadvantages.

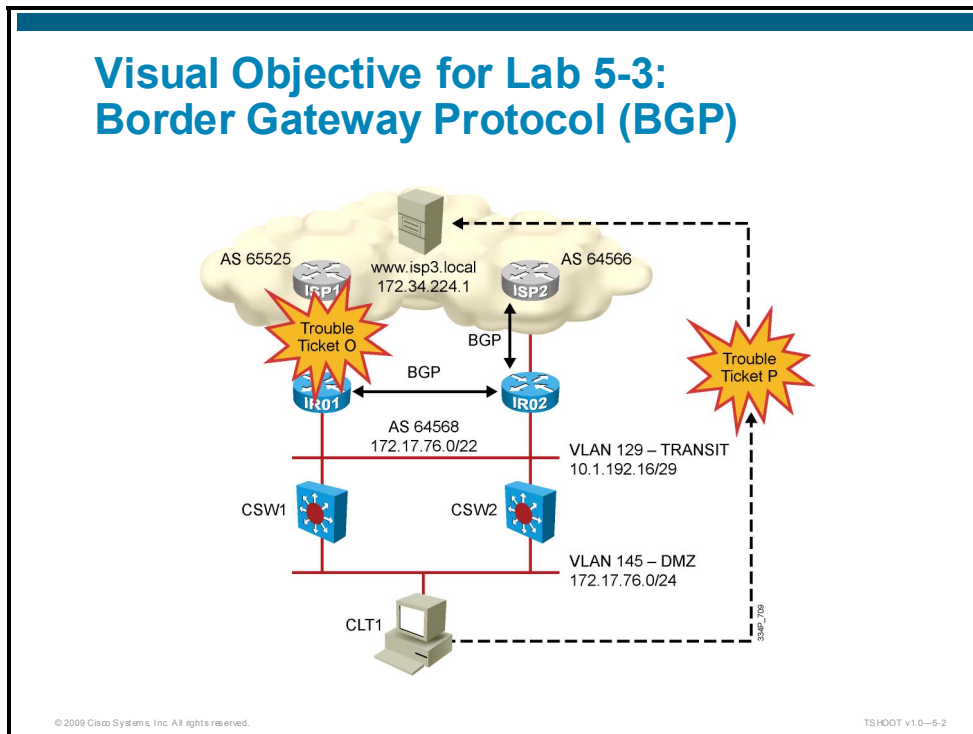
Objectives

Upon completing this lesson, you will be able to diagnose and resolve problems related to BGP. This ability includes being able to meet these objectives:

- Compare your solution, findings, and action log against a set of checkpoints provided by the instructor and identify common and alternate solutions
- Consolidate the lessons learned during the review discussions into a set of best-practice methods and commands to aid you in future troubleshooting procedures

Review and Verification

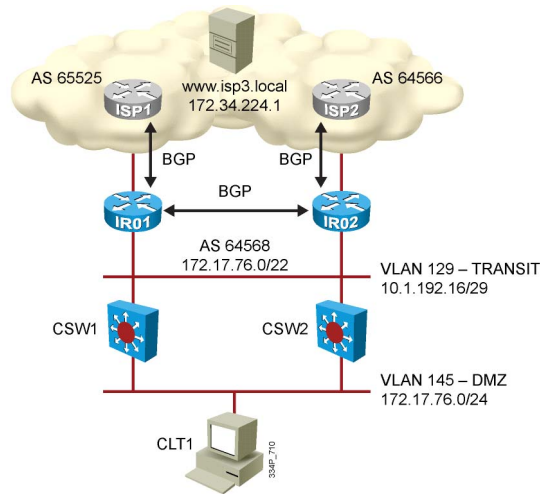
This topic describes the problems that were introduced in Lab 5-3, asks how you can verify that you have solved the problems, and gives an example of a troubleshooting process that will allow you to find and resolve the issues.



This lab consists of two trouble tickets: Trouble Ticket O, which revolves around the BGP peering between routers IRO1 and ISP1, and Trouble Ticket P, which deals with a connectivity problem from client PC CLT1 to the Internet via routers IRO2 and ISP2.

When you combine the text of the tickets, the overall objective of this lab is to make sure that there is redundant Internet connectivity for client PC CLT1. Traffic from client PC CLT1 should be routed via routers IRO1 and ISP1 if the path via routers IRO2 and ISP2 is not available and in a similar manner, traffic from client PC CLT1 should be routed via routers IRO2 and ISP2 if the path via routers IRO1 and ISP1 is not available.

Lab 5-3: BGP Design



The two trouble tickets are embedded in a larger scenario: The implementation and verification of BGP between the company network and the two Internet service providers. The text introducing the scenario was the following:

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

Your company is already using two different Internet service providers for redundant outbound Internet access by use of Network Address Translation (NAT). From a recent acquisition, your company has obtained a registered Autonomous System (AS) number (64568) and address block (172.17.76.0/22), which will be used for the new services. After consulting with both Internet service providers ISP1 and ISP2, it has been decided to use BGP with both of these service providers to provide redundant inbound connectivity to your company AS and IP address block.

Because BGP is new technology to your organization, it has been decided to implement BGP on the existing Internet routers IR01 and IR02 in preparation of the new data center project. This will allow some services to be migrated to the new IP address block before moving them to the newly built datacenter.

Your support team has been working closely together with the engineering team to prepare the implementation. You have received confirmation from both Internet service providers that they have prepared their routers for the BGP implementation.”

The BGP design is shown in the figure, and further guidelines relating to the design and implementation were given in the introduction of the trouble tickets:

“An external BGP peering will be established between routers IRO1 and ISP1 and a second external peering will be established between routers IRO2 and ISP2. In addition, an internal BGP peering between routers IRO1 and IRO2 will be established.

Routers IRO1 and IRO2 will advertise the full 172.17.76.0/22 block to both routers ISP1 and ISP2. No other prefixes are allowed to be advertised to routers ISP1 and ISP2 in order to protect the company AS from accidentally becoming a transit AS.

Each of the ISP routers will send a default route and a limited set of additional prefixes to routers IRO1 and IRO2. The default route will be redistributed into EIGRP by both routers IRO1 and IRO2. No other routes will be redistributed.

It is Friday evening and the engineering team has just configured routers IRO1 and IRO2 for BGP. To facilitate testing, VLAN 145 DMZ and the corresponding subnet 172.17.76.0/24 have been created. The client PC CLT1 has been temporarily assigned to this VLAN for testing purposes. All other devices, which have IP addresses in the 10.1.0.0/16 range, are still using NAT and their Internet access is not affected by the BGP configuration.

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

Planning Troubleshooting

How did your team approach the two trouble tickets?

- Did you troubleshoot all tickets in parallel, in sequence, or did you use a combination of methods?
- How did you decide on the order that you chose to address the tickets in?
- How did you test that both problems were fully resolved?
- How did you coordinate device access between your team members?
- How did you communicate with your team members?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-4

Note This lesson provides sample answers and solutions to the questions posed during the debrief discussions. Keep in mind that alternate solutions and methods might be just as valid and that the solutions provided here only highlight a sample approach and solution.

Neither ticket is more critical or urgent than the other. The problems described in the tickets do not affect any of the normal user traffic on the network, and there is no business impact other than the BGP implementation, which is part of a larger project. Timelines for that project might depend on the resolution of these problems. However, this applies to the successful implementation in general and not to either of the two trouble tickets specifically. Therefore, any approach that results in a working implementation is acceptable. Efficiency is the most important factor.

Working on both tickets in parallel, at least for the diagnostic phase of the troubleshooting process, is the most efficient approach. However, changes to any of the configurations on routers IRO1 or IRO2 are likely to affect both tickets and therefore it is very important to coordinate any changes between team members.

Finally, after both problems have been resolved it is important to execute proper failover tests to ensure that both the path via router ISP1 and the path via router ISP2 will be used for both inbound and outbound traffic if the other path fails. Without failover testing, it is possible that not all problems in the two tickets are uncovered and resolved.

Because this ticket involves only routers IRO1 and IRO2 and switches CSW1, CSW2, and ASW1, it is probably most efficient to split your team into two subteams and have each subteam work on one of the two tickets. Each subteam will control the corresponding router: router IRO1 for Trouble Ticket O and router IRO2 for Trouble Ticket P. Control of the switches can be coordinated during the lab as needed.

Trouble Ticket O: BGP Peering to Router ISP1 Not Established

The text introducing this trouble ticket was the following:

When you ask your colleague from the engineering team for a status update, you hear that the peering to router ISP2 has been established, but that the peering to router ISP1 is not being established. He has contacted the support team of Internet service provider 1 to find out if there is a problem at their end, but they state that everything is correctly configured on router ISP1. You offer to help troubleshoot this problem.

Your task is to diagnose the problem and, if possible, establish the BGP peering session between router IRO1 and router ISP1. After the peering has been established, you need to verify that traffic from subnet 172.17.76.0/24 can be sent to the Internet via router ISP1 and that the return traffic can be received via router ISP1.

Trouble Ticket O: Review and Discuss

How did your team approach Trouble Ticket O?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you accomplish the goal of establishing the BGP peering between router IRO1 and router ISP1?
- Did you confirm that client PC CLT1 can reach the Internet via routers IRO1 and ISP1 if the path via router ISP2 is not available?
- How did you verify that you accomplished these goals?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-5

The main problem in this ticket is a misconfigured AS number on the **neighbor** statement on router IRO1 that defines the peering to router ISP1. This causes router IRO1 to close the BGP session immediately after it has been established, because it receives a different AS number than the configured number in the Open message from router ISP1.

After correcting the autonomous system number on router IRO1 and establishing the peering to router ISP1, correct traffic forwarding via router IRO1 and IRO2 needs to be verified. At this point, the second problem in this ticket might be revealed: Router IRO1 does not inject prefix 172.17.76.0/22 into its BGP table due to the lack of a matching route in the IP routing table for the **network** statement configured under the **router bgp** process. However, because router IRO2 does inject the prefix and forwards it to router IRO1, this problem is not likely to be noticed unless a failover test is executed by shutting down the interfaces or BGP peerings on router IRO2.

Although there are many possible methods that you could use to solve this problem, the following example of a troubleshooting log shows you a methodical approach to resolve this problem.

Trouble Ticket	Actions and results
Ticket O	IRO1: Verified problem: Peering to ISP1 (192.168.224.254) is in state "Active".
	IRO1: Ping to ISP1 succeeds.
	IRO1: debug ip tcp transactions reveals that the TCP session is established and torn down again immediately. The log also reveals a message "%BGP-3-NOTIFICATION: sent to neighbor 192.168.224.254 2/2 (peer in wrong AS) 2 bytes FFF5 FFFF FFFF FFFF FFFF FFFF FFFF FFFF 002D 0104 FFF5 00B4 C0A8 6401 1002 0601 0400 0100 0102 0280 0002 0202 00." Disabled debug.
	IRO1: Verified AS number in configuration: Did not spot any errors.
	IRO1: debug ip bgp reveals the following "BGP: 192.168.224.254 bad OPEN, remote AS is 65525, expected 65255."
	IRO1: Verified AS number again. AS number 65255 is configured instead of 65525.
	Verify design and implementation guidelines: AS number of ISP1 is 65525.
	IRO1: Configuration changed: Changed AS number for BGP neighbor 192.168.224.254 to 65525. Both pre- and post-change configurations were saved in flash on the router. Communicated this information to team members.
	IRO1: BGP session is established and prefixes are learned from router ISP1. Default route points to ISP1 and our IP block (172.17.76.0/22) is advertised to router ISP1.
	Discuss test procedure with team members. Decision: shut down peering to ISP1 while the other team works ticket P. After successful resolution of ticket P failover tests will be coordinated and performed.
	Notification from team members: Ready for failover testing. Re-enable peering to ISP1.
	Initiate continuous ping from CLT1 to www.isp3.local.
	IRO1: Reload router. Result as expected: No packet loss.
	IRO2: Reload router. Unexpected result: Connectivity is not restored until after the reload of router IRO2 finishes. Conclusion: Routing via IRO1 and ISP1 does not function correctly.
	Decision: Shut down all BGP peerings on router IRO2 to allow isolated testing of BGP on router IRO1.
	CLT1: Problem is confirmed: Connectivity from CLT1 to www.isp3.local is lost after the sessions on IRO2 have been administratively disabled.
	CLT1: Traceroute to www.isp3.local reaches router IRO1 (10.1.192.19) and times out after that.
	IRO1: show ip route for 172.34.224.1 shows that the BGP route to 172.34.224.0/19 is used to route packets to ISP1. Traceroute to www.isp3.local from IRO1 succeeds. Conclusion: Outbound traffic is forwarded correctly. Inbound traffic must be the problem.
	IRO1: show ip bgp neighbor 192.168.224.254 advertised-routes reveals that no routes are advertised to neighbor ISP1.
	IRO1: Our IP block 172.17.76.0/22 is not present in the BGP table.
	IRO1: Verify BGP configuration: network 172.17.76.0 mask 255.255.224.0 is present in the BGP configuration.
	IRO1: Verify routing table: No route to 172.17.76.0/22 is present.
	IRO2: Verify routing table: Static route to null 0 present for 172.17.76.0/22.
	IRO1: Configuration changed: Added static route to null 0 for 172.17.76.0/22. Both prechange and postchange configurations were saved in flash on the router.

Trouble Ticket	Actions and results
	Communicated this information to team members.
	IRO1: 172.17.76.0/22 is now advertised to neighbor ISP1.
	CLT1: Ping to www.isp3.local succeeds. Browsing to www.isp3.local succeeds.
	Notify team members: Problem solved. BGP peerings on router IRO2 can be re-enabled.
	Problem fixed. Documented changes. Backed up configurations. Closed ticket.

Key Clue: Wrong Peer AS in Logging and Debug Messages

- The log of router IRO1 contains a message that indicates the problem:

```
IR01#show logging | include BGP
Apr 30 01:44:03 PDT: %BGP-3-NOTIFICATION: sent to neighbor 192.168.224.254
2/2 (peer in wrong AS) 2 bytes FFF5 FFFF FFFF FFFF FFFF FFFF FFFF FFFF
002D 0104 FFF5 00B4 C0A8 6401 1002 0601 0400 0100 0102 0280 0002 0202 00
```

- The **debug ip bgp** command reveals more detail about the exact problem:

```
IR01#debug ip bgp
BGP debugging is on for address family: IPv4 Unicast
IR01#show logging | include BGP
<... output omitted ...>
Apr 30 01:54:01.123 PDT: BGP: 192.168.224.254 bad OPEN, remote AS is 65525,
expected 65255
Apr 30 01:54:01.123 PDT: BGP: 192.168.224.254 went from OpenSent to Closing
Apr 30 01:54:01 PDT: %BGP-3-NOTIFICATION: sent to neighbor 192.168.224.254
2/2 (peer in wrong AS) 2 bytes FFF5 FFFF FFFF FFFF FFFF FFFF FFFF FFFF
002D 0104 FFF5 00B4 C0A8 6401 1002 0601 0400 0100 0102 0280 0002 0202 00
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-6

The most important clues about the problem that causes the peering between router IRO1 and IRO2 are provided by the system log messages. When router IRO1 closes the BGP session due to the reception of a different AS number than what is configured for the neighbor, it logs a message that lists the cause as “peer in wrong AS.” The first four characters (FFF5) in the hexadecimal string that follows the notification message indicate the AS number that was received when converted to decimal (65525).

This same information is also shown in a clearer manner when the **debug ip bgp** command is enabled. When the open message from router ISP1 is received, this command logs a message that states “192.168.224.254 bad OPEN, remote AS is 65525, expected 65255.” This clearly shows what the received autonomous system in the open message was (65525) and what the locally configured number is (65255).

When you verify the implementation and design guidelines in the text that introduced the tickets and compare this to the neighbor statement for ISP1 (192.168.224.254) in the configuration of router IRO1, you must come to the conclusion that the remote AS number configured for ISP1 on router IRO1 is incorrect and needs to be changed.

Key Clue: Local Network Not in BGP Table on IRO1

- When the BGP peerings are disabled on router IRO2, router IRO1 does not advertise 172.17.76.0/22 to router ISP1.

```
IRO1#show ip bgp neighbor 192.168.224.254 advertised-routes
Total number of prefixes 0
```

- Verifying the BGP table reveals that network 172.17.76.0/22 is not present in the table.

```
IRO1#show ip bgp 172.17.76.0 255.255.252.0
% Network not in table
```

- The network is also not present in the routing table.

```
IRO1#show ip route 172.17.76.0 255.255.252.0
% Subnet not in table
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v10-5-7

The second problem is hard to spot unless BGP on router IRO2 is temporarily disabled by administratively shutting down both peerings on IRO2. After BGP has been disabled on IRO2, router IRO1 no longer advertises the local IP range 172.17.76.0/22 to router ISP1, causing return traffic to PC CLT1 to fail.

The fact that the network is not advertised to neighbor router ISP1 (192.168.224.254) can be displayed using the **show ip bgp neighbors 192.168.224.254 advertised-routes** command. The output of this command reveals that zero prefixes are advertised to neighbor router ISP1. When you subsequently verify whether the network is available in the local BGP table in router IRO1, you see that it is missing in the BGP table, even though the network has been configured under the router BGP process. However, for a locally configured network to be injected in the BGP table, it is necessary that an exact match for the route exists in the IP routing table. Verification of the routing table reveals that no matching route is present, which explains why the configured network is not placed into the BGP table.

Key Clue: Static Route for 172.17.76.0/22 Configured on IRO2

- On router IRO2, network 172.17.76.0/22 is injected into the BGP table:

```
IRO2#show ip bgp 172.17.76.0 255.255.252.0
BGP routing table entry for 172.17.76.0/22, version 3
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Local
    0.0.0.0 from 0.0.0.0 (10.1.220.4)
      Origin IGP, metric 0, localpref 100, weight 32768, valid, sourced,
local, best
```

- A matching static route is present in the routing table:

```
IRO2#show ip route 172.17.76.0 255.255.252.0
Routing entry for 172.17.76.0/22
  Known via "static", distance 1, metric 0 (connected)
  Redistributing via eigrp 1
  Advertised by bgp 64568
  Routing Descriptor Blocks:
  * directly connected, via Null0
    Route metric is 0, traffic share count is 1
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-8

To find a solution to this problem, you need to spot the difference with router IRO2, which does inject network 172.17.76.0/22 into its BGP table. When you display the routing table for network 172.17.76.0/22, the output reveals that a static route has been configured on router IRO2 pointing to the Null0 interface. This is a common way to ensure that a matching route is present in the routing table to allow the injection of a configured BGP network into the local BGP table.

After the configuration of a similar static route on router IRO1, the network is injected into the local BGP table on router IRO1 as well and subsequently advertised to router ISP1.

Trouble Ticket O Checkpoints

Minimum checkpoints to prove that you have resolved this trouble ticket:

- The BGP peering between router IRO1 and router ISP1 has been established.
- You have verified that traffic from client PC CLT1 to <http://www.isp3.local> can be routed via routers IRO1 and ISP1 and that traffic from the Internet back to client PC CLT1 can return to the company network via that same path.
- You have documented your process, your solution, and any changes that you have made to the device configurations.

What else should you have checked?

Are there any unresolved issues?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-9

The figure shows a list of minimum requirements that should be met to consider this trouble ticket to be resolved.

Note that the verification of the second item, traffic being routed via routers IRO1 and ISP1, can be verified only if both BGP peerings on router IRO2 are temporarily disabled.

Suggested Solution

Correcting the configuration of router IRO1 as follows restores the peering between routers IRO1 and ISP1 and ensures connectivity from client PC CLT1 to server <http://www.isp3.local> when the path via routers IRO2 and ISP2 is not available.

Suggested Configuration Changes

- On router IRO1, change the remote autonomous system number configured for neighbor 192.168.224.254 (ISP1):

```
IRO1(config)#router bgp 64568
IRO1(config-router)# neighbor 192.168.224.254 remote-as 65525
```

- On router IRO1, add a static route for network 172.17.76.0/22 to the Null 0 interface:

```
IRO1(config)#ip route 172.17.76.0 255.255.252.0 null 0
```

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0-5-10

To establish the peering between routers IRO1 and ISP1, the autonomous system number that is configured on router IRO1 for neighbor ISP1 needs to be changed to the correct value of 65525.

To ensure that network 172.17.76.0/22 is injected into the local BGP table on router IRO1, a static route needs to be configured to guarantee that a matching route for the configured network is always available in the IP routing table. Pointing this route to the Null 0 interface has the added advantage that any packets destined for an IP address in the 172.17.76.0/22 block that do not have a matching more specific route in the routing table will be discarded and not routed back out to the Internet.

Trouble Ticket P: Client CLT1 Cannot Reach the Internet

The text introducing this trouble ticket was the following:

Even without the BGP session between routers IRO1 and ISP1, Internet connectivity from test PC CLT1 should be available via router IRO2 and Internet service provider 2. When one of your colleagues from engineering tries to test this by browsing to <http://www.isp3.local>, it does not work. You offer to assist in troubleshooting this problem.

Your task is to diagnose this problem and, if possible, resolve it.

Trouble Ticket P: Review and Discuss

How did your team approach Trouble Ticket P?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you accomplish the goal of restoring the connectivity to <http://www.isp3.local> from client PC CLT1?
- How did you verify that you accomplished your goal?
- How did you confirm that traffic is routed via routers IRO2 and ISP2 and not via routers IRO1 and ISP1?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-11

The problem in this ticket is that the prefix list named “LOCAL-ROUTES,” which is configured on router IRO2 to filter the routes advertised to router ISP2, permits prefix 172.16.76.0/22 instead of the local IP address block 172.17.76.0/22.

As a result, the local IP address block 172.17.76.0/22 is not advertised to router ISP2, and return traffic to client PC CLT1 is dropped by lack of a matching route.

Troubleshooting this problem in isolation is relatively straightforward, but if other team members are working on Trouble Ticket O in parallel, you need to be very careful that changes that they make to the configuration on router IRO1 do not affect your troubleshooting process. After the peering between router IRO1 and ISP1 is established, router IRO1 will advertise the 172.17.76.0/22 prefix to router ISP1 and traffic can return to client CLT1 via that path. If you are unaware of this, you might conclude that the problem is resolved while this is not actually the case.

Proper coordination and failover testing can help avoid these issues.

Although there are many possible methods that you could use to solve this problem, the following example of a troubleshooting log shows you a methodical approach to resolve this problem.

Trouble Ticket	Actions and results
Ticket P	CLT1: Verified problem: Cannot browse to www.isp3.local.
	CLT1: Ping to default gateway succeeds. Traceroute to www.isp3.local reaches router IRO2 (10.1.192.20) and times out after that.
	CLT2: Client CLT2 can browse to www.isp3.local. Traceroute goes via IRO2 and reaches www.isp3.local (172.34.224.1). Conclusion: Site and path to the site via IRO2 are available via NAT. Problem is BGP related.
	IRO2: BGP peering to router ISP2 has been established.
	IRO2: show ip route for 172.34.224.1 shows that the BGP route to 172.34.224.0/19 is used to route packets to ISP2. Traceroute to www.isp3.local from IRO2 succeeds. Conclusion: Outbound traffic is forwarded correctly. Inbound traffic must be the problem.
	IRO2: show ip bgp neighbor 172.24.244.86 advertised-routes reveals that no routes are advertised to neighbor ISP2.
	IRO2: Our IP block 172.17.76.0/22 is present in the local BGP table and advertised to IRO1.
	IRO2: Verified BGP configuration. Outbound prefix list is configured for neighbor ISP2.
	Hypothesis: Prefix list causes the problem.
	Notification from team members: They restored the peering to ISP1. Discuss test procedure with team members. Decision: shut down peering to ISP1 while this ticket is being resolved. After successful resolution of this tickets failover tests will be coordinated and performed.
	IRO2: Configuration changed: Removed outbound prefix list from neighbor ISP2. Pre-change configuration was saved in flash on the router. Communicated this information to team members.
	IRO2: Performed soft outbound clear to ISP2. 172.17.76.0/22 is now advertised. Conclusion: Prefix list is not correct.
	IRO2: Verify prefix list. Spotted mistake: Prefix 172.16.76.0/22 is permitted instead of prefix 172.17.76.0/22.
	IRO2: Configuration changed: Changed prefix list to permit correct prefix and added as outbound prefix list to neighbor ISP2. Post-change configuration was saved in flash on the router. Communicated this information to team members.
	IRO2: Performed soft outbound clear to ISP2. 172.17.76.0/22 is still advertised.
	CLT1: Browsing to www.isp3.local now succeeds.
	Notify team members: Ready for failover testing.
	Initiate continuous ping from CLT1 to www.isp3.local.
	IRO1: Reload router. Result as expected: No packet loss.
	IRO2: Reload router. Unexpected result: Connectivity is not restored until after the reload of router IRO2 finishes. Conclusion: Routing via IRO1 and ISP1 does not function correctly.
	Decision: Shut down all BGP peerings on router IRO2 to allow isolated testing of BGP on router IRO1.
	Received notification from team members: Problem solved. Re-enable BGP peerings on router IRO2.
	Problem fixed. Documented changes. Backed up configurations. Closed ticket.

Key Clue: Local Network Not Advertised to ISP2

- Router IRO2 does not advertise 172.17.76.0/22 to router ISP1.

```
IRO2#show ip bgp neighbor 172.24.244.86 advertised-routes
Total number of prefixes 0
```

- Verifying the BGP table reveals that network 172.17.76.0/22 is present in the table and advertised to update group 2.

```
IRO2#show ip bgp 172.17.76.0 255.255.252.0
BGP routing table entry for 172.17.76.0/22, version 3
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Advertised to update-groups:
    2
  Local
    0.0.0.0 from 0.0.0.0 (10.1.220.4)
      Origin IGP, metric 0, localpref 100, weight 32768, valid,
sourced, local, best
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-12

Using a generic IP connectivity troubleshooting process, you should first eliminate potential problem causes until you have determined that the problem is most likely caused by the fact that return traffic from server <http://www.isp3.local> does not reach client CLT1. When you start troubleshooting the return path for traffic to the IP address of CLT1, which is part of the 172.17.76.0/22 block, you need to realize that the only thing that can be done now is to investigate whether prefix 172.17.76.0/22 (or a subnet of this prefix that contains the IP address of CLT1) is correctly advertised to router ISP2. You cannot access the server or any of the routers on the Internet, so you do not have the option to troubleshoot the return path from any point closer to the source.

The **show ip bgp neighbor *ip-address* advertised-routes** command can be used to verify which routes are advertised to a particular neighbor. In this specific situation, you know that you do not expect to see a large number of routes. In situations where you expect to see many routes, you might need to apply additional filtering to select the routes that you are interested in. Issuing this command in this scenario reveals that no routes are advertised to router ISP2.

When you investigate the BGP table for prefix 172.17.76.0/22, which is the prefix that should be advertised to router ISP2, you see that it is present in the BGP table and advertised to update group 2. On older IOS versions, you might actually see the BGP neighbors listed instead of the update group. Starting with Cisco IOS release 12.3(4)T, BGP update groups were introduced and enabled by default.

Note Different update group numbers might be displayed on your router, but the corresponding neighbors should be similar.

Key Clue: Local Network Not Advertised to ISP2 (Cont.)

- Update group 2 does not include router ISP2:

```
IRO2#show ip bgp update-group
BGP version 4 update-group 1, external, Address Family: IPv4 Unicast
BGP Update version : 36/0, messages 0
Outgoing update prefix filter list is LOCAL-ROUTES
Update messages formatted 3, replicated 0
Number of NLRI's in the update sent: max 1, min 1
Minimum time between advertisement runs is 30 seconds
Has 1 member (* indicates the members currently being sent updates):
 172.24.244.86

BGP version 4 update-group 2, internal, Address Family: IPv4 Unicast
BGP Update version : 36/0, messages 0
Update messages formatted 12, replicated 0
Number of NLRI's in the update sent: max 2, min 0
Minimum time between advertisement runs is 0 seconds
Has 1 member (* indicates the members currently being sent updates):
 10.1.220.3
```

To find out which routers are members of an update group, you can use the **show ip bgp update-group** command. In this case, it shows that update group 2 contains neighbor 10.1.220.3 and not neighbor 172.24.244.86.

The output of these commands confirms that the route is present in the BGP table, selected as the best route, advertised to neighbor 10.1.220.3 (IRO1), but not advertised to neighbor 172.24.244.86 (ISP2).

To find out what is preventing the route to be advertised to router ISP2, you need to examine the BGP configuration on router IRO2. This reveals that a prefix list is applied to the outbound BGP updates to router ISP2.

At this point, you should be able to spot the configuration mistake in the prefix list: prefix 172.16.76.0/22 is permitted instead of the intended 172.17.76.0/22. Another way to confirm that the prefix list is the cause of the problem is by removing it from the neighbor. After performing a soft reset of the BGP session to router ISP2, you can see that prefix 172.17.76.0/22 is advertised to router ISP2. It is important that you do not stop at this point, but examine the prefix list, correct the configuration, and reapply it to neighbor ISP2.

Trouble Ticket P Checkpoints

Minimum checkpoints to prove that you have resolved this trouble ticket:

- Client PC CLT1 can use a web browser to connect to <http://www.isp3.local>.
- You have verified that traffic from client PC CLT1 to <http://www.isp3.local> can be routed via routers IRO2 and ISP2 and that traffic from the Internet back to client PC CLT1 can return to the company network via that same path.
- You have documented your process, your solution, and any changes that you have made to the device configurations. What else should you have checked?

Are there any unresolved issues?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0–6-14

The figure shows a list of minimum requirements that should be met to consider this trouble ticket to be resolved.

Note that the verification of the second item, traffic being routed via routers IRO2 and ISP2 can only be verified if the peering from router IRO1 to router ISP1 is temporarily disabled.

You should carefully coordinate failover tests within your team to ensure that both paths to the Internet can be used for outbound and inbound traffic.

Suggested Solution

Correcting the configuration of router IRO2 as follows restores connectivity from client PC CLT1 to server <http://www.isp3.local> using the path via routers IRO2 and ISP2.

Suggested Configuration Changes

- On router IRO2, change the prefix list named LOCAL-ROUTES to permit prefix 172.17.76.0/22 instead of prefix 172.16.76.0/22:

```
IRO2(config)#no ip prefix-list LOCAL-ROUTES seq 5 permit 172.16.76.0/22 le 24
IRO2(config)#ip prefix-list LOCAL-ROUTES seq 5 permit 172.17.76.0/22 le 24
```

- **Note:** Removing the prefix list entirely or removing it from the neighbor is not considered a valid solution, because that could cause the local autonomous system to become a transit autonomous system.

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0—5-15

To enable connectivity between client PC CLT1 and server <http://www.isp3.local> the prefix list named LOCAL-ROUTES on router IRO2 needs to be changed to permit prefix 172.17.76.0/22 instead of prefix 172.16.76.0/22.

Removing the prefix list from the neighbor statement or removing the prefix list entirely can be a valid step during the troubleshooting process. However, the reason that the prefix list was implemented is that it prevents the local autonomous system from becoming a transit autonomous system. Only local routes are advertised to routers ISP1 and ISP2. Routes that are learned from ISP1 are not passed to ISP2 and routes that are learned from ISP2 are not passed to ISP1. This ensures that only traffic destined for networks that are advertised by the local AS 64568 will be forwarded to routers IRO1 and IRO2.

Therefore, it is important that at the end of the lab the prefix list has been reapplied as an outbound route filter to neighbor ISP2.

The only acceptable solution (without using the prefix list) is if some other mechanism, such as an AS path filter, has been applied to prevent AS 64568 from becoming a transit AS.

Consolidation

This topic describes the key lessons that could be learned from the lab exercise.

Discussion: Lessons Learned

Method and process:

- How could you improve your troubleshooting methods?
- What alternative methods did you discover?

Communication and procedures:

- How could the troubleshooting process be made more effective?
- What kind of procedures would be useful and why?

Technology and tools:

- Which tools were most useful during troubleshooting?
- Which tools could have improved the effectiveness of your process?
- Which useful Cisco IOS commands did you discover?

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0—5-16

In addition to thinking of the methods, processes, and tools as they were used in the lab, reflect on how these would apply to your own organization. Think about all the things that you learned during the lab itself and during the debrief discussions. There is room to write down key learning points in the Lab Debrief Notes section of the lab guide.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- You have reviewed and verified your lab results.
- You have consolidated the experiences and discoveries that all students got from the lab and you have derived a number of key learning points from these experiences.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-17

Troubleshooting Performance Problems on Routers

Overview

Performance problems on network devices can cause degraded application performance and connectivity issues. This can result in problems at the business level. Employees are not as productive as they could be or they might not be able to service their customers correctly. Diagnosing and resolving router performance problems is therefore an important skill for any network support engineer.

Common causes for performance problems on routers are high CPU utilization, and memory allocation problems. Therefore, it is important to be able to recognize the typical symptoms associated with CPU or memory issues and to know what would typically cause these types of issues.

Objectives

Upon completing this lesson, you will be able to diagnose problems caused by high CPU utilization on routers using the Cisco IOS command-line interface. Also, this lesson explains the typical symptoms and possible causes of memory allocation failures, and it offers guidelines for troubleshooting memory problems. This ability includes being able to meet these objectives:

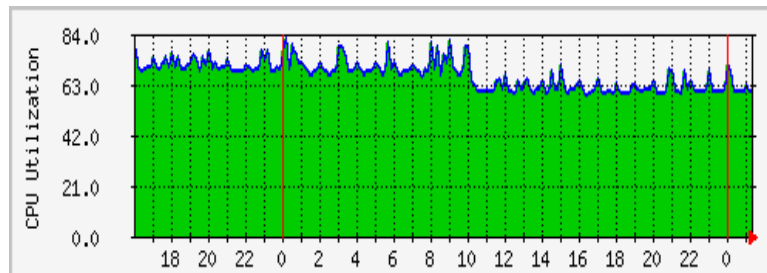
- Use Cisco IOS commands to analyze CPU usage to determine the root cause of high CPU usage on a router
- Use Cisco IOS commands to analyze packet forwarding through a router
- Use Cisco IOS commands to analyze memory usage to troubleshoot router performance problems

Troubleshooting High CPU on Routers

This topic describes typical symptoms and common causes of high CPU utilization.

Introduction to High CPU Utilization

- What is the significance of high CPU utilization on a router?
- When is high CPU utilization problematic?
- How can you differentiate between high CPU utilization that is a normal state and high utilization that is a problem?



© 2009 Cisco Systems, Inc. All rights reserved.

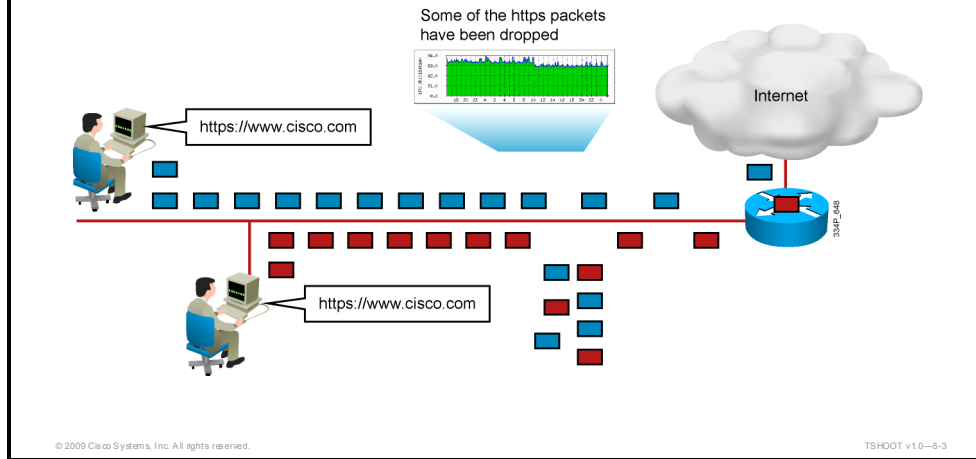
TSHOOT v1.0-6-2

The CPU on a router performs two major tasks: forwarding packets and executing management and control plane processes. The CPU can become too busy when the CPU either has many packets to forward or when a system process consumes a large amount of the available CPU time. For example, if the CPU is receiving many SNMP packets because of intensive network monitoring, it can become so busy processing all those packets that the other system processes cannot get access to CPU resources.

It is very important to understand when high CPU utilization is problematic and when it is considered to be normal. In some cases, high CPU utilization is normal and does not cause network problems. If CPU utilization is high for a short period of time, this does not necessarily indicate a problem. This can be caused by a short burst of network management requests or expected peaks of network traffic for short periods of time. But if CPU utilization is consistently very high, and packet forwarding or process performance on the router performance degrades, this is usually considered to be a problem and needs to be investigated.

Slow Router Performance

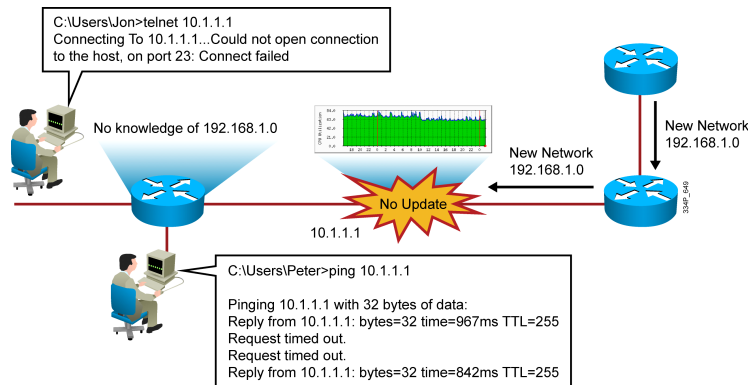
- High CPU utilization can result in packet loss, high delay, and other network performance issues.



When the router CPU is too busy to forward all packets as they arrive, the router might start to buffer packets, increasing latency, or even drop packets. This affects the application traffic passing through the router and as a result, network performance will suffer. Also, because the CPU is spending most of its available time on packet forwarding, control plane processes might not be able to get sufficient access to the CPU, which could lead to further disruptions due to failing routing protocols or other control plane protocols.

Router Does Not Respond to Service Requests

- Slow or no response on Telnet sessions
- Slow response on the console
- Slow or no response to ping
- Router not sending routing updates to other routers



© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--6-4

A common symptom of a router CPU that is too busy is that the router fails to respond to certain service requests. This can result in the following behavior:

- Slow response to commands that are issued in Telnet sessions, or even being unable to use Telnet to connect to the router.
- Slow response to commands issued on the console.
- High latency on ping responses coming from the router or no response to ping at all.
- The router fails to send routing protocol packets to other routers.

Common Causes of High CPU Utilization

- **ARP Input process:** Responsible for the origination of ARP requests.
- **Net Background process:** Creates the necessary buffers from the main buffer pool whenever a buffer is required, but not available to the process or interface.
- **IP Background process:** Responsible for changing the encapsulation type on an interface, moving an interface to a new state (up or down), and changes to the IP address of an interface.
- **TCP Timer process:** Responsible for TCP sessions running on the router.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-5

The following are some of the most common router processes that could cause high CPU utilization:

- **ARP Input process:** This process is responsible for the origination of ARP requests.
- **Net Background process:** This process creates buffers from the main buffer pool whenever a buffer is required, but there is none available to the process or interface.
- **IP Background process:** This process is responsible for encapsulation type changes on an interface, the move of an interface to a new state (up or down), and changes of the IP address on an interface.
- **TCP Timer process:** This process is responsible for TCP sessions running on the router.

Common Causes of High CPU Utilization (Cont.)

- The ARP Input process originates ARP requests.

```
router#show running-config | include ip route
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
```

- When a default route is configured to point to a broadcast interface, it causes the generation of many ARP requests for different IP addresses:

```
router#show arp
Protocol Address      Age (min)  Hardware Addr  Type   Interface
Internet 10.10.10.1      -         0013.1918.caae ARPA   FastEthernet0/0
Internet 10.16.243.249   0         Incomplete     ARPA
Internet 10.16.243.250   0         Incomplete     ARPA
Internet 10.16.243.251   0         Incomplete     ARPA
Internet 10.16.243.252   0         Incomplete     ARPA
Internet 10.16.243.253   0         Incomplete     ARPA
Internet 10.16.243.254   0         Incomplete     ARPA
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--5-5

- **ARP Input:** High CPU utilization by the Address Resolution Protocol (ARP) Input process occurs if the router has to originate an excessive number of ARP requests. Multiple ARP requests for the same IP address are rate-limited to one request every two seconds, so excessive numbers of ARP requests can only occur if the router needs to originate ARP requests for many different IP addresses. This can happen if an IP route has been configured pointing to a broadcast interface. This causes the router to generate an ARP request for each IP address that is not reachable through a more specific route. An excessive amount of ARP requests can also be caused by a malicious network traffic, which scans through locally attached subnets on the router. An indication of such traffic would be the presence of a very high number of incomplete ARP entries in the ARP table.

Common Causes of High CPU Utilization (Cont.)

- Net Background process: Creates the necessary buffers from the main buffer pool whenever a buffer is required, but not available to the process or interface.
- The **show interface** *interface-id* command shows excessive numbers of throttles, overruns, and ignored packets .

```
router#show interfaces FastEthernet 0/0
<... output omitted ...>
 5 minute input rate 4950000 bits/sec, 12762 packets/sec
 5 minute output rate 5370000 bits/sec, 12761 packets/sec
 83959472 packets input, 3159528427 bytes
 Received 2450500 broadcasts, 0 runs, 0 giants, 3204 throttles
 138 input errors, 0 CRC, 0 frame, 235 overrun, 1380 ignored
<... output omitted ...>
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-5-7

- **Net Background:** The Net Background process runs whenever a buffer is required but is not available to a process or an interface. It uses the main buffer pool to provide the requested buffers. Net Background also manages the memory used by each process and cleans up freed-up memory. The symptoms of high CPU are increases in throttles, ignores, overruns, and resets on an interface. The output of the **show interface** command in the figure displays many throttles (3204 throttles), ignores (1380 ignores) and overruns (135 overrun).

Common Causes of High CPU Utilization (Cont.)

- The **show tcp statistics** command displays detailed TCP-related information.

```
router#show tcp statistics
Rcvd: 22771 Total, 153 no port
  0 checksum error, 0 bad offset, 0 too short
  4661 packets (357163 bytes) in sequence
  7 dup packets (860 bytes)
  0 partially dup packets (0 bytes)
  0 out-of-order packets (0 bytes)
  0 packets (0 bytes) with data after window
  0 packets after close
  0 window probe packets, 0 window update packets
  4 dup ack packets, 0 ack packets with unsend data
  4228 ack packets (383828 bytes)
Sent: 22490 Total, 0 urgent packets
  16278 control packets (including 17 retransmitted)
  5058 data packets (383831 bytes)
  7 data packets (630 bytes) retransmitted
  0 data packets (0 bytes) fastretransmitted
  1146 ack only packets (818 delayed)
  0 window probe packets, 1 window update packets
8 Connections initiated, 82 connections accepted, 65 connections established
32046 Connections closed (including 27 dropped, 15979 embryonic dropped)
24 Total rxmt timeout, 0 connections dropped in rxmt timeout
0 Keepalive timeout, 0 keepalive probe, 0 Connections dropped in keepalive
```

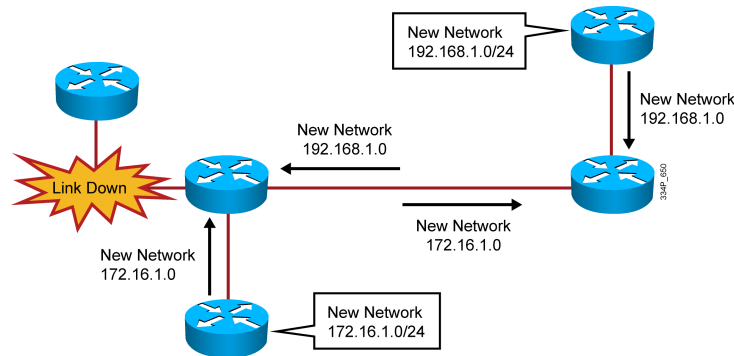
© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-8

- **TCP Timer:** When the TCP timer process uses a lot of CPU resources, there are too many TCP peers (such as Border Gateway Protocol [BGP] or Data-Link Switching Plus [DLSw+] peers). The **show tcp statistics** command displays detailed TCP information.

Common Causes of High CPU Utilization (Cont.)

- The IP background process manages interface changes:
 - Changes in interface status (up or down)
 - Changes to the interface IP address
 - Modification of the routing table based on interface status



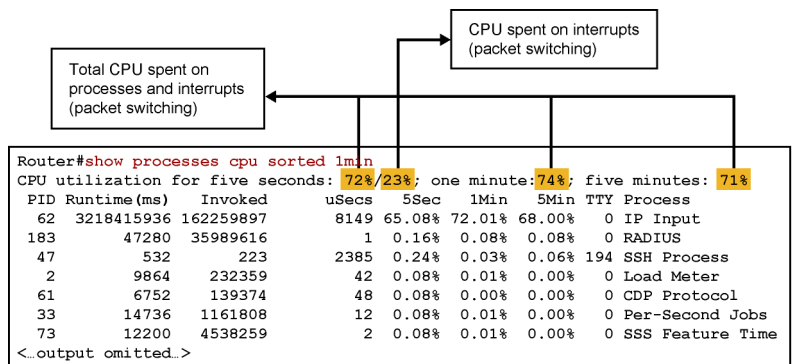
© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-5-9

- **IP Background:** The IP Background process is involved in moving an interface to a new state (such as up or down), or a change in the IP address of the interface. The IP Background process modifies the routing table in accordance with the status of the interfaces, while the IP Background process assumes that there is a link state change when it receives link state change messages. It then notifies all routing protocols to check the affected interface.

Useful Commands

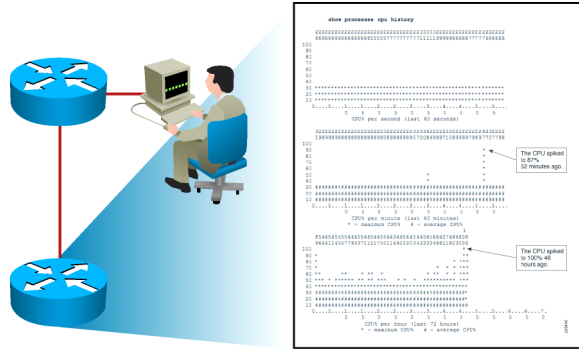
- The **show processes cpu** command displays the overall CPU utilization and the corresponding processes running on the router.



To determine the CPU utilization on a router, use the **show processes cpu** command. The output of this command shows how busy the CPU has been in the past 5 seconds, the past 1 minute, and the past 5 minutes. The output also shows the percentage of the available CPU time that each system process has used during these periods. In the output shown in the figure, the CPU utilization for the last 5 seconds was 72 percent. Out of this total of 72 percent, 23 percent of the CPU time was spent in interrupt mode, which corresponds to switching of packets. On the same line of output you can also see the average utilization for the last 1 minute (74 percent in this example) and the average utilization for the past 5 minutes (71 percent in this example).

Useful Commands (Cont.)

- The **show processes cpu history** command provides long-term CPU utilization information.



Use the **show processes cpu history** command to see the CPU utilization for the last 60 seconds, 60 minutes, and 72 hours. The command output for this command provides graphical views of how busy the CPU has been. You can see if the CPU has been constantly busy or if utilization has been spiking. CPU utilization spikes caused by a known network event or activity do not indicate problems, but if you see prolonged spikes that do not seem to correspond to any known network activity, this is reason to investigate.

Understanding Cisco IOS Switching Paths

This topic describes the different options that can be used for packet forwarding by Cisco routers.

Understanding Cisco IOS Switching Options

Cisco IOS switching paths are router packet forwarding methods, not to be confused with Layer 2 switching on switching.

- Switching methods:
 - Process switching
 - Fast switching
 - Cisco Express Forwarding
- Router platforms:
 - Software-based platforms
 - Hardware-based platforms

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0–5-12

To understand the different switching options and how they work, it is necessary to understand that there are different types of router platforms and each of these platforms has its own behavior. For example, Cisco 2800 Series Routers are based on a single CPU, and all functions of the router can be executed by the Cisco IOS Software running on the main CPU. However, many of the functions can be offloaded to separate network modules that can be installed into these routers. Cisco 7600 Series Routers are based on special hardware that is responsible for all packet-forwarding actions, which means that the main CPU is not involved in the processing of most packets.

Each router performs two steps when routing packets:

- Make a routing decision for the packet.
- Switch the packet.

The routing decision is made based on network topology information and configured policies. Information about network destinations, gathered by a routing protocol, and possible restrictions like access lists or policy-based routing (PBR), are used to decide where to send each packet.

Switching packets on a router (not to be confused with Layer 2 switching) involves moving a packet from an input buffer to an output buffer and rewriting the data link layer header of the frame to forward the packet on to the next hop toward the final destination.

The data link layer addresses that are necessary to rewrite the frame are stored in different tables such as the ARP table, which lists the MAC addresses for known IP devices reachable via Ethernet interfaces. Usually routers discover the data link layer addresses to be used for a destination via an address resolution process that matches the Layer 3 address to the Layer 2 address of a next hop device.

Three types of packet switching modes are supported by Cisco routers:

1. Process switching
2. Fast switching
3. Cisco Express Forwarding

The newest switching mode is Cisco Express Forwarding. It is the default, preferred, and recommended switching mode.

Process switching is the oldest mode, and before the router will fall back on it, first Cisco Express Forwarding and fast switching need to be disabled.

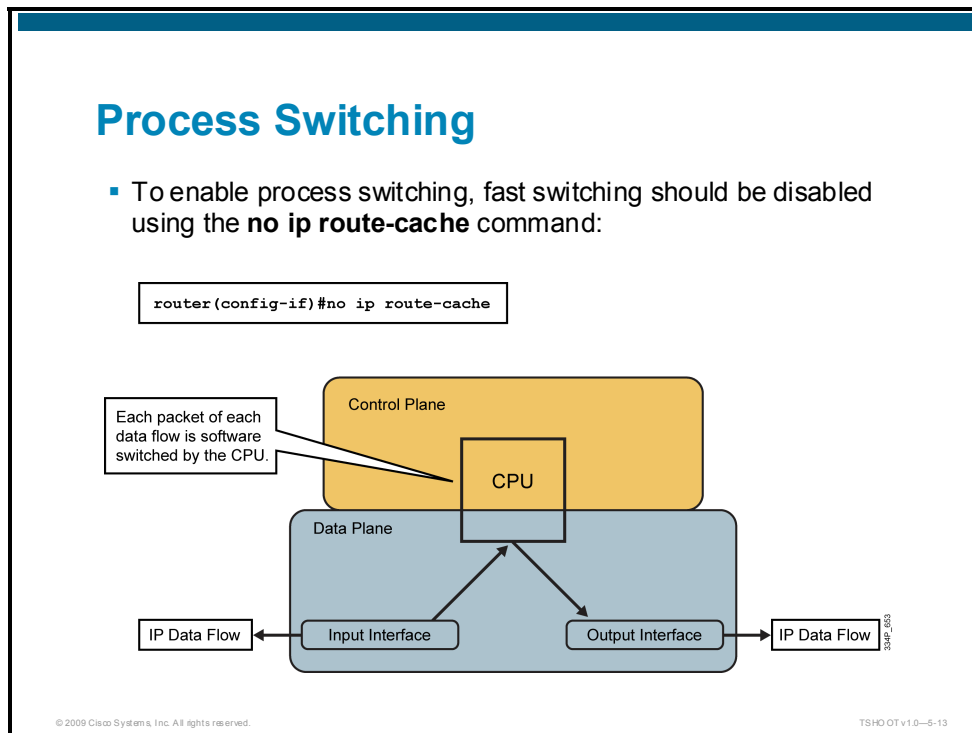
It is important to remember that the switching method that is used affects the router's performance. The switching method can be altered globally or per interface for several reasons:

- During troubleshooting, to verify whether the observed behavior is caused by the switching method
- During debugging, to direct all packets to CPU for processing
- Because some IOS features require a specific switching method

To successfully troubleshoot problems related to the switching path it is essential to understand which method is used and how it works. Specific troubleshooting techniques are explained and demonstrated in the following sections.

Process Switching

This subtopic describes how a router forwards packets using process switching.



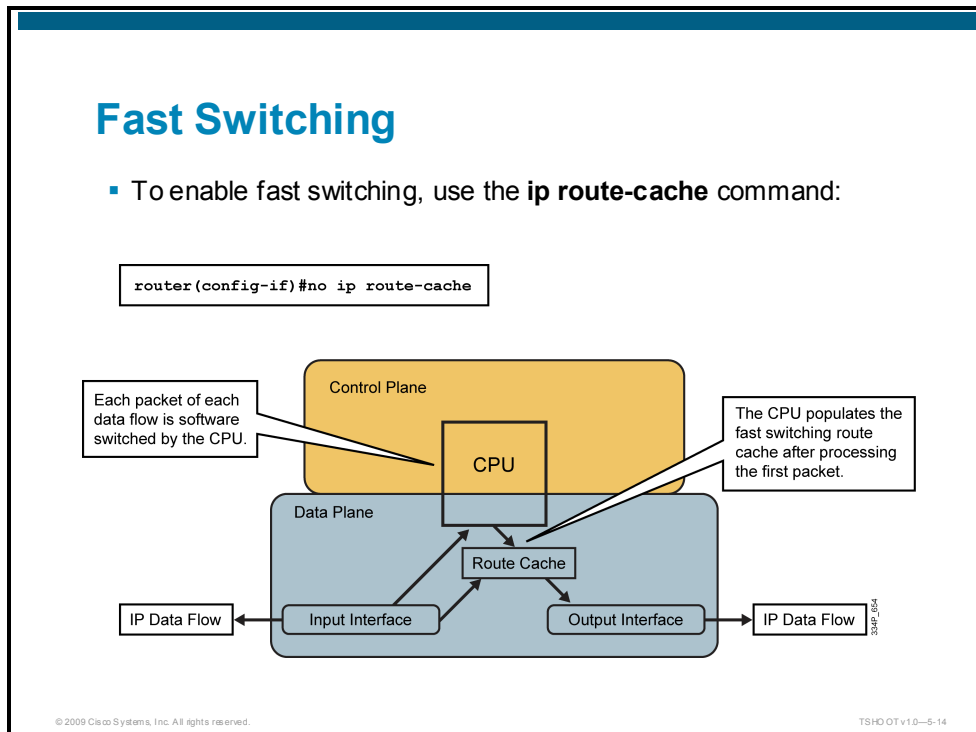
When using process switching to forward packets, the router strips the Layer 2 header from an incoming frame, looks up the Layer 3 network address in the routing table for the packet, and then sends the frame with a rewritten Layer 2 header, including a newly computed cyclical redundancy check (CRC) to the outgoing interface. All these operations are performed for each individual frame by the IP Input process that is running on the central CPU.

Process switching is configured on an interface by disabling fast switching (and Cisco Express Forwarding) on that interface. Remember that both process switching and fast switching are not the default modes of operation for a router.

Note Process switching is the most CPU-intensive method available on Cisco routers. It will greatly degrade performance figures like throughput, jitter, latency, and so on. That is why this method should be used only temporarily, as a last resort, during troubleshooting.

Fast Switching

This subtopic describes the differences between process switching and fast switching.



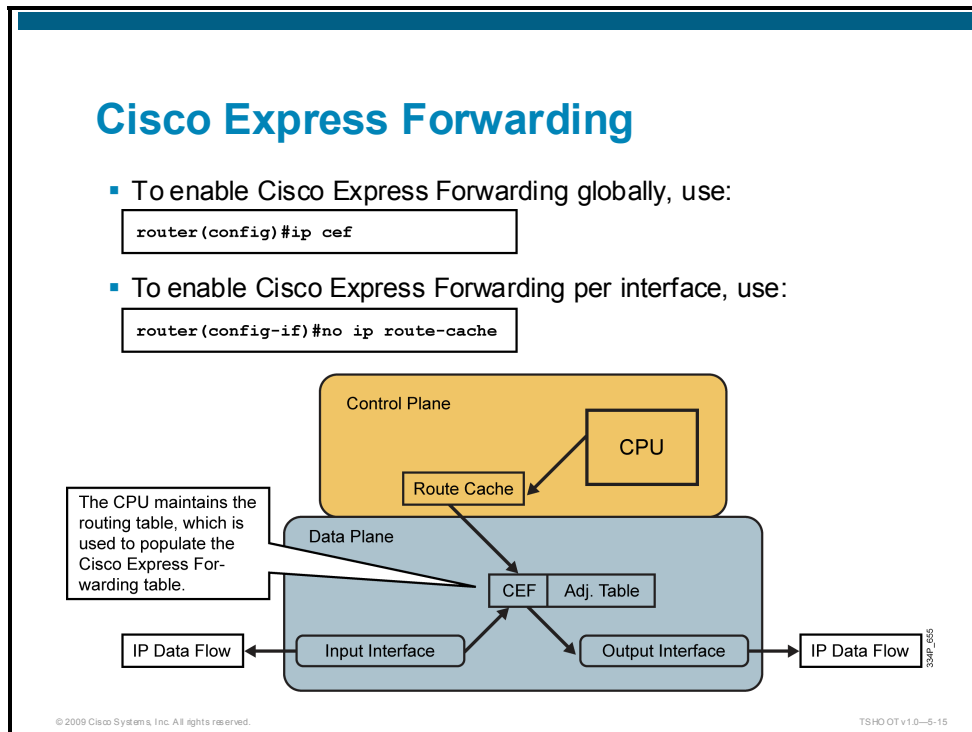
After performing a routing table lookup for the first packet destined for that IP network, the router also initializes the fast-switching cache that is used by the fast switching process. When subsequent frames to that same destination arrive, a cache lookup is performed and the destination is found in the fast switching cache. Then the frame is rewritten with the corresponding Data Link Layer header that was stored in the cache, and the frame is sent to the outgoing interface. The interface processor computes the cyclical redundancy check (CRC) for the frame. Because the cache is destination based, fast switching can provide load sharing on a per-destination basis.

By default, fast switching is enabled on all interfaces that support this mode. It is less processor intensive than process switching, because it uses a cache entry created by the first packet sent to a particular destination.

Note Note that the fast switching method can lead to high CPU utilization in case there are a high number of new flows per second. This effect is normal for this switching mode and can lead to CPU overload in case of a network attack that generates too many new flows rapidly.

Cisco Express Forwarding

This subtopic describes Cisco Express Forwarding.



Cisco Express Forwarding is the default switching mode on Cisco routers. Cisco Express Forwarding is less CPU-intensive than fast switching or process switching. Cisco Express Forwarding is a highly scalable and resilient switching technique. For example, during dynamic network changes, there is no need to rebuild and maintain fast-switching cache entries for many different destinations by doing packet route lookups.

When Cisco Express Forwarding is enabled, information used for packet forwarding purposes resides in the following two tables:

- Cisco Express Forwarding Information Base (FIB)
- Adjacency table

A router that has Cisco Express Forwarding enabled uses the FIB to make IP destination prefix-based switching decisions. This table is updated after each network change, but only once, and it contains all known routes. There is no need to build a route-cache by first using process switching for some of the packets. Each change in the IP routing table triggers a similar change in the FIB table, because it contains all next-hop addresses associated with all network destinations.

The adjacency table contains Layer 2 frame headers for all next hops used by the FIB. These addresses are used to rewrite frame headers for packets that are forwarded by a router.

Both tables are built independently, and a change in one table does not lead to a change in the other.

Cisco Express Forwarding is an efficient mechanism for traffic load balancing. In this case, both the FIB and the adjacency table contain multiple entries for a single network destination to reflect the multiple network paths toward it.

It is important to note that there are Cisco IOS features that require Cisco Express Forwarding to be enabled for their operation because they rely on the data structures that are built and maintained by Cisco Express Forwarding. Some of these are Network-Based Application Recognition (NBAR), Cisco AutoQoS, Modular QoS CLI (MQC)-based Frame Relay traffic shaping (FRTS), Multiprotocol Label Switching (MPLS) quality of service (QoS), and class-based weighted random early detection (CBWRED).

Troubleshooting Process and Fast Switching

This subtopic describes the Cisco IOS commands that can be used to troubleshoot process switching and fast switching.

Troubleshooting Process and Fast Switching

- The **show ip interface** command can be used to display which switching method is used on a particular interface:

```
router#show ip interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
<... output omitted ...>
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast
<... output omitted ...>
```

The figure shows an example of the output of the **show ip interface** command after disabling the default Cisco Express Forwarding packet switching mode.

In the output, it can be seen that fast switching is enabled for all packets, except for packets that are sent back to the same interface that they came in on. Cisco Express Forwarding switching is disabled. Flow switching, which is also disabled, is related to NetFlow—a Cisco IOS feature that can be used to collect, export, and store accounting data for IP traffic.

If you decide that you need to use process switching, you can achieve this by disabling fast switching on the interface (which is turned on by default) as follows:

```
router(config-if)#no ip route-cache
```

When you repeat the **show ip interface command** you can see that this particular interface is not using fast switching anymore:

```
router#show ip interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
<... output omitted ...>
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast
<... output omitted ...>
```

Multicast fast switching, however is still enabled. This is because IP multicast routing is configured entirely separately from IP unicast routing, and there are separate configuration statements related to unicast and multicast operations. The command used here to disable fast switching only applies to unicast packets. To disable fast switching for multicast packets, the following command is available:

```
router(config-if)#no ip mroute-cache
```

Disabling fast switching increases the load on the system CPU, because every packet is processed by the IP Input process on the router CPU. There are however situations when disabling fast switching might be necessary—for example, during troubleshooting of connectivity problems, to eliminate the use of the fast-switching cache, and to allow processing of all packets by the router CPU.

Troubleshooting Process and Fast Switching (Cont.)

- The **show ip cache** command can be used to display the current entries in the fast switching cache:

```
router#show ip cache
IP routing cache 4 entries, 784 bytes
  5 adds, 1 invalidates, 0 refcounts
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
  quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last second, 0 in last 3 seconds
Last full cache invalidation occurred 00:11:31 ago

Prefix/Length      Age           Interface     Next Hop
10.1.1.1/32        00:07:20     FastEthernet0/0 10.1.1.1
10.2.1.1/32        00:04:18     FastEthernet0/1 10.2.1.1
10.10.1.0/24       00:01:06     FastEthernet0/0 10.1.1.1
10.11.1.0/24       00:01:20     FastEthernet0/1 10.2.1.1
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--5-17

The **show ip cache** command displays the content of the fast switching cache. If fast switching is disabled on a particular interface, this cache will not have any network entries for that interface. The route cache is periodically cleared to remove stale entries and make room for new entries.

This command is very useful when troubleshooting, because it shows that the fast switching cache is initialized and populated with information for different network prefixes and associated outgoing interfaces.

In addition, you can check the router CPU utilization due to packet processing. You should look for the “IP Input” process by using the following command:

```
router#show processes cpu | include Input
15      28145908 168211769      167  0.23%  0.12%  0.12%  0 ARP Input
43       741036  48271269       15   0.00%  0.00%  0.00%  0 Net Input
51         0      1         0   0.00%  0.00%  0.00%  0 SDCC Input
68      86097192 868428111       99  0.47%  0.36%  0.44%  0 IP Input
108        0      10        0   0.00%  0.00%  0.00%  0 Probe Input
109        0      6         0   0.00%  0.00%  0.00%  0 RARP Input
146     56294460 144682916      389  0.39%  0.11%  0.11%  0 LSDp Input Proc
```

Troubleshooting Cisco Express Forwarding

This topic describes the Cisco IOS commands that can be used to troubleshoot Cisco Express Forwarding.

Troubleshooting Cisco Express Forwarding

- The **show ip interface** command can be used to display whether Cisco Express Forwarding is enabled on the interface:

```
router#show ip interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
<... output omitted ...>
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast
<... output omitted ...>
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-18

Cisco Express Forwarding builds two main data structures for its operation: the FIB and adjacency tables. When troubleshooting Cisco Express Forwarding you need to check both tables and correlate entries between them.

The following list shows items that should be checked and verified when troubleshooting Cisco Express Forwarding:

- Is Cisco Express Forwarding enabled globally and per interface?
- Is there a Forwarding Information Base (FIB) entry for a given network destination?
- Is there a next hop associated with this entry?
- Is there an adjacency entry for this next hop?

To find out if Cisco Express Forwarding is enabled on particular interface, use the **show ip interface** command. As you can see in the figure, the output of this command clearly states whether Cisco Express Forwarding switching is enabled or not.

Troubleshooting Cisco Express Forwarding (Cont.)

- The **show ip cef** command can be used to display whether Cisco Express Forwarding is enabled globally and to display the prefixes present in the Cisco Express Forwarding FIB:

```
router#show ip cef
Prefix          Next Hop          Interface
0.0.0.0/0       10.14.14.19      GigabitEthernet0/0
0.0.0.0/32      receive
10.14.14.0/24   attached         GigabitEthernet0/0
10.14.14.0/32   receive
<... output omitted ...>
10.14.14.255/32 receive
224.0.0.0/4     drop
224.0.0.0/24    receive
255.255.255.255/32 receive
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--5-19

If Cisco Express Forwarding is enabled on the router, output similar to the output in the figure can be observed when you issue the **show ip cef** command. This command displays the contents of the FIB table of a router.

All directly connected networks in the output are marked as “attached” in the “next-hop” field. Network prefixes that are local to the router are marked as “receive.”

Note that Cisco Express Forwarding switching mode is enabled globally, and the command output shown in the figure reflects this situation. This command can also be used to verify whether Cisco Express Forwarding is disabled globally on a router. The command does not display the interfaces on which Cisco Express Forwarding is explicitly disabled.

In this example, we have a default static route configured in a router, and this piece of routing information is entered as forwarding information into the FIB table with following details:

```
router#show ip cef 0.0.0.0 0.0.0.0
0.0.0.0/0, version 22, epoch 0, cached adjacency 10.14.14.19
0 packets, 0 bytes
  via 10.14.14.19, 0 dependencies, recursive
    next hop 10.14.14.19, GigabitEthernet0/0 via 10.14.14.19/32
    valid cached adjacency
```

The output shows that the router uses output interface GigabitEthernet0/0 and next-hop 10.14.14.19/32 to reach the destination of the default route. We can also see what other destinations are associated with this interface/next-hop pair:

```
router#show ip cef adjacency GigabitEthernet0/0 10.14.14.19 detail
IP CEF with switching (Table Version 24), flags=0x0
 23 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 0
 2 instant recursive resolutions, 0 used background process
28 leaves, 22 nodes, 26516 bytes, 79 inserts, 51 invalidations
0 load sharing elements, 0 bytes, 0 references
universal per-destination load sharing algorithm, id 56F4BAB5
4(1) CEF resets, 2 revisions of existing leaves
Resolution Timer: Exponential (currently 1s, peak 1s)
1 in-place/0 aborted modifications
refcounts: 6223 leaf, 6144 node
```

```

Table epoch: 0 (23 entries at this epoch)

Adjacency Table has 13 adjacencies
0.0.0.0/0, version 22, epoch 0, cached adjacency 10.14.14.19
0 packets, 0 bytes
  via 10.14.14.19, 0 dependencies, recursive
    next hop 10.14.14.19, GigabitEthernet0/0 via 10.14.14.19/32
    valid cached adjacency
10.14.14.19/32, version 11, epoch 0, cached adjacency 10.14.14.19
0 packets, 0 bytes
  via 10.14.14.19, GigabitEthernet0/0, 1 dependency
    next hop 10.14.14.19, GigabitEthernet0/0
    valid cached adjacency

```

This output shows you that this specific combination of output interface and next hop is used to reach two network destinations: the default route and a specific host destination.

Troubleshooting Cisco Express Forwarding (Cont.)

- The **show adjacency** command can be used to display the entries in the adjacency table:

```
router#show adjacency GigabitEthernet 0/0 detail | begin 10.14.14.19
Protocol Interface Address
IP GigabitEthernet0/0 10.14.14.9(5)
0 packets, 0 bytes
001200A2BC41001BD5F9E7C00800
ARP 03:19:39
Epoch: 0
<... further output omitted ...>
```

Points to remember:

- Both the Cisco Express Forwarding FIB and adjacency tables should be checked.
- Entries in both tables need to be correlated.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--5-20

The next thing to check is the adjacency table entries for this next hop:

```
router#show adjacency GigabitEthernet 0/0 detail | begin 10.14.14.19
Protocol Interface Address
IP GigabitEthernet0/0 10.14.14.9(5)
0 packets, 0 bytes
001200A2BC41001BD5F9E7C00800
ARP 03:19:39
Epoch: 0
[...]
```

In this entry you can see the full Layer 2 frame header associated with this next hop, which has been built through ARP. The Layer 2 MAC address for this next-hop IP address can also be checked in the ARP cache:

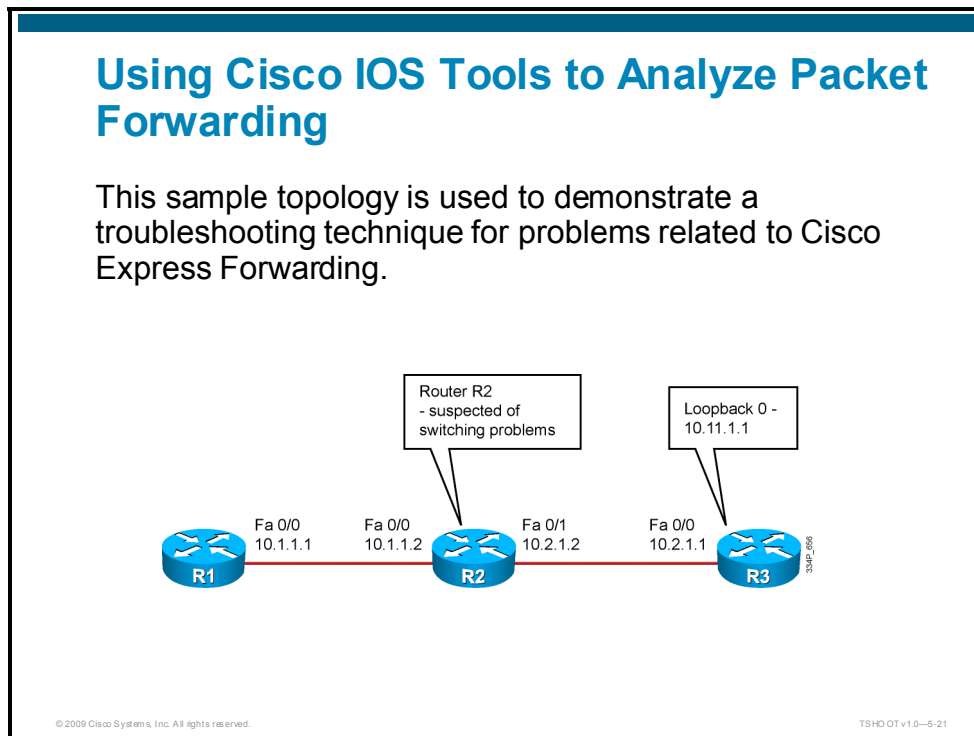
```
router#show ip arp 10.14.14.19
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.14.14.19 4 0012.009a.0c42 ARPA
GigabitEthernet0/0
```

Finally, the CPU might process some packets, even if Cisco Express Forwarding is enabled. This can happen for reasons such as an incomplete adjacency table or packets that need special handling by the main processor:

```
router#show cef not-cef-switched
CEF Packets passed on to next switching layer
Slot No_adj No_encap Unsupp'ted Redirect Receive Options Access Frag
RP 424260 0 5227416 67416 2746773 9 15620 0
```

Cisco IOS Tools to Analyze Packet Forwarding

This subtopic shows an example of how to use the different Cisco IOS commands to troubleshoot problems related to router switching paths.



Cisco IOS Software is a powerful operating system that has an embedded set of tools to assist in troubleshooting various networking problems. These tools allow network administrators to quickly and effectively find, isolate, and repair IP communication problems.

The following series of steps shows you an example of a troubleshooting process that could be used to find problems related to the switching path used by a router. Be aware that the actual routers used for command outputs in this example do not have any problems. The aim is to show the Cisco IOS commands in action.

Step 1 First try to find the problematic router along the path with the traceroute utility:

```
R1#traceroute 10.11.1.1

Type escape sequence to abort.
Tracing the route to 10.11.1.1

 0 10.1.1.1 0 msec 0 msec 0 msec
 1 10.1.1.2 72 msec 56 msec 64 msec
 2 10.2.1.1 76 msec 104 msec *
```

Although the output seems normal, suppose for the case study that the **traceroute** command would have shown a much higher delay or packet loss on router R2 compared to router R3. Such symptoms can lead you to suspect problems in router R2.

Step 2 Check the CPU utilization on router R2 for load due to packet processing:

```
R2#show processes cpu | exclude 0.00
CPU utilization for five seconds: 4%/0%; one minute: 1%; five minutes: 1%
PID Runtime(ms)   Invoked    uSecs   5Sec   1Min   5Min  TTY Process
   2      3396         650      5224   0.08%   0.07%  0.10%   0 Load Meter
   3     11048         474     23308   3.27%   0.51%  0.37%   0 Exec
  99     13964        6458      2162   0.90%   0.66%  0.71%   0 DHCPD Receive
 154       348         437       796   0.08%   0.09%  0.08%   0 CEF process
```

In this case study, there are no problems related to packet processing.

Step 3 Check the routing table for the corresponding destination prefix:

```
R2#show ip route 10.11.1.1
Routing entry for 10.11.1.1/32
  Known via "ospf 1", distance 110, metric 11, type intra area
  Last update from 10.2.1.1 on FastEthernet0/1, 00:29:20 ago
  Routing Descriptor Blocks:
    * 10.2.1.1, from 10.11.1.1, 00:29:20 ago, via FastEthernet0/1
      Route metric is 11, traffic share count is 1
```

In this case study, the routing information is present.

Step 4 Find which switching mode is used by the router and on the interfaces involved in packet forwarding:

```
R2#show ip cef
Prefix                Next Hop                Interface
0.0.0.0/0             drop                   Null0 (default route handler entry)
0.0.0.0/32            receive
10.1.1.0/24           attached              FastEthernet0/0
10.1.1.0/32           receive
10.1.1.1/32           10.1.1.1              FastEthernet0/0
10.1.1.2/32           receive
10.1.1.255/32         receive
10.2.1.0/24           attached              FastEthernet0/1
10.2.1.0/32           receive
10.2.1.1/32           10.2.1.1              FastEthernet0/1
10.2.1.2/32           receive
10.2.1.255/32         receive
10.10.1.1/32          10.1.1.1              FastEthernet0/0
10.11.1.1/32          10.2.1.1              FastEthernet0/1
224.0.0.0/4           drop
224.0.0.0/24          receive
255.255.255.255/32    receive
```

```
R2#show ip interface FastEthernet 0/0 | include CEF
IP CEF switching is enabled
IP CEF Fast switching turbo vector
IP route-cache flags are Fast, CEF
```

```
R2#show ip interface FastEthernet 0/1 | include CEF
IP CEF switching is enabled
IP CEF Fast switching turbo vector
IP route-cache flags are Fast, CEF
```

In this case study, Cisco Express Forwarding is enabled globally, and all involved interfaces are enabled for Cisco Express Forwarding switching.

Step 5 Check the FIB entry for the routing information referenced here:

```
R2#show ip cef 10.11.1.1 255.255.255.255
10.11.1.1/32, version 13, epoch 0, cached adjacency 10.2.1.1
0 packets, 0 bytes
  via 10.2.1.1, FastEthernet0/1, 0 dependencies
    next hop 10.2.1.1, FastEthernet0/1
    valid cached adjacency
```

In this case study, the related adjacency entry shows interface FastEthernet0/1 with next-hop 10.2.1.1.

Step 6 Check adjacency table for the next-hop referenced here:

```
R2#show adjacency FastEthernet0/1 detail
Protocol Interface                Address
IP        FastEthernet0/1         10.2.1.1(7)
                                         203 packets, 307342 bytes
                                         C40202640000C4010F5C00010800
ARP        02:57:43
```

In this case study, relevant adjacency is built via ARP protocol.

Step 7 Check the ARP cache entry for this next hop:

```
R2#show ip arp
Protocol Address          Age (min)  Hardware Addr  Type   Interface
Internet 10.2.1.1              67        c402.0264.0000 ARPA   FastEthernet0/1
Internet 10.1.1.2              -         c401.0f5c.0000 ARPA   FastEthernet0/0
Internet 10.1.1.1              67        c400.0fe4.0000 ARPA   FastEthernet0/0
Internet 10.2.1.2              -         c401.0f5c.0001 ARPA   FastEthernet0/1
```

You see that the MAC address information is present in the router. So, based on this verification process, you can conclude that the routers in this case study do not have any switching-related problems.

Nevertheless, the steps shown here can be used as a generic procedure for finding issues with Cisco Express Forwarding switching. The advantage of using Cisco IOS commands for troubleshooting is that these commands are always available for use by networking staff.

Troubleshooting Router Memory Issues

This topic describes typical symptoms and common causes of router memory problems.

Troubleshooting Router Memory Issues

- Router memory issues occur when:
 - A router has used all available memory either temporarily or permanently.
 - The memory has fragmented into such small pieces that the router cannot find a usable available block.
- Symptoms of memory problems:
 - %SYS- 2- MALLOCFAIL messages are logged.
 - No output from **show** commands.
 - “Low on memory” messages are displayed.
 - The console message “Unable to create EXEC—no memory or too many processes.”

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-22

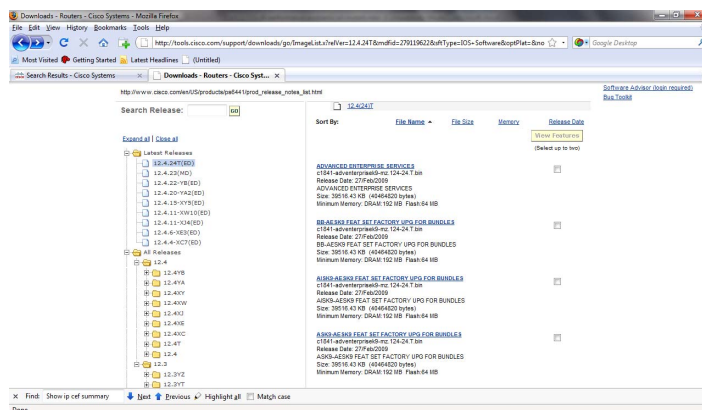
Memory allocation failure is the most common router memory issue. Memory allocation failures happen when the router has used all available memory (temporarily or permanently), or when the memory has been fragmented into such small pieces that the router cannot find a usable available block. This can happen to the processor memory, which is used by the Cisco IOS Software, or to the packet memory, which is used to buffer incoming and outgoing packets.

Symptoms of memory allocation failures include these:

- Messages such as "%SYS-2-MALLOCFAIL: Memory allocation of 1028 bytes failed from 0x6015EC84, Pool Processor, alignment 0" being displayed in the router logs.
- Not getting any output from **show** commands.
- Receiving “low on memory” messages.
- Receiving the message “Unable to create EXEC – no memory or too many processes” on the console.
- When a router is low on memory, in some instances it is not even possible to use Telnet to connect to the router. When you get to this point, you need to get access to the console port to collect data for troubleshooting. When connecting to the console port, however, you might see the “Unable to create EXEC – no memory or too many processes” message. If you see this message, there is not even enough available memory to allow for a console connection.

Common Memory Problems

- The router memory does not support the Cisco IOS Software image:
 - You can research memory requirements for Cisco IOS Software online.
 - For example, the Cisco 1841 Advanced Enterprise Services IOS image requires at least 192 MB of DRAM and 64 MB of flash memory.



- **Memory size does not support the Cisco IOS Software image:** First, check the Release Notes (available to registered customers only) or the Cisco IOS Upgrade Planner (available to registered customers only) for the minimum memory size for the Cisco IOS Software feature set and version that you are running. Make sure that you have sufficient memory in your router to support the software image. The actual memory requirements vary based on protocols used, routing tables, and traffic patterns on the network.

Common Memory Problems (Cont.)

- Memory leak bugs:
 - The **show memory allocating-process totals** command displays how much memory is used by the router processes, how much memory is free, and the per-process memory utilization.
 - This information can be used to identify memory leaks caused by software bugs.

```
router# show memory allocating-process totals
      Head      Total(b)    Used(b)    Free(b)    Lowest(b)    Largest(b)
Processor 62A2B2D0 183323952 26507580 156816372 155132764 154650100
I/O      ED900000 40894464 4957092 35937372 35887920 35930524
Allocator PC Summary for: Processor
      PC      Total    Count    Name
0x6136A5A8 5234828      1    Init
0x608E2208 3576048     812    TTY data
0x6053ECBC 1557568     184    Process Stack
0x61356928 1365448      99    Init
<... output truncated ...>
```

© 2009 Cisco Systems, Inc. All rights reserved.

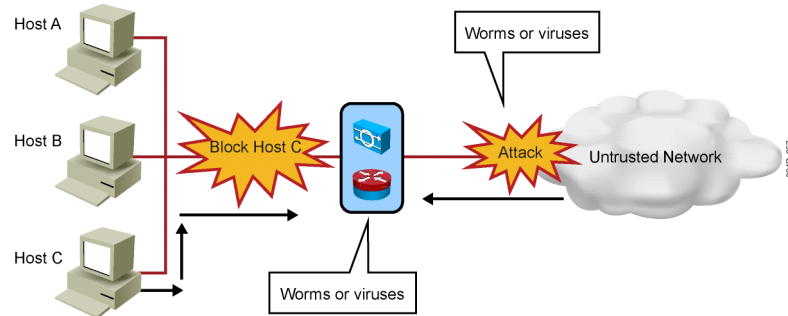
TSHOOT v1.0—5-24

- **Memory leak bug:** A memory leak occurs when a process requests or allocates memory and then forgets to free (deallocate) the memory when it is finished with that task. As a result, the memory block stays reserved until the router is reloaded. The **show memory allocating-process totals** command will help you to identify how much memory is used, how much memory is free, and the per-process memory utilization of the router. Memory leaks are caused by bugs in the Cisco IOS code, and the only solution is to upgrade the Cisco IOS Software on the device to a version that fixes the issue.

Common Memory Problems (Cont.)

Security-related problem:

- You have a security issue in your network.
- Add additional entries to the access list to block infected host.
- Use a firewall and an IPS to protect your internal network.



© 2009 Cisco Systems, Inc. All rights reserved.

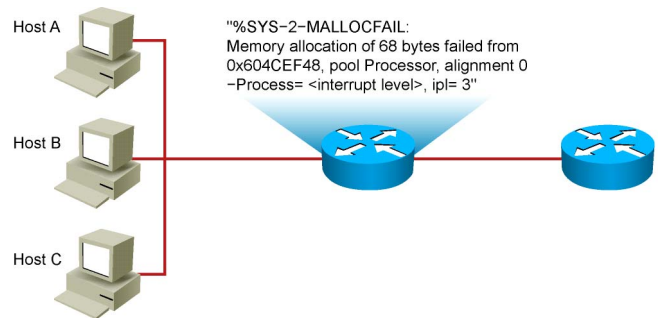
TSHOOT v1.0-6-25

- **Security-related problems:** MALLOCFAIL errors can also be caused by a security issue, such as a worm or virus operating in your network. This is especially likely to be the cause if there have not been any recent changes to the network, such as router Cisco IOS upgrades or configuration changes. The effect of this type of problem can often be mitigated by adding a number of configuration statement to your router, such as an access list that drops the traffic generated by the worm or virus. The Cisco Product Security Advisories and Notices page contains information on detection of the most likely causes and specific workarounds.

Common Memory Problems (Cont.)

Memory allocation failure:

- When you see a %SYS-2- MALLOCFAIL log message:
 - Use the Bug Toolkit to search for a matching software bug.
 - Upgrade the Cisco IOS Software to a version that resolves the issue.



- **Memory allocation failure at process = interrupt level:** The process in the error message can identify this situation. If the process is listed as <interrupt level>, as in the following example, then the memory allocation failure is being caused by a software problem. You can use the Bug Toolkit to search for a matching software bug ID (unique bug identification) for this issue. After the software bug has been identified, upgrade to a Cisco IOS Software version that contains the fix to resolve the problem.

```
%SYS-2-MALLOCFAIL: Memory allocation of 68 bytes failed from
0x604CEF48, pool Processor, alignment 0-Process= <interrupt
level>, ipl= 3
```

Common Memory Problems (Cont.)

- Buffer leak bugs
 - The **show interfaces** command displays interface status, input, output queue size, interface error, and packet drops.
 - The output in this example shows a “wedged” input queue, which is a symptom of a buffer leak.

```
router#show interfaces
<... output omitted ...>
ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:58, output never, output hang never
  Last clearing of "show interface" counters never
  input queue 76/75, 1250 drops
  Output queue 0/40, 0 drops;
<... output omitted ...>
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-27

- **Buffer leak bug:** When a process is finished using a buffer, the process should free the buffer. A buffer leak occurs when the code forgets to free it. As a result, the buffer pool continues to grow as more and more packets are stuck in the buffers.

The **show interfaces** command displays statistics for all interfaces configured on the router. The figure shows an example of output from the **show interfaces** command, which shows that the interface input queue is wedged

The symptom of such buffer leak is a full input queue (76/75). Here, the values 76 and 75 represent the number of packets in the input queue, and the maximum size of the input queue, respectively. In this case, the number of packets in the input queue is larger than the queue depth. This is called a wedged interface. When the input queue of an interface is wedged, the router no longer forwards traffic that enters the affected interface.

Common Memory Problems (Cont.)

- Buffer leak bugs
 - The **show buffer** command displays information related to the packet buffers on the router.
 - The output in this example shows symptoms of a buffer leak in one of the system buffer pools.

```
router#show buffers
<... output omitted ...>
Middle buffers, 600 bytes (total 17602, permanent 170):
  11 in free list (10 min, 400 max allowed)
    498598 hits, 148 misses, 671 trims, 657 created
    0 failures (0 no memory)
<... output omitted ...>
```

The **show buffers** command displays statistics for the buffer pools on the router. In the figure, the **show buffers** command output reveals a buffer leak in the middle buffers pool. There are 17602 middle buffers in the router, and only 11 are in the free list. This implies that some process takes all the buffers but does not return them. Other symptoms of this type of buffer leak are “%SYS-2-MALLOCFAIL” error messages for the pool “processor” or “input/output (I/O),” based on the platform. Similar to a generic memory leak, a buffer leak is caused by a software bug, and the only solution is to upgrade the Cisco IOS Software on the device to a version that fixes the issue.

BGP Memory Use

- BGP is very memory intensive and requires careful planning.
- The **show process memory** command can be used to determine the total amount of memory allocated to the processor pool and the I/O pool and how much memory has been allocated to certain process, such as BGP in this case.

```
router#show processes memory
```

Processor Pool	Total:	140312928	Used:	24470312	Free:	115842616
I/O Pool	Total:	12582912	Used:	4960688	Free:	7622224

PID	TTY	Allocated	Freed	Holding	Getbufs	Retbufs	Process
266	0	40808	636	11948	4	4	BGP Router
267	0	5316	0	12376	22	22	BGP I/O
268	0	0	0	10060	0	0	BGP Scanner
269	0	0	0	7060	0	0	BGP Event

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-29

Cisco IOS has three main processes used by BGP: BGP I/O, BGP router, and BGP scanner. The BGP I/O process handles reading, writing, and executing of all BGP messages. This process is also the interface between TCP and BGP. The BGP router process is responsible for initiation of a BGP process, session maintenance, processing of incoming updates, sending of BGP updates, and updating the IP Routing Information Base (RIB) with BGP entries. The BGP scanner process performs periodic scans of the BGP RIB to update it as necessary, and it scans the IP RIB to ensure that all BGP next hops are valid.

As you can see, the BGP Router process consumes the majority of the memory used by BGPs. The BGP router process uses memory to store the BGP RIB, IP RIB for BGP prefixes, and IP switching data structures for BGP prefixes. If you do not have enough memory to store this information, BGP cannot operate in a stable manner, and network reliability will be compromised.

If you are using chassis-based routers, which distribute routing information to the line cards, you should check not only the memory availability for the route processor, but also the memory availability on the line cards.

BGP Memory Use (Cont.)

- The **show diag** command can be used to display memory installed on router line cards.
- This command can help establish whether enough memory is available on the line cards.

```
Router# show diag | i (DRAM|SLOT)
SLOT 0 (RP/LC 0 ): 1 Port SONET based SRP OC-12c/STM-4 Single Mode
  DRAM size: 268435456 bytes
  FrFab SDRAM size: 134217728 bytes, SDRAM pagesize: 8192 bytes
  ToFab SDRAM size: 134217728 bytes, SDRAM pagesize: 8192 bytes
SLOT 2 (RP/LC 2 ): 12 Port Packet over E3
  DRAM size: 67108864 bytes
  FrFab SDRAM size: 67108864 bytes
  ToFab SDRAM size: 67108864 bytes
SLOT 3 (RP/LC 3 ): 1 Port Gigabit Ethernet
  DRAM size: 134217728 bytes
  FrFab SDRAM size: 134217728 bytes, SDRAM pagesize: 8192 bytes
  ToFab SDRAM size: 134217728 bytes, SDRAM pagesize: 8192 bytes
SLOT 5 (RP/LC 5 ): Route Processor
  DRAM size: 268435456 bytes
```

The **show diag** command displays the different types of cards present in your router, and their respective amounts of memory. This command can be useful to identify a lack of memory on the line cards when the router runs BGP.

Summary

Summary

- You have learned to recognize the typical symptoms associated with high CPU utilization on a router, the associated causes, and how to use Cisco IOS commands to identify and solve performance problems caused by high CPU utilization.
- Troubleshooting switching paths is a complex process that requires in-depth knowledge of Cisco IOS switching operation.
- You have learned to recognize the symptoms associated with memory allocation failures and common memory problems; how to identify different types of buffer leaks, such as wedged interface buffers and system buffer leaks; and how to plan and determine BGP memory requirements to prevent memory problems.

Lab 5-4 Debrief

Overview

In this lab, you have practiced troubleshooting router performance problems related to high CPU usage and memory exhaustion. You have created a troubleshooting plan to coordinate the work between the team members. You have methodically researched the problems, kept a log of your actions and findings, resolved the problems, and documented your solutions.

During the lab debrief, the instructor will lead a group discussion during which you can present your solutions. You will get an opportunity to verify your solution against a number of checkpoints provided by the instructor and compare your solution to other students' solutions. The instructor will discuss alternate solutions and their benefits and drawbacks.

Objectives

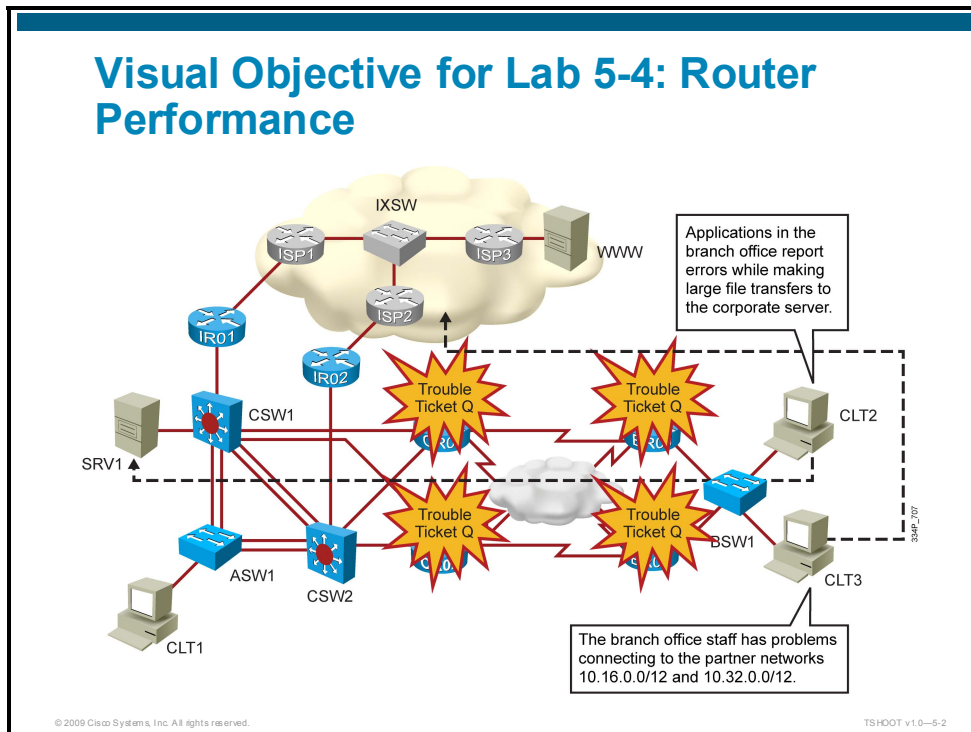
Upon completing this lesson, you will be able to diagnose and resolve performance problems related to high CPU and memory utilization. This ability includes being able to meet these objectives:

- Review and verify your solution, your findings, and your action log against a set of checkpoints provided by the instructor
- Consolidate the lessons learned during the review discussions into a set of best-practice methods and commands to aid you in future troubleshooting procedures

Review and Verification

This topic describes the problems that were introduced in Lab 5-4, asks how you can verify that you have solved the problems, and gives an example of a troubleshooting process that will allow you to find and resolve the issues.

Note This lesson provides sample answers and solutions to the questions posed during the debrief discussions. Keep in mind that alternate solutions and methods might be just as valid and that the solutions provided here only highlight a sample approach and solution.



This lab consists of one trouble ticket, which provided an opportunity to experience the typical symptoms associated with high CPU utilization and memory exhaustion. The memory problems introduced in this ticket were caused by the reception of several huge Border Gateway Protocol (BGP) tables by routers BRO1 and BRO2. The major causes of the problems related to high CPU utilization were that Cisco Express Forwarding and fast switching had been disabled on routers CRO1 and CRO2, and that these same routers were also configured to process a huge access list for all packets that flow through these routers.

Trouble Ticket Q: Problems with Connectivity

The text introducing this trouble ticket was the following:

It is Monday morning, and as soon as you enter your office in the headquarters you receive a call from your colleague from the branch office. He tells you that client applications report errors while connecting to the corporate server for large file transfers. In addition, he has received complaints from sales staff about slow or no connection at all to partner servers outside the corporate network, which reside in the IP address blocks 10.16.0.0/12 and 10.32.0.0/12.

You remember a colleague of yours, working on night shifts in that office, who currently studies Cisco CCNP® materials and has full access to branch and central office routers. What could he have done? As usual you must rely on your great troubleshooting skills to resolve this mess quickly.

Your intuition tells you that you need to deal with the connectivity to networks 10.16.0.0/12 and 10.32.0.0/12 first.

Trouble Ticket Q: Review and Discuss

How did your team approach Trouble Ticket Q?

- What was your work plan?
- What method did you use to solve this ticket?
- How did you coordinate and communicate with your team?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you accomplish the goal of restoring connectivity to external networks 10.16.0.0/12 and 10.32.0.0/12?
- Did you accomplish to correct the switching path in both CRO1 and CRO2 routers?
- How did you verify that you accomplished your goal?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--6-3

Although there are various ways to approach these problems, you should probably focus on the memory allocation problems on routers BRO1 and BRO2 first. The memory allocation problems on these routers cause packet forwarding on these routers to be affected to the point where many packets are dropped and it is not possible to forward even a minimal amount of traffic through these routers without losing packets. Only after addressing the memory problems caused by BGP on routers BRO1 and BRO2 will it be possible to generate enough traffic to overload the CPU on routers CRO1 and CRO2.

Key Clue: Memory Allocation Problems on Routers BRO1 and BRO2

- Ping from switch BSW1 and client PCs CLT2 and CLT3 to IP addresses in networks 10.16.0.0/12 and 10.32.0.0/12 experience high packet loss.
- The logs of routers BRO1 and BRO2 contain messages that indicate the problem:

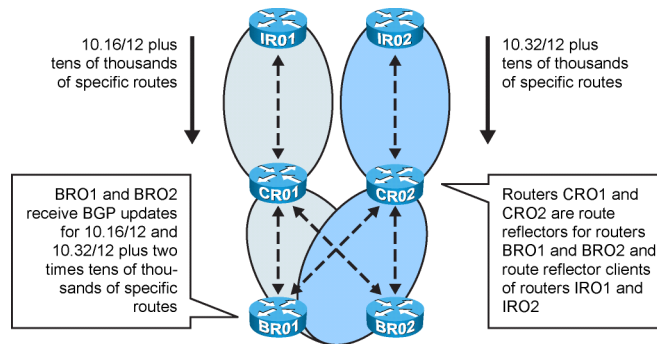
```
*May 26 10:39:09 PDT: %SYS-2-MALLOCFAIL: Memory allocation of 65536 bytes
failed from 0x601EE254, alignment 16
Pool: Processor Free: 18668 Cause: Not enough free memory
Alternate Pool: None Free: 0 Cause: No Alternate pool
-Process= "IP RIB Update", ipl= 3, pid= 76 -Traceback= 0x60965578 0x601DE0A8
0x601E2E5C 0x601E428C 0x601EE25C 0x601EF2EC 0x60219388 0x60B5857C 0x60B5DAD4
0x60B65228 0x60B6689C 0x60B7FF5C 0x60F442E8 0x60F15500 0x615714E8 0x615714CC
*May 26 10:39:09 PDT: %FIB-3-NOMEM: Malloc Failure, disabling CEF -Traceback=
0x60965578 0x60B585D8 0x60B5DAD4 0x60B65228 0x60B6689C 0x60B7FF5C 0x60F442E8
0x60F15500 0x615714E8 0x615714CC
*May 26 10:39:14 PDT: %BGP-3-NOTIFICATION: sent to neighbor 10.1.220.2 3/1
(update malformed) 0 bytes
```

Several clues regarding the memory allocation problems caused by BGP can be found on routers BRO1 and BRO2:

- Using ping to test the connectivity to 10.16.0.1 and 10.32.0.1 reveals a high percentage of packet loss.
- The logs in routers BRO1 and BRO2 contain “%SYS-2-MALLOCFAIL” and “%FIB-3-NOMEM” log messages that indicate memory exhaustion.
- The logs in routers BRO1, BRO2, CRO1 and CRO2 contain messages that point to flapping BGP and EIGRP neighbors, which indicate routing instability.

Internal BGP Session Design

- The Internal BGP sessions have been set up using hierarchical route reflectors.



© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--5-5

To successfully troubleshoot the issues caused by BGP in this ticket you need to know how the internal BGP sessions have been implemented. Has a full mesh of sessions been implemented, or has some other scheme been used?

In this lab a hierarchical route reflector scheme has been implemented, with routers IR01 and IR02 acting as route reflectors for routers CR01 and CR02, which in turn act as route reflectors for routers BR01 and BR02. Because of this design, only routers BR01 and BR02 receive the full feed of 70,000 specific prefixes.

Key Clue: Slow Response to Traceroute and Ping Under Load

- Generate traffic load on the network using the TTCP utility on switches ASW1 and BSW1:
 - On switch BSW1 issue the command **ttcp receive**.
 - On switch ASW1 issue the command **ttcp transmit 10.1.163.193**.
- Traceroute and ping from client PC CLT2 to server SRV1 reveal high delays:

```
C:\Documents and Settings\Administrator>tracert -d srv1

Tracing route to srv1.tshoot.local [10.1.152.1]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    10.1.160.124
  1  124 ms    124 ms    124 ms    10.1.193.1
  2  146 ms    131 ms    200 ms    10.1.192.9
  3  212 ms    250 ms    354 ms    10.1.152.1
    Trace complete.
```

A primary clue to resolving the connectivity problem to the corporate server can be obtained by using the traceroute utility to trace the path from the branch (for instance from switch BSW1) to the headquarters (for instance to server SRV1) and notice the unusually high round-trip times. However, be aware that these results will be reliably observed only if you are generating a large amount of traffic at the same time, either by performing several large file transfers, or by simulating these transfers using the **ttcp** utility.

Key Clue: High CPU Utilization Caused by the IP Input Process

- Verifying the CPU load on routers CRO1 and CRO2 reveals that the IP Input process consumes a large amount of CPU time:

```
CRO1#show processes cpu | exclude 0.00
CPU utilization for five seconds: 99%/34%; one minute: 99%; five minutes:
87%
  PID Runtime(ms)   Invoked    uSecs   5Sec   1Min   5Min  TTY Process
    4    191656       35655      5375    1.79%  0.23%  0.15%  0 Check heaps
   55    973228      485423     2004   61.95% 62.14% 55.85%  0 IP Input
  195    20824        211     98691    1.95%  1.47%  1.70%  0 BGP Scanner
```

- Further verification reveals that Cisco Express Forwarding and fast switching have been disabled:

```
CRO1#show ip cef
%CEF not running
Prefix          Next Hop          Interface
CRO1#show ip interface FastEthernet 0/0 | include switching
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is disabled
<... output omitted ...>
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--5-7

When you log in to router CRO1, you should check for the router's resource usage and notice that the CPU utilization is very high. The majority of the CPU load is caused by the "IP Input" process, which tells you that there is something wrong. Such a high utilization caused by this process can be the result of an inappropriate switching mode.

Trouble Ticket Q Checkpoints

Minimum checkpoints to prove that you have resolved this trouble ticket:

- Client PCs CLT2 and CLT3 can ping IP addresses 10.16.0.1 and 10.32.0.1 without any packet loss.
- Both routers CRO1 and CRO2 are using Cisco Express Forwarding to switch packets.
- You have documented your process, your solution, and any changes that you have made to the device configurations.

What else should you have checked?

Are there any unresolved issues?

- Did you notice that some BGP speakers are configured with a minimum BGP scanner timer of 5 seconds?
- Did you notice the huge access list applied to several interfaces on routers CRO1 and CRO2?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-8-8

The figure shows a list of minimum requirements that should be met to consider this trouble ticket to be resolved.

In addition to the major issues described in this ticket, you might also have noticed that the BGP scanner timer has been tuned down to 5 seconds and that a huge access list was applied to interfaces on routers CRO1 and CRO2.

Suggested Solutions

Correcting the configuration of routers CRO1 and CRO2 as follows limits the number of routes sent to routers BRO1 and BRO2, alleviating the memory exhaustion on routers BRO1 and BRO2.

Suggested Configuration Changes

- Configure BGP route aggregation on routers CRO1 and CRO2 to prevent the memory exhaustion problems on BRO1 and BRO2.

```
CRO1(config)#router bgp 65000  
CRO1(config-router)#aggregate-address 10.16.0.0 255.240.0.0 summary-only
```

```
CRO2(config)#router bgp 65000  
CRO2(config-router)#aggregate-address 10.32.0.0 255.240.0.0 summary-only
```

- **Note:** It is recommended to reload routers BRO1 and BRO2 after configuring the aggregation on routers CRO1 and CRO2.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--5-9

A straightforward method to resolve the memory exhaustion issues experienced on routers BRO1 and BRO2 is to configure route aggregation on routers CRO1 and CRO2, to reduce the number of BGP routes sent to routers BRO1 and BRO2.

Suggested Configuration Changes: Alternative Solution

- Configure route maps on routers BRO1 and BRO2 to filter the incoming routing updates:

```
BRO1(config)#route-map stop-many permit 10
BRO1(config-route-map)#match ip address prefix-list partner
BRO1(config-route-map)#route-map stop-many deny 20
BRO1(config-route-map)#exit
BRO1(config)#ip prefix-list partner seq 5 permit 10.16.0.0/12
BRO1(config)#ip prefix-list partner seq 10 permit 10.32.0.0/12
BRO1(config)#router bgp 65000
BRO1(config-router)#neighbor 10.1.220.1 route-map stop-many in
BRO1(config-router)#neighbor 10.1.220.2 route-map stop-many in
```

- **Note:** It is recommended to reload routers BRO1 and BRO2 after configuring the route maps and saving the configuration to NVRAM.

An alternative solution to reduce the number of prefixes sent to routers BRO1 and BRO2 is to filter out all the unnecessary specific subnets. This is configured on routers BRO1 and BRO2 and is achieved by applying an inbound route-map to BGP neighbors CRO1 and CRO2 to only allow the 10.16.0.0/12 and 10.32.0.0/12 prefixes and drop all other prefixes. The drawback of this solution is that the prefixes are actually received by the branch routers BRO1 and BRO2 only to be immediately discarded. However, this method also solves the problem of memory exhaustion on routers BRO1 and BRO2 (as long as the “soft-inbound” feature is not configured for BGP neighbors CRO1 and CRO2).

Suggested Configuration Changes (Cont.)

- Enable Cisco Express Forwarding on routers CRO1 and CRO2. Enable it both globally and on interfaces where it was disabled:

```
CRO1(config)#ip cef
CRO1(config)#interface FastEthernet 0/0
CRO1(config-if)#ip route-cache cef
```

- Unnecessary CPU utilization is also caused by the application of a badly written access list, which should be removed from all interfaces:

```
CRO1(config)#interface FastEthernet 0/0
CRO1(config-if)#no ip access-group huge-acl in
CRO1(config-if)#no ip access-group huge-acl out
CRO1(config-if)#exit
CRO1(config)#no ip access-list standard huge-acl
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-11

To correct the packet forwarding problems on routers CRO1 and CRO2, Cisco Express Forwarding should be re-enabled. You need to enable Cisco Express Forwarding globally and you also need to enable all interfaces that are involved in traffic forwarding explicitly for Cisco Express Forwarding. (Usually, Cisco Express Forwarding is enabled or disabled globally, but in this case it was specifically disabled on all interfaces.)

Another strange issue you could have spotted here is a huge access list applied both inbound and outbound to these interfaces. When you display it you see a very large number of lines that all specifically permit traffic, and no lines that actually deny anything. Obviously, this access list is either a sign of bad design or misconfiguration. You should remove it from the configurations of routers CRO1 and CRO2.

Consolidation

This topic describes the primary lessons that could be learned from the lab exercise.

Discussion: Lessons Learned

Method and process:

- How could you improve your troubleshooting methods?
- What alternative methods did you discover?

Communication and procedures:

- How could the troubleshooting process be made more effective?
- What kind of procedures would be useful and why?

Technology and tools:

- Which tools were most useful during troubleshooting?
- Which tools could have improved the effectiveness of your process?
- Which useful Cisco IOS commands did you discover?

© 2009 Cisco Systems, Inc. All rights reserved.TSHO OT v1.0—5-12

Think about all the things that you learned during the lab itself and during the debrief discussions. There is room to write down primary learning points in the Lab Debrief Notes section of the lab guide.

In addition to thinking of the methods, processes, and tools as they were used in the lab, reflect on how these would apply to your own organization.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- You have reviewed and verified your lab results.
- You have consolidated the experiences and discoveries that all students got from the lab and you have derived a number of key learning points from these experiences.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-13

References to Additional Troubleshooting on NAT, DHCP, and Other Protocols in E-Learning

Overview

The *Troubleshooting and Maintaining Cisco IP Networks* (TSHOOT) v1.0 instructor-led training (ILT) course is a comprehensive learning experience. Among the learning tools available to you, it includes e-learning modules that complement the classroom instructor-led content and add to your experience with self-paced materials and demonstrations. Upon accessing the e-learning content, you will be able to reinforce the knowledge acquired in class and to witness real-life troubleshooting scenarios demonstrated using real routers and switches. The content structure is flexible, and you can navigate it at your own pace, at the time of your choosing, and at the depth you want according to your level of experience.

This lesson presents additional topics in routing technologies, and overviews these e-learning modules: “Troubleshooting NAT and PAT”; “Troubleshooting DHCP”; and “Troubleshooting IPv6, OSPFv3, and RIPng.”

Objectives

Upon completing this lesson, you will be able to review the e-learning modules that pertain to additional topics in routing technologies. This ability includes being able to meet these objectives:

- Describe the content of the “Troubleshooting NAT and PAT” e-learning module
- Describe the content of the “Troubleshooting DHCP” e-learning module
- Describe the content of the “Troubleshooting IPv6, OSPFv3, and RIPng” e-learning module
- Understand the process of accessing and using e-learning content

Preview of E-Learning on Additional Routing Technologies

This topic describes e-learning products to teach configuring of implementation of additional routing technologies.

CCNP E-Learning

- Complement and enhance your classroom experience
- Reinforce concepts and their application
- Learn at your own pace
- Review advanced topics
- Experience real-life scenarios through directed demonstrations
- Use the trouble-ticket approach to consolidate your troubleshooting method

© 2009 Cisco Systems, Inc. All rights reserved.ROUTE v1.0—5-2

One of the primary ideas behind the design of the Cisco CCNP® curriculum is the understanding that there is no one best method of learning for every student. Some students prefer individual labs, while others prefer one-on-one tutoring, hands-on sessions, self-paced computer-assisted instruction, direct, discovery learning, or cooperative learning, among others.

E-learning solutions offer new approaches that complement and enhance classroom-based learning. Designed with flexibility and learning effectiveness in mind, the e-learning modules presented in this lesson are based on knowledge you acquired during your *Troubleshooting and Maintaining Cisco IP Networks* (TSHOOT) v1.0 instructor-led training course.

All e-learning modules presented in this lesson utilize the trouble-ticket approach you know very well by now: A case is presented, using certain assumptions and baseline information. The demonstrations show one or more of the possible paths to gathering information, identifying symptoms, prioritizing hypotheses, and gathering conclusions. The content is as much about the technical aspects presented as it is about applying a troubleshooting method to a specific scenario, controlled by certain variables.

Troubleshooting NAT and PAT

Lesson	Description
Identifying Problems in NAT Deployments	Briefly reviews NAT types, terminology, advantages, and disadvantages. Lay out the troubleshooting scenarios for various types of NAT deployments.
Directed Demo: Troubleshooting NAT	Troubleshoots NAT in scenarios of asymmetric routing, application networking, and port mapping.
Self-Check Assessment	Assesses your understanding of the lesson.

© 2009 Cisco Systems, Inc. All rights reserved.

ROUTE v1.0—5-3

The “Troubleshooting NAT and PAT” e-learning module covers topics that complement the classroom module that you are reviewing. Different NAT types and deployment scenarios are presented, all of them having NAT as a support service in network design. The trouble ticket lesson allows you to follow directed demonstrations of real-life scenarios such as asymmetric routing, port mapping, and support for application networking. Remember, our focus is the troubleshooting method that you use in your approach to problem solving.

Troubleshooting DHCP

Lesson	Description
Identifying Wireless Integration Issues	Highlights some common issues that you can encounter when deploying DHCP services in your network. This includes scenarios where Cisco IOS routers become DHCP servers and clients, or simply where the readiness of network devices becomes crucial for a smooth deployment of DHCP.
Directed Demo: Trouble Tickets for Wireless Integration	Assesses problems that might arise during network operations, the tools you can use to fix those problems, and an overall view of the troubleshooting method as it applies to DHCP environments.
Self-Check Assessment	Assesses your understanding of the lesson.

© 2009 Cisco Systems, Inc. All rights reserved.

ROUTE v1.0--6-4

The “Troubleshooting DHCP” e-learning module covers topics that complement the classroom module that you are reviewing. DHCP is presented as a support service that might have an impact on network connectivity, routing, and path control. The trouble ticket scenarios highlight the fundamental job of DHCP when implemented. These scenarios include DHCP relay agents, DHCP options, and DHCP misconfigurations.

Troubleshooting IPv6, OSPFv3, and RIPng

Lesson	Description
Identifying Unified Communications Integration Issues	Presents the most commonly found issues in IPv6 networks. This includes issues that affect multiple areas of IPv6 deployments, such as neighbor discovery, routing protocols, and tunneling implementations.
Directed Demo: Trouble Tickets for Unified Communications Integration	Trouble ticket scenarios include stateless autoconfiguration issues, redistribution, suboptimal routing, and OSPFv3 in NBMA networks.
Self-Check Assessment	Assesses your understanding of the lesson.

© 2009 Cisco Systems, Inc. All rights reserved.

ROUTE v1.0—5-5

The “Troubleshooting IPv6, OSPFv3, and RIPng” e-learning module covers topics that complement the classroom module that you are reviewing. IPv6 fundamentals are set aside to focus on potential issues on multiple scenarios, from addressing to routing to transitioning to IPv6. The trouble tickets focus on the method and on using the appropriate Cisco IOS configuration tools and commands to effectively and timely solve the problem.

Where to Find E-Learning Modules



© 2009 Cisco Systems, Inc. All rights reserved.

ROUTE v1.0—5-6

The e-learning modules presented in this lesson are available on a CD as part of your classroom materials. Please contact your instructor with questions on finding and accessing the CD.

The objectives of these module are part of your CCNP certification exam, and they should be reviewed by candidates to the CCNP certification.

E-Learning Module Structure

The screenshot displays a three-panel interface for an e-learning module. The top-left panel, titled "Addressing and Topology Specifics", shows a network topology with three routers (R1, R2, R3) and their interfaces. R1 and R2 are connected via a 10.2.7.0/24 link, R2 and R3 via a 10.3.7.0/24 link, and R1 and R3 via a 10.1.7.0/24 link. R1 is connected to a 192.168.2.0/24 network, R2 to a 192.168.1.0/24 network, and R3 to a 192.168.253.0/24 network. The top-right panel, titled "Debrief : Alternative Configuration", shows a configuration snippet for route-map TAGS. The bottom panel shows a console output for R1, displaying policy routing matches and a trace command.

Addressing and Topology Specifics

OSPF
EIGRP

10.2.7.0/24
10.3.7.0/24
10.1.7.0/24
192.168.2.0/24
192.168.1.0/24
192.168.253.0/24

Debrief : Alternative Configuration

```
route-map TAGS deny 10
match tag 1000
route-map TAGS permit 20
set tag 1000
....
router ospf 1
 redistribute eigrp 1 metric 4 route-map TAGS
....
router eigrp 1
 redistribute ospf 1 metric 1000000 0 255 1 800 route-map TAGS
....
```

R1 R2 ISP

Policy routing matches: 0 packets, 0 bytes
route-map SETTAG, permit, sequence 20
Match clauses:
Set clauses:
Policy routing matches: 0 packets, 0 bytes
R1#trace 192.168.254.1

Type escape sequence to abort.
Tracing the route to 192.168.254.1

1 192.168.2.2 12 msec * 12 msec
R1#
R1#

Utilizing a combination of lecture sessions, animated content, lab demonstrations, and assessments, each e-learning module presents a hierarchical structure of lessons and topics. You can navigate that structure by using an intuitive graphical user interface that includes playback controls, slide selection, and lesson and topic selection. Using these tools you will be able to navigate the content at your own pace.

The three-panel screen presented in the directed demonstrations allows you to focus on the device console demonstrations, while having the command syntax and the topology diagram in sight for verification and additional information.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Describe the content of the “Troubleshooting NAT and PAT” e-learning module.
- Describe the content of the “Troubleshooting DHCP” e-learning module.
- Describe the content of the “Troubleshooting IPv6, OSPFv3, and RIPng” e-learning module.
- Understand the process of accessing and using e-learning content.

© 2009 Cisco Systems, Inc. All rights reserved.

ROUTE v1.0—6-8

Module Summary

This topic summarizes the key points that were discussed in this module.

Module Summary

- Network layer problems can be diagnosed by careful analysis of key Layer 3 data structures, such as the IP routing table.
- The EIGRP interface, neighbor, and topology tables are the key data structures used to troubleshoot EIGRP problems.
- Understanding the different types of link-state advertisements and their role is essential to troubleshoot OSPF effectively.
- Seed metrics and administrative distance are the main factors that influence routing decisions in an environment that deploys route redistribution between multiple routing protocols.
- Understanding BGP session establishment, route exchange, and route selection is essential to troubleshooting BGP.
- Memory problems and high CPU utilization due to inadequate routing processes and internal switching parameters are the main factors that affect router performance.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—5-1

Diagnosing and resolving problems in a routed IP network has many aspects. A good understanding of the IP routing and forwarding process, the interaction between the network layer and underlying layers, and key network layer data structures, such as the routing table and Cisco Express Forwarding data structures, is essential to isolate, diagnose, and resolve IP connectivity problems. Tracking the path of packets between hosts from router to router is a common way to diagnose network layer problems, and understanding the relation between the flow of traffic and the exchange of routing information between routers is vital to this process.

For all routing protocols, it is important to understand how they establish neighbor relationships, exchange routing information, store routing information, and select the best path. Information about these processes and decisions can be gathered from the IP routing table, and also from the data structures that are specific to each routing protocol. Each of the major routing protocols used in enterprise networks, the Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), and the Border Gateway Protocol (BGP), along with their associated data structures and processes, were reviewed. The processes that these protocols use have many similarities, and as a result, experience with troubleshooting one routing protocol can be translated to a different routing protocol. However, the details of the processes and the Cisco IOS commands used to gather information from these data structures and processes are protocol specific. Detailed knowledge of these data structures, processes, and commands is required to diagnose problems related to these protocols.

When a network uses multiple routing protocols and exchanges routing information between these protocols via route redistribution, detailed knowledge of the individual protocols and the way these protocols interact on a router is necessary to diagnose and resolve IP connectivity problems effectively.

Memory and the router CPU are the major components that affect router performance, and problems can emerge if these resources are not sufficiently available or inefficiently used. Information about these elements needs to be gathered, interpreted, and analyzed to determine whether a router could be the cause of a network performance problem

References

For additional information, refer to these resources:

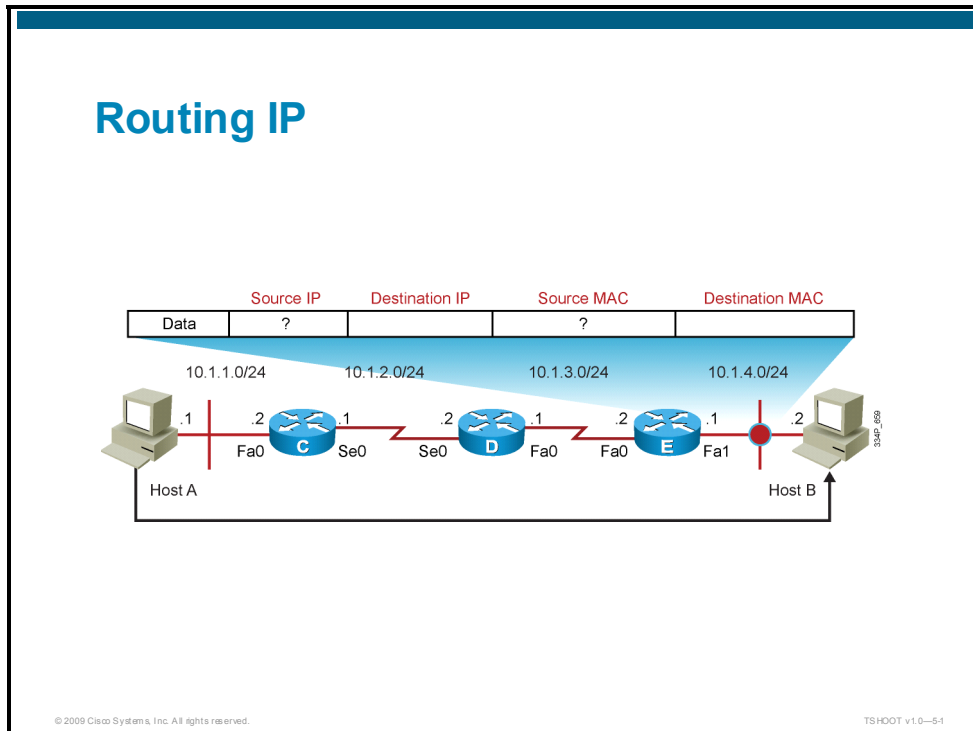
- Cisco Systems Inc., *Using the Extended ping and Extended traceroute Commands*:
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f22.shtml
- Cisco Systems Inc., *Route Selection in Cisco Routers*:
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094823.shtml
- Cisco Systems Inc., *Troubleshooting EIGRP*:
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094613.shtml
- Cisco Systems Inc., *OSPF Neighbor Problems Explained*:
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094050.shtml
- Cisco Systems Inc., *Why Does the show ip ospf neighbor Command Reveal Neighbors in the Init State*:
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f11.shtml
- Cisco Systems Inc., *Why Does the show ip ospf neighbor Command Reveal Neighbors Stuck in Two-Way State*:
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094059.shtml
- Cisco Systems Inc., *Why Are OSPF Neighbors Stuck in Exstart/Exchange State*:
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f0d.shtml
- Cisco Systems Inc., *Troubleshooting Duplicate Router IDs with OSPF*:
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080117102.shtml
- Cisco Systems Inc., *Troubleshooting BGP*:
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a008009478a.shtml
- Cisco Systems Inc., *BGP Best Path Selection Algorithm*:
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094431.shtml
- Cisco Systems Inc., *Why Do BGP Neighbors Toggle Between Idle, Connect, and Active States*:
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093fb8.shtml
- Cisco Systems Inc., *Troubleshooting When BGP Routes Are Not Advertised*:
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a008009478a.shtml
- Cisco Systems Inc., *Troubleshooting Flapping BGP Routes (Recursive Routing Failure)*:
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800945fe.shtml
- Cisco Systems Inc., *Cisco IOS IP Switching Configuration Guide, Release 12.4*:
http://cisco.com/en/US/docs/ios/ipswitch/configuration/guide/12_4/isw_12_4_book.html
- Cisco Systems Inc., *Cisco IP Switching technology support page*:
http://www.cisco.com/en/US/tech/tk827/tk831/tsd_technology_support_protocol_home.html

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

- Q1) Which two items are recorded in the routing table for a prefix? (Choose two.) (Source: Troubleshooting Network Layer Connectivity)
- A) VLAN
 - B) next-hop IP address
 - C) egress interface
 - D) ingress interface
 - E) next-hop MAC address
- Q2) After consulting the routing table to route a packet, which other data structure on a router needs to be consulted to encapsulate the packet in an Ethernet frame? (Source: Troubleshooting Network Layer Connectivity)
- A) MAC address table
 - B) link state database
 - C) topology table
 - D) ARP cache
 - E) none of the above; all information necessary to route a packet and encapsulate it is contained in the routing table.
- Q3) For a route that has a point-to-point interface as the egress interface, a next-hop IP address is not mandatory. (Source: Troubleshooting Network Layer Connectivity)
- A) true
 - B) false
- Q4) Which two data structures contain similar information when using Cisco Express Forwarding? (Choose two.) (Source: Troubleshooting Network Layer Connectivity)
- A) The routing table and the FIB contain similar information.
 - B) The routing table and the adjacency table contain similar information.
 - C) The FIB and the Layer 3 to Layer 2 mapping tables, such as the ARP cache, contain similar information.
 - D) The adjacency table and the Layer 3 to Layer 2 mapping tables, such as the ARP cache, contain similar information.

- Q5) The figure shows an IP packet that is in transit from host A to host B as it traverses the Ethernet LAN between router E and host B. Which two addresses are contained in the two fields marked with a question mark (?) in the figure? (Source: Troubleshooting Network Layer Connectivity)



- A) IP address 10.1.4.1 and MAC address of host B
 B) IP address 10.1.4.1 and MAC address of router E
 C) IP address 10.1.4.2 and MAC address of host B
 D) IP address 10.1.1.1 and MAC address of host A
 E) IP address 10.1.1.1 and MAC address of router E
 F) IP address 10.1.4.1 and MAC address of host A
- Q6) Which Cisco IOS command displays the exact adjacency that is used to forward a packet from a specific source IP address to a specific destination IP address on a router that is using Cisco Express Forwarding? (Source: Troubleshooting Network Layer Connectivity)
-
- Q7) Which Cisco IOS command displays the full Layer 2 header that will be used to forward frames to an adjacency on a router that is using Cisco Express Forwarding? (Source: Troubleshooting Network Layer Connectivity)
-

- Q8) Which three data structures does EIGRP use? (Choose three.) (Source: Troubleshooting EIGRP)
- A) link state database
 - B) topology table
 - C) ARP cache
 - D) interface table
 - E) adjacency table
 - F) neighbor table
- Q9) The EIGRP topology table contains all the routes that were received from all EIGRP routers in the autonomous system. (Source: Troubleshooting EIGRP)
- A) true
 - B) false
- Q10) Which Cisco IOS command displays the transmission and reception of EIGRP packets such as hellos, updates, queries, and replies? (Source: Troubleshooting EIGRP)
- A) **debug ip eigrp packets**
 - B) **debug ip eigrp**
 - C) **debug eigrp packets**
 - D) **debug eigrp updates**
 - E) **debug eigrp adj**
 - F) **debug ip eigrp neighbor**
- Q11) When you issue the **show ip eigrp interfaces** command on a router, it lists interface FastEthernet 0/1, but it does not list interface FastEthernet 0/0. Which two statements could be a possible explanation for the absence of interface FastEthernet 0/0? (Choose two.) (Source: Troubleshooting EIGRP)
- A) Interface FastEthernet 0/0 has been configured as a passive interface.
 - B) EIGRP is not enabled on the router.
 - C) The command **ip eigrp as-number** is not configured on interface FastEthernet 0/0.
 - D) None of the configured **network** statements matches the IP address of FastEthernet 0/0.
 - E) There are no active EIGRP neighbors on interface FastEthernet 0/0.
 - F) Interface FastEthernet 0/0 is not a feasible successor.

Q12) Based on the command output displayed here, which route is the successor? (Source: Troubleshooting EIGRP)

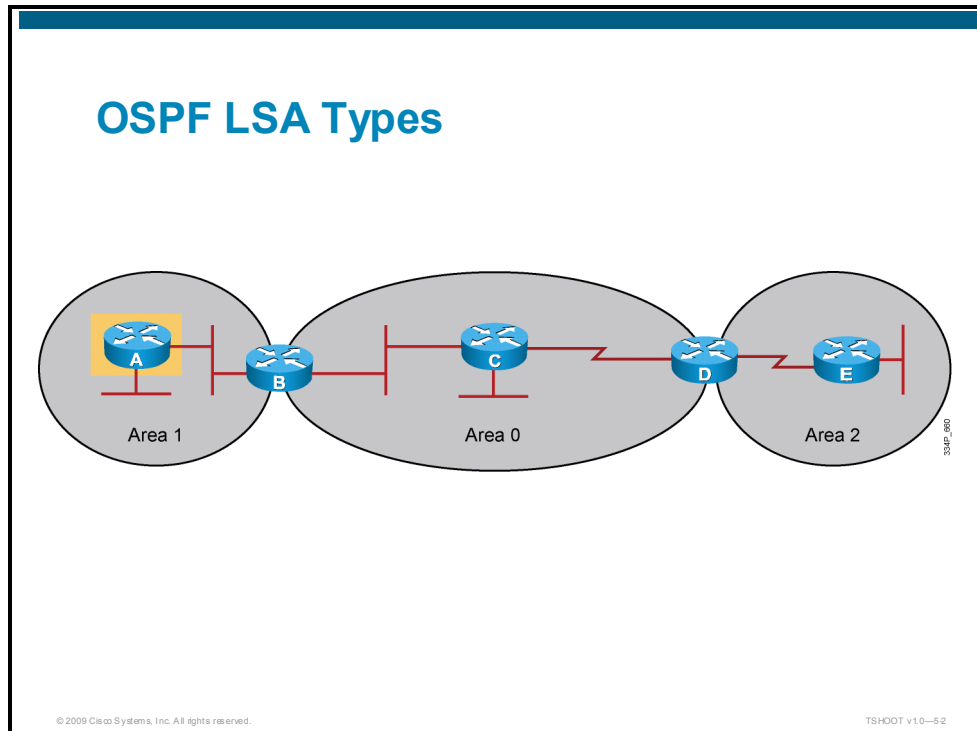
```
BRO1#show ip eigrp topology 10.1.220.1 255.255.255.255
IP-EIGRP (AS 1): Topology entry for 10.1.220.1/32
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 40640000
  Routing Descriptor Blocks:
    10.1.194.1 (Serial0/0/0.111), from 10.1.194.1, Send flag is 0x0
      Composite metric is (40640000/128256), Route is Internal
      Vector metric:
        Minimum bandwidth is 64 Kbit
        Total delay is 25000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
    10.1.163.130 (FastEthernet0/1.30), from 10.1.163.130, Send flag is 0x0
      Composite metric is (40642560/40640000), Route is Internal
      Vector metric:
        Minimum bandwidth is 64 Kbit
        Total delay is 25100 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 2
```

- A) The route via 10.1.194.1, because it has the lowest hop count.
- B) The route via 10.1.163.130, because a Fast Ethernet interface has a higher bandwidth than a serial interface.
- C) The route via 10.1.163, because its feasible distance (40642560) is better than the composite feasible distance (40640000).
- D) The route via 10.1.194.1, because its metric (40640000) is better than the metric via 10.1.163.1 (40642560).
- E) The route via 10.1.194.1, because its metric (128256) is better than the metric via 10.1.163.1 (40640000).

Q13) Which three data structures does the OSPF protocol use? (Choose three.) (Source: Troubleshooting OSPF)

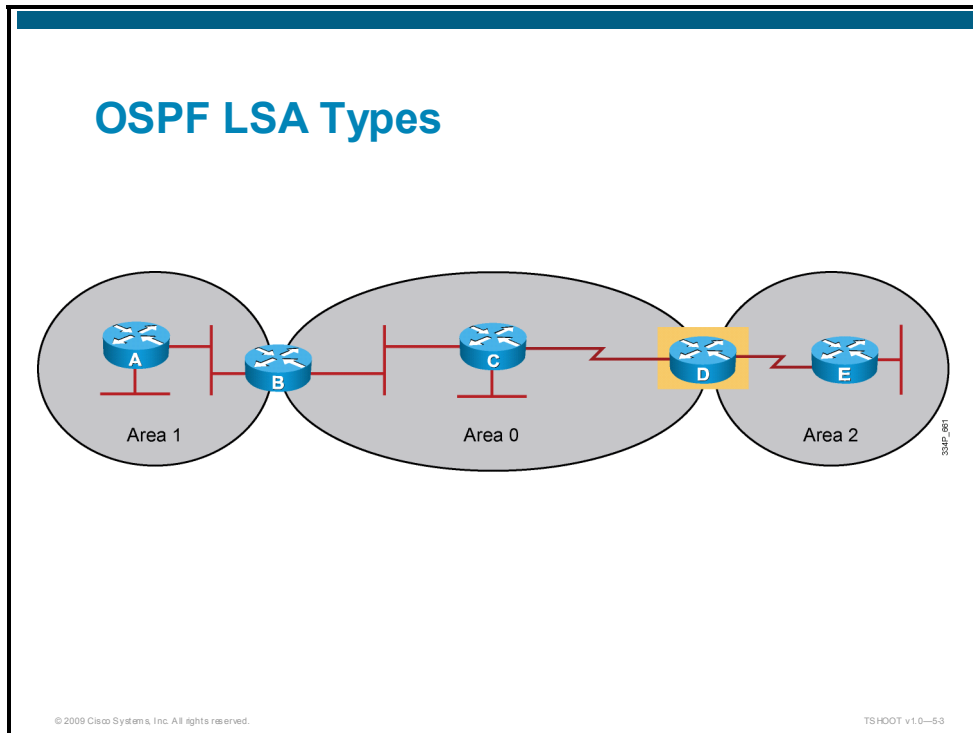
- A) link state database
- B) topology table
- C) ARP cache
- D) interface table
- E) adjacency table
- F) neighbor table

- Q14) The figure shows an OSPF network consisting of three areas. No redistribution or summarization has been configured, and each link represents a single subnet. How many type-1 and type-2 LSAs are contained in the OSPF link-state database on router A? (Source: Troubleshooting OSPF)



- A) Two type-1 LSAs and two type-2 LSAs
 - B) Five type-1 LSAs and five type-2 LSAs
 - C) One type-1 LSA and one type-2 LSA
 - D) Two type-1 LSAs and one type-2 LSA
 - E) Two type-1 LSAs and five type-2 LSAs
- Q15) Which three parameters need to match in the hello packets for two OSPF routers to become neighbors? (Choose three.) (Source: Troubleshooting OSPF)
- A) hello and dead timer
 - B) autonomous system number
 - C) area number
 - D) subnet mask on a point-to-point link
 - E) area type
 - F) router type

- Q16) The figure shows an OSPF network consisting of three areas. No redistribution or summarization has been configured, and each link represents a single subnet. How many type-3 LSAs are contained in the OSPF link-state database on router D? (Source: Troubleshooting OSPF)



- Q17) Which statement best describes the subsequent stages of the establishment of an OSPF adjacency? (Source: Troubleshooting OSPF)

- A) Init
- B) 2-way
- C) Exstart
- D) Loading

- ____ 1. This state indicates that the routers are starting the database exchange by establishing a master and slave relationship and determining the initial sequence number for the DBD packets.
- ____ 2. A neighbor is in this state if a hello has been received from the neighbor, but the neighbor is not listing this router in its neighbor list yet.
- ____ 3. During this stage, each of the two routers can request missing LSAs from the other router.
- ____ 4. This is the state that a neighbor relationship is in when the router sees its own router ID listed in the active neighbor list in the hello packets received from that neighbor.

- Q18) Which four OSPF neighbor states are transitory states? (Choose four.) (Source: Troubleshooting OSPF)
- A) Init
 - B) 2-way
 - C) Exstart
 - D) Exchange
 - E) Loading
 - F) Full
- Q19) Which Cisco IOS **debug** command displays events that are related to the adjacency building process and allows you to see a neighbor relationship transition from one state to the next? (Source: Troubleshooting OSPF)
-
- Q20) Which Cisco IOS command can be used to display the content of the OSPF link-state database? (Source: Troubleshooting OSPF)
- A) **show ip ospf lsdb**
 - B) **show ip ospf link-states**
 - C) **show ip ospf database**
 - D) **show ip route ospf**
 - E) None of the above. Only the results of the SPF calculation can be displayed, not the content of the database itself.
- Q21) When you issue the **show ip ospf interface** command on a router, it lists interface FastEthernet 0/1, but it does not list interface FastEthernet 0/0. Which statement could be a possible explanation for the absence of interface FastEthernet 0/0? (Source: Troubleshooting OSPF)
- A) Interface Fast Ethernet 0/0 has been configured as a passive interface.
 - B) OSPF is not enabled on the router.
 - C) None of the configured **network** statements matches the IP address of FastEthernet 0/0.
 - D) There are no active OSPF neighbors on interface FastEthernet 0/0.
 - E) The router is not a designated router for interface FastEthernet 0/0.

- Q22) Which type of OSPF LSA is displayed in the output of the command displayed below?
(Source: Troubleshooting OSPF)

```
CRO1#show ip ospf database summary 10.1.152.0
```

```
OSPF Router with ID (10.1.220.1) (Process ID 100)
```

```
Summary Net Link States (Area 0)
```

```
Routing Bit Set on this LSA
```

```
LS age: 201
```

```
Options: (No TOS-capability, DC, Upward)
```

```
LS Type: Summary Links(Network)
```

```
Link State ID: 10.1.152.0 (summary Network Number)
```

```
Advertising Router: 10.1.220.252
```

```
LS Seq Number: 80000001
```

```
Checksum: 0x1C97
```

```
Length: 28
```

```
Network Mask: /24
```

```
TOS: 0 Metric: 1
```

- A) Type-1 LSA
B) Type-2 LSA
C) Type-3 LSA
D) Type-4 LSA
E) Type-5 LSA
- Q23) How does a router determine which route to install in the routing table if two routes for the same prefix from different routing protocols are available? (Source: Troubleshooting Redistribution)
- A) It compares the metrics of the two protocols and installs the route with the lowest metric.
B) It compares the administrative distance of the two protocols and installs the route with the lowest administrative distance.
C) It converts the metric of each of the routing protocols to the URM and then installs the route with the lowest URM.
D) It installs both routes in the routing table and load-balances the traffic across the two paths.
- Q24) Which two routing protocols have their default seed metric for redistribution set to “infinity” or “unreachable”? (Choose two.) (Source: Troubleshooting Redistribution)
- A) RIP
B) IS-IS
C) OSPF
D) EIGRP
E) BGP

- Q25) Which Cisco IOS **debug** command displays routes being installed or removed from the routing table in real time? (Source: Troubleshooting Redistribution)
-
- Q26) Which two information elements are exchanged by EIGRP for an external route that was redistributed from OSPF? (Choose two.) (Source: Troubleshooting Redistribution)
- A) Originating OSPF area number
 - B) EIGRP router ID of the redistributing router
 - C) OSPF router ID of the originating router
 - D) Source routing protocol (OSPF)
- Q27) Which two data structures does BGP use? (Choose two.) (Source: Troubleshooting BGP)
- A) link state database
 - B) topology table
 - C) BGP table
 - D) ARP cache
 - E) interface table
 - F) adjacency table
 - G) neighbor table
- Q28) The BGP table on a router contains all the routes that were received from all its BGP peers. (Source: Troubleshooting BGP)
- A) true
 - B) false
- Q29) BGP neighbors are discovered by use of a hello protocol. (Source: Troubleshooting BGP)
- A) true
 - B) false
- Q30) Which two reasons could cause the establishment of a BGP session to fail? (Choose two.) (Source: Troubleshooting BGP)
- A) The source IP address used by the router that initiates the session does not match the configured IP address on the receiving router.
 - B) The TCP source port used by the router that initiates the session is not set to 179.
 - C) The autonomous system number of the router that initiates the session does not match the configured autonomous system number for the peer router on the receiving router.
 - D) The BGP keepalive and hold timer of the peers do not match.
- Q31) Which Cisco IOS command displays the subsequent phases of establishing a BGP peering relationship? (Source: Troubleshooting BGP)
- A) **debug ip bgp**
 - B) **debug ip bgp adj**
 - C) **debug ip bgp peer**
 - D) **debug ip bgp updates**
 - E) **debug ip bgp events**

- Q32) The output of the **show ip bgp summary** command displays “Active” as the state of a neighbor. What does this mean? (Source: Troubleshooting BGP)
- A) The peering session has been established and the routers are actively exchanging routes.
 - B) BGP has lost the best route in the BGP table for a prefix and is attempting to find a backup route via a query and reply process.
 - C) BGP is attempting to establish a TCP session to the neighbor, but has not succeeded yet.
 - D) This is the state that a peering relationship is in when the router sees its own router ID listed in the active peer list in the hello packets received from that peer.
- Q33) Which two situations can cause high CPU utilization? (Choose two.) (Source: Troubleshooting Performance Problems on Routers)
- A) The router performance degrades.
 - B) The router receives too many packets that need to be processed by the CPU.
 - C) The **show processes cpu** command displays high CPU utilization.
 - D) A system process consumes too much CPU time.
- Q34) Which three are common symptoms of high CPU utilization? (Choose three.) (Source: Troubleshooting Performance Problems on Routers)
- A) slow performance
 - B) many errors on the input interface
 - C) remote access problems
 - D) routing update problems
 - E) low percentages in the show processes cpu command output
- Q35) Which two are common causes of high CPU utilization? (Choose two.) (Source: Troubleshooting Performance Problems on Routers)
- A) different processes
 - B) interface flaps
 - C) security issues
- Q36) Which is a Cisco IOS tool for troubleshooting high CPU utilization? (Source: Troubleshooting Performance Problems on Routers)
- A) **show processes cpu**
 - B) **show version**
 - C) **show buffers**
 - D) **show controllers**
- Q37) Which three are the proper memory allocation failure symptoms? (Choose three.) (Source: Troubleshooting Performance Problems on Routers)
- A) refused Telnet sessions
 - B) too many log messages
 - C) no output from the **show** commands
 - D) lack of memory on the router line cards
 - E) slow performance in packet processing

- Q38) Which three are common memory problems? (Choose three.) (Source: Troubleshooting Performance Problems on Routers)
- A) the “dead” process
 - B) memory leak bug
 - C) routing problems
 - D) slow IGP convergence
 - E) security-related memory problems
- Q39) Which two are buffer leak problems? (Choose two.) (Source: Troubleshooting Performance Problems on Routers)
- A) route processor buffer leaks
 - B) wedged interface buffer leaks
 - C) system buffer leak
 - D) SVI buffer leaks
- Q40) Which two tables should you check if you suspect issues with Cisco Express Forwarding switching? (Choose two.) (Source: Troubleshooting Performance Problems on Routers)
- A) ARP table and routing table
 - B) adjacency table and FIB table
 - C) CLNS table and ARP table
 - D) FIB table and GBRC table
- Q41) Which command should you use if you suspect performance problems related to IP switching? (Source: Troubleshooting Performance Problems on Routers)
- A) **show processes memory**
 - B) **show processes cpu**
 - C) **show processes switching**
 - D) **show ip switching**
- Q42) Which three are symptoms of a buffer leak? (Choose three.) (Source: Troubleshooting Performance Problems on Routers)
- A) %SYS-2-MALLOCFAIL error messages
 - B) packet drops on the router interfaces
 - C) frequent router reload
 - D) **show buffer** command output indicating a buffer leak in some of the buffer pools

Module Self-Check Answer Key

- Q1) B, C
- Q2) D
- Q3) A
- Q4) A, D
- Q5) E
- Q6) **show ip cef exact-route** *source destination*
- Q7) **show adjacency detail**
- Q8) B, D, F
- Q9) B
- Q10) C
- Q11) A, D
- Q12) D
- Q13) A, D, F
- Q14) D
- Q15) A, C, E
- Q16) Nine type-3 LSAs. Four in the Area 0 database and five in the Area 2 database.
- Q17) 1-C
2-A
3-D
4-B
- Q18) A, C, D, E
- Q19) **debug ip ospf adj**
- Q20) C
- Q21) C
- Q22) C
- Q23) B
- Q24) A, D
- Q25) **debug ip routing**
- Q26) B, D
- Q27) C, G
- Q28) A
- Q29) B
- Q30) A, C
- Q31) A
- Q32) C
- Q33) B, D

- Q34) A, C, D
- Q35) A, C
- Q36) A
- Q37) A, C, D
- Q38) A, B, E
- Q39) A, C
- Q40) A, B
- Q41) B
- Q42) A, B, D

Maintaining and Troubleshooting Network Security Solutions

Overview

Any network that is deployed needs to be secured. The level of security that you need and the features that will be deployed are dependent on the organization and its security policies.

Implementation of infrastructure security has a definite impact on network maintenance and troubleshooting processes. The implemented security features add an extra layer of complexity to the network and introduce a plethora of new potential problem causes. Security features tend to focus on restricting the flow of traffic, and because of that, engineers should be aware of the features that are implemented at each point in the network and how they affect network connectivity.

A second important aspect of troubleshooting in a secured network is that the actions that an engineer is allowed to perform might be limited by the security policy. As part of the change control procedures, each change needs to be evaluated for compliance with the security policy. Even temporary changes made as part of the diagnosis during troubleshooting processes need to be carefully evaluated against the policies of the organization.

This module reviews security features that are commonly deployed in routed and switched network infrastructures and focuses on the diagnosis and resolution of network connectivity problems in a secured infrastructure.

Module Objectives

Upon completing this module, you will be able to diagnose and correct problems found in a secured network infrastructure. This ability includes being able to meet these objectives:

- Diagnose problems related to security features implemented on routers and switches
- Diagnose and resolve problems related to Cisco IOS-based security features

Troubleshooting Security Features

Overview

Any network that is deployed needs to be secured. The level of security that is needed and the features that will be deployed are dependent on the organization and its security policies. However, in any network, at least a basic level of security needs to be implemented. Access to the network infrastructure devices themselves needs to be secured in order to prevent unauthorized access. The control plane of the devices needs to be hardened to prevent infrastructure denial of service (DoS). In addition, routers and switches can fulfill a role in securing user traffic through implementation of packet filtering, virtual private network (VPN), and intrusion prevention system (IPS) features.

Deployment of security features on routers and switches adds an extra layer of complexity to network troubleshooting. Because most security features, by nature, aim to restrict connectivity, their implementation adds many potential problem causes that need to be eliminated during the troubleshooting process. Also, reported problems and possible solutions need to be validated against the security policy of the organization.

This lesson reviews the security features that are most commonly implanted on routers and switches, and analyzes their impact on network troubleshooting.

Objectives

Upon completing this lesson, you will be able to diagnose problems related to security features implemented on routers and switches. This ability includes being able to meet this objective:

- Describe the impact of security features on network troubleshooting

Network and Device Security

This topic describes the Cisco IOS Software features that could be implemented on routers and switches and how they can influence the network troubleshooting process.

Network Security

In building a secure network, the security of all layers and devices should be considered.

Access to routers and switches should be secured:

- When the infrastructure itself is compromised, the entire system can be compromised.

Routers and switches can provide security services:

- Packet filtering and firewall functionality
- Intrusion prevention system
- Virtual private networks

Routers and switches can be used as a component of a distributed security system.

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0--6.2

In the past, network security was often implemented as an additional layer on top of the network infrastructure. Special devices, such as firewalls, VPN concentrators, and intrusion detection systems (IDSs) were added to the network to implement specific security features, while the routers and switches would provide the basic network connectivity and not be involved in the security aspects of the network. A common approach was to design and implement a network infrastructure to provide connectivity, and then design and implement a security solution on top of that.

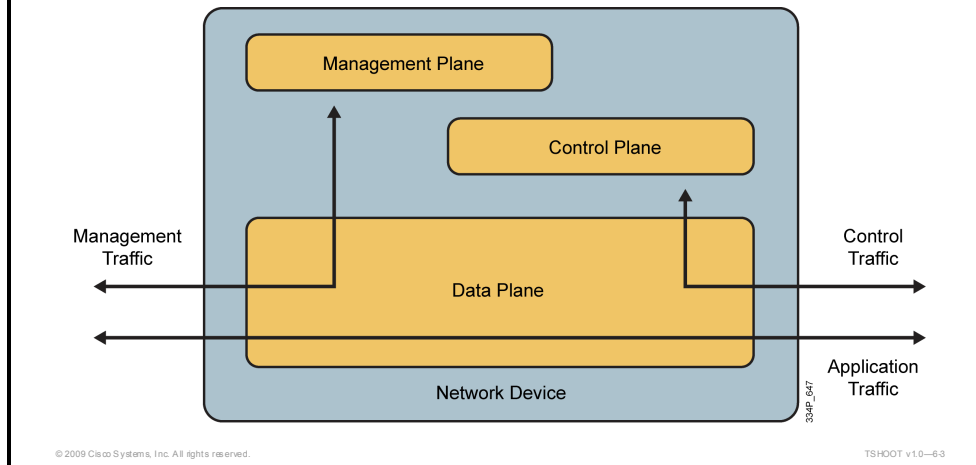
Over the years, it was realized that a more holistic approach to security is necessary to build secure networks. A system is as secure as its weakest component, and therefore the security risks and vulnerabilities of each component and layer of the network should be evaluated and addressed. In addition to using specialized security devices, such as firewalls, IPSs, and VPN concentrators, network devices such as routers and switches and the protocols that are used between these devices should be secured. If the network infrastructure itself is compromised, the entire system can be compromised.

In addition, in smaller networks, routers can have a dual role, functioning as both a router and as a security device by providing firewall, IPS, or VPN services.

Finally, infrastructure devices such as routers and switches can function as a component in a distributed security system, such as a Network Admission Control (NAC) solution or a threat mitigation system.

Network Device Security

Security features can affect routers and switches on different planes.



The implementation of security features can affect router and switch operation on different planes. There are three fundamental categories of functionality and corresponding types of traffic that are implemented on a network device. Security features can be implemented on each of those different planes.

- **Management plane:** The management plane represents all the functions and protocols involved in managing the device. This includes accessing information about the device configuration, device operation, and statistics. It also includes changing the device configuration to alter its behavior. Securing this plane is vital to the overall security of the device. If the management plane is compromised, the other planes are also exposed.
- **Control plane:** The control plane represents all the functions and protocols that are used between network devices to control the operation of the network, such as routing protocols, the Spanning Tree Protocol (STP), or other signaling and control protocols. Because the control plane affects the behavior of the data plane, the control plane protocols need to be secured. If unauthorized devices are allowed to participate in the control plane protocols, this opens up possibilities for an attacker to block or divert traffic.
- **Data plane:** The data plane represents all the functions involved in forwarding traffic through the device. Routers and switches can inspect, filter, and manipulate traffic as part of the implementation of a security policy. It is important to note that all management and control plane traffic also flows through the data plane. Consequentially, security features on the data plane can be used to secure the management and control planes. Also, this implies that failures on the management and control plane might be caused by the implementation of security features on the data plane.

Management Plane Security

Common methods and protocols used for management access are:

- Command-line access:
 - Serial console
 - Telnet
 - SSH
- Web-based access:
 - HTTP
 - HTTPS
- SNMP

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0–64

The management functions of a router or switch are commonly accessed via three different methods: via the Cisco IOS command-line interface (CLI), via web-based device management, or via a network management platform that uses the Simple Network Management Protocol (SNMP).

The CLI that is part of the Cisco IOS Software is the most common and most powerful method to manage routers and switches. It can be accessed directly through a serial connection to the console of the device, or remotely via Telnet or Secure Shell (SSH). For all these methods, at the very least, some form of authentication should be implemented to ensure that only authorized personnel can access the devices. Also, it is wise to restrict the locations that these devices can be accessed from. For example, allow access via Telnet or SSH only from specific subnets. Whenever possible, SSH should be used as an access method instead of Telnet, because it is inherently more secure. Telnet transmissions contain unencrypted data (including the password), while SSH uses encryption to secure its transmission. If it is not possible to use SSH to the devices themselves, and Telnet must be used, additional precautions need to be taken to secure the management traffic. For example, Telnet access could be restricted to a secure part of the network that is used only for management, and access to this network itself could be secured through use of VPN techniques or SSH using a bastion host.

Finally, you should be aware that the physical security of the device itself is also vital to the security of the management plane. The CLI can always be accessed through the serial console of the device itself, and therefore having physical access to the device implies having access to the command line. Again, authentication can limit access, but you need to be aware that if someone has access to the console of the device and the ability to power cycle the device, a password-recovery procedure can be executed to gain control of the device.

Note On some devices, the effect of a successful password recovery procedure can be limited by using the **no service password-recovery** command. By enabling this command, the original configuration and passwords of the device cannot be recovered using the password recovery procedure. However, the device configuration can still be erased, causing the device to be reset to factory defaults. If no additional control plane and data plane security measures have been implemented and the attacker has sufficient knowledge of the network, it might be possible to rebuild the configuration and gain access to the network.

An alternative method of managing routers and switches is by use of a web-based device manager installed on the device itself or on a PC, such as Cisco Configuration Professional or the older Cisco Router and Security Device Manager (SDM). The protocol used by these web-based device managers is either HTTP or HTTPS. HTTPS is more secure than HTTP, because HTTPS uses encryption to secure its transmissions, while HTTP transmits unencrypted data. Therefore, similar arguments to those that were used in the discussion about the use of Telnet versus SSH can be applied to the use of HTTP versus HTTPS. In addition, as with the command-line access method, authentication should be implemented to restrict web-based access to authorized users only, and it is wise to restrict the locations that these devices can be accessed from.

A third method to access the management functions of the device is by use of a network management platform using SNMP. Most commonly, this method is only used to access operational parameters and statistics of the device, not to change the configuration. In that case, devices are only configured for read access, and the configuration cannot be changed. From a security standpoint, this means that the associated security risk is generally lower. If the devices have been configured for read-write access, the configuration can be changed and the same level of security should be applied that is also applied for command-line or web-based access.

Management Plane Security (Cont.)

Common features used to secure the management plane are:

- Packet or session filtering using access lists:
 - Generic packet filtering
 - Protocol-specific access lists
- AAA:
 - Simple password authentication
 - TACACS+
 - RADIUS
 - Token card services

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6.6

To secure management access, two common techniques can be applied. First, access to the management plane can be restricted using packet or session filters. Access is allowed only from specific source IP addresses. This can be implemented in several ways. Because all access to the management plane goes through the data plane, generic access lists can be applied to the interfaces of the device to restrict the access to the management IP addresses and ports of the device. If packet filtering using access lists or the Cisco IOS firewall feature has already been implemented, this is simply a small addition to the existing filtering policies. If packet filtering or firewalling has not been configured yet, this might not be the best way to secure the management plane, because it will also affect the forwarding of all data plane traffic. All the management protocols, such as Telnet, SSH, HTTP, HTTPS, and SNMP, allow access lists to be specifically applied to the sessions directed to these management plane applications. Incoming access requests are evaluated against an access list and permitted or denied based on the source of the session. The advantage of this method is that only management plane traffic is affected, and the forwarding of data plane traffic is unaffected.

After a management session is established from an authorized source IP address, it is necessary to authenticate the user that is attempting to access the device. This can be done through a simple password authentication or an authentication based on a username and password combination. These usernames and passwords can be stored locally on the device itself or, for a more scalable solution, they can be stored in a central database. The router or switch can verify these credentials against the central database through use of the TACACS+ or RADIUS protocols. In addition to centralized authentication, the use of a TACACS+ or RADIUS server also allows for added authorization and accounting capabilities. Further, the use of a TACACS+ or RADIUS server also opens up the possible use of more sophisticated and secure authentication methods through token card services.

From a troubleshooting standpoint, it is very important to know what security policies have been implemented for management access to the devices. From which IP addresses can you access the devices? What type of authentication, authorization, and accounting (AAA) is used on the devices? If centralized AAA services are deployed, what happens when these servers fail or become unreachable? Are there any back doors or fallback mechanisms to access the devices?

Clearly, the more restrictive the policy is, the more secure the network will be. However, you need to be careful not to create a situation where devices cannot be accessed during a network outage. Otherwise, a very dangerous “catch-22” situation can be created: A network problem causes you to lose management access to the devices. To diagnose and resolve the problem, you first need access to the devices. However, to access the devices, you first need to solve the problem. However, to solve the problem, you first need access to the devices. Eventually, you might not have another option than hoping that you can get physical access to the device to perform a password recovery procedure and gain access to the command line of the device.

Control Plane Security

- Many control plane protocols such as routing protocols, and FHRPs can be secured using authentication mechanisms.
- The Spanning Tree Protocol can be secured using features such as root guard and BPDU guard.
- Switches can inspect ARP and DHCP traffic and intercept malicious packets.
- Control plane policing and control plane protection features can be implemented on routers and switches to protect the devices from DoS attacks.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6.6

Control plane protocols such as routing protocols, spanning tree, and the Address Resolution Protocol (ARP) fill the data structures that are used by the data plane to forward packets. Therefore, any device that participates in these protocols can influence the forwarding behavior of the network. By manipulating routing tables, ARP caches, or the spanning-tree topology, packets can be diverted or dropped. In the same way, First Hop Redundancy Protocols (FHRPs), DHCP, and ARP can be used to influence the forwarding behavior between hosts and routers. Therefore, unauthorized participation in any of these protocols should be prevented to secure the network.

Most routing protocols support neighbor authentication based on Message Digest 5 (MD5) hashes, allowing only a router that is in possession of a shared key to become a neighbor. A similar mechanism is supported by FHRPs, such as the Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and Gateway Load Balancing Protocol (GLBP). Using an authentication mechanism prevents unauthorized devices from participating in these important control plane protocols and misdirecting or black-holing application traffic.

The IEEE 802.1D Spanning Tree Protocol (STP) does not have an authentication mechanism. Therefore, other mechanisms must be used to prevent unauthorized interaction with the spanning tree protocol. To facilitate this, Cisco switches support the bridge protocol data unit (BPDU) guard feature, which shuts down a port if unauthorized BPDUs are detected on a port. Cisco switches also support the root guard feature, which allows a neighboring switch to participate in the spanning tree protocol but shuts down the port if it attempts to become the root bridge.

The DHCP and ARP protocols can be protected by enabling the DHCP snooping and Dynamic ARP Inspection (DAI) features, which can inspect DHCP and ARP packets in order to allow only legitimate ARP and DHCP traffic and block malicious traffic that aims to redirect user traffic by manipulating the ARP and DHCP tables.

Finally, the control plane policing and control plane protection features can be implemented to protect the CPU of infrastructure devices such as routers and switches from being overloaded by unwanted control plane traffic. These features use the Cisco Modular QoS CLI (MQC) to protect the infrastructure from DoS attacks.

For more information about this feature, see the control plane protection feature guide at:

https://www.cisco.com/en/US/docs/ios/12_4t/12_4t4/htcpp.html

How do these features affect troubleshooting?

It is important to know which of these features have been implemented in your network and where they have been implemented, because they restrict which devices can participate in the control plane protocols. If these features are misconfigured, they can cause the operation of a control plane protocol between two devices to fail.

Data Plane Security

Routers and switches can inspect and filter traffic

- Access lists
- VLAN access maps
- uRPF
- Cisco IOS firewall
- IPS

Routers can encrypt and authenticate traffic

- VPN

Routers and switches can control network access

- NAC
- 802.1X

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0-6.7

When the management plane and control plane are secured, the devices and the network itself are secured. As such, the techniques reviewed previously are used to harden the infrastructure and protect the network itself against attacks.

In addition, routers and switches can play an important role in protecting the hosts on the network and securing the exchange of traffic on the network. Because routers and switches are involved in passing network traffic, they can play a role in inspecting and filtering traffic as it flows through the network. Unauthorized or unwanted traffic can be blocked by implementing traffic filtering features, such as access lists, VLAN access maps on switches, and the Cisco IOS firewall and IPS features on routers. Also, the Unicast Reverse Path Forwarding (uRPF) feature can be deployed as an antispoofing mechanism by filtering packets that enter a router or a switch through an interface that is not on the best path back to the source IP address of the packet.

Another role in protecting network traffic that can be implemented on routers is the use of IP Security (IPsec) encryption and authentication technology to guarantee the integrity and confidentiality of traffic that needs to be tunneled across an unsecure network.

A third category of security features that can be used to secure the data plane are the features that allow controlled access to interfaces on switches and, to a lesser extent, routers. For example, technologies such as 802.1X and Network Admission Control (NAC) can be used to allow network access through a switch port only if certain criteria are met. In case of 802.1X a device is allowed access to the network only after successfully authenticating against a username and password database stored on a RADIUS server. In case of NAC, the criteria for successful admission to the network can be even more sophisticated, such as allowing access only if the device has a specific patch level for its operating system or a minimum version of antivirus software.

What does this mean from a troubleshooting standpoint? Again, it is vital that you know which security features are implemented at which points in the network. Misconfigured security features can cause valid traffic to be dropped. Therefore, security features should always be considered as a possible cause of network connectivity problems. Especially when your troubleshooting process has indicated that there is network layer connectivity between two hosts, but upper layers are not working as expected, you should consider whether any form of packet filtering might be implemented between the two hosts that could cause the connectivity to fail.

Additionally, when you are observing problems on the management plane or control plane of a network device, you should always keep in mind that management and control traffic also passes through the data plane, and data plane security features could be the cause of the failure.

Troubleshooting Network Security Guidelines

Know the security policy of your network.

Know which security features have been implemented to enforce this policy at each point in the network.

Temporarily disabling a security feature or allowing access can be useful as a diagnostic technique, but needs to be balanced against the possible risk.

Check the security policy before making any changes.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6.8

What is the impact of security features on the network troubleshooting process?

For most of the features that are used in the building of a network infrastructure, the objective is to enable connectivity between devices or between different parts of the network. The objective for most security features is actually the complete opposite. Security features usually aim to restrict connectivity and only allow traffic that is specifically permitted by the security policy to support the business processes of the organization.

This adds another dimension to network troubleshooting. In a network that is completely open and has been designed to enable connectivity from any point to any point in the network, it is easy to validate a reported problem. If there is no connectivity between any two hosts or applications, this constitutes a problem. You initiate a troubleshooting process to isolate the problem, find the point where connectivity is failing, and restore the connectivity by implementing the necessary changes.

However, in a secured environment, a reported connectivity problem does not automatically translate to a valid problem that needs to be resolved. First, you need to determine whether the reported lack of connectivity actually concerns authorized traffic according to the security policy of your organization. If this is not the case, the problem is not a technical problem but should be resolved at the business level. If there is a valid reason why a user would need connectivity that is currently not allowed by the security policy, then the security policy might need to be reevaluated and changed. Eventually, changes in the policy should result in changes in the implementation, such as the addition of a firewall rule.

After you have validated the problem and determined that the reported lack of connectivity concerns traffic that should be allowed according to the policy, the implemented security features complicate the troubleshooting process, because they add more potential problem causes that need to be eliminated to diagnose the problem.

Therefore, it is vital that you know which security features have been implemented at each point in your network, because this will help you to quickly assess whether a misconfigured security feature might be a potential cause of the problem.

After you have partially diagnosed a problem and you are trying to establish whether the problem is caused by a security feature, a useful diagnostic technique can be to temporarily disable the security feature to see if this fixes the problem. However, you should realize that by doing this, you are creating a situation that is not compliant with the security policy, and as such, you are taking a risk of opening the network to an attack. Therefore, you should always try to estimate the potential risk of the change, and balance that against the criticality of the problem that you are troubleshooting.

For example, you might be troubleshooting a major network issue that is caused by the fact that two routers do not establish an Open Shortest Path First (OSPF) adjacency. The security policy states that MD5 authentication should be used between OSPF routers. You are wondering whether the authentication is the cause of the failure, or if another issue is causing it. In this case, it would probably be permissible to remove the OSPF authentication between these two routers temporarily to confirm or eliminate OSPF authentication as the source of the problem. The criticality and urgency of the problem is high, and the risk of an actual security incident if you remove OSPF authentication for a couple of minutes is very low.

Now consider the following example: You are troubleshooting a connectivity problem of a user that cannot reach a particular site on the Internet. You suspect that this might be caused by an access list on an Internet-facing router. Should you temporarily remove the access list to verify whether this is the cause of the problem?

Finally, you need to realize that if disabling a security feature restores connectivity, this does not actually constitute a solution to the problem. It might have helped you in establishing that the security feature is causing the problem, but if the new situation is not compliant with the security policy, it is not a solution, but a workaround at best. You should roll back the change and continue your troubleshooting process until you find a solution that is compliant with the security policy.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- You have reviewed the security features that are most commonly implemented on routers and switches and their impact on the network troubleshooting process.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—6-6

Lab 6-1 Debrief

Overview

In this lab, you have practiced troubleshooting problems related to the generic security features available in the Cisco IOS Software, such as access lists and authentication, authorization, and accounting (AAA) methods. In addition, you have practiced recovering from lost password and authentication failures. You have created a troubleshooting plan to coordinate the work between the team members. You have methodically researched the problems, kept a log of your actions and findings, resolved the problems, and documented your solutions.

During the lab debrief, the instructor will lead a group discussion during which you can present your solutions. You will get an opportunity to verify your solution against a number of checkpoints provided by the instructor and compare your solution to other students' solutions. The instructor will discuss alternate solutions along with their advantages and disadvantages.

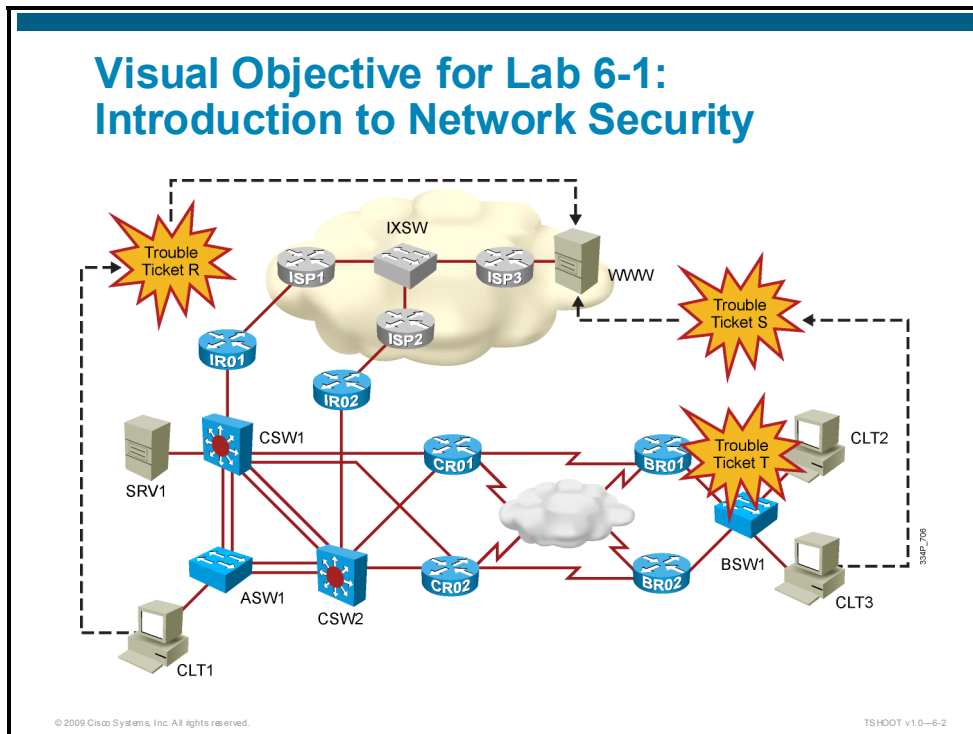
Objectives

Upon completing this lesson, you will be able to diagnose and resolve problems related to access lists and authentication using a structured, methodical approach. This ability includes being able to meet these objectives:

- Compare your solution, findings, and action log against a set of checkpoints provided by the instructor and identify common and alternate solutions
- Consolidate the lessons learned during the review discussions into a set of best-practice methods and commands to aid you in future troubleshooting procedures

Review and Verification

This topic describes the problems that were introduced in Lab 6-1, asks how you can verify that you have solved the problems, and provides an example of a troubleshooting process that will allow you to find and resolve the issues.



This lab consists of three trouble tickets: Trouble Ticket R involves the connectivity from client PC CLT1 at headquarters to the Internet. Trouble Ticket S involves connectivity from client PC CLT3 at the branch site to the Internet. Trouble Ticket T involves overall network connectivity from client PC CLT2, where the reported symptom is that the client cannot ping any destination on the network.

The introduction of the trouble ticket states that several security measures have been implemented, including several access lists and a TACACS+ server for centralized authentication. Also, a rough security policy has been defined, and any changes that you make during your troubleshooting process need to be validated against this policy.

Planning Troubleshooting

How did your team approach the three trouble tickets?

- Did you troubleshoot all tickets in parallel, in sequence, or using a combination of methods?
- How did you decide on the order in which you chose to address the tickets?
- How did you coordinate device access among your team members?
- How did you communicate with your team members?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—6-3

Note This lesson provides sample answers and solutions to the questions posed during the debrief discussions. Keep in mind that alternate solutions and methods might be just as valid and that the solutions provided here only highlight a sample approach and solution.

The urgency of the three tickets is more or less equal. (Although you could argue that guest access is less important than office user connectivity and that therefore Trouble Ticket S should be addressed only after Trouble Tickets R and T have been resolved). It should be noted that Trouble Tickets R and S both revolve around connectivity to the Internet. This means that there is a chance that the root cause of these two tickets is the same, so if these tickets are addressed in parallel, close coordination is needed between the team members working on these tickets.

Based on this, a possible work plan for a team consisting of three members would be the following:

- Team member 1 will focus on Trouble Ticket R. This team member will primarily control switches ASW1, CSW1, and CSW2. Control of routers IRO1 and IRO2 will be coordinated between this team member and the team member handling Trouble Ticket S as needed.
- Team member 2 will focus on Trouble Ticket T. This team member will coordinate control of switch ASW1 and routers BRO, BRO2, CRO1, and CRO2 with the team member working on Trouble Ticket S.
- Team member 3 will focus on Trouble Ticket S. This team member will coordinate device access with the other team members as needed. Also, this team member will function as the team coordinator and work closely with the other team members to ensure that any discoveries that are relevant to other tickets are shared within the team.

Trouble Ticket R: Internet not Reachable from Client PC CLT1

The text introducing this trouble ticket was the following:

One of the headquarters office users who uses client PC CLT1 has reported that he cannot open the web page located at <http://www.isp3.local>.

Your task is to diagnose this problem and restore connectivity to <http://www.isp3.local> and any other connectivity that this user is entitled to according to the security policy. Ensure that no other traffic is allowed other than the traffic specifically permitted by the security policy.

Trouble Ticket R: Review and Discuss

How did your team approach Trouble Ticket R?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you accomplish the goal of restoring the connectivity from client PC CLT1 to the Internet?
- How did you verify that you accomplished your goal?
- Does your solution comply with the security policy?
- Did you make any temporary changes as part of your troubleshooting process that might have violated the security policy?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—6-4

The problem in this ticket is caused by a misconfigured access list on routers IRO1 and IRO2 that matches destination ports 80 and 443 for return traffic from the Internet, while it should match the source ports, based on the direction of the traffic.

During the diagnosis of this issue, you are likely to encounter a second problem: The exec timeout on the console of router IRO1 has been set to one second instead of the value of one hour that is used on all other devices. As a result, you will be logged out of the console after one second of inactivity. To fix this problem, you should access the router via Telnet and reset the exec timeout for the console.

Although there are many possible methods that you could use to solve this problem, the following example of a troubleshooting log shows you a methodical approach to solve this problem.

Trouble Ticket	Actions and results
Ticket R	CLT1: Verified problem: Cannot browse to http://www.isp3.local.
	Verify security policy: HTTP and HTTPS from office users to the Internet is allowed.
	CLT1: Ping to default gateway (10.1.128.126) succeeds. Ping to www.isp3.local succeeds.
	CLT1: Telnet to www.isp3.local on port 80 fails (timeout).
	Conclusion: This is likely to be caused by an access list or firewall issue. The most likely point of access list implementation is on routers IRO1 and IRO2.
	CLT1: Traceroute to www.isp3.local shows that this client is routed via router IRO1.
	IRO1: Console session is immediately logged out after logging in.
	CLT1: Telnet to IRO1. Session stays logged in normally.
	IRO1: Verify console settings: Exec timeout is set to 1 second.
	IRO1: Verified security policy: No specific value for exec timeout is mentioned. Verify other devices: 60 minutes seems to be the common value. Configuration changed: Set exec timeout for console to 60 minutes to be consistent with other devices. Both prechange and postchange configurations were saved in flash on the device. Communicated this information to team members.
	IRO1: Return to original problem. Examine access lists on this router: No access list is implemented to filter outbound traffic, but return traffic from the Internet is filtered.
	IRO1: Temporarily added an explicit "deny" line to the end of the access-list to log all packets that are not permitted by any other rule.
	IRO1: The log shows packets from www.isp3.local (172.34.224.1) port 80 to client PC CLT1 (10.1.128.65) being dropped.
	IRO1: Verify access list: The lines that should control returning HTTP and HTTPS traffic filter destination port 80 and 443 instead of source port 80 and 443.
	IRO1: Configuration changed: Changed lines that filter destination ports 80 and 443 (lines 140-170) to filter the source port instead. Prechange configuration was saved in flash on the device. Communicated this information to team members.
	CLT1: Browsing to http://www.isp3.local succeeds.
	IRO1: Access list shows packets being permitted by the altered lines.
	IRO1: Remove the temporary line at the end of the access-list that was added during troubleshooting. Saved configuration to NVRAM.
	IRO2: Compare access list to see if a comparable problem exists on router IRO2: Access list is misconfigured in the same manner.
	IRO2: Configuration changed: Changed lines that filter destination ports 80 and 443 (lines 140-170) to filter the source port instead. Both prechange and postchange configurations were saved in flash on the device. Communicated this information to team members.
	Problem fixed. Documented changes. Backed up configurations. Communicated to team members. Closed ticket.

Key Clue: Packets Dropped by Access List

- To verify whether the access list on router IRO1 is causing the problem, add an additional line at the end of the access list to drop packets explicitly and log any packets being dropped.
- The logging then reveals that return packets for the HTTP session to <http://www.isp3.local> initiated by client CLT1 are indeed being dropped:

```
IR01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
IR01(config)#ip access-list extended IN-FROM-INTERNET
IR01(config-ext-nacl)#180 deny ip any any log
IR01(config-ext-nacl)#end
IR01#clear logging
Clear logging buffer [confirm]
IR01#show logging
<... output omitted ...>
Jul 15 00:54:43 PDT: %SEC-6-IPACCESSLOGP: list IN-FROM-INTERNET
denied tcp 172.34.224.1(80) -> 10.1.128.65(1093), 1 packet
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-5

A useful technique that you can use to troubleshoot access list problems is to define an explicit line at the end of the access lists that drops all packets that are not specifically permitted by earlier lines. Logging any packets that are being denied by this line can then be used to verify whether the specific traffic that you are investigating is being dropped instead of being permitted by the appropriate line. Clearly, earlier lines could also be dropping the traffic, but at least this technique will give you a starting point for further investigation.

In this specific case the log clearly shows that return traffic from <http://www.isp3.local> (172.34.224.1) on port 80 to client PC CLT1 (10.1.128.65) is dropped by the access-list.

Trouble Ticket R Checkpoints

Minimum checkpoints to prove that you have resolved this trouble ticket:

- Client PC CLT1 can use a web browser to connect to <http://www.isp3.local>.
- You have verified that client PC CLT1 can access all resources that it is entitled to by the security policy (but not more than that).
- You have documented your process, your solution, and any changes that you have made to the device configurations.

What else should you have checked?

Are there any unresolved issues?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-6

The figure shows a list of minimum requirements that should be met to consider this trouble ticket to be resolved.

The second item implies that you will need to validate the any changes that you have made during the resolution of this ticket against the security policy.

Suggested Solution

Correcting the configurations of routers IRO1 and IRO2 as follows can restore the connectivity from client PC CLT1 to the Internet.

Suggested Configuration Changes

- On router IRO1, change the exec timeout for the console to one hour (60 minutes) to be consistent with the other devices.

```
IRO1(config)#line con 0
IRO1(config-line)#exec-timeout 60 0
```

- On routers IRO1 and IRO2, change access list IN-FROM-INTERNET to filter on source ports 80 and 443 instead of on destination ports:

```
IRO1(config)#ip access-list extended IN-FROM-INTERNET
IRO1(config-ext-nacl)# no 140
IRO1(config-ext-nacl)# 140 deny tcp any eq www 10.1.160.64 0.0.0.63
IRO1(config-ext-nacl)# no 150
IRO1(config-ext-nacl)# 150 deny tcp any eq 443 10.1.160.64 0.0.0.63
IRO1(config-ext-nacl)# no 160
IRO1(config-ext-nacl)# 160 permit tcp any eq www 10.1.128.0 0.0.127.255
IRO1(config-ext-nacl)# no 170
IRO1(config-ext-nacl)# 170 permit tcp any eq 443 10.1.128.0 0.0.127.255
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-7

Changing the exec timeout on router IRO1 to a value of less than 60 minutes is valid as well. However, for the sake of consistency, you should then change the exec timeout to the same value as on the other devices. Removing the exec timeout entirely is not considered to be a valid solution, because it decreases the security of the network.

You can change the access list in various manners to achieve the same result. However, you need to ensure that the changes do not open up the possibility for clients that are members of the office VLAN at the branch (such as client PC CLT2) to access the Internet, which is explicitly forbidden by the security policy.

Also, it is important that the changes to the access list are made on both routers IRO1 and IRO2. The traffic from client PC CLT1 is routed via router IRO1, so making the change on router IRO1 only will actually resolve the issue for client PC CLT1. However, other clients that are routed via router IRO2 will experience similar problems if the access list is not changed in a similar manner on router IRO2.

Trouble Ticket S: Internet Not Reachable from Client PC CLT3

The text introducing this trouble ticket was the following:

An external contractor in the branch office who uses client PC CLT3 has reported that he cannot browse to <http://www.isp3.local>.

Your task is to diagnose this problem and restore connectivity to <http://www.isp3.local>. Ensure that no other traffic is allowed other than the traffic specifically permitted by the security policy.

Trouble Ticket S: Review and Discuss

How did your team approach Trouble Ticket S?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you accomplish the goal of restoring the connectivity from client PC CLT3 to the Internet?
- How did you verify that you accomplished your goal?
- Does your solution comply with the security policy?
- Did you make any temporary changes as part of your troubleshooting process that might have violated the security policy?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—6-8

The problem in this ticket is caused by a misconfigured IP address in an access list on routers CRO1 and CRO2, which causes Domain Name System (DNS) lookups to fail. As a result, connecting by hostname, such as browsing to <http://www.isp3.local> fails. Connections based on an IP address, such as browsing to <http://172.34.224.1> will succeed, as long as the issues found in Trouble Ticket R have already been resolved.

During the troubleshooting process for this problem you might find two other issues: The enable secret password on router BRO1 has been accidentally changed and needs to be recovered, and the key used by TACACS+ between router CRO2 and the Cisco Secure Access Control Server (ACS) on server SRV1 is mismatched and needs to be corrected. For both these problems, you need to initiate a password recovery procedure.

Although there are many possible methods that you could use to solve this problem, the following example of a troubleshooting log shows you a methodical approach to solve this problem.

Trouble Ticket	Actions and results
Ticket S	CLT3: Verified problem: Cannot browse to http://www.isp3.local.
	Verify security policy: HTTP and HTTPS from guest users to the Internet is allowed.
	CLT3: Ping to default gateway (10.1.160.254) succeeds. Ping to www.isp3.local fails. The IP address for www.isp3.local cannot be resolved through DNS.
	Check baseline: IP address for www.isp3.local is 172.34.224.1.
	CLT3: Browsing to http://172.34.224.1 succeeds.
	CLT3: Ping to 10.1.152.1 (DNS server) succeeds.
	Conclusion: Either the DNS service is not running on the server, or DNS packets are being blocked by an access list in the path.
	BRO1: Cannot access privileged mode on router BRO1: Enable password seems to be different than the documented password.
	Checked with engineering team and security officer: TACACS+ was not implemented on this router yet and the enable password should not have changed. Password recovery to reset the password is warranted.
	BRO1: Executed password recovery and change the password to the documented password. Saved the configuration and made a backup to server SRV1.
	BRO1: Ping to www.isp3.local succeeds. Conclusion: DNS service is running on server SRV1. The problem is likely to be caused by an access list.
	BRO1: Verify access list for the guest VLAN: DNS is specifically permitted to 10.1.152.1. Matched packets are shown on the corresponding line after clearing the access list counters. Problem is likely to be further downstream.
	CRO1: Line in the access list that should allow DNS traffic to server SRV1 does not show any matches: Does DNS traffic not arrive or is there a problem with this line?
	CRO1: Added a line at the beginning of the access list to permit all DNS traffic and log it.
	CLT3: Ping to www.isp3.local works now. DNS is correctly resolved.
	CRO1: The log shows the DNS request being permitted by the newly inserted line.
	CRO1: Verify original access list lines again. Spotted the error: The IP address configured for the DNS server in the access list line is 10.1.252.1 instead of 10.1.152.1.
	CRO1: Configuration changed: Changed lines that permit DNS traffic (lines 10-20) to reference the correct IP address 10.1.152.1. Removed the line at the beginning of the access list that was added for troubleshooting purposes. Prechange configuration was saved in flash on the device. Communicated this information to team members.
	CLT3: Ping to www.isp3.local succeeds after clearing the DNS cache.
	CLT3: Browsing to http://www.isp3.local succeeds.
	CRO1: Access list shows packets being permitted by the altered lines.
	CRO1: Saved configuration to NVRAM.
	CRO2: Compare access list to see if a comparable problem exists on router IRO2: Can't get access to CRO2. Login prompt is not presented.
	Checked with engineering team and security officer: TACACS+ was implemented on this router and the ACS server has been implemented to support this. TACACS+ authentication was also configured on router CRO1.
	CRO1: Confirmed that TACACS+ is configured and working.
	SRV1: Confirmed that TACACS+ is set up correctly for router CRO2. Configured key in ACS is "cisco." Failed attempts log shows "Key Mismatch" for router CRO2.

Trouble Ticket	Actions and results
	CRO2: Perform password recovery procedure to get access to privileged mode. (Password is not actually changed).
	CRO2: Verify that a key mismatch is the cause of the problem through use of the debug tacacs command.
	CRO2: Configuration changed: Changed the tacacs key to "cisco" to match the configuration on the ACS server. Both prechange and postchange configurations were saved in flash on the device. Communicated this information to team members.
	CRO2: Resume troubleshooting of the original problem: Compare access list to the access list on router CRO1 to check if the IP address of the DNS server was also misconfigured on this router.
	CRO2: Found identical problem. IP address 10.1.252.1 was configured instead of 10.1.152.1.
	CRO2: Configuration changed: Changed lines that permit DNS traffic (lines 10-20) to reference the correct IP address 10.1.152.1. Both prechange and postchange configurations were saved in flash on the device. Communicated this information to team members.
	Problem fixed. Documented changes. Backed up configurations. Communicated to team members. Closed ticket.

Key Clue: Packets Dropped by Access List

- To verify whether the access lists on routers CRO1 and CRO2 are causing the problem, add an additional line to the beginning of the access list to permit DNS traffic explicitly and log any packets being forwarded.
- The logging then reveals that DNS packets from client PC CLT3 are now being forwarded:

```
CRO1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CRO1(config)#ip access-list extended LIMIT-HQ-ACCESS
CRO1(config-ext-nacl)#5 permit udp any any eq domain log
CRO1(config-ext-nacl)#end
CRO1#clear logging
Clear logging buffer [confirm]
CRO1#show logging
<... output omitted ...>
Jul 15 04:30:03 PDT: %SEC-6-IPACCESSLOGP: list LIMIT-HQ-ACCESS
permitted udp 10.1.160.193(56873) -> 10.1.152.1(53), 1 packet
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-9

A variation on the technique used in Trouble Ticket R is to add a line to the beginning of an access list that you suspect is causing the problem and specifically permit the traffic that you are investigating. If the problem symptoms disappear, this confirms that this access list was the cause of the problem. Again, logging the matches on the access list line will help in tracking the specific traffic. Be aware that at this point you have implemented a workaround, not a solution. You still need to determine which line in the access list was dropping the traffic and how to reconfigure the access list to forward the traffic as intended. Do not forget to remove the line you temporarily added after repairing the original access list.

In this example, you can see that the DNS traffic from client PC CLT3 (10.1.160.193) is now correctly forwarded to server SRV1 (10.1.152.1).

Key Clue: Invalid AUTHEN Packet

- Using the **debug tacacs** command on router CRO2 reveals that a TACACS+ key mismatch might be the cause of the problem:

```
CRO2#debug aaa authentication
AAA Authentication debugging is on
CRO2#debug tacacs
TACACS access control debugging is on
CRO2#show logging
<... output omitted ...>
Jul 15 06:10:55.810 PDT: AAA/AUTHEN/LOGIN (00000004): Pick method list
'default'
Jul 15 06:10:55.810 PDT: TPLUS: Queuing AAA Authentication request 4 for
processing
Jul 15 06:10:55.814 PDT: TPLUS: processing authentication start request id 4
Jul 15 06:10:55.814 PDT: TPLUS: Authentication start packet created for 4()
Jul 15 06:10:55.814 PDT: TPLUS: Using server 10.1.152.1
Jul 15 06:10:55.814 PDT: TPLUS(00000004)/0/NB_WAIT/63A854B8: Started 5 sec
timeout
<... output omitted ...>
Jul 15 06:10:55.858 PDT: TPLUS(00000004)/0/63A854B8: Processing the reply
packet
Jul 15 06:10:55.858 PDT: TPLUS: received bad AUTHEN packet: length = 6,
expected 53603
Jul 15 06:10:55.858 PDT: TPLUS: Invalid AUTHEN packet (check keys).
Jul 15 06:10:55.858 PDT: TPLUS(00000004)/0/REQ_WAIT/63A854B8: timed out
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--6-10

After performing password recovery on router CRO2, there are two ways to establish that a mismatched TACACS+ key is the cause of the problem. You can examine the “Failed Attempts” log on the Cisco Secure ACS server, or alternatively, you can use the **debug tacacs** command to find the cause of the failure.

Trouble Ticket S Checkpoints

Minimum checkpoints to prove that you have resolved this trouble ticket:

- Client PC CLT3 can use a web browser to connect to <http://www.isp3.local>.
- You have verified that client PC CLT3 can access all resources that it is entitled to by the security policy (but not more than that).
- You have documented your process, your solution, and any changes that you have made to the device configurations.

What else should you have checked?

Are there any unresolved issues?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-11

The figure shows a list of minimum requirements that should be met to consider this trouble ticket to be resolved.

Be aware that in order to meet the requirement in the first item, it is necessary to resolve the Internet access issue covered in Trouble Ticket R.

The second item implies that you will need to validate the changes that you have made during the resolution of this ticket against the security policy.

Suggested Solution

Correcting the configurations of routers BRO1, CRO1, and CRO2 as follows can restore the connectivity from client PC CLT3 to the Internet.

Suggested Configuration Changes

- After performing a password recovery procedure, the TACACS+ key on router CRO2 needs to be changed to match the key configured on the TACACS+ server:

```
CRO2(config)#tacacs-server key cisco
```

- After performing a password recovery procedure, the enable secret password needs to be reset on router BRO1:

```
BRO1(config)#enable secret cisco
```

- On routers CRO1 and CRO2 change access list LIMIT-HQ-ACCESS to reference the correct IP address for server SRV1:

```
CRO1(config)#ip access-list extended LIMIT-HQ-ACCESS
CRO1(config-ext-nacl)# no 10
CRO1(config-ext-nacl)# 10 permit udp 10.1.128.0 0.0.127.255 host 10.1.152.1
eq domain
CRO1(config-ext-nacl)# no 20
CRO1(config-ext-nacl)# 20 permit tcp 10.1.128.0 0.0.127.255 host 10.1.152.1
eq domain
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—6-12

Performing a password recovery procedure and correcting the TACACS+ key on router CRO2 is necessary to change the misconfigured access list on this router.

Performing a password recovery procedure on router BRO1 is not strictly necessary to resolve this ticket. Depending on your troubleshooting method, you might not discover this problem until you start working on Trouble Ticket T.

You can change the access list in various other manners to achieve the same result. However, you need to ensure that the change does not allow any unintended traffic to be forwarded.

Trouble Ticket T: Client PC CLT2 Has No Network Connectivity

The text introducing this trouble ticket was the following:

One of the branch office users (who uses CLT PC CLT2) reports that the network is broken and he cannot connect anywhere. He reports that ping does not even work! (This user worked as a part-time server administrator in his previous job and thinks he knows a lot about networking).

Your task is to diagnose this problem and restore all connectivity that this user is entitled to according to the security policy.

Trouble Ticket T: Review and Discuss

How did your team approach Trouble Ticket T?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you accomplish the goal of restoring network connectivity for client PC CLT2?
- How did you verify that you accomplished your goal?
- Does your solution comply with the security policy?
- Did you make any temporary changes as part of your troubleshooting process that may have violated the security policy?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--6-13

The remaining problem that needs to be resolved is that it is not possible to ping from client PC CLT2 to any remote destination on the network. This is caused by the absence of the ICMP echo and echo reply messages from the list of permitted ICMP messages that is defined in the access list for the office VLAN defined on routers BRO1 and BRO2.

This causes ping to fail, but any other traffic that is allowed according to the security policy will work at this point. For example, opening the shared folder `\\SRV1\Public` will succeed, even if a ping to server SRV1 fails. (The assumption here is that all issues from the other tickets have been solved at this point. The DNS problem from Trouble Ticket S also affects this ticket if it has not been resolved yet.)

Although there are many possible methods that you could use to solve this problem, the following example of a troubleshooting log shows you a methodical approach to solve this problem.

Trouble Ticket	Actions and results
Ticket T	CLT2: Verified problem: Cannot ping to server SRV1. Received “destination net unreachable” messages from 10.1.160.125 (BRO2).
	Verify security policy: “Management and control traffic should be permitted, but only as necessary.” Confirmed with security officer: Using ping for diagnostic purposes should be allowed.
	CLT2: Even ping to default gateway (10.1.160.126) fails, with a similar error message.
	CLT3: Ping to default gateway succeeds. Ping to www.isp3.local succeeds.
	Conclusion: There seems to be a difference in the way ping is treated for the office VLAN and the guest VLAN.
	BRO2: Scanned access lists for ICMP and IP protocols. The access list “LIMIT-OFFICE-ACCESS” does not allow “echo” and “echo reply” messages, while the access list “LIMIT-GUEST-TRAFFIC” allows these messages.
	BRO2: Configuration changed: Added the ICMP echo and echo reply messages to the list of allowed ICMP messages for access list “LIMIT-OFFICE-TRAFFIC.” Both prechange and postchange configurations were saved in flash on the device. Communicated this information to team members.
	CLT2: Ping to default gateway still fails. This time, the “destination net unreachable” messages are received from 10.1.160.124 (BRO1).
	BRO1: Compare access list to see if a comparable problem exists on router BRO1: ICMP echo and echo reply are also missing in the access list on router BRO1.
	BRO1: Configuration changed: Added the ICMP echo and echo reply messages to the list of allowed ICMP messages for access list “LIMIT-OFFICE-TRAFFIC.” Both prechange and postchange configurations were saved in flash on the device. Communicated this information to team members.
	CLT2: Ping to server SRV1 succeeds. Opening the shared folder \\SRV1\Public succeeds. Browsing to http://www.isp3.local fails, which is in line with the security policy.
	Problem fixed. Documented changes. Backed up configurations. Communicated to team members. Closed ticket.

Key Clue: Different Lists of Permitted ICMP Messages

- Comparison of ICMP messages defined in the access lists reveals that echo and echo-reply are missing.

```
BRO2#show access-list | include list|icmp|ip
Extended IP access list LIMIT-GUEST-ACCESS
 50 permit icmp 10.1.160.192 0.0.0.63 any host-unreachable
 60 permit icmp 10.1.160.192 0.0.0.63 any host-unknown
 70 permit icmp 10.1.160.192 0.0.0.63 any net-unreachable
 80 permit icmp 10.1.160.192 0.0.0.63 any network-unknown
 90 permit icmp 10.1.160.192 0.0.0.63 any port-unreachable (1 match)
100 permit icmp 10.1.160.192 0.0.0.63 any echo (33 matches)
110 permit icmp 10.1.160.192 0.0.0.63 any echo-reply
120 deny icmp any any
130 deny ip any 10.1.128.0 0.0.127.255 (135 matches)
160 deny ip any any
Extended IP access list LIMIT-OFFICE-ACCESS
 30 permit icmp 10.1.160.64 0.0.0.63 any host-unreachable
 40 permit icmp 10.1.160.64 0.0.0.63 any host-unknown
 50 permit icmp 10.1.160.64 0.0.0.63 any net-unreachable
 60 permit icmp 10.1.160.64 0.0.0.63 any network-unknown
 70 permit icmp 10.1.160.64 0.0.0.63 any port-unreachable
 80 deny icmp any any (13 matches)
110 deny ip any any (99 matches)
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--6-14

You can use the same techniques highlighted in the previous two trouble tickets to reveal the cause of this problem. Another method that you can employ is to use the “spot-the-differences” approach. After you have determined that ping works for client PC CLT3, but not for client PC CLT2, an obvious approach is to compare the access lists that filter the office VLAN traffic and guest VLAN traffic on routers BRO1 and BRO2. Using the **| include** option on the **show access-list** command can help to display only the information that is relevant and reduces the chance of overlooking things.

Trouble Ticket T Checkpoints

Minimum checkpoints to prove that you have resolved this trouble ticket:

- Client PC CLT2 can ping server SRV1 (10.1.152.1).
- You have verified that client PC CLT2 can access all resources that it is entitled to by the security policy (but not more than that).
- You have documented your process, your solution, and any changes that you have made to the device configurations.

What else should you have checked?

Are there any unresolved issues?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-15

The figure shows a list of minimum requirements that should be met to consider this trouble ticket to be resolved.

It is important to note that the requirements of this ticket will not be met if client PC CLT2 can browse to <http://www.isp3.local>, because Internet access for office users in the branch is specifically denied by the security policy.

This ticket can be fully resolved only if the DNS issue from Trouble Ticket S has also been resolved.

Suggested Solution

Correcting the configurations of routers BRO1 and BRO2 as follows can restore the ability to ping from client PC CLT2 to server SRV1 and other points in the network.

Suggested Configuration Changes

- Add the ICMP echo and echo-reply messages to the list of permitted messages in access-list LIMIT-OFFICE-ACCESS on routers BRO1 and BRO2:

```
BRO1(config)#ip access-list extended LIMIT-OFFICE-ACCESS  
BRO1(config-ext-nacl)# 72 permit icmp 10.1.160.64 0.0.0.63 any echo  
BRO1(config-ext-nacl)# 74 permit icmp 10.1.160.64 0.0.0.63 any echo-reply
```

- The exact sequence numbers used are irrelevant, as long as these lines are inserted before the **deny icmp any any** statement in the access list.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—6-16

Trouble Ticket S needs to be resolved before this ticket can be fully resolved, because otherwise, the DNS lookup will fail and ping by name will not work (even if a ping based on IP address works).

You can change the access list in various other manners to achieve the same result. However, it is important that the additional lines are inserted before the generic **deny icmp any any** statement that is present in this access list. Also, you need to ensure that the change does not allow any unintended additional traffic to be forwarded. This means that the statement should not be too generic, but only add the ICMP echo and echo reply messages.

Consolidation

This topic describes the primary lessons that could be learned from the lab exercise.

Discussion: Lessons Learned

Method and process:

- How could you improve your troubleshooting methods?
- What alternative methods did you discover?

Communication and procedures:

- How could the troubleshooting process be made more effective?
- What kind of procedures would be useful and why?

Technology and tools:

- Which tools were most useful during troubleshooting?
- Which tools could have improved the effectiveness of your process?
- Which useful Cisco IOS commands did you discover?

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0-6-17

Think about all the things that you learned during the lab itself and during the debrief discussions. There is room to write down primary learning points in the Lab Debrief Notes section of the lab guide.

In addition to thinking of the methods, processes, and tools as they were used in the lab, reflect on how these would apply to your own organization.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- You have reviewed and verified your lab results.
- You have consolidated the experiences and discoveries that all students got from the lab and you have derived a number of key learning points from these experiences.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—6-18

Security Features Review

Overview

The deployment of security features in the network infrastructure adds a layer of complexity to network troubleshooting. To troubleshoot effectively and efficiently in a secure infrastructure, it is important to understand which features are deployed and how they operate.

Most security features operate at the transport layer and above. Therefore, it is important to be familiar with the generic principles of troubleshooting Layer 4 connectivity. Using a generic troubleshooting process can help to determine whether the problems are likely to be related to security features or caused by underlying Layer 1, 2, or 3 connectivity issues. When you have determined that the problem must be related to a security feature, you will need to have detailed knowledge of the specific feature to diagnose and resolve the issue. Depending on your organization, you might need to escalate the issue to a security specialist when you arrive at this point in the troubleshooting process.

In this lesson, a generic structured method for troubleshooting Layer 4 problems is covered and some of the most common Cisco IOS security features are reviewed, including Cisco IOS firewall and authentication, authorization and accounting (AAA) using TACACS+ and RADIUS.

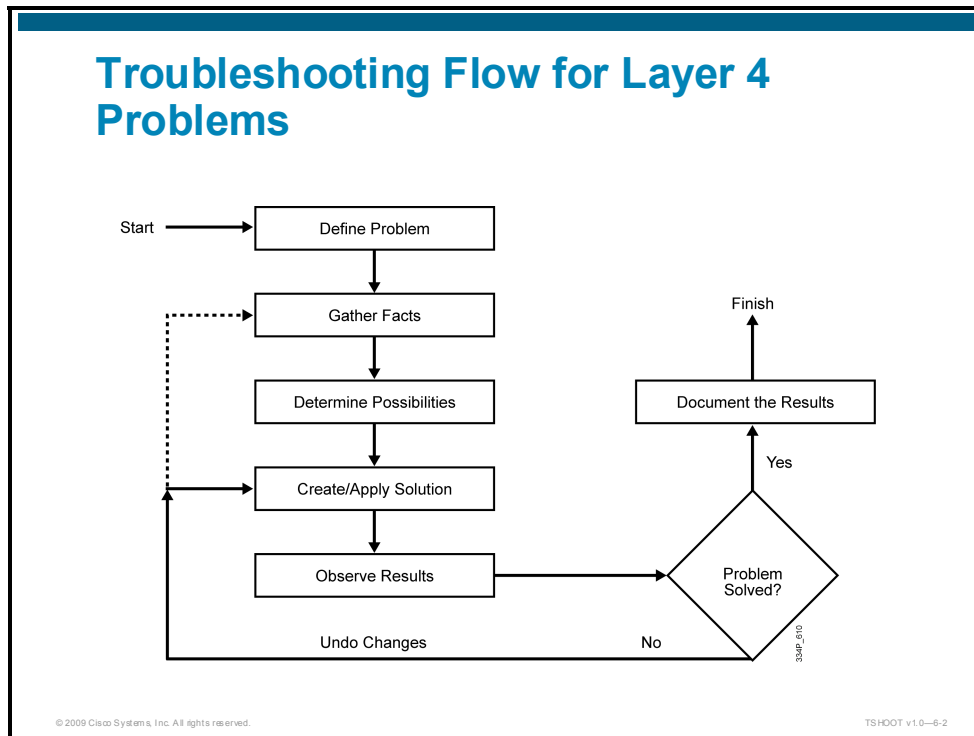
Objectives

Upon completing this lesson, you will be able to diagnose and resolve problems related to specialized Cisco IOS security features. This ability includes being able to meet these objectives:

- Diagnose and resolve transport layer problems in a structured manner
- Verify the operation of Cisco IOS Firewall stateful packet inspection
- Diagnose and resolve problems related to the use of AAA on routers and switches

Troubleshooting Transport Layer Problems

This topic describes a generic structured approach to diagnosing and resolving transport layer problems.

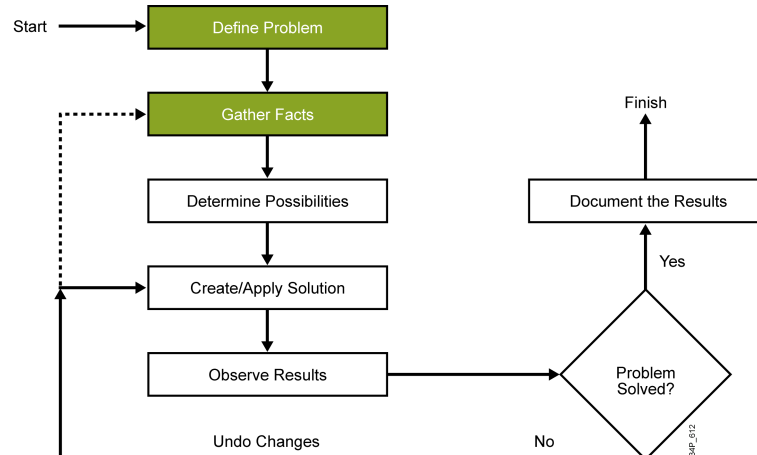


The troubleshooting flow shown in the figure outlines a troubleshooting process. In this process, the initial goal is to clearly define the problem. After defining the problem, you should gather more facts and consider possible problem causes. Next, you create an action plan for how to test your hypothesis of the most likely cause. Then, you implement the plan and observe the results. If the problem persists, you need to develop and try another action plan. It might be necessary to gather more facts at this point. Also, it is important that you undo any changes that you made at this point.

If, after implementing your solution, the problem symptoms disappear, you document how you resolved the problem. The following sections describe each of these steps in more detail.

Troubleshooting Flow for Layer 4 Problems (Cont.)

- Describe the problem and its symptoms.
- Gather facts from affected users, network administrator, and managers.

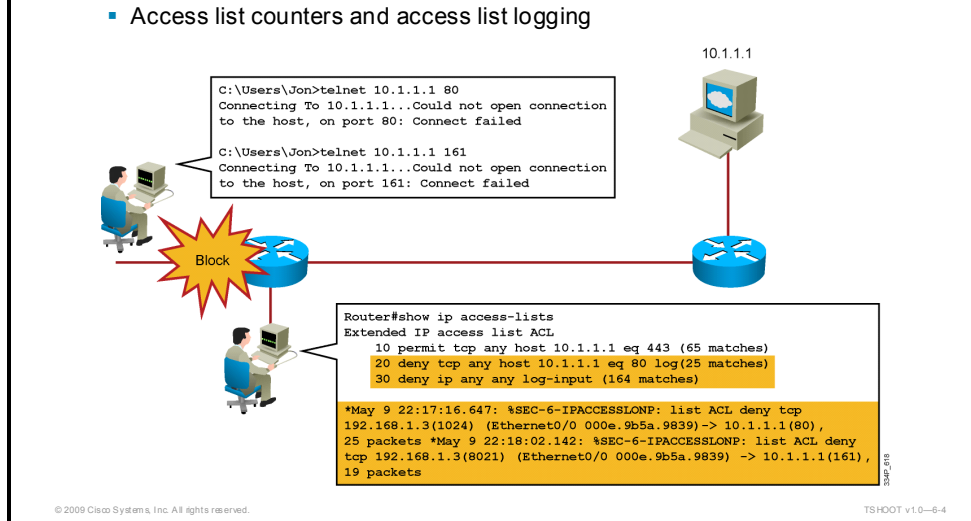


The first step is to define the problem. Writing a detailed description of the problem and its symptoms is a good way to start a troubleshooting process and will save time later. Documenting the problem might help you to come to a possible solution, which reduces the amount of work in later steps. You should have an understanding of the baseline behavior of your network (errors, throughput, response time, and efficiency). Defining how the current situation deviates from the baseline will help in establishing the nature of the problem. Focus on symptoms and what might cause them.

The next step is to gather facts from affected users, network administrators, and other major persons involved with the network. Collect information from network management systems, protocol analyzers, and the command-line interface (CLI) of routers and switches. Compare the current configuration with archived configurations to see if any changes have been made.

Troubleshooting Flow for Layer 4 Problems (Cont.)

- Telnet to a specific port
- Access list counters and access list logging



Telnet can be a useful tool to troubleshoot problems at the transport layer. The Telnet utility has the ability to connect to a specific destination port on a remote server, allowing it to be used to confirm correct traffic flow from a client to remote server. This makes it particularly useful for transport layer diagnostics. To use Telnet to connect to a specific TCP port, you can use the command syntax **telnet** *[ip-address | hostname] [port-number]*.

For example, to connect to host 10.1.1.1 on TCP port 80, you issue the command **telnet 10.1.1.1 80**.

Access lists can cause problems on the transport layer. One of the most useful ways to gain an insight in access list operation is to use the **log** keyword for specific access list entries. This keyword instructs the router to log a message to the system log whenever specific access list entry is matched. The logged event includes details of the packet that matched the access list entry. This technique can also be used to log information on intrusion attempts that are being blocked by the access list. For example, if the last element in an extended access control list (ACL) is configured as **deny ip any any log**, the details of any packet that does not match a preceding condition in the access list is recorded in the system log.

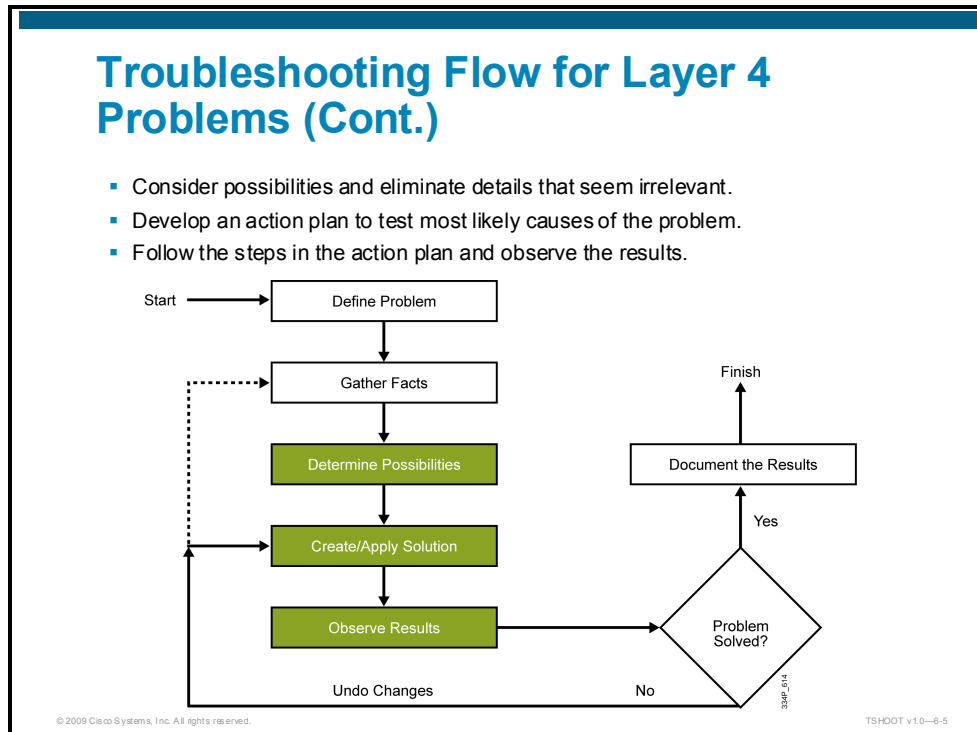
```
*May 9 22:17:16.647: %SEC-6-IPACCESSLONP: list ACL deny tcp
192.168.1.3(1024) (Ethernet0/0 000e.9b5a.9839) -> 10.1.1.1(80), 25
packets
*May 9 22:18:02.142: %SEC-6-IPACCESSLONP: list ACL deny tcp
192.168.1.3(8021) (Ethernet0/0 000e.9b5a.9839) -> 10.1.1.1(161), 19
packets
```

In the output, you can see how the access list named ACL blocks HTTP traffic from source IP address 192.168.1.3 to destination IP address 10.1.1.1.

In addition to the configuration of logging for specific access list entries, the hit counter of an access list entry can be used to determine errors in the access list configuration. It also helps in confirming whether certain traffic has passed through the access list or not.

```
Router#show ip access-lists
Extended IP access list ACL
 10 permit tcp any host 10.1.1.1 eq 443 (65 matches)
 20 deny tcp any host 10.1.1.1 eq 80 log(25 matches)
 30 deny ip any any log-input (164 matches)
```

In the output, you can see that 25 HTTP packets have been dropped by line 20 of the access list.

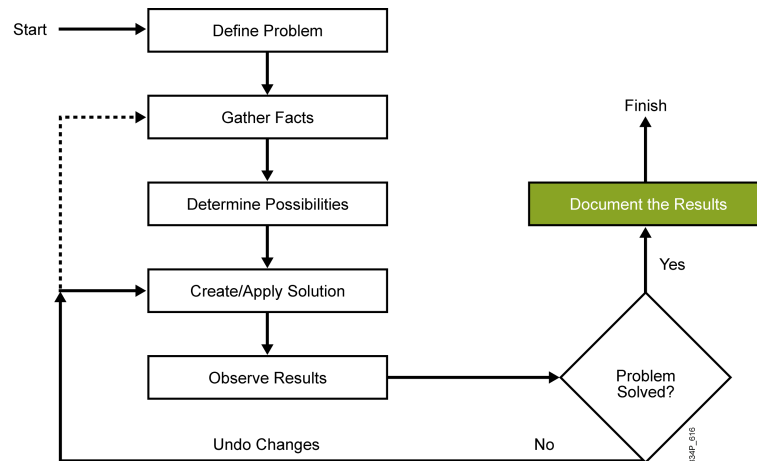


Consider possibilities and set aside details that seem irrelevant. Analyze symptoms to determine which possibilities are unlikely. Create a list of possibilities you graduate from the most likely to least likely.

Develop a plan for how you will test for the most likely causes of the problem. Plan to make only one change at a time to know exactly what resulted in the fix. Document your action plans. Each plan must include all the steps that must be fulfilled. Follow the steps in your action plan and observe the results. Record any plan you use; otherwise, you might repeat yourself. Test all solutions that you make and be sure that you do not make the problem worse or introduce a new one. Try to minimize the impact of your actions on network users. After performing each step of the plan, gather information to determine whether the problem is solved. Ask users to test their applications to know whether the problem is cured. If the problem is resolved, document the results and any changes you have made. If the problem still exists, continue with the next action plan.

Troubleshooting Flow for Layer 4 Problems (Cont.)

- When you have resolved the problem, document the resolution.



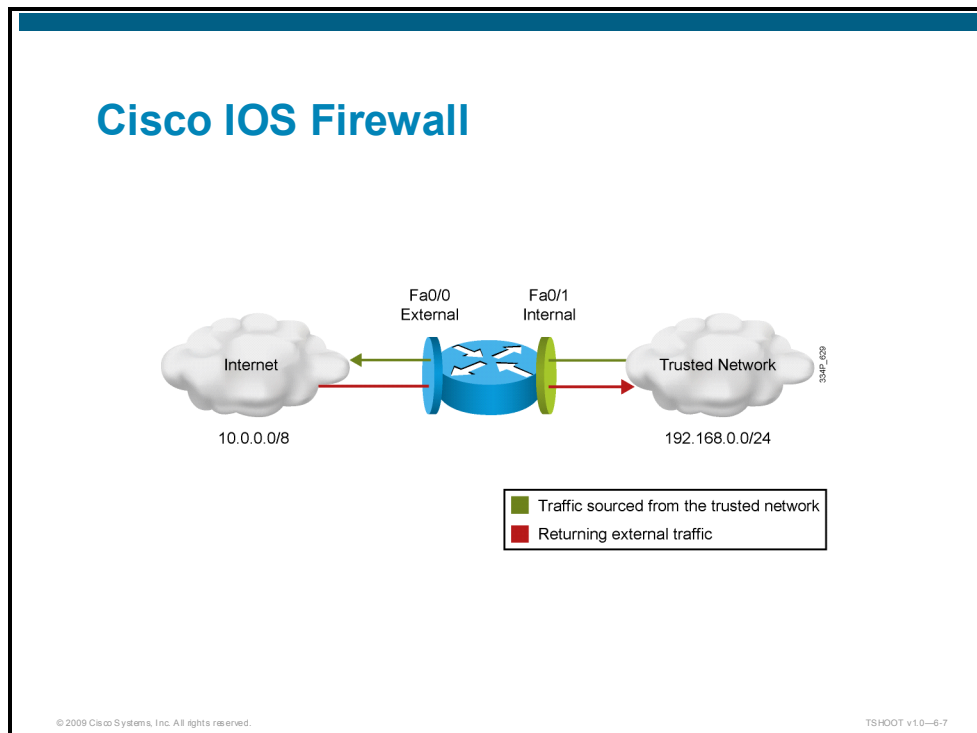
© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-6

When you have resolved the problem, an important final step remains: documenting the results and which action plan worked. Documenting of the fix will help in the future to solve similar problems that might arise.

Cisco IOS Firewall

This topic describes the capabilities and operation of the Cisco IOS Firewall.



The Cisco IOS Firewall software provides enhanced security functions for your Cisco IOS device. There are two types of Cisco IOS Firewall: Classic Cisco IOS Firewall and Zone-Based Policy Firewall.

Cisco IOS stateful packet inspection (formerly Context-Based Access Control) is a component of the Cisco IOS Firewall. Cisco IOS stateful packet inspection allows certain incoming flows by first inspecting and recording flows initiated from the trusted network. Cisco IOS stateful packet inspection is able to inspect all the way to the application layer, taking into consideration the characteristics of a flow on a per-protocol basis (context). Cisco IOS stateful packet inspection offers interface-based stateful inspection. The combination of the inspection policy and the access list based policy defines the overall firewall policy.

Look at the simple scenario shown in the figure: a router with two interfaces (one internal and one external) placed between two networks, one trusted (internal) and one untrusted (external). Your goal is to protect the trusted network from the untrusted network. You can see that there are four logical points at which the router can inspect traffic:

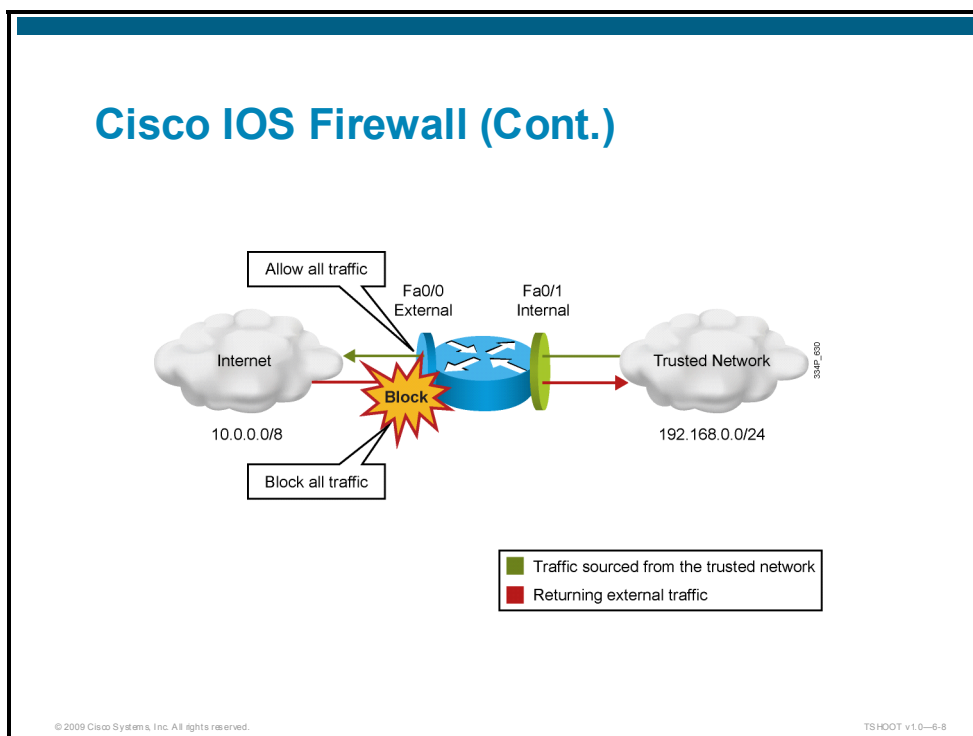
- Inbound on the internal interface
- Outbound on the external interface
- Inbound on the external interface
- Outbound on the internal interface

Cisco IOS stateful packet inspection is configured and operates per interface, dynamically modifying access list entries facing one direction based on the traffic it sees flowing in the opposite direction.

First, allow by default all traffic traversing the router from the internal LAN (192.168.0.0/24) to the Internet (10.0.0.0/8). You also want to deny by default all traffic flowing from the Internet toward the LAN. To do this, a simple access list to deny all IP traffic will be applied on the inbound direction of the external interface.

```
Router(config)# ip access-list extended DENY_ALL
Router(config-ext-nacl)# deny ip any any
Router(config-ext-nacl)# exit
Router(config)# interface f0/0
Router(config-if)# ip access-group DENY_ALL in
```

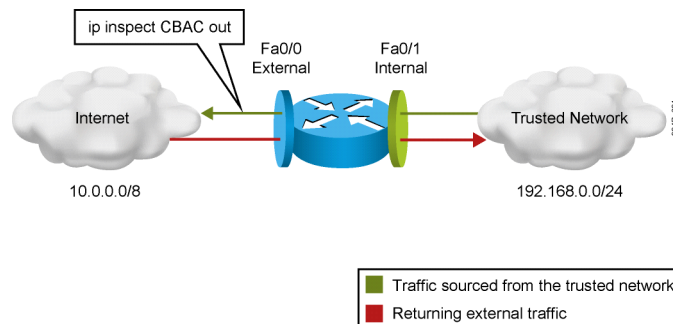
Note Implementation and verification of Cisco IOS Firewall is covered in more detail in the Implementing Cisco IOS Network Security (IINS) and Securing Networks with Cisco Routers (SNRS) courses.



Allow web access initiated from the internal network to return. Cisco IOS stateful packet inspection allows you to define an inspection rule for each protocol you want to monitor. In this case, you want to track HTTP sessions.

```
Router(config)# ip inspect name CBAC http
```

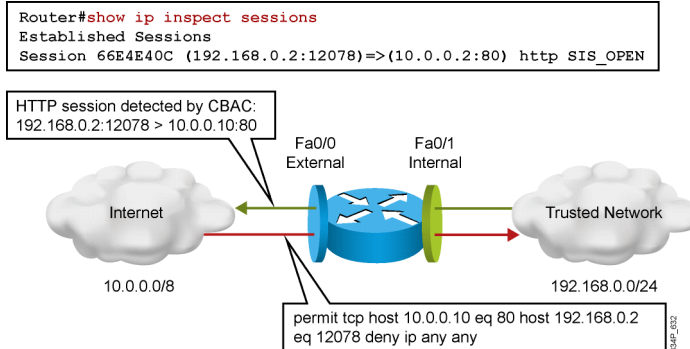
Cisco IOS Firewall (Cont.)



The inspection rule needs to be applied on the interface in a particular direction. The direction is outbound on the external interface because the router inspects traffic originating from the trusted network and dynamically adjusts the ACL restricting traffic inbound on the external interface.

```
Router(config)# interface f0/0
Router(config-if)# ip inspect CBAC out
```

Cisco IOS Firewall (Cont.)



© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-10

Cisco IOS stateful packet inspection is enabled in one direction for HTTP traffic on this interface. Outbound traffic (going toward the Internet) is tracked in the state table by session, and the DENY_ALL extended ACL restricting inbound traffic is automatically modified to accommodate legitimate return traffic. From the output of the **show ip inspect sessions** command, you can see that the trusted host 192.168.0.2 has opened an HTTP connection to 10.0.0.2. Cisco IOS stateful packet inspection will continue to track this session until it is closed by either end or the configured idle timer is reached.

Cisco IOS Firewall Verification

- Use the **show ip inspect all** command to verify the Cisco IOS stateful packet inspection configuration:

```
Router#show ip inspect all
Session audit trail is enabled
Session alert is enabled
<... output omitted ...>
Inspection Rule Configuration
  Inspection name CBAC
    http alert is on audit-trail is on timeout 3600
    https alert is on audit-trail is on timeout 3600
Interface Configuration
  Interface FastEthernet0/0
    Inbound inspection rule is not set
    Outgoing inspection rule is CBAC
      http alert is on audit-trail is on timeout 3600
      https alert is on audit-trail is on timeout 3600
    Inbound access list is DENY_ALL
    Outgoing access list is not set
<... output omitted ...>
```

354P_003

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—6-11

To display Cisco IOS stateful packet inspection configuration and session information, use the **show ip inspect all** command in privileged EXEC mode. Cisco added ACL bypass functionality to allow a packet to avoid redundant ACL checks by allowing the firewall to permit the packet on the basis of existing inspection sessions instead of dynamic ACLs. Because input and output dynamic ACLs have been eliminated from the firewall configuration, the **show ip inspect session detail** command output no longer shows dynamic ACLs. Instead, the output displays the matching inspection session for each packet that is permitted through the firewall.

Cisco IOS Firewall Logging and Debugging

- When audit trails are enabled, syslog messages are generated for each stateful inspection session:

```
Router(config)# ip inspect audit-trail
Router(config)#
%FW-6-SESS_AUDIT_TRAIL_START: Start http session: initiator
(192.168.0.2:10032) -- responder (10.0.0.10:80)
```

334P_284

- Debugging stateful inspection using the **debug ip inspect** command yields more detailed information:

```
Router#debug ip inspect
object-creation INSPECT Object Creations debugging is on
Router#
CBAC* OBJ_CREATE: Pak 6621F7A0 sis 66E4E154 initiator_addr
(192.168.0.2:10032) responder_addr (10.0.0.10:80) initiator_alt_addr
(192.168.0.2:10032) responder_alt_addr (10.0.0.2:80)
CBAC OBJ_CREATE: sid 66E684B0 acl DENY_ALL Prot: tcp
Src 10.0.0.10 Port [80:80]
Dst 192.168.0.2 Port [10032:10032]
CBAC OBJ_CREATE: create host entry 66E568DC addr 10.0.0.10 bucket 8
(vrf 0:0) insp_cb 0x66B61C0C
```

334P_305

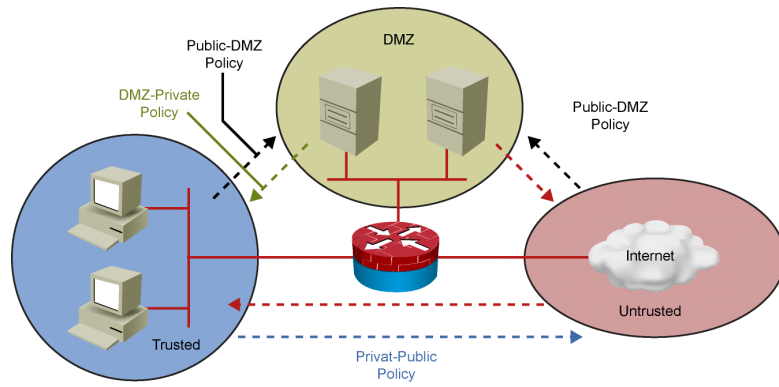
© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-12

Audit trails can be enabled to generate syslog messages for each stateful inspection session creation and deletion. Also, debugging stateful inspection can be used to observe object creation.

Zone-Based Policy Firewall

- Allows grouping of physical and virtual interfaces.
- Firewall policies are applied to traffic traversing zones.
- Simpler to add or remove interfaces and integrate them into the firewall policy.



© 2009 Cisco Systems, Inc. All rights reserved.

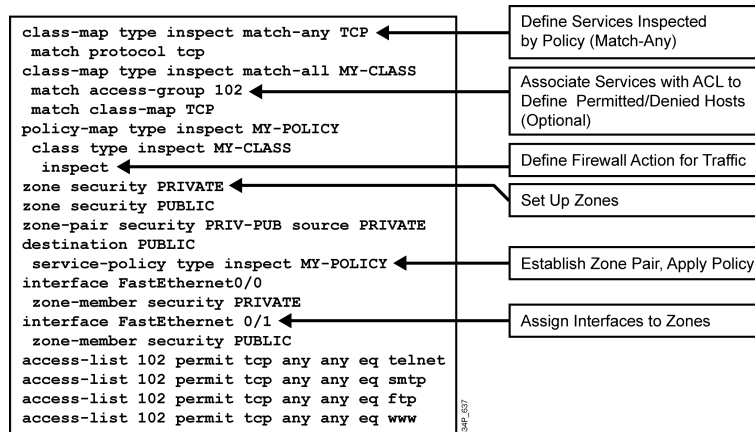
TSHOOT v1.0—6-13

The newer Zone-Based Policy Firewall offers easy-to-understand configuration model. Firewall policies are configured on traffic moving between zones. Zone-Based Policy Firewall simplifies firewall policy troubleshooting by applying explicit policy on interzone traffic. Firewall policy configuration is very flexible. Varying policies can be applied to different host groups, based on ACL configuration.

Zone-Based Policy Firewall supports the following functionalities:

- Stateful inspection
- Application inspection: IM, Post Office Protocol (POP), Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol/Extended Simple Mail Transfer Protocol (SMTP/ESMTP), HTTP
- URL filtering
- Per-policy parameter
- Transparent firewall
- Virtual routing and forwarding (VRF)-aware firewall

Zone-Based Policy Firewall Configuration Example



The figure shows a simple Zone-Based Policy Firewall configuration. First, the inspect class map MY-CLASS is defined, and match all TCP-based traffic as defined by access list 102 (Telnet, SMTP, FTP, and HTTP). Next, the policy map MY-POLICY defines which action to perform on the traffic matching the class map MY-CLASS. In the figure, the action is to inspect the traffic to create dynamic inspection objects. Before you can apply this policy to the traffic, you need to define security zones. A corresponding zone-pair is then created to represent the direction of the traffic to which the policy will be applied. Finally, the zones need to be assigned to the appropriate interfaces. In this example, there are two zones: PRIVATE and PUBLIC. Interface FastEthernet 0/0 is in zone PRIVATE and interface FastEthernet 0/1 is in zone PUBLIC. Zone pair PRIV-PUB states that all traffic sourced from zone PRIVATE and destined for zone PUBLIC will be processed according to policy map MY-POLICY.

Zone-Based Policy Firewall Logging and Debugging

- Troubleshooting tools for the zone-based firewall are similar to the tools used for classical Cisco IOS Firewall:
 - When audit trails are enabled, syslog messages are generated for each stateful inspection session.
 - Debugging can be used to obtain more detailed information.

```
May 31 18:02:34.739 UTC: %FW-6-SESS_AUDIT_TRAIL_START: (target:class)-  
publicPrivateOut:myClassMap):Start http session: initiator (10.1.1.100:3372)  
-- responder (172.16.1.100:80)  
May 31 18:02:34.907 UTC: %APFW-4-HTTP_JAVA_APPLET: HTTP Java Applet  
detected - resetting session 172.16.1.100:80 10.1.1.100:3372 on zone-pair  
publicPrivateOut class myClassMap appl-class HttpAic  
May 31 18:02:34.919 UTC: %FW-6-SESS_AUDIT_TRAIL: (target:class)-  
(publicPrivateOut:myClassMap):Stop http session: initiator  
(10.1.1.100:3372) sent 297 bytes -- responder (172.16.1.100:80) sent 0 bytes
```

354P-209

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--6-15

Syslog is the most effective troubleshooting tool available for Zone-Based Policy Firewall. It captures alert, audit trail, and debug command output.

For example, a user complains that he is unable to browse to a web server with 172.16.1.100. An administrator searches the syslog for the string 172.16.1.100. From the search results, it was realized that a Java Applet reset option was configured to the web server. The class-map is “myClassMap” and AIC policy “HttpAic.” The fix is to allow the embedded Java applet to the server in the HTTP AIC policy (HttpAic).

Zone-Based Policy Firewall Verification

- To display zones and member interfaces, use the **show zone security** command.
- To display zone pairs and their configuration, use the **show zone-pair** command:

```
Router#show zone-pair security source PRIVATE destination PUBLIC
Zone-pair name PRIV-PUB
Source-Zone PRIVATE Destination-Zone PUBLIC
service-policy MY-POLICY
```

33ap_038

- To display policy statistics and sessions, use the **show policy-map type inspect** command.

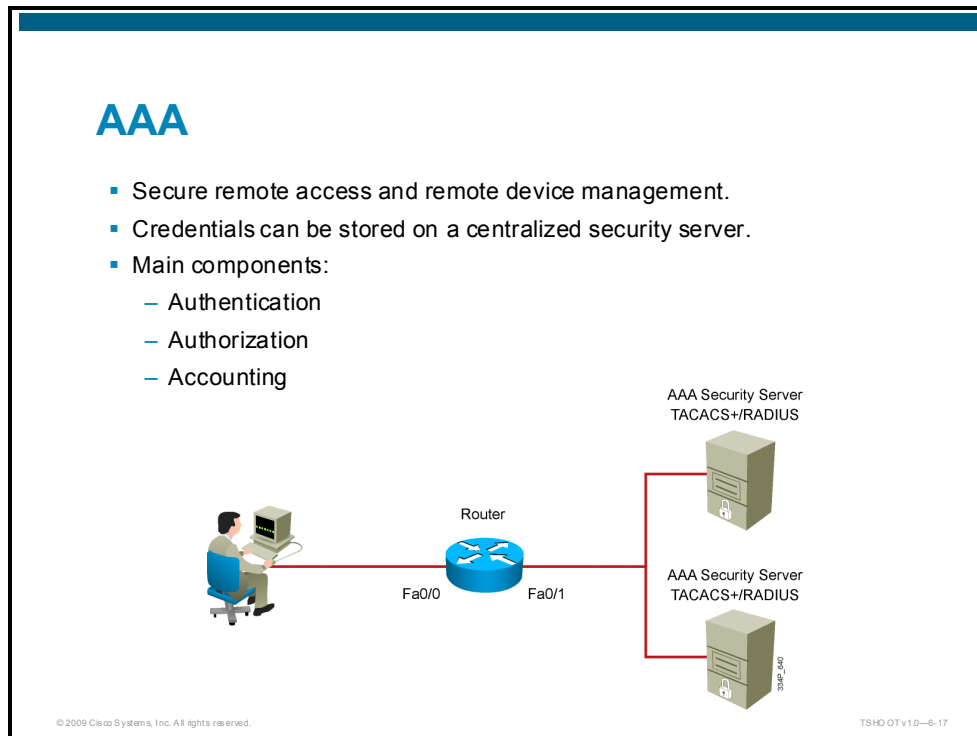
© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-16

The figure shows some useful Zone-Based Policy Firewall **show** commands. The **show zone security** command displays information for all zones configured on the router and the corresponding member interfaces. With this command, you can verify the configuration and assignment of zones. The **show zone-pair security** command provides important information about how zones are combined, the direction of the traffic, and the policy applied on the traffic. The **show policy-map type inspect** command shows the relevant information for the policy, and what traffic is matched in which class.

Authentication, Authorization, and Accounting

This topic describes the operation of the AAA framework and how to diagnose and solve device access problems caused by AAA.



AAA is a major part in the overall network security of the organization. AAA is the basis for providing secure remote access to the network and remote management of network devices. Network devices can use a centralized security server containing all the security policies that define the list of users and what they are allowed to do. AAA has three main components:

- Authentication
- Authorization
- Accounting

Authentication

- Use **debug aaa authentication** to troubleshoot authentication
- The following log displays a successful login to the router:

```
Router#debug aaa authentication
13:21:20: AAA/AUTHEN: create_user user='' ruser='' port='tty6'
rem_addr='10.0.0.32' authn_type=1 service=1 priv=1
13:21:20: AAA/AUTHEN/START (0): port='tty6' list=''
action=LOGIN service=LOGIN
13:21:20: AAA/AUTHEN/START (0): using "default" list
13:21:20: AAA/AUTHEN/START (70215483): Method=TACACS+
13:21:20: TAC+ (70215483): received authen response status = GETUSER
13:21:20: AAA/AUTHEN (70215483): status = GETUSER
13:21:23: AAA/AUTHEN/CONT (70215483): continue_login
13:21:23: AAA/AUTHEN (70215483): status = GETUSER
13:21:23: AAA/AUTHEN (70215483): Method=TACACS+
13:21:23: TAC+: send AUTHEN/CONT packet
13:21:23: TAC+ (70215483): received authen response status = GETPASS
13:21:23: AAA/AUTHEN (70215483): status = GETPASS
13:21:27: AAA/AUTHEN/CONT (70215483): continue_login
13:21:27: AAA/AUTHEN (70215483): status = GETPASS
13:21:27: AAA/AUTHEN (70215483): Method=TACACS+
13:21:27: TAC+: send AUTHEN/CONT packet
13:21:27: TAC+ (70215483): received authen response status = PASS
13:21:27: AAA/AUTHEN (70215483): status = PASS
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-18

Authentication provides a method for identifying users based on credentials such as a user name and password. Only after the identity of the user has been verified is access to network devices or network services granted. AAA authentication on routers and switches is configured by defining a named list of authentication methods to be used for a specific service, such as logging in to the device or connecting to an interface using PPP. The list determines which types of authentication will be used and the sequence in which the different authentication methods will be tried. If a default authentication method is defined for a particular service, this method will be used for all authentications of that type of service. The default list can be overruled by specifying an alternative named method list, which should then be specifically assigned to a line (for logins) or interface (for network-based authentication).

The output of the **debug aaa authentication** command can be very useful to troubleshoot AAA authentication problems.

The example in the figure shows the following events:

1. A remote user coming from IP address 10.0.0.32 attempts to log in to the router.
2. The router checks to see if AAA authentication for the “LOGIN” service is enabled, which is the case.
3. The router sees that the default method list is used, and the first method defined by the method list is TACACS+.
4. The authentication process now prompts the user for a user name and password and sends these credentials to the TACACS+ server for verification. The TACACS+ server checks the credentials against its database and responds with a successful authentication.

Note In the example in the figure the **debug tacacs** command has also been enabled to show the responses from the TACACS+ server. The lines in the output that are preceded by **AAA** are generated by the **debug aaa authentication** command, while the lines preceded by **TAC+** are originated by the **debug tacacs** command.

Authorization

- Use **debug aaa authorization** to troubleshoot authorization
- The following log displays a failed attempt by a user to initiate a Cisco IOS EXEC command shell:
 - After authentication the user admin1 attempts to initiate a shell.
 - The authorization method lists defines that TACACS+ is to be used to authorize EXEC shell access.
 - The authorization attempt is denied by the TACACS+ server.

```
Router#debug aaa authorization
2:23:21: AAA/AUTHOR (0): user='admin1'
2:23:21: AAA/AUTHOR (0): send AV service=shell
2:23:21: AAA/AUTHOR (0): send AV cmd*
2:23:21: AAA/AUTHOR (342885561): Method=TACACS+
2:23:21: AAA/AUTHOR/TAC+ (342885561): user=admin1
2:23:21: AAA/AUTHOR/TAC+ (342885561): send AV service=shell
2:23:21: AAA/AUTHOR/TAC+ (342885561): send AV cmd*
2:23:21: AAA/AUTHOR (342885561): Post authorization status = FAIL
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--6-19

Authorization determines what resources the user has access to on the router. In other words, AAA authorization assembles a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database can be located locally on the device or it can be hosted remotely on a RADIUS or TACACS+ security server. As with authentication, you configure AAA authorization by defining a named list of authorization methods, and then applying that list to various interfaces.

Debug AAA authorization output can be very useful to troubleshoot AAA authorization:

1. The user is attempting to do something that requires authorization (in our example, the user attempts to gain an EXEC shell).
2. The cmd parameter specifies a command that the user is trying to execute. If it lists *, this refers to plain EXEC access.
3. The method used to authorize this access is TACACS+.
4. The router sends the necessary information through TACACS+ to the security server.
5. The security server verifies the authorization, determines that the user is not authorized to perform this function, and sends back a FAIL message.

Accounting

- Use **debug aaa accounting** to troubleshoot accounting
- The following log displays an accounting record being sent for the creation of a Cisco IOS EXEC shell:
 - The default method was used.
 - An EXEC shell was successfully started for the user.

```
Router#debug aaa accounting
May 10 14:48:33.011: AAA/ACCT/EXEC(00000005): Pick method list 'default'
May 10 14:48:33.011: AAA/ACCT/SETMLIST(00000005): Handle 0, mlist 81CA79CC,
Name default
May 10 14:48:33.011: Getting session id for EXEC(00000005): db=82099258
May 10 14:48:33.011: AAA/ACCT/EXEC(00000005): add, count 2
May 10 14:48:33.011: AAA/ACCT/EVENT/(00000005): EXEC UP
```

336P_042

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-20

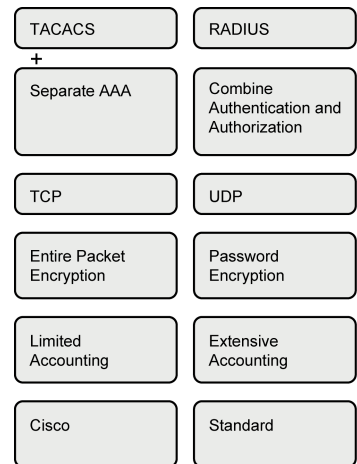
Accounting provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes. When AAA accounting is activated, the network access server reports user activity to the RADIUS or TACACS+ security server in the form of accounting records. This data can then be analyzed for network management, client billing, and/or auditing. All accounting methods must be defined through AAA. As with authentication and authorization, you configure AAA accounting by defining a named list of accounting methods, and then applying that list to various interfaces.

Debug AAA accounting output can be very useful to troubleshoot AAA accounting.

In this example, the default method was used, and you can see that a user successfully gained access to the router's EXEC shell.

TACACS+ and RADIUS

- **Functionality:** TACACS+ separates the three AAA functions. RADIUS combines authentication and authorization and separates accounting.
- **Transport protocol:** TACACS+ uses TCP. RADIUS uses UDP.
- **Confidentiality:** TACACS+ encrypts full packets. RADIUS encrypts only the password.
- **Accounting:** RADIUS accounting records can contain more information than TACACS+ accounting records.
- **Customization:** TACACS+ is more flexible and provides better per-user customization.
- **Standardization:** RADIUS is based on an open standard.



© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--6-21

TACACS+ and RADIUS are commonly used protocols to forward certain information from network device to a centralized security server. These are some of their characteristics:

- RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization.
- TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting.
- RADIUS uses User Datagram Protocol (UDP), while TACACS+ uses TCP. TCP offers several advantages over UDP. TCP offers a connection-oriented transport, while UDP offers best-effort delivery.
- RADIUS encrypts only the password in the access-request packet, from the client to the server. The remainder of the packet is unencrypted. Other information, such as username, authorized services, and accounting, can be captured by a third party.
- TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header. Within the header is a field that indicates whether the body is encrypted or not. For debugging purposes, it is useful to have the body of the packets unencrypted. However, during normal operation, the body of the packet is fully encrypted for more secure communications.
- RADIUS does not allow users to control which commands can be executed on a router and which cannot. Therefore, RADIUS is not as useful for router management or as flexible for terminal services.
- TACACS+ provides two methods to control the authorization of router commands on a per-user or per-group basis. The first method is to assign privilege levels to commands and have the router verify with the TACACS+ server whether the user is authorized at the specified privilege level. The second method is to explicitly specify in the TACACS+ server, on a per-user or per-group basis, the commands that are allowed.
- RADIUS is based on an open standard (RFC 2865), while TACACS+ was developed by Cisco Systems.

Common TACACS+ Failures

- The TACACS+ server is down or the device has no connectivity to the server:

```
TAC+: TCP/IP open to 171.68.118.101/49 failed -  
Connection refused by remote host  
AAA/AUTHEN (2546660185): status = ERROR  
AAA/AUTHEN/START (2546660185): Method=LOCAL  
AAA/AUTHEN (2546660185): status = FAIL  
Asl CHAP: Unable to validate Response. Username chapuser: Authentication failure
```

- The key on the device and TACACS+ server do not match:

```
TAC+: received bad AUTHEN packet: length = 68, expected 67857  
TAC+: Invalid AUTHEN/START packet (check keys)  
AAA/AUTHEN (1771887965): status = ERROR
```

- Bad user name, bad password, or both:

```
AAA/AUTHEN: free_user (0x170940) user='chapuser' ruser=''  
port='Async1' rem_addr='async' authn_type=CHAP service=PPP priv=1  
TAC+: Closing TCP/IP 0x16EF4C connection to 171.68.118.101/49  
AAA/AUTHEN (2082151566): status = FAIL  
Asl CHAP: Unable to validate Response. Username papuser: Authentication failure
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-22

The example in the figure demonstrates symptoms of problems commonly experienced with TACACS+.

One common problem is loss of connectivity between the network device and the TACACS+ server. If the TACACS+ server is down or has no connectivity, the network device produces an error because the user is not in the local database, and failover to the local database fails. For this reason, configure the network device to use the local database in a pinch.

The other problem can be the misconfiguration of the key on the network device and TACACS+ server. Both keys should be the same to allow communication between network devices and the TACACS+ server. In other cases, the information cannot be decrypted and processed.

The last line of output demonstrates a wrong username, password, or both.

Note In the example in the figure, both the **debug tacacs** and the **debug aaa authentication** commands have been enabled. The lines in the output that are preceded by AAA are generated by the **debug aaa authentication** command, while the lines preceded by TAC+ are originated by the **debug tacacs** command.

Common RADIUS Failures

- The RADIUS server is down or the device has no connectivity to the server:

```
As1 CHAP: I RESPONSE id 12 len 28 from "chapadd"
RADIUS: id 15, requester hung up.
RADIUS: No response for id 15
RADIUS: No response from server
AAA/AUTHEN (1866705040): status = ERROR
AAA/AUTHEN/START (1866705040): Method=LOCAL
AAA/AUTHEN (1866705040): status = FAIL
As1 CHAP: Unable to validate Response. Username chapadd: Authentication failure
As1 CHAP: O FAILURE id 12 len 26 msg is "Authentication failure"
```

- The key on the device and RADIUS server do not match:

```
RADIUS: Received from id 21 171.68.118.101:1645, Access-Reject, len 20
RADIUS: Reply for 21 fails decrypt
NT client sends 'DOMAIN\user' and Radius server expects 'user':
RADIUS: Received from id 16 171.68.118.101:1645, Access-Reject, len 20
AAA/AUTHEN (2974782384): status = FAIL
As1 CHAP: Unable to validate Response. Username CISCO\chapadd: Authentication failure
As1 CHAP: O FAILURE id 13 len 26 msg is "Authentication failure"
```

SNAP-246

© 2009 Cisco Systems, Inc. All rights reserved.

TSO-OT v1.0-6-23

The example in the figure demonstrates symptoms of problems commonly experienced with RADIUS.

One common problem is loss of connectivity between a network device and the RADIUS server. If the RADIUS server is down or has no connectivity, the network device produces an error because the user is not in the local database, and failover to local database fails. For this reason, configure the network device to use a local database in a pinch.

Another problem can be the misconfiguration of the key on the network device and RADIUS server. Both keys should be the same to allow communication between the network device and the RADIUS server. In other cases, the information cannot be decrypted and processed.

Common RADIUS Failures (Cont.)

- Username and password are correct but authorization failed:

```
RADIUS: Received from id 19 171.68.118.101:1645, Access-Accept, len 20
RADIUS: no appropriate authorization type for user.
AAA/AUTHOR (2370106832): Post authorization status = FAIL
AAA/AUTHOR/LCP As1: Denied
```

- Bad user name, bad password, or both:

```
RADIUS: Received from id 17 171.68.118.101:1645, Access-Reject, len 20
AAA/AUTHEN (3898168391): status = FAIL
As1 CHAP: Unable to validate Response. Username ddunlap: Authentication failure
As1 CHAP: O FAILURE id 14 len 26 msg is "Authentication failure"
As1 PPP: Phase is TERMINATING
```

6000_0000

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-24

If a user is trying to get service for which is not authorized, you will get an “authorization status failed” message in the log. Be sure that this is not a configuration mistake in the RADIUS server.

The second output example demonstrates a wrong username, password, or both.

Cisco Secure Access Control Server



Cisco Secure Access Control Server (ACS) offers centralized command and control for all user authentication, authorization, and accounting from a web-based, graphical interface.

Under the Reports and Activity button, Cisco Secure ACS provides a mechanism to troubleshoot AAA-related problems.

Accounting Reports: The accounting reports contain a record of all successful authentications during the period covered by the report. Information captured includes time, date, username, type of connection, amount of time logged in, and bytes transferred.

Administration Reports: This report contains all TACACS+ commands requested during the period covered by the report. This is typically used when Cisco Secure ACS is being used to manage access to routers.

Passed Authentications: This report lists successful authentications during the period covered by the report.

Failed Attempts: This report contains a record of all unsuccessful authentications during the period covered by the report for both TACACS+ and RADIUS. The reports capture the username attempted, time, date, and cause of failure.

Logged-In Users: This report shows all users currently logged in, grouped by AAA client.

Disabled Accounts: This list contains accounts that have been disabled. They might have been manually disabled or disabled automatically based on the aging information defined under User Setup.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- You have learned how to diagnose and resolve transport layer problems in a structured manner.
- You have reviewed the operational principles of the Cisco IOS Firewall and how to gather information about its state for troubleshooting purposes.
- You have reviewed the operation of the AAA framework, which can be used on routers and switches to grant access rights based on credentials stored in a central security server, such as the Cisco Secure ACS.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-26

Lab 6-2 Debrief

Overview

In this lab, you practiced troubleshooting problems related to specialized security features available in the Cisco IOS Software, such as DHCP snooping, Cisco IOS Firewall, VLAN access maps, port security, secure shell (SSH), and spanning-tree protection features. In addition, you have practiced recovering from a lost password and authentication failures. You have created a troubleshooting plan to coordinate the work between the team members. You have methodically researched the problems, kept a log of your actions and findings, and resolved the problems and documented your solutions.

During the lab debrief, the instructor will lead a group discussion during which you can present your solutions. You will get an opportunity to verify your solution against a number of checkpoints provided by the instructor and compare your solution to other students' solutions. The instructor will discuss alternate solutions and their advantages and disadvantages.

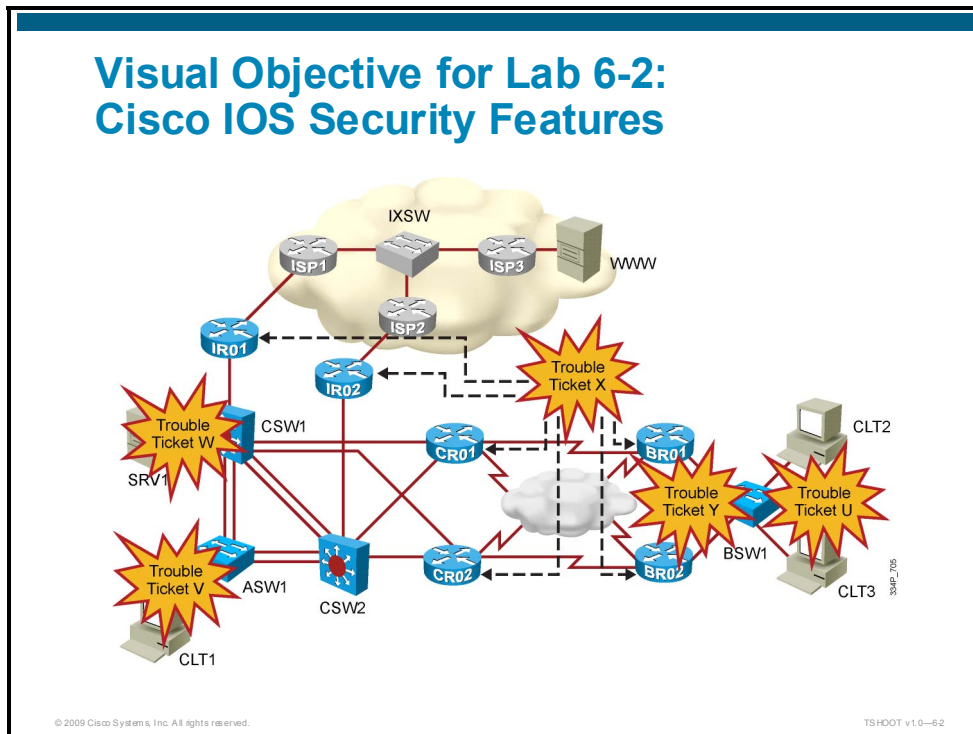
Objectives

Upon completing this lesson, you will be able to diagnose and resolve problems related to access lists and authentication using a structured, methodical approach. This ability includes being able to meet these objectives:

- Compare your solution, findings, and action log against a set of checkpoints provided by the instructor and identify common and alternate solutions
- Consolidate the lessons learned during the review discussions into a set of best-practice methods and commands to aid you in future troubleshooting procedures

Review and Verification

This topic describes the problems that were introduced in Lab 6-2, asks how you can verify that you have solved the problems, and provides an example of a troubleshooting process that will allow you to find and resolve the issues.



This lab consists of five trouble tickets: Trouble Ticket U is concerned with client PCs CLT2 and CLT3 at the branch, which have lost all network connectivity and cannot even obtain an IP address. Trouble Ticket V involves the connectivity from client PC CLT1, which suffers from a similar issue. Trouble Ticket W involves server SRV1, which cannot be reached from any point in the network. Trouble Ticket X involves Secure Shell (SSH) connectivity to the routers and switches. Finally, Trouble Ticket Y involves a macro that is used to enable several security features on the ports of switch BSW1.

The introduction to the trouble ticket states that several new security measures have been implemented. It further states that you are allowed to roll back the implementation of these features if necessary, but you need to provide an analysis to support your decision to roll back.

Planning Troubleshooting

How did your team approach the five trouble tickets?

- Did you troubleshoot all tickets in parallel, in sequence, or did you use a combination of methods?
- How did you decide on the order that you chose to address the tickets in?
- How did you coordinate device access between your team members?
- How did you communicate with your team members?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-63

Note This lesson provides sample answers and solutions to the questions posed during the debrief discussions. Keep in mind that alternate solutions and methods might be just as valid and that the solutions provided here only highlight a sample approach and solution.

When you assess the urgency of the tickets, Trouble Ticket W is probably the most important, because many different users are dependent on the availability of server SRV1. Because this server is the Domain Name System (DNS) server for the network, it affects network connectivity throughout the network. Trouble Tickets U and V are equally important, given that it is likely that these issues affect all users on these VLANs and not only the PCs used for testing. The SSH problem reported in Trouble Ticket X also has an operational effect, because it affects the capability to manage the routers and switches remotely without using out-of-band management access. Trouble Ticket Y is the least important, because it revolves around a testing scenario, which does not need to be resolved at this time, but can be tackled later.

Therefore, a straightforward approach would be to work on Trouble Tickets W, U, and V first and then move on to Trouble Tickets X and Y. However, depending on the size of your team, you might elect to simply distribute the tickets over the different team members and start working on all the issues in parallel. This is a viable approach, because it seems that the problems are not related and can be tackled independently.

Based on this, a possible work plan for a team consisting of four members would be the following:

- Team member 1 will focus on Trouble Ticket U. This team member will primarily control switch BSW1 and routers BRO1 and BRO2. This team member will continue to work on Trouble Ticket Y after Trouble Ticket U has been resolved.
- Team member 2 will focus on Trouble Ticket V. This team member will control switches ASW1 and CSW2. Possible changes on switch CSW1 will be coordinated with team member 3.

- Team member 3 will focus on Trouble Ticket W. This team member will control switch CSW1. Possible changes on switches ASW1 and CSW2 will be coordinated with team member 4.
- Team member 4 will focus on Trouble Ticket X. Initially this team member will focus troubleshooting on routers CRO1, CRO2, IRO1, and IRO2 in order not to disturb the process of the other team members. After the problem has been diagnosed and resolved on these routers, this team member will coordinate necessary changes on the other devices with the controlling team members.

To reflect the priority of the tickets, this lesson will cover Trouble Ticket W first, followed by Trouble Tickets U, V, X, and Y.

Trouble Ticket W: No Connectivity to Server SRV1

The text introducing this trouble ticket was the following:

It looks like your team will have a lot of work to do this afternoon. The next report that you receive involves server SRV1. Your colleague reports that he cannot reach server SRV1 from any of the switches or routers. Because this server is the DNS server for your network, this implies that you will not be able to connect to any network device by name until this problem is resolved.

You remember that the network interface card (NIC) of this server has been replaced just a week ago and you wonder if this has anything to do with this problem.

Your task is to restore network connectivity to server SRV1 (within the constraints laid down in the security policy). If you do not succeed in resolving the problem, you are allowed to roll back any newly implemented features as necessary. However, the security features that were implemented during earlier security implementations should not be removed.

Trouble Ticket W: Review and Discuss

How did your team approach Trouble Ticket U?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you accomplish the goal of restoring network connectivity to server SRV1?
- How did you verify that you accomplished your goal?
- Did you roll back any of the implemented features and if so, why?
- Does your solution comply with the security policy?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-64

The problem in this ticket is caused by a misconfigured secure MAC address for the port security feature that has been enabled on switch CSW1.

Although there are many possible methods that you could use to solve this problem, the following list provides an example of a troubleshooting log to show you a methodical approach to resolve this problem.

Trouble Ticket	Actions and results
Ticket W	CSW1: Verified problem: Cannot ping to server SRV1 (10.1.152.1).
	CSW1: Verified interface status for interface Fa 0/10: Port is in error-disabled state.
	CLT1: Ping to default gateway (10.1.128.126) succeeds. Ping to www.isp3.local succeeds.
	CSW1: Check security features enabled on the port: Port security has been enabled limiting the number of addresses to one and listing a specific MAC address.
	SRV1: Verify MAC address of the server: This is different from the configured secure MAC address.
	CSW1: Configuration changed: Changed secure MAC address to the actual MAC address of server SRV1. Shut down and re-enabled the port to clear the error-disabled state. Both prechange and postchange configurations were saved in flash on the device. Communicated this information to team members.
	CSW1: Ping to server SRV1 now succeeds.
	BSW1 & IRO1: Ping to server SRV1 succeeds: Server SRV1 is reachable from various points in the network. Assume problem has been solved unless new problems are reported.
	Problem fixed. Documented changes. Backed up configurations. Communicated to team members. Closed ticket.

Key Clue: Port in Error-Disabled State

- Given that server SRV1 is not reachable from any point in the network, checking the switch port that connects to server SRV1 is an obvious first step.
- This reveals that the port is in error-disabled state:

```
CSW1#show interface FastEthernet 0/10 status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/10	FE to SRV1	err-disabled	112	auto	auto	10/100BaseTX

- Verifying the log shows that the port was disabled by the port security feature because of reception of a wrong MAC address:

```
CSW1#show logging | include SECURITY
```

```
*Feb 28 16:00:32 PST: %PORT_SECURITY-2-PSECURE VIOLATION: Security violation occurred, caused by MAC address 0050.5684.22e6 on port FastEthernet0/10.
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6.6

Because the problem report states that server SRV1 is not reachable from any point on the network, it makes sense to start with a bottom-up approach and verify whether the port that connects the server is up. A quick check of the port status on switch CSW1 reveals that the port is in the error-disabled state. At this point, you could check the logs to see what caused the port to be disabled. This reveals that the port security feature disabled the port, because a wrong MAC address was received on the port. Checking the configuration at this point reveals a mismatch between the configured secure address and the actual MAC address of server SRV1.

Trouble Ticket W Checkpoints

Minimum checkpoints to prove that you have resolved this trouble ticket:

- You can ping server SRV1 from all routers and switches.
- Client PCs CLT1 and CLT2 can access the shared folder [\\SRV1\\Public](#) on server SRV1.
- You have documented your process, your solution, and any changes that you have made to the device configurations.

What else should you have checked?

Are there any unresolved issues?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-66

The figure shows a list of minimum requirements that should be met to consider this trouble ticket to be resolved.

To check the second item, Trouble Tickets U and V need to be resolved first, because this requires client PCs CLT1 and CLT2 to have network connectivity. However, given the fact that you can reach the server from all network devices, it is reasonable to expect that this will work when general network connectivity for client PCs CLT1 and CLT2 has been restored.

Suggested Solution

Correcting the configurations of switch CSW1 as follows can restore the connectivity to server SRV1.

Suggested Configuration Changes

- On switch CSW1, change the secured MAC address on port FastEthernet 0/10 to the actual MAC address of server SRV1:

```
CSW1(config)#interface FastEthernet 0/10
CSW1(config-if)# shutdown
CSW1(config-if)# no switchport port-security mac-address 0000.0cc0.fee
CSW1(config-if)# switchport port-security mac-address 0050.5684.22e6
CSW1(config-if)# no shutdown
```

Note: The actual MAC address will be different for each pod. The MAC address listed here is just an example.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-67

If you did not configure the actual MAC address of server SRV1 as a secured address, but only removed the existing secure MAC address, this is also considered a valid solution. The security policy is not specific enough to know whether configuring an explicit MAC address on the port is required.

Trouble Ticket U: No Connectivity from Client PCs CLT2 and CLT3

The text introducing this trouble ticket was the following:

The first report that you receive is that both client PCs CLT2 and CLT3 have no network connectivity at all. According to your colleague, the PCs cannot even obtain an IP address.

Your task is to diagnose this problem and restore any connectivity that the users on these PCs are entitled to according to the security policy. Ensure that no other traffic is allowed other than the traffic specifically permitted by the security policy. If you do not succeed in resolving the problem, you are allowed to roll back any newly implemented security features as necessary. However, the security features that were implemented during earlier security implementations should not be removed.

Trouble Ticket U: Review and Discuss

How did your team approach Trouble Ticket U?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you accomplish the goal of restoring network connectivity for client PCs CLT2 and CLT3?
- How did you verify that you accomplished your goal?
- Did you roll back any of the implemented features and if so, why?
- Does your solution comply with the security policy?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-68

This problem actually consists of two separate issues. Although the symptoms are related and both client PCs CLT2 and CLT3 cannot obtain an IP address, the root cause is different. The reason that client PC CLT2 cannot obtain an IP address is that DHCP snooping has been configured for VLAN 17 on switch BSW1, but the uplink ports that lead to the DHCP server have not been configured as trusted ports. The reason that client PC CLT3 cannot obtain an IP address is that the DHCP broadcasts are blocked by a VLAN access map that was configured for VLAN 19 on switch BSW1.

After you resolve the DHCP issues and test the connectivity to the Internet, you will run into another issue. The Cisco IOS firewall configuration on routers IRO1 and IRO2 is incorrect. The **ip inspect** statement is applied in the wrong direction and TCP has not been included in the list of inspected protocols. This prevents return traffic from the Internet from entering the network.

Although there are many possible methods that you could use to solve these issues, the following example of a troubleshooting log shows you a methodical approach to resolve these issues.

Trouble Ticket	Actions and results
Ticket U	CLT2: Verified problem: PC cannot obtain an IP address via DHCP.
	BSW1: Verify link status: The port interface that connects to client PC CLT2 is up.
	Check security implementation: "Protection from rogue DHCP servers" has been implemented.
	BSW1: DHCP snooping has been implemented for VLAN 17.
	BSW1: Configuration changed temporarily: Disabled DHCP snooping for VLAN 17 for testing purposes. Prechange configuration was saved in flash on the device.
	CLT2: Client can now obtain an IP address.
	BSW1: Configuration changed: Re-enabled DHCP snooping for VLAN 17.
	CLT2: Attempt to release and renew the lease: PC cannot obtain an IP address. This confirms that the DHCP snooping feature causes the problem.
	Research DHCP snooping: Ports that lead to the DHCP server should be configured as trusted ports.
	BSW1: Configuration changed: Configured interfaces Fa 0/3 and Fa 0/4 as trusted ports for DHCP snooping. Both prechange and postchange configurations were saved in flash on the device. Communicated this information to team members.
	CLT2: Client can obtain an IP address again.
	CLT2: Opening the shared folder \\SRV1\Public succeeds. Browsing to http://www.isp3.local fails.
	CLT2: DNS resolution for www.isp3.local fails.
	CLT2: Ping to 172.34.224.1 fails. Traceroute to 172.34.224.1 leads to router IRO2 and then times out.
	Check security implementation: Stateful packet inspection has been enabled on routers IRO1 and IRO2.
	CLT2: Start continuous ping to 172.34.224.1.
	IRO2: show ip inspect sessions shows no active sessions.
	IRO2: Verify the Cisco IOS Firewall configuration: Inspection is enabled in the wrong direction (inbound instead of outbound).
	IRO2: Configuration changed: Changed direction for stateful inspection rule INTERNET-TRAFFIC on interface Fa 0/1 to outbound. Both prechange and postchange configurations were saved in flash on the device. Communicated this information to team members.
	IRO2: show ip inspect sessions shows an active ICMP session from client PC CLT2.
	CLT2: Ping to 172.34.224.1 succeeds. Ping to www.isp3.local succeeds.
	CLT2: Browsing to http://www.isp3.local fails.
	IRO2: show ip inspect sessions does not show a session for the HTTP session from client PC CLT2.
	IRO2: show ip nat translations reveals a translation entry for the HTTP session from client PC CLT2. This proves that the traffic is forwarded to router IRO2.
	IRO2: Verify the Cisco IOS firewall configuration: Only udp and icmp traffic is inspected.
	IRO2: Configuration changed: Added TCP to the list of inspected protocols. Both prechange and postchange configurations were saved in flash on the device. Communicated this information to team members.
	CLT2: Browsing to http://www.isp3.local succeeds.

Trouble Ticket	Actions and results
	IRO1: Check if router IRO1 was misconfigured in the same way: Configuration is identical.
	IRO1: Configuration changed: Changed direction for stateful inspection rule INTERNET-TRAFFIC on interface Fa 0/0 to outbound. Added TCP to the list of inspected protocols. Both prechange and postchange configurations were saved in flash on the device. Communicated this information to team members.
	Problem seems to be solved. Verify ticket: Similar problems were reported for client CLT3.
	CLT3: Verified problem: PC cannot obtain an IP address via DHCP.
	Check security implementation: "Added protection against worms by blocking specific TCP ports (starting with ports 25 and 135) and unnecessary broadcast and multicast traffic on all VLANs. The guest VLAN in the branch office (VLAN 19) will be implemented first as a pilot."
	BSW1: Verify configuration: VLAN access map is implemented for VLAN 19.
	BSW1: Configuration changed temporarily: Disabled VLAN filtering for VLAN 19 for testing purposes. Prechange configuration was saved in flash on the device.
	CLT3: Client can now obtain an IP address.
	BSW1: Configuration changed: Re-enabled VLAN filtering for VLAN 19.
	CLT3: Attempt to release and renew the lease: PC cannot obtain an IP address. This confirms that the VLAN filtering feature causes the problem.
	BSW1: Analyze VLAN access map: All broadcasts are dropped except broadcasts defined by the access list named NECESSARY-BROADCASTS. This access list only allows UDP port 3222.
	Hypothesis: DHCP needs to be added to the access list that permits the necessary broadcasts.
	BSW1: Configuration changed: Added UDP port 67 and 68 to the access list NECESSARY-BROADCASTS. Both prechange and postchange configurations were saved in flash on the device. Communicated this information to team members.
	CLT3: Client can obtain an IP address again.
	CLT3: Client can browse to http://www.isp3.local.
	Problem fixed. Documented changes. Backed up configurations. Communicated to team members. Closed ticket.

Suggested Troubleshooting Methods

- There are no key commands that yield obvious clues for this ticket.
- The problems in this ticket can be resolved by:
 - Reviewing the list of implemented security measures to find obvious candidates that could cause the problem.
 - Temporarily disabling a feature, such as DHCP snooping, to confirm that the feature is the cause of the problem.
 - Adding temporary access list lines to confirm that packets travel up to a particular point in the network.
 - Researching the syntax of the implemented features to find potential configuration errors.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6.9

There are no real primary commands that clearly show the underlying problem causes. However, like most networking problems, you can uncover the issues in this ticket by following a structured method. First, the scenario includes a list of implemented security features, which you can scan to see if any of these features might apply to the issue that you are facing.

For example, the line in the scenario that reads “Protection from rogue DHCP servers on all VLANs. The office VLAN in the branch office (VLAN 17) will be implemented first as a pilot” gives you a hint that the problem that client PC CLT2 cannot obtain an IP address through DHCP might be caused by this feature. When you have a suspicion that a certain feature could be causing the problem, you can temporarily disable it to confirm this hypothesis. Clearly, you need to consider whether such a temporary change is allowed under the security policy. In this case, you are dealing with a test scenario, and this is a valid method.

After you have determined that a particular feature is the cause of the problem and you are not familiar with that feature, you should spend some time researching the feature to see if you can spot the error. Many problems in new implementations are caused by misconfigurations, so reviewing known good examples and comparing these to the actual implementation is a suitable strategy. Alternatively, you might need to escalate the problem to a specialist.

Trouble Ticket U Checkpoints

Minimum checkpoints to prove that you have resolved this trouble ticket:

- Client PC CLT2 can obtain an IP address via DHCP.
- You have verified that client PC CLT2 can access all resources that it is entitled to by the security policy (but not more than that).
- Client PC CLT3 can obtain an IP address via DHCP.
- You have verified that client PC CLT3 can access all resources that it is entitled to by the security policy (but not more than that).
- You have documented your process, your solution, and any changes that you have made to the device configurations.

What else should you have checked?

Are there any unresolved issues?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOTv1.0—6-10

The figure shows a list of minimum requirements that should be met to consider this trouble ticket to be resolved.

The second and fourth items imply that you will need to validate the changes that you have made during the resolution of this ticket against the security policy.

Suggested Solution

Correcting the configurations of switch BSW1 and routers IRO1 and IRO2 as follows can restore the network connectivity from client PCs CLT2 and CLT3.

Suggested Configuration Changes

- On switch BSW1 trust the ports that lead to routers BRO1 and BRO2 for DHCP snooping:

```
BSW1(config-if-range)#interface range FastEthernet 0/3 - 4
BSW1(config-if-range)# ip dhcp snooping trust
```

- On switch BSW1 add DHCP to the access list that defines necessary broadcasts for VLAN 19:

```
BSW1(config)#ip access-list ext NECESSARY-BROADCASTS
BSW1(config-ext-nacl)#permit udp any any eq 67
BSW1(config-ext-nacl)#permit udp any any eq 68
```

- On routers IRO1 and IRO2 change the direction of the stateful inspection and add TCP to the list of inspected protocols:

```
IRO1(config)#ip inspect name INTERNET-TRAFFIC tcp
IRO1(config)#interface FastEthernet 0/0
IRO1(config-if)# no ip inspect INTERNET-TRAFFIC in
IRO1(config-if)# ip inspect INTERNET-TRAFFIC out
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-11

Changing the value of the exec timeout on router IRO1 to a shorter value than 60 minutes is valid as well. However, for the sake of consistency, you should then change the exec timeout to the same value on all other devices. Removing the exec timeout entirely is not considered to be a valid solution, because it decreases the security of the network.

The access list can be changed in various manners to achieve the same result. However, you need to ensure that the changes do not open up the possibility for clients that are members of the office VLAN at the branch (such as client PC CLT2) to access the Internet, which is explicitly forbidden by the security policy.

Also, it is important that the changes to the access list are made on both routers IRO1 and IRO2. The traffic from client PC CLT1 is routed via router IRO1, so making the change on router IRO1 only will actually resolve the issue for client PC CLT1. However, other clients that are routed via router IRO2 will experience similar problems if the access list is not changed in a similar manner on router IRO2.

Trouble Ticket V: No Connectivity from Client PC CLT1

The text introducing this trouble ticket was the following:

The second report you receive concerns client PC CLT1. This PC has also lost all network connectivity. This is remarkable because client PC CLT1 is not in any of the VLANs that the rogue DHCP and worm protection measures have been implemented on.

Your task is to diagnose this problem and restore any connectivity that the user on client PC CLT1 is entitled to according to the security policy. Ensure that no other traffic is allowed other than the traffic specifically permitted by the security policy. If you do not succeed in resolving the problem, you are allowed to roll back any newly implemented security features as necessary. However, the security features that were implemented during earlier security implementations should not be removed.

Trouble Ticket V: Review and Discuss

How did your team approach Trouble Ticket V?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you accomplish the goal of restoring network connectivity for client PC CLT1?
- How did you verify that you accomplished your goal?
- Did you roll back any of the implemented features and if so, why?
- Does your solution comply with the security policy?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-12

The problem in this ticket is caused by an underlying spanning-tree problem. Root guard has been configured on switches CSW1 and CSW2 for the Port-channel interfaces that lead to switch ASW1. However, on switch CSW1 it has also been enabled on interface Port-channel 10, which leads to switch CSW2. As a result, both Port-channel interfaces on switch CSW1 are put in the spanning-tree “broken” state for all VLANs that switch CSW2 is the root for. This effectively prevents all traffic for those VLANs from reaching switch CSW1. VLAN 17, which client PC CLT1 is a member of, is one of those VLANs and as a result, the DHCP requests from client PC CLT1 never reach switch CSW1, which is the DHCP server for VLAN 17. This causes DHCP to fail for VLAN 17.

Although there are many possible methods that you could use to solve this problem, the following example of a troubleshooting log shows you a methodical approach to resolve this problem.

Trouble Ticket	Actions and results
Ticket V	CLT1: Client PC cannot obtain an IP address through DHCP.
	Check security implementation: No specific features have been implemented for this VLAN.
	Check baseline: Switch CSW1 is the DHCP server for VLAN 17.
	ASW1: The MAC address of client PC CLT1 is learned in VLAN 17 on interface Fa 0/7.
	ASW1: Verify spanning tree for VLAN 17: Both Port-channel interfaces are forwarding. The link to CSW2 is the root port. This is unexpected. Normally one of the two Port-channels would be blocking.
	CSW1: Verify spanning tree for VLAN 17: Both Port-channel interfaces are in "broken" state.
	CSW1: Log shows that the root guard feature has disabled the Port-channel interfaces.
	Verify security implementation: "Protection against users plugging in switches, which might attempt to become the root for the Spanning Tree Protocol". Conclusion: Root guard should be enabled, but only on ports connected to end-users, not on inter-switch links.
	CSW1: Configuration changed: Removed root guard from Port-channel interfaces 1 and 10. Both prechange and postchange configurations were saved in flash on the device. Communicated this information to team members.
	CLT1: Client PC can now obtain an IP address through DHCP.
	CLT1: Client PC can open the shared folder \\SRV1\Public on server SRV1. Client PC can browse to http://www.isp3.local.
	CSW2: Check for misconfigured root guard feature: Found similar configuration for Port-channel interface 1.
	CSW2: Configuration changed: Removed root guard from Port-channel interface 1. Both prechange and postchange configurations were saved in flash on the device. Communicated this information to team members.
	Problem fixed. Documented changes. Backed up configurations. Communicated to team members. Closed ticket.

Key Clue: Spanning Tree Broken

- Verification of the spanning-tree topology for VLAN 17 on switch CSW1 reveals that the port channel interfaces are marked as broken.

```
CSW1#show spanning-tree vlan 17

VLAN0017
Spanning tree enabled protocol rstp
Root ID    Priority    28689
           Address    001e.f7bb.f780
           This bridge is the root
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID   Priority    28689 (priority 28672 sys-id-ext 17)
           Address    001e.f7bb.f780
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300

Interface      Role Sts Cost      Prio.Nbr Type
-----
Po1            Desg BKN*12    128.56   P2p *ROOT_Inc
Po10           Desg BKN*12    128.128  P2p *ROOT_Inc
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-B

After you have checked the implemented security features, you see that no specific features have been implemented for VLAN 17 in the headquarters LAN. This means that the problem is more generic in nature. Although you suspect that the problem is security related, this is a good point to initiate a Layer 2 troubleshooting process to verify connectivity along the path between the client PC CLT1 and the DHCP server for the VLAN, switch CSW1. This commonly involves verifying the spanning-tree topology for the VLAN, and this will soon lead you to check spanning tree for VLAN 17 on switch CSW1. This command clearly reveals the cause of the problem: The Port-channel interfaces are in spanning-tree “broken” state for VLAN 17, blocking all traffic from the other switches to switch CSW1. After you have spotted this issue, you need to find out what caused the ports to be put into “broken” state. This information can be obtained in several ways. The logs contain the following messages:

```
CSW1#show logging | include SPANTREE
*Mar 1 00:00:25.652: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for
type vlan
*Feb 28 16:00:31 PST: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port
Port-channel1 on VLAN0019.
*Feb 28 16:00:33 PST: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port
Port-channel1 on VLAN0017.
```

From this, you can conclude that the root guard feature is the cause of the problem.

Another way to find the same information is to use the **show spanning-tree inconsistent-ports** command. This reveals the following:

```
CSW1#sh spanning-tree inconsistentports
```

Name	Interface	Inconsistency
VLAN0017	Port-channel1	Root Inconsistent
VLAN0017	Port-channel10	Root Inconsistent
VLAN0018	Port-channel1	Root Inconsistent
VLAN0018	Port-channel10	Root Inconsistent
VLAN0019	Port-channel1	Root Inconsistent
VLAN0019	Port-channel10	Root Inconsistent
VLAN0021	Port-channel10	Root Inconsistent
VLAN0022	Port-channel10	Root Inconsistent

VLAN0023	Port-channel10	Root Inconsistent
VLAN0025	Port-channel10	Root Inconsistent
VLAN0026	Port-channel10	Root Inconsistent
VLAN0027	Port-channel10	Root Inconsistent
VLAN0112	Port-channel10	Root Inconsistent

Number of inconsistent ports (segments) in the system : 13

Researching the output of this command also leads to the root guard feature as the cause of the problem.

Trouble Ticket V Checkpoints

Minimum checkpoints to prove that you have resolved this trouble ticket:

- Client PC CLT1 can obtain an IP address via DHCP.
- You have verified that client PC CLT1 can access all resources that it is entitled to by the security policy (but not more than that).
- You have documented your process, your solution, and any changes that you have made to the device configurations.

What else should you have checked?

Are there any unresolved issues?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—6-14

The figure shows a list of minimum requirements that should be met to consider this trouble ticket to be resolved.

Be aware that in order to meet the requirement in the second item, it is necessary to resolve the Internet access issues covered in Trouble Ticket U.

The second item also implies that you will need to validate the changes that you have made during the resolution of this ticket against the security policy.

Suggested Solution

Correcting the configurations of switches CSW1 and CSW2 as follows can restore the network connectivity from client PC CLT1.

Suggested Configuration Changes

- Remove the root guard feature from the port channel interfaces on switch CSW1:

```
CSW1(config)#interface range Port-channel 1 , Port-channel 10
CSW1(config-if-range)# no spanning-tree guard root
```

- For consistency, also remove the root guard feature from the port channel interface on switch CSW2:

```
CSW2(config)#interface Port-channel 1
CSW2(config-if)# no spanning-tree guard root
```

Note: You can leave root guard enabled on Port-channel 1 on both switches. However, this goes against the implementation guidelines for root guard and does not add any real protection in this scenario.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—6-15

The scenario mentions that “Protection against users plugging in switches, which might attempt to become the root for the Spanning Tree Protocol.” This implies that root guard should be enabled on the switches, but only on user-facing ports. It should not be used on ports between switches that are under your control. From a purely technical standpoint, disabling root guard only on Port-channel 10 on switch CSW1 solves the problem. However, having it enabled on Port-channel 1 on switches CSW1 and CSW2 is not necessary to meet the requirements of the scenario. Actually, it could be argued that it should be removed, because it limits the resilience of the network. When root guard is enabled on Port-channel 1, this link will be blocked in case Port-channel 10 goes down.

Trouble Ticket X: Lost Remote Connectivity to All Routers

The text introducing this trouble ticket was the following:

To roll out SSH version 2 on all routers and switches one of your colleagues from engineering has created a small script, which executed the following commands on all routers:

```
ip ssh version 2
ip ssh source-interface Loopback0
line vty 0 15
transport input ssh
```

On the switches, a similar script was executed, setting the source interface to the management VLAN instead of a loopback interface:

```
ip ssh version 2
ip ssh source-interface Vlan128
line vty 0 15
transport input ssh
```

After execution of these configuration commands, the script has saved the configurations on all devices.

When your colleague tries to test the connectivity to the routers and switches, he notices that he cannot connect to the devices using SSH. Because he cannot figure out what has happened, he asks for your help.

It is your task to diagnose this problem and ensure SSH connectivity to all routers and switches.

Trouble Ticket X: Review and Discuss

How did your team approach Trouble Ticket X?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you accomplish the goal of enabling SSH connectivity to all routers and switches?
- How did you verify that you accomplished your goal?
- Did you roll back any of the implemented features and if so, why?
- Does your solution comply with the security policy?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOTv1.0--6-98

The cause of the problem in this trouble ticket is that SSH has been enabled in the configuration, but no Rivest, Shamir, and Adleman (RSA) keys have been generated. As a result, the SSH server on the device is still disabled and cannot accept any connections. This is a relatively simple problem, but it is frequently encountered. Especially when a router or switch is replaced, you should be aware that copying the configuration will not transfer the keys and that new keys need to be generated (and the clients need to be updated to accept these new keys).

Although there are many possible methods that you could use to solve this problem, the following example of a troubleshooting log shows you a methodical approach to resolve this problem.

Trouble Ticket	Actions and results
Ticket X	CLT1: Verified problem: Cannot use SSH to connect to router CRO1. Connection is refused.
	CRO1: show ip ssh states that the SSH server is disabled. It also states %Please create RSA keys to enable SSH .
	Research SSH: RSA keys need to be generated for SSH to work. Use the command crypto key generate rsa .
	CRO1: Configuration changed: Generated 1024 bits RSA keys. Communicated this information to team members.
	CLT1: Can connect to router CRO1 using SSH now.
	All routers and switches: Generated 1024 bits RSA keys. Saved configurations. Communicated this information to team members.
	CLT1: Tested SSH access to all devices.
	Problem fixed. Documented changes. Backed up configurations. Communicated to team members. Closed ticket.

Key Clue: Create Keys to Enable SSH

- The **show ip ssh** command reveals that RSA keys need to be generated before SSH is enabled:

```
CR01#show ip ssh
SSH Disabled - version 2.0
%Please create RSA keys to enable SSH.
Authentication timeout: 120 secs; Authentication retries: 3
```

Note: Keys are not shown in the configuration.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-17

The **show ip ssh** command tells you exactly what you need to do to enable SSH. It states that RSA keys need to be created before SSH is enabled. When you configure SSH parameters, such as the SSH version, a router or switch will also generate a message to remind you that you need to generate RSA keys before SSH is enabled. However, in this trouble ticket, the commands were supposedly configured by use of a script, and this is why this might have been missed. This also applies when you replace a router or a switch and you copy the configuration to NVRAM. Because the configuration is not parsed when the file is copied, you might miss this message and forget that keys need to be generated for the SSH server to become operational. It is important to note that the keys are not stored in the configuration, which means that they are not transferred when you copy the configuration from one device to another.

Trouble Ticket X Checkpoints

Minimum checkpoints to prove that you have resolved this trouble ticket:

- You can access any router or switch via SSH from any other router or switch using the command **ssh -l admin ip-address**.
- You can access any router or switch via SSH from client PCs CLT1 and CLT2 and server SRV1.
- You have documented your process, your solution, and any changes that you have made to the device configurations.

What else should you have checked?

Are there any unresolved issues?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOTv1.0-6-8

The figure shows a list of minimum requirements that should be met to consider this trouble ticket to be resolved.

Suggested Solution

Generating RSA keys on all routers and switches as follows enables the SSH server on the devices and makes it possible to connect using SSH.

Suggested Configuration Changes

- Generate RSA keys on all devices by issuing the following commands (example is given for router CRO1):

```
CRO1(config)#crypto key generate rsa
The name for the keys will be: CRO1.mgmt.tshoot.local
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Note: Although the keys are not stored in the configuration, it is necessary to save the configuration for the keys to be stored in NVRAM and to be preserved across a reboot.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-9

To enable SSH you should generate RSA keys on all the devices. Make sure that you save the configuration to NVRAM. The keys are not stored in the configuration, but in a separate section of the device's NVRAM. However, the **copy running-config startup-config** command is still necessary to store the keys in NVRAM and to ensure that they are preserved across reboots.

Trouble Ticket Y: Port Security Problems on Switch BSW1

The text introducing this trouble ticket was the following:

The same colleague who has just informed you about the SSH problem also asks for your help with a different problem. A week ago, while he was preparing for the security implementation, he tried to create a macro on switch BSW1 that enables a number of security features. The macro itself worked without any issues and the security features were applied to the port. However, during a failover test the next day, switch BSW1 lost connectivity to routers BRO1 and BRO2, disrupting all communications between the branch office and headquarters. He rolled back the changes and managed to restore connectivity. However, he would still like to get this to work and asks for your help in testing. He tells you that to enable the security features you should log in to switch BSW1 and execute the following commands:

```
interface range FastEthernet 0/1 - 24
macro apply SECURE-PORTS
```

Your colleague claims that this works as intended, but after a reload of router BRO1 or BRO2 problems start being experienced.

It is your task to verify and diagnose this problem and, if possible, resolve it. Ensure that failover between routers BRO1 and BRO2 works as intended by the network design.

Trouble Ticket Y: Review and Discuss

How did your team approach Trouble Ticket Y?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you accomplish the goal of preventing the problems experienced on failover of routers BRO1 and BRO2?
- How did you verify that you accomplished your goal?
- Did you roll back any of the implemented features and if so, why?
- Does your solution comply with the security policy?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-20

The problem in this trouble ticket is caused by an incompatibility between the Gateway Load Balancing Protocol (GLBP) and the port security feature. The suggested use of the macro enables port security on all ports on switch BSW1, including the uplink ports to routers BRO1 and BRO2. GLBP is used on these routers, and GLBP uses virtual MAC addresses to achieve transparent default gateway redundancy. The problem is triggered after a failover, because when one of the routers is rebooted and reinitializes, it will initially claim the same virtual MAC address that is also used by the other router. The port security feature records the same secured MAC address on both uplink ports, perceives this as a security violation, and disables the uplink ports as a result. There is no solution to this issue; this is simply an incompatibility between these two features, and this means that the macro should not be applied to these ports.

Although there are many possible methods that you could use to solve this problem, the following example of a troubleshooting log shows you a methodical approach to resolve this problem.

Trouble Ticket	Actions and results
Ticket Y	BSW1: Apply the macro as prescribed. Copied prechange configuration to flash.
	BRO1: Reload to test. Communicated to team members.
	BSW1: Confirmed problem: Interfaces Fa 0/3 and Fa 0/4 are error-disabled as a result of a security violation.
	BSW1: Shutdown and re-enabled interfaces Fa 0/3 and Fa 0/4. The problem repeats itself. Both interfaces are again error-disabled.
	BSW1: Attempted shutting down and re-enabling the interfaces again. The problem is consistent. Both interfaces come up and are then error-disabled within a couple of seconds. The offending MAC address that causes the violation is listed as 0007.b400.8002.
	Research MAC address: Vendor code 00:07:B4 is registered to Cisco Systems. These MAC addresses are used for GLBP.
	Research GLBP: The routers that participate in GLBP share these MAC addresses, which is why they are seen on both the uplink ports of switch BSW1 when the ports are first enabled. Port security records this as a security violation.
	Conclusion: There does not seem to be a solution to this problem. Either port security needs to be disabled on these ports, or GLBP should be removed. There does not seem to be a good reason to enable port security on these ports, while GLBP is essential.
	BSW1: Rolled back configuration to pre-change backup. Shut down and re-enabled interfaces Fa 0/3 and Fa 0/4.
	BSW1: Configuration changed: Applied the macro to all ports except Fa 0/3 and Fa 0/4. Both prechange and postchange configurations were saved in flash on the device. Communicated this information to team members.
	BRO1: Reload to test. Communicated to team members.
	BSW1: Interfaces Fa 0/3 and Fa 0/4 are no longer error-disabled on failover.
	Problem fixed. Documented changes. Backed up configurations. Communicated to team members. Closed ticket.

Key Clue: Port Security Failures for GLBP Virtual MAC Address

- The port security log messages show that the MAC address that causes the security violation is a GLBP MAC address:

```
Jul 22 23:36:18 PDT: %PM-4-ERR_DISABLE: psecure-violation error detected on
Fa0/4, putting Fa0/4 in err-disable state
Jul 22 23:36:18 PDT: %PORT_SECURITY-2-PSECURE VIOLATION: Security violation
occurred, caused by MAC address 0007.b400.1201 on port FastEthernet0/4.
Jul 22 23:36:18 PDT: %PORT_SECURITY-2-PSECURE VIOLATION VLAN: Security
violation on port FastEthernet0/4 due to MAC address 0007.b400.1201 on VLAN 18
Jul 22 23:36:20 PDT: %LINK-3-UPDOWN: Interface FastEthernet0/4, changed state
to down
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-21

After you enable the macro and test the failover by reloading router BRO1 or BRO2, you see that interfaces FastEthernet 0/3 and FastEthernet 0/4 are disabled by the port security feature. The log messages generated by port security include the MAC address that caused the security violation. You should notice that this MAC address has a very specific format and that it is not the physical MAC address of router BRO1 or BRO2. Some research will reveal that this MAC address is one of the virtual MAC addresses used by GLBP.

When you have determined that GLBP is causing the port security failures you should be able to analyze what happens. Eventually this should lead to the conclusion that there is no solution. Port security and GLBP are simply not compatible, due to the way the mechanisms work.

Trouble Ticket Y Checkpoints

Minimum checkpoints to prove that you have resolved this trouble ticket:

- The security commands are properly applied to all relevant ports by use of the macro on switch BSW1.
- After a reload of router BRO1 or BRO2, network connectivity is restored as expected based on the high-availability features implemented in the branch network.
- You have documented your process, your solution, and any changes that you have made to the device configurations.

What else should you have checked?

Are there any unresolved issues?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOTv1.0—6-2

The figure shows a list of minimum requirements that should be met to consider this trouble ticket to be resolved.

The primary phrase in the first checkpoint is “all relevant ports.” After a detailed analysis of the interaction between port security and GLBP, you should come to the conclusion that the macro should not be applied to all ports on switch BSW1, but to all ports except FastEthernet 0/3 and FastEthernet 0/4.

Suggested Solution

Correcting the configuration of switch BSW1 as follows will achieve maximum security, without causing failover problems.

Suggested Configuration Changes

- Remove the port security commands applied by the macro from FastEthernet 0/3 and FastEthernet 0/4 on switch BSW1:

```
BSW1(config)#interface range FastEthernet 0/3 - 4
BSW1(config-if-range)# no switchport port-security maximum 10
BSW1(config-if-range)# no switchport port-security
BSW1(config-if-range)# no macro description SECURE-PORTS
BSW1(config-if-range)# shutdown
BSW1(config-if-range)# no shutdown
```

Note: Do not forget to re-enable the ports. Only removing port security from the configuration will not clear the error-disabled state of the ports.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-6-20

Alternatively, you could roll back the configuration to an archived copy that you made before applying the macro. After that, you should apply the macro to all ports except the uplink ports FastEthernet 0/3 and FastEthernet 0/4. This solution is considered to be in line with the security policy. Given the nature of the features that are implemented by this macro, it seems that it was intended to be applied to user-facing ports.

Do not forget to shut down and re-enable interfaces FastEthernet 0/3 and FastEthernet 0/4 after you change the configuration. Removing port security from the configuration will not clear the error-disabled status of the ports.

Consolidation

This topic describes the primary lessons that could be learned from the lab exercise.

Discussion: Lessons Learned

Method and process:

- How could you improve your troubleshooting methods?
- What alternative methods did you discover?

Communication and procedures:

- How could the troubleshooting process be made more effective?
- What kind of procedures would be useful and why?

Technology and tools:

- Which tools were most useful during troubleshooting?
- Which tools could have improved the effectiveness of your process?
- Which useful Cisco IOS commands did you discover?

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0—6-38

Think about all the things that you learned during the lab itself and during the debrief discussions. There is room to write down primary learning points in the Lab Debrief Notes section of the lab guide.

In addition to thinking of the methods, processes, and tools as they were used in the lab, reflect on how these would apply to your own organization.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- You have reviewed and verified your lab results.
- You have consolidated the experiences and discoveries that all students got from the lab and you have derived a number of key learning points from these experiences.

References to Additional Security Troubleshooting in E-Learning

Overview

The *Troubleshooting and Maintaining Cisco IP Networks* (TSHOOT) v1.0 instructor-led training (ILT) course is a comprehensive learning experience. Among the learning tools available to you, it includes e-learning modules that complement the classroom instructor-led content and add to your experience with self-paced materials and demonstrations. Upon accessing the e-learning content, you will be able to reinforce the knowledge acquired in class, and witness real-life troubleshooting scenarios demonstrated in real routers and switches. The content structure is flexible, and you can navigate it at your own pace, at the time of your choosing, and at the depth you want according to your level of experience.

This lesson presents additional topics in security troubleshooting, and provides an overview of these e-learning modules: “Troubleshooting Network Applications Services” and “Troubleshooting Branch Office and Remote Worker Problems.”

Objectives

Upon completing this lesson, you will be able to review the e-learning modules that pertain to additional topics in security troubleshooting. This ability includes being able to meet these objectives:

- Describe the content of the “Troubleshooting Network Applications Services” e-learning module
- Describe the content of the “Troubleshooting Branch Office and Remote Worker Problems” e-learning module
- Understand the process of accessing and using e-learning content

Preview of E-Learning on Additional Security Troubleshooting

This topic describes e-learning products to teach configuring of implementation of additional security troubleshooting.

CCNP E-Learning

- Complement and enhance your classroom experience
- Reinforce concepts and their application
- Learn at your own pace
- Review advanced topics
- Experience real-life scenarios through directed demonstrations
- Use the trouble-ticket approach to consolidate your troubleshooting method

© 2009 Cisco Systems, Inc. All rights reserved.ROUTE v1.0—6-2

One of the primary ideas behind the design of the Cisco CCNP® curriculum is the understanding that there is no one best method of learning for every student. Some students prefer individual labs, while others prefer one-on-one tutoring, hands-on sessions, self-paced computer-assisted instruction, direct, discovery learning, or cooperative learning, among others.

E-learning solutions offer new approaches that complement and enhance classroom-based learning. Designed with flexibility and learning effectiveness in mind, the e-learning modules described in this lesson are based on knowledge you acquired during your *Troubleshooting and Maintaining Cisco IP Networks* (TSHOOT) v1.0 instructor-led training course.

All e-learning modules described in this lesson utilize the trouble-ticket approach you know very well by now: A case is presented, using certain assumptions and baseline information. The demonstrations will show one or more of the possible paths to gathering information, identifying symptoms, prioritizing hypotheses, and gathering conclusions. The content is as much about the technical aspects presented as it is about applying a troubleshooting method to a specific scenario controlled by certain variables.

Troubleshooting Network Applications Services

Lesson	Description
Maintaining Applications Services	Introduces the concept of application networking and the need to integrate multiple network functions to deploy application-aware network services. Examples include NBAR, IP SLA, Auto QoS, and NetFlow.
Identifying Applications Services Problems	Provides an overview of common scenarios where network issues affect application-aware network services.
Directed Demo: Troubleshooting Applications Services Problems	Troubleshoots application services scenarios of NetFlow misconfigurations, IP SLA time synchronization, and missing Auto QoS requirements.
Self-Check Assessment	Assesses your understanding of the lesson.

© 2009 Cisco Systems, Inc. All rights reserved.

ROUTE v1.0—6-3

The “Troubleshooting Network Applications Services” e-learning module covers topics that complement the classroom module you are reviewing. In this module, a comprehensive introduction to application networking is followed by a description of common issues in utilizing technologies such as NetFlow, IP service level agreements (IP SLAs), Network-Based Application Recognition (NBAR), and Cisco AutoQoS. The trouble tickets focus on demonstrating hands-on scenarios where either those technologies interfere with other network services, or existing functions such as routing, access control, and change management cause issues in the deployment of all four features.

Troubleshooting Branch Office and Remote Worker Problems

Lesson	Description
Identify Problems with Branch Office and Remote Workers	Provides an overview of remote access connectivity issues in the context of security functions such as VPNs and other security controls.
Directed Demo: Troubleshooting Branch Office and Remote Workers Problems	Trouble tickets focus on routing issues around IPsec VPNs. They include problems with NAT, routing protocols, addressing in general, and GRE tunnels.
Self-Check Assessment	Assesses your understanding of the lesson.

© 2009 Cisco Systems, Inc. All rights reserved.

ROUTE v1.0—6-4

The “Troubleshooting Branch Office and Remote Worker Problems” e-learning module covers topics that complement the classroom module you are reviewing. This module introduces issues that pertain to remote-access connectivity. This includes branch office and remote worker services. In general, the breadth of these topics touches multiple areas, from virtual private networks (VPNs) to firewalls to application networking. The focus will be on the impact of the overall solution in routing and switching, and the underlying requirements that routers and switches need in order to support branch and remote worker connectivity.

The trouble tickets demonstrated in this module touch on the readiness of the network for IPsec VPN deployments, including services such as addressing, routing, and access control.

Where to Find E-Learning Modules



The e-learning modules described in this lesson are available on a CD as part of your classroom materials. Please contact your instructor with questions on finding and accessing the CD.

The objectives of these modules are part of your CCNP certification exam, and they should be reviewed by candidates to the CCNP certification.

E-Learning Module Structure

The screenshot displays a three-panel interface for an e-learning module. The top-left panel, titled "Addressing and Topology Specifics", shows a network topology with three routers (R1, R2, R3) and their interfaces. R1 and R2 are connected via a 10.2.7.0/24 link. R2 and R3 are connected via a 10.3.7.0/24 link. R1 and R3 are connected via a 192.168.2.0/24 link. R2 and R3 are connected via a 192.168.1.0/24 link. R1 and R3 are also connected via a 192.168.253.0/24 link. The topology is labeled with OSPF and EIGRP. The top-right panel, titled "Debrief : Alternative Configuration", shows a configuration snippet for route-maps and redistribution. The bottom panel shows a console output for a policy routing configuration on R1, including a route-map named SETTAG, match clauses, and a trace command for 192.168.254.1. The console output shows the trace results for the route to 192.168.254.1, indicating a successful path through R1 and R2.

Addressing and Topology Specifics

OSPF

EIGRP

10.2.7.0/24

10.3.7.0/24

192.168.2.0/24

192.168.1.0/24

192.168.253.0/24

Debrief : Alternative Configuration

```
route-map TAGS deny 10
match tag 1000
route-map TAGS permit 20
set tag 1000
....
router ospf 1
redistribute eigrp 1 metric 4 route-map
TAGS
....
router eigrp 1
redistribute ospf 1 metric 1000000 0 255
1 800 route-map TAGS
....
```

Keep it simple.

R1 R2 ISP

Policy routing matches: 0 packets, 0 bytes

route-map SETTAG, permit, sequence 20

Match clauses:

Set clauses:

Policy routing matches: 0 packets, 0 bytes

R1#trace 192.168.254.1

Type escape sequence to abort.

Tracing the route to 192.168.254.1

1 192.168.2.2 12 msec * 12 msec

R1#

R1#

Utilizing a combination of lecture sessions, animated content, lab demonstrations, and assessments, each e-learning module presents a hierarchical structure of lessons and topics. You can navigate that structure by using an intuitive graphical user interface that includes playback controls, slide selection, and lesson and topic selection. Using these tools, you will be able to navigate the content at your own pace.

The three-panel screen presented in the directed demonstrations allows you to focus on the device console demonstrations, while having the command syntax and the topology diagram in sight for verification and additional information.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Describe the content of the “Troubleshooting Network Applications Services” e-learning module.
- Describe the content of the “Troubleshooting Branch Office and Remote Worker Problems” e-learning module.
- Understand the process of accessing and using e-learning content.

© 2009 Cisco Systems, Inc. All rights reserved.

ROUTE v1.0—6-7

Module Summary

This topic summarizes the key points that were discussed in this module.

Module Summary

- In a secured network, the troubleshooting processes need to be aligned to the security policy of the organization.
- Security features add an extra layer of complexity to network troubleshooting.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—64

Any network infrastructure that is deployed needs to be secured. Access to the management, control, and data plane of the infrastructure devices needs to be protected. Authentication mechanisms, packet filtering, and other, more specialized security features are commonly implemented to protect both the infrastructure itself and the traffic it is carrying.

Troubleshooting processes in a secured network infrastructure need to be aligned to the security policies of the organization. Any change that is made during network troubleshooting needs to be evaluated against the security policy. This applies to changes that are made to resolve a problem, and also to temporary changes that are made during the diagnostic process.

Network security features add an additional layer of complexity to network troubleshooting. In an unsecured network, any lack of connectivity is to be taken as an indication that there is a problem. However, in a secured network infrastructure, connectivity is often specifically disallowed, and a lack of connectivity is not necessarily a sign of problems. This means that to troubleshoot effectively in a secured network infrastructure, an engineer needs to know which traffic is allowed and which traffic is not allowed on the network according to the security policy. Also, an engineer needs to be aware of which specific features are implemented at each point in the network to enforce the security policy and how these features affect network connectivity.

References

For additional information, refer to these resources:

- Cisco Systems Inc., *Cisco SAFE Reference Guide*:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.html
- Cisco Systems Inc., *Control Plane Protection*:
https://www.cisco.com/en/US/docs/ios/12_4t/12_4t4/htcpp.html
- Cisco Systems Inc., *Configuring Unicast Reverse Path Forwarding*:
http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_unicast_rpf.html
- Cisco Systems Inc., *Common Problems in Debugging RADIUS, PAP and CHAP*:
http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080093f4b.shtml

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

- Q1) Which three security services can be provided by routers and switches? (Choose three.) (Source: Troubleshooting Security Features)
- A) IPS
 - B) TACACS+ services
 - C) VPNs
 - D) packet filtering and firewall functionality
 - E) antivirus updates
 - F) spam filtering
- Q2) Which two security mechanisms can be used to protect the management plane of a router or switch? (Choose two.) (Source: Troubleshooting Security Features)
- A) uRPF
 - B) BPDU guard
 - C) AAA
 - D) generic packet filtering
- Q3) Which two security mechanisms can be used to protect the control plane of a router or switch? (Choose two.) (Source: Troubleshooting Security Features)
- A) root guard
 - B) routing protocol authentication
 - C) SSH
 - D) NAC
- Q4) Which three security mechanisms can be used to protect the data plane of a router or switch? (Choose three.) (Source: Troubleshooting Security Features)
- A) root guard
 - B) routing protocol authentication
 - C) uRPF
 - D) SSH
 - E) VPN
 - F) IPS
- Q5) Which three are valid steps when troubleshooting transport layer problems? (Choose three.) (Source: Security Features Review)
- A) define problem
 - B) create solution
 - C) stop affected service
 - D) observe results

- Q6) Which three best describe the “Gather Facts” step of the troubleshooting transport layer problems flow? (Choose three.) (Source: Security Features Review)
- A) get more information from the affected users
 - B) make notes about every change you have made
 - C) use the command line interface to collect more information
 - D) compare the current configuration with the last working for changes
 - E) document the solution
- Q7) Which two best describe the “Create/Apply Solution” step of the troubleshooting transport layer problems flow? (Choose two.) (Source: Security Features Review)
- A) create a list of most likely causes of the problem
 - B) check service operation as you try all possible fixes
 - C) document all action plans you have used
 - D) obligatory reload of the network equipment when you apply fixes
- Q8) Which statement best describes Cisco IOS stateful inspection? (Source: Security Features Review)
- A) allow certain incoming flows by first inspecting and recording flows initiated from the trusted network
 - B) can inspect only Layer 4 information of the session
 - C) statically define all entries in the access list of the outside interface to allow bidirectional communication between the trusted and untrusted networks
- Q9) Which command can be used to apply an inbound inspection rule named “WEB” on the interface? (Source: Security Features Review)
- A) router#**ip inspect WEB in**
 - B) router (config)# **ip inspect WEB in**
 - C) router(config)# **inspect WEB in**
 - D) router (config-if)# **ip inspect WEB in**
 - E) router(config-if)# **inspect WEB in**
- Q10) Which two commands display configuration and session information for the stateful inspection feature? (Choose two.) (Source: Security Features Review)
- A) **show ip inspect all**
 - B) **show ip access-list**
 - C) **show running-config**
 - D) **show ip inspec**
 - E) **show inspec all**
- Q11) Which three are components of AAA? (Choose three.) (Source: Security Features Review)
- A) authentication
 - B) administration
 - C) authorization
 - D) accounting
 - E) activation

- Q12) What does the term “authorization” mean? (Source: Security Features Review)
- A) determining which resources the user can access on the network
 - B) providing accounting records for billing purposes
 - C) providing a username and password prompt when someone uses Telnet to connect to the router
 - D) authorizing network equipment to communicate with the security server
- Q13) What is the purpose of the RADIUS and TACACS+ protocols? (Source: Security Features Review)
- A) They provide comprehensive tools for network device monitoring.
 - B) They transport user-related information between two routers.
 - C) They transport user-related information between a network device and a centralized security server.
 - D) They are obsolete and not in use.
- Q14) What are three differences between RADIUS and TACACS+? (Choose three.) (Source: Security Features Review)
- A) RADIUS uses TCP, and TACACS+ uses UDP.
 - B) RADIUS uses UDP, and TACACS+ uses TCP.
 - C) RADIUS offers limited accounting, and TACACS+ provides extensive accounting.
 - D) RADIUS encrypts the whole packet, while TACACS+ encrypts only the password.
 - E) TACACS+ offers limited accounting, and RADIUS provides extensive accounting.
 - F) TACACS+ encrypts the whole packet, while RADIUS encrypts only the password.

Module Self-Check Answer Key

- Q1) A, C, D
- Q2) C, D
- Q3) A, B
- Q4) C, E, F
- Q5) A, B, D
- Q6) A, C, D
- Q7) A, C
- Q8) A
- Q9) D
- Q10) A, C
- Q11) A, C, D
- Q12) A
- Q13) C
- Q14) B, E, F

Maintaining and Troubleshooting Integrated, Complex Enterprise Networks

Overview

The networks of today incorporate many different technologies, protocols, devices, and features. To maintain and troubleshoot these complex, integrated enterprise networks efficiently and effectively you need to acquire broad knowledge and a wide range of skills. In addition to detailed knowledge of individual technologies, protocols, devices, and features you need to understand how these components interact and depend on each other. You need to know the tools that are available to support network maintenance and troubleshooting processes and know how to use these tools. In addition, you need to be able to plan, communicate, document, and execute structured network maintenance and troubleshooting processes.

In the previous labs and lessons of this course the different aspects of network maintenance and troubleshooting processes were reviewed, analyzed, discussed, and practiced. In this module, you will have the opportunity to practice the skills you acquired and assess your performance in an integrated, complex lab environment.

Module Objectives

Upon completing this module, you will be able to troubleshoot and maintain integrated, complex enterprise networks. This ability includes being able to meet these objectives:

- Summarize the lessons that you learned about network maintenance and troubleshooting in this course
- Practice, assess, and improve your network maintenance and troubleshooting skills in a complex network environment

Troubleshooting Complex Environments

Overview

To troubleshoot complex enterprise networks, you need a comprehensive set of skills and knowledge. In addition to understanding individual network technologies you need to understand how the different technologies interact and build upon each other. You need to know and understand the methods that you could use to isolate problems to a particular device, protocol, or feature and have the ability to plan a troubleshooting process and adjust your plan based on the results of the process. You need to know how to find the documentation for technologies, protocols, or features that you are not familiar with and you should be able to document and communicate the results of your troubleshooting process as part of regular network maintenance or escalation procedures.

Practicing these skills in a noncritical environment is an important tool that you can use to assess whether you have understood and incorporated the lessons that could be learned during the earlier labs in this course and to improve your troubleshooting skills even more.

In this lesson, the key learning points from the previous labs are summarized. In addition, you are given the instructions and guidelines that you need to start a lab that gives you an opportunity to practice and assess your network maintenance and troubleshooting skills.

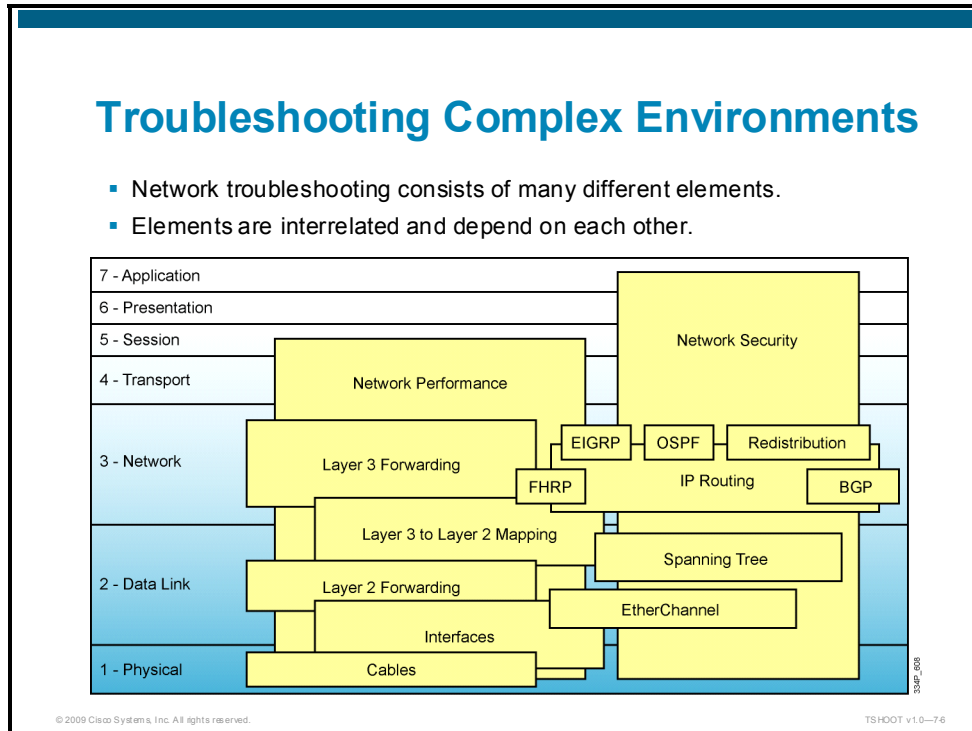
Objectives

Upon completing this lesson, you will be able to summarize the lessons about network maintenance and troubleshooting that you learned during this course and commence troubleshooting complex enterprise networks using a structured approach. This ability includes being able to meet these objectives:

- List the primary lessons that you learned about network maintenance and troubleshooting tasks during previous labs
- Initiate Lab 7-1, Troubleshooting Complex Environments, in order to practice troubleshooting in a complex environment and be assessed on the skills acquired during this course

Troubleshooting Complex Networks

This topic describes the major components of network troubleshooting and maintenance that were presented in previous modules and the role of each of these components in troubleshooting processes for complex environments. This topic also summarizes the most important lessons that should have been learned from the labs in this course.



In complex, integrated networks, many different protocols and technologies are used to deliver network services to support the enterprise applications. These protocols and technologies interact with each other. Some processes interact with or are dependent on other processes, while other processes perform their functions in parallel.

If one of the elements fails or does not perform as expected, this failure affects the system as a whole. At some point, symptoms will become noticeable at the application level and a user will report a problem. A diagnostic process is used to begin to find the elements that are causing the problem and eliminate the problem by implementing a solution or workaround.

To be able to troubleshoot a complex network in an effective and efficient manner, you need to have a thorough understanding of the following aspects:

- **Individual technologies, protocols, and features that are used in your network:** At the least, you should have a high-level knowledge of the functionality that is offered by each of the technologies, protocols, and features. You might not need the level of knowledge that a specialist has about each particular technology, but if you do not have that level of knowledge, then you should know how to obtain the required background knowledge, documentation, or expert support in your organization.
- **Interactions and dependencies between the different technologies, protocols, and features in your network:** If someone notices a symptom of a problem in one of the elements, the presence of that symptom does not necessarily mean that the root cause of the problem exists in that element. The root cause might be in another element upon which the element that you are researching depends or with which the element you are researching interacts. For example, a routing protocol failure might be caused by an underlying Layer 2 problem.
- **How control plane processes influence data plane processes:** Symptoms of a problem are usually noticed and reported on the data plane, while in many cases, the root cause is on the control plane and, therefore, the solutions or workarounds are implemented on the control plane. To successfully diagnose and resolve network problems, it is essential for you to know how control plane data structures are used in data plane forwarding and how these data structures are populated.
- **The tools that are available to gather information about the operation of the various technologies, protocols, features and processes:** It is also important that you have experience with these tools. Your knowledge and experience should include specialized troubleshooting tools and tools that are used in support of the regular maintenance processes, such as tools that support change processes, baseline collection, communication, and documentation.

In this course, you were introduced to many of the individual technologies that are commonly used in complex, integrated enterprise networks and you practiced using tools and structured methods during the labs. Group experiences from the labs were discussed, important lessons were learned, and best practices were derived from these experiences. This topic reviews the technology areas that you learned about in the labs and discusses the lessons that you learned.

Summary of Lab 2-1

This lab provided you with an opportunity to experience troubleshooting without access to tools, documentation, assigned responsibilities, or established procedures.

Lab 2-1: Introduction to Troubleshooting

This lab served as an introduction to structured troubleshooting.

- Problems that were encountered:
 - Misconfiguration of EIGRP network statements
- Lessons that were learned:
 - Structuring a troubleshooting process makes it more effective.
 - Communication is vital to troubleshooting as a team.
 - Network documentation, a baseline, and tools are essential to an efficient troubleshooting process.

Review: What is the most important lesson that you learned from this lab?

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0-7.7

The main objective of this first lab was to provide you with an opportunity to experience the results of troubleshooting in an unstructured manner. Documentation and specialized tools were not available and communication procedures were not established at the beginning of the lab.

This lab served as an introduction to the structured troubleshooting methods presented in the “Plan Troubleshooting Processes for Complex Enterprise Networks” module. The problem introduced in the trouble ticket, misconfiguration of Enhanced Interior Gateway Routing Protocol (EIGRP) network statements, was an elementary problem and no special tools or commands were required to solve this problem.

The following items are the main lessons that you learned in this lab:

- A structured troubleshooting approach increases the chances of diagnosing and resolving a problem in a timely manner. Even if you do not solve the problem, if you use a structured approach and document troubleshooting progress you will be able to give the results to a different person or team for further investigation.
- Without proper communication procedures, a team troubleshooting process can be severely hampered. If changes are made by one team member that other team members are not aware of, conclusions that are reached during the troubleshooting process can be invalidated. If you do not share results or discoveries among team members, the efficiency of the process may be affected, because multiple team members gather the same or unnecessary information, or execute the same tests.
- If you have access to up-to-date and correct documentation, have a baseline of network behavior, and know what tools are available, you can greatly increase the effectiveness of the troubleshooting process.

Write down the most important lesson that *you* learned from this lab:

Summary of Lab 3-1

This lab provided you with an opportunity to become familiar with the lab environment, available documentation, and tools.

Lab 3-1: Assembling Maintenance and Troubleshooting Tools

This lab served as an introduction to the lab environment and the tools that are available.

- No problems were introduced in this lab.
- Tools and commands that were used:
 - Cisco IOS features and tools related to network maintenance, such as DNS, NTP, TFTP, SNMP, NetFlow and syslog.
- Lessons that were learned:
 - Establishing a baseline and documenting the network.
 - Assembling a network maintenance toolkit and preparing the network devices to communicate with the tools.

Review: What is the most important lesson that you learned from this lab?

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0--7-8

The main objective of this lab was to allow you to familiarize yourself with the lab network, before any problems were introduced. You reviewed the documentation and compared it to the network configuration. You discovered the tools that are available in the lab network to support maintenance and troubleshooting tasks. In addition, you assigned responsibilities and established communication procedures with your team members.

No problems were introduced in this lab. This situation gave your team a chance to observe the network behavior under normal circumstances and establish a baseline of network behavior.

The tools that were provided in the lab on server SRV1 to support troubleshooting and maintenance included the following:

- **Name services:** Server SRV1 is configured as a Domain Name System (DNS) server to provide name resolution for the lab devices.
- **Backup and restore:** Server SRV1 runs a TFTP service to provide backup and restore capabilities for the network. In addition to TFTP, other services such as FTP or web services may have been provided. Automatic configuration archiving to the TFTP service on server SRV1 was configured on the routers and switches.
- **Logging:** Server SRV1 runs a syslog service to collect logging from the routers and switches, which have been configured to log all messages except debug messages to server SRV1.

- **Time services:** Routers IRO1 and IRO2 have been configured to synchronize their clocks to two Network Time Protocol (NTP) servers on the Internet. All other routers and switches synchronize their clocks to routers IRO1 and IRO2 via NTP.
- **Network management tools:** Routers IRO1, IRO2, CRO1, and CRO2 have been configured to send Cisco IOS NetFlow information to server SRV1. All devices have been configured to send Simple Network Management Protocol (SNMP) trap messages to server SRV1 and allow SNMP polling. Whether actual network management software was provided to process this information depends on the Learning Partner lab setup.
- **Traffic analysis:** Packet capturing software was provided on server SRV1 and could be installed on all client PCs in the network.

The main lessons that you learned in this lab were how to assemble a network maintenance and troubleshooting toolkit, how to prepare the communication between the network devices and the tools, and how to collect the necessary documentation and establish a network baseline in preparation for troubleshooting and maintenance processes.

Write down the most important lesson that *you* learned from this lab:

Summary of Lab 4-1

This lab provided you with an opportunity to practice structured troubleshooting of Layer 2 and spanning-tree problems.

Lab 4-1: Layer 2 Connectivity and Spanning Tree

This lab focused on structured troubleshooting of Layer 2 and spanning-tree problems.

- Problems that were encountered:
 - Spanning tree problems
 - VLAN and trunking problems
- Noteworthy commands:
 - The **show mac address-table** and **show spanning-tree** command are the critical commands that are used to trace a Layer 2 path.
- Lessons that were learned:
 - Following the Layer 2 path from switch to switch is an effective method of troubleshooting various Layer 2 problems.

Review: What is the most important lesson that you learned from this lab?

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0-7.0

The main objective of this lab was for you to learn how to apply a structured troubleshooting method to troubleshoot a variety of Layer 2 problems. The following problems were encountered:

- A spanning-tree problem caused by a spanning-tree type mismatch
- A Layer 2 connectivity problem caused by the bridge protocol data unit (BPDU) guard feature
- A Layer 2 connectivity problem caused by a trunk encapsulation mismatch
- A Layer 2 connectivity problem caused by VLANs that were not allowed on certain trunks
- An IP connectivity problem caused by a missing VLAN

All problems in this lab could be solved using common Cisco IOS Software commands. To trace the Layer 2 path between hosts, the **show spanning-tree** and **show mac address-table** commands are essential. The **show spanning-tree** command can be used to determine or verify the Layer 2 topology, while the **show mac address-table** command can be used to determine whether frames from a certain source reached a particular point in the switched network.

An important lesson that could be learned from this lab is that many Layer 2 connectivity problems can be diagnosed by following the path from switch to switch to find the point where frames start being dropped.

Write down the most important lesson that *you* learned from this lab:

Summary of Lab 4-2

This lab provided you with an opportunity to practice structured troubleshooting of multilayer switching and first-hop redundancy problems.

Lab 4-2: Layer 3 Switching and First-Hop Redundancy

This lab focused on troubleshooting multilayer switching and First Hop Redundancy Protocols (FHRPs).

- Problems that were encountered:
 - Various typing errors in the configurations
 - VLAN related problems
- Lessons that were learned:
 - Paying attention to details and spotting differences are critical troubleshooting skills.
 - Problems related to multilayer switching and FHRPs are often caused by underlying Layer 2 problems.

Review: What is the most important lesson that you learned from this lab?

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0-7-10

The focus points for this lab were multilayer switching and First Hop Redundancy Protocols (FHRPs), such as the Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and the Gateway Load Balancing Protocol (GLBP).

Most of the problems in this lab were caused by small typing errors in the configurations, such as mismatched IP addresses, group numbers, and passwords. Once found, these problems are easy to solve, but finding these types of problem can be difficult. A mistyped password, a wrong IP address, or a mismatched parameter is easily overlooked.

Some of the problems were not caused by problems related to the operation of the multilayer switching process or FHRPs themselves, but were caused by underlying Layer 2 problems related to trunks and VLANs.

In addition to practicing Cisco IOS Software commands related to the specific protocols and technologies covered in this lab, a major lesson that could be learned from this lab is that attention to detail is very important when troubleshooting. Sometimes reconfiguring a feature can help you spot these small differences and errors. This technique is specifically useful when you are troubleshooting new implementations.

Another lesson that could be learned from this lab is the following: When you troubleshoot a feature (such as multilayer switching or a FHRP), if you know that the configuration is correct and has been tested, and you also know that no changes have been made to the configuration of that feature, you should realize that the problem might not be related to the feature itself, but might be caused by a problem on one of the underlying layers. When you observe symptoms of a problem in a particular protocol, technology, or feature, it does not automatically mean that the problem must be with that protocol, technology, or feature. The problem might be caused by a different problem in an element that the protocol, technology, or feature depends on or interacts with.

Write down the most important lesson that *you* learned from this lab:

Summary of Lab 5-1

This lab provided you with an opportunity to practice structured troubleshooting of generic Layer 3 connectivity issues and problems related to the Enhanced Interior Gateway Routing Protocol (EIGRP).

Lab 5-1: Layer 3 Connectivity and EIGRP

This lab focused on Layer 3 troubleshooting in general and routing using EIGRP.

- Problems that were encountered:
 - Configurations swapped on routers CRO1 and CRO2
 - Various misconfigured IP addresses and parameters
- Lessons that were learned:
 - Planning for disaster recovery can greatly reduce the impact of outages.
 - Following the Layer 3 path from router to router is an effective method of troubleshooting Layer 3 problems.

Review: What is the most important lesson that you learned from this lab?

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0—7-11

The focus in this lab was on troubleshooting Layer 3 connectivity in general, and as part of that, because EIGRP is the routing protocol in use on the network, problems related to EIGRP.

The most significant problem in this lab was that the configurations of routers CRO1 and CRO2 were swapped and had to be restored from a backup. After diagnosing the problem, it is important to find the quickest possible method to restore connectivity on the WAN and restore the original configuration. As such, the procedural aspects of this lab were more important than the technical aspects. Analyzing problems under time pressure, communicating clearly and making quick and effective decisions were the most important skills to practice during this lab.

After the main problem had been resolved, several smaller configuration problems needed to be diagnosed and resolved. By carefully tracking the Layer 3 path between the affected source and destination host, the problems could be isolated and fixed.

Therefore, an important lesson that can be learned from this lab is that if you plan for outages by defining procedures and ensuring that the necessary resources to recover from an outage are available, you will save much time when disaster strikes.

From a technical standpoint, another important lesson that can be learned from this lab is that tracking the Layer 3 path between hosts, both on the data plane and the control plane, is an effective method that you can use to diagnose Layer 3 connectivity problems.

Write down the most important lesson that *you* learned from this lab:

Summary of Lab 5-2

This lab provided you with an opportunity to practice structured troubleshooting of routing problems related to Open Shortest Path First (OSPF) and to route redistribution between OSPF and EIGRP.

Lab 5-2: OSPF and Route Redistribution

This lab focused on troubleshooting routing problems involving OSPF and route redistribution.

- Problems that were encountered:
 - Missing seed metrics and **subnets** option on redistribution
 - Various mismatched OSPF parameters
- Noteworthy commands:
 - The **debug ip ospf events** and **debug ip ospf adj** commands can uncover the cause of failing OSPF adjacencies.
- Lessons that were learned:
 - Always define seed metrics when configuring redistribution.

Review: What is the most important lesson that you learned from this lab?

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0-7-12

This lab introduced OSPF and redistribution between OSPF and EIGRP was enabled, allowing you to practice troubleshooting these technologies.

The problems regarding redistribution revolved around missing options in the configuration, such as missing seed metrics for the redistribution from OSPF to EIGRP and a missing **subnets** option for the redistribution from EIGRP to OSPF. Although these options are not mandatory, redistribution between OSPF and EIGRP does not work when the options are not defined.

Most of the problems with OSPF revolved around parameter mismatches, such as mismatched hello timers, areas, and authentication passwords that prevented routers from becoming neighbors. The **debug ip ospf adj** and **debug ip ospf event** commands proved useful in uncovering the exact cause of failing OSPF adjacencies.

An important lesson that can be learned in this lab is to always define seed metrics and other key redistribution options, even if they are not mandatory.

Write down the most important lesson that *you* learned from this lab:

Summary of Lab 5-3

This lab provided you with an opportunity to practice structured troubleshooting of routing problems related to the Border Gateway Protocol (BGP).

Lab 5-3: Border Gateway Protocol

This lab focused on troubleshooting routing problems involving the Border Gateway Protocol (BGP).

- Problems that were encountered:
 - Mismatched AS numbers
 - Misconfigured prefix list
 - Missing static route to the Null 0 interface
- Lessons that were learned:
 - BGP a complex protocol and its behavior is tightly controlled by the configuration.
 - BGP operation is dependent on the routing table.

Review: What is the most important lesson that you learned from this lab?

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOTv1.0-7-13

This lab focused on using the Border Gateway Protocol to connect to external service providers and provided an opportunity for you to troubleshoot problems related to BGP.

The following problems were encountered:

- An incorrectly configured remote autonomous system number for one of the neighbors, causing the proper establishment of the BGP peering to fail
- A missing static route to the Null 0 interface, which caused the configured local network not to be injected in the BGP table
- A misconfigured prefix list preventing the local network from being advertised

All these errors were caused by missing or incorrect configuration commands. Essentially BGP is a tool that can be used to implement routing policies, not a routing protocol only. As a consequence, BGP has very few automatic processes. Almost all its behavior is controlled by configuration commands. This situation results in more complex configurations than the configurations of common interior gateway protocols (IGPs), such as OSPF or EIGRP. More complex and larger configurations increase the chance of problems occurring that are caused by typing errors. Problems caused by missing configuration statements are also more likely because BGP needs explicit configuration for many things that are taken care of automatically in other protocols.

Another lesson that could be learned from this lab is that BGP depends on a correct routing table for many of its processes, such as the establishment of sessions, resolution of the next-hop IP address, or injection of networks in the BGP table. Troubleshooting BGP, therefore, is often closely associated with troubleshooting the underlying routing mechanisms.

Write down the most important lesson that *you* learned from this lab:

Summary of Lab 5-4

This lab provided you with an opportunity to practice structured troubleshooting of performance problems on routers.

Lab 5-4: Router Performance

This lab focused on troubleshooting performance problems on routers.

- Problems that were encountered:
 - High CPU load caused by suboptimal switching methods
 - Memory allocation problems caused by huge BGP tables
- Lessons that were learned:
 - Using a router in a role that it was not designed for can lead to network performance problems.
 - The switching method that is used by a router has a major impact on its throughput.

Review: What is the most important lesson that you learned from this lab?

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0—7-14

This lab focused on the way router performance is affected by misconfiguration of the switching method and by deploying a router in a role that it was not designed for. The lab provided an opportunity for you to troubleshoot performance problems caused by these issues and observe the typical symptoms associated with this type of problem.

The following problems were encountered:

- A huge BGP table was forwarded to some of the routers, which were not designed to take on a full BGP load.
- Cisco Express Forwarding was disabled on some of the routers causing a higher than normal load on the CPU of these routers.
- A huge access list was configured on some of the routers, adding more strain on the CPU.

These errors were caused by misconfiguration of the parameters that affect the forwarding capacity of a router, such as the switching method, and by putting a higher load on the routers than they were designed for. The main lesson that could be learned in this lab is how these issues affect the performance of a router and which symptoms can typically be observed when a router is under severe stress.

Write down the most important lesson that *you* learned from this lab:

Summary of Lab 6-1

This lab provided you with an opportunity to practice structured troubleshooting of problems related to security features available on routers and switches.

Lab 6-1: Introduction to Network Security

This lab focused on troubleshooting problems related to basic network security features.

- Problems that were encountered:
 - Misconfigured access lists
 - Password and authentication problems
- Lessons that were learned:
 - Passwords and authentication can be circumvented when you have physical access to a device.
 - Small errors in access lists are hard to find.
 - The troubleshooting process should be aligned with the security policies of your organization.

Review: What is the most important lesson that you learned from this lab?

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0-7-15

This lab allowed you to experience how the deployment of security features affects network troubleshooting processes.

The problems introduced in this lab consisted of various access list configuration errors combined with a number of authentication issues that forced you to perform a password recovery procedure on the affected devices. This situation served to illustrate the point that all network security starts with securing the physical access to your devices.

In addition to learning to diagnose and resolve problems related to basic security features embedded in the Cisco IOS Software running on routers and switches, this lab demonstrated the impact of the security policy of your organization on the troubleshooting process.

Write down the most important lesson that *you* learned from this lab:

Summary of Lab 6-2

This lab provided you with an opportunity to practice structured troubleshooting of problems related to specialized security features embedded in the Cisco IOS Software running on routers and switches.

Lab 6-2: Cisco IOS Security Features

This lab focused on troubleshooting problems related to specialized Cisco IOS Software security features.

- Problems that were encountered:
 - Ports being disabled by switch security features
 - DHCP being blocked by DHCP snooping and VLAN maps
 - Cisco IOS stateful packet inspection configuration issues
- Lessons that were learned:
 - Implementation of security features adds an extra layer of complexity to the network, which complicates troubleshooting.
 - It is vital to know which security features have been implemented at each point in your network.

Review: What is the most important lesson that you learned from this lab?

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0—7-16

This lab revolved around a number of specialized security features that are available on routers and switches.

The following problems were encountered:

- Various problems caused by switch protection features such as DHCP snooping, port security and root guard erroneously disabling ports on switches
- Configuration errors in the Cisco IOS stateful packet inspection feature causing traffic to be dropped

A major lesson that can be learned from this lab is that the deployment of security features in the infrastructure adds an extra layer of complexity to the network and that for efficient troubleshooting it is vital that you know exactly which features are implemented at each point in the network.

Write down the most important lesson that *you* learned from this lab:

Introduction to Lab 7-1

This topic describes the guidelines and background information that is needed to start the capstone lab, Troubleshooting Complex Environments, successfully.

Lab 7-1: Troubleshooting Complex Environments

This lab serves as a capstone lab and covers all aspects of network troubleshooting.

The lab will be scored to measure your performance and compare it against the performance of your peers.

Elements of the score:

- Result: Resolution of the reported problem
- Solution: Addressing the root cause of the problem
- Solution: Compliance with the documented design and policies
- Process: Followed troubleshooting method and procedures
- Timing: Time taken to resolve the problem
- Multiplier: Weighting factor based on the difficulty and urgency of the problem

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0—7-17

This lab allows you to practice all the network maintenance and troubleshooting skills that you have acquired in earlier modules. Instead of focusing on a specific area of technology, problems in this lab are taken from various different technology areas, including technologies that have not been covered previously. This lab allows you to practice all the skills that you would need when troubleshooting a complex enterprise network.

Your performance in the lab is scored on several aspects. The scoring serves two purposes. First, it allows you to measure your performance and compare your performance to the performance of your peers. Secondly, it adds a sense of time pressure to the trouble tickets to make them resemble real-life troubleshooting scenarios more closely.

The labs will be scored on the following aspects:

- **Result:** The problems in the trouble tickets are reported from the perspective of an end user who cannot accomplish a certain task. For instance, a problem could be reported as: “The user on client PC CLT1 cannot browse to <http://www.isp3.local>.” When you manage to restore the connectivity for this user and ensure that the user can browse to <http://www.isp3.local>, you will score points for the corresponding “Result” section of the trouble ticket. The method you used to accomplish this objective is not taken into account for this specific section. The result is measurable and the objective is clearly defined in the “Activity Verification” section for the trouble ticket in the lab guide.
- **Solution:** You need to provide your change log and troubleshooting log to the instructor who will check to see if you implemented a true solution and your changes addressed the root cause of the problem or if you only implemented a workaround, which resolves the symptoms, but not the root cause.

- **Solution:** Based on your change log, the instructor will also judge if the changes that you made comply with the policies that are set down in the documentation that accompanies the trouble tickets.
- **Process:** The instructor will review your troubleshooting log to assess how well you have documented your process. The main factor that your logs are judged on is if they contain sufficient information to escalate the problem to another engineer without losing essential information. Secondly, the logs are used to verify if you have taken the steps that are essential to any troubleshooting or maintenance process, such as creating backups and ensuring that you can roll back if necessary. The instructor may perform checks on your equipment to verify the steps that are documented in your logs.
- **Timing:** You receive points for the time you need to implement a workaround or solution. For each extra half hour that you need to achieve the objectives in the “Result” sections, a point is subtracted from your score. Note that it is the “Results” section that counts for the score, not the “Solution” section. In other words, if you manage to restore connectivity for the user through a workaround and implement a real solution later, the time that the workaround was implemented and demonstrated is the time that determines the score.
- **Multiplier:** Each trouble ticket has a multiplier, which represents the combined difficulty and urgency of the problems in relation to the other tickets. The multiplier determines the total number of points that can be scored for the exercise and should be taken into account during your troubleshooting process to optimize your score.

There are four trouble tickets and one network maintenance task. For each of these, the score consists of the elements mentioned above. The maximum total score for each of the tasks ranges between 150 and 250 points and the maximum total points that can be scored is 1000 points.

Lab 7-1: Lab Procedure

To have your lab scored, follow this procedure:

- Notify the instructor when your team has accomplished the objectives stated in the “Activity Verification” section of a trouble ticket.
 - Demonstrate that the solution of your team meets the stated objectives.
 - Hand in your team's troubleshooting and change logs for the ticket.
- The instructor verifies if your solution and the method you followed meet the objectives and then determines the score.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—7-8

To have one of the five lab sections (trouble ticket or maintenance task) scored, you should contact the instructor when your team has met the objectives stated for the task in the “Activity Verification” section of the lab. You have to demonstrate your solution and hand in your team's process logs and change logs for the ticket, and the instructor will determine the score for this section. Points for timing are based on the time at which you contact the instructor to have the lab scored.

Points that are lost cannot be regained later, so carefully check to verify that you have met the stated objectives before calling over the instructor to score a lab section.

Lab 7-1: Lab Procedure (Cont.)

- No points can be gained for a ticket after it has been scored.
 - Exception: If you implemented a workaround to resolve the reported problem, you can ask the instructor to rescore the lab after you have implemented a solution that addresses the root cause. In this case you will not lose the points for timing.
- During the lab debrief the final score is determined.
 - Points are lost for any objective that is no longer met at the end of the lab.
- **Caution:** Do not look at the lab answer key or debrief lesson before the end of the lab. This action will invalidate your score and deprive you and your team of an important opportunity to assess your skills.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOTv1.0—7-9

There is one exception to the rule that points cannot be gained later. If you have implemented a workaround and you meet the objectives for the “Results” items, you can ask the instructor to score this section of the lab. If you implement a solution later, you can gain the points for the “Solution” item without changing the points for the “Timing” item.

The final score is determined at the end of the lab. Points can be lost if the stated objectives for a section are no longer met. For example, if a change that is made while troubleshooting Trouble Ticket D causes the required connectivity for Trouble Ticket A to fail, you will lose those points for Trouble Ticket A.

Caution	The answers to the problems are provided in the answer key in the lab guide and discussed in the lab debrief lesson in this module. Looking at these answers will invalidate your score and you and your teammates will lose an important opportunity to assess your skills.

Documentation

Where can you find documentation to guide you during the lab?

- Documentation of the lab topology and other aspects of its design and implementation are available in the lab guide at the beginning of the lab.
- The **Sample Troubleshooting Flows** section of the lab guide contains directions and sample command output to help you troubleshoot specific technology areas.
- Detailed information about command output and configuration options can be found in the command references on <http://www.cisco.com>.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--7-20

The lab environment is similar, but not identical, to the environment that you have experienced in the previous labs. The major differences in the physical, logical, and routing design have been documented in the lab guide at the beginning of Lab 7-1.

For guidelines about troubleshooting specific technology areas and sample command output, refer to the Sample Troubleshooting Flows sections of the previous modules. Because no new technology areas are introduced in this module, no additional sample flows were added as part of Lab 7-1.

For further documentation about commands and technology, you can use any online documentation that you would also use in your job. Detailed information about command output and configuration options can be found in the command references on <http://www.cisco.com>.

Questions?

If you have questions about the interpretation of the lab instructions, trouble ticket texts, or about the network design guidelines and policies, ask your instructor for clarification.

Final questions: Do you have any questions before starting the lab?

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0—7-2

During the lab, you can ask the instructor for clarification if you find certain aspects of the trouble ticket texts, lab instructions, or the network design and policies to be unclear. The instructor will help you interpret the directions, but will not provide hints or solutions to the problems until after you have finished the lab.

Like the previous labs, this lab is a team exercise and if one of the team members is stuck on a particular problem, it is up to the team to resolve the problem and for team members to help each other.

If you have any questions about the lab procedures, scoring, documentation, or other aspects of the lab you should ask the instructor for clarification now.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- You have assessed and consolidated the lessons learned during the course labs.
- You are fully prepared to start the capstone lab.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—7-22

Lab 7-1 Debrief

Overview

In this lab, you practiced troubleshooting various network problems in a complex environment. You also created a troubleshooting plan to coordinate the work between the team members. You methodically researched the problems, kept a log of your actions and findings, and resolved the problems and documented your solutions. In addition, you worked under time pressure to optimize your results, solutions, and process. You were scored to measure your performance.

During the lab debrief, the instructor will lead a group discussion during which you can present your solutions. You will have an opportunity to verify your solution against a number of checkpoints provided by the instructor and compare your solution to the solutions of other students. The instructor will discuss alternate solutions and their advantages and disadvantages. You will also receive your team score for the lab and you will have an opportunity to learn how your performance was assessed.

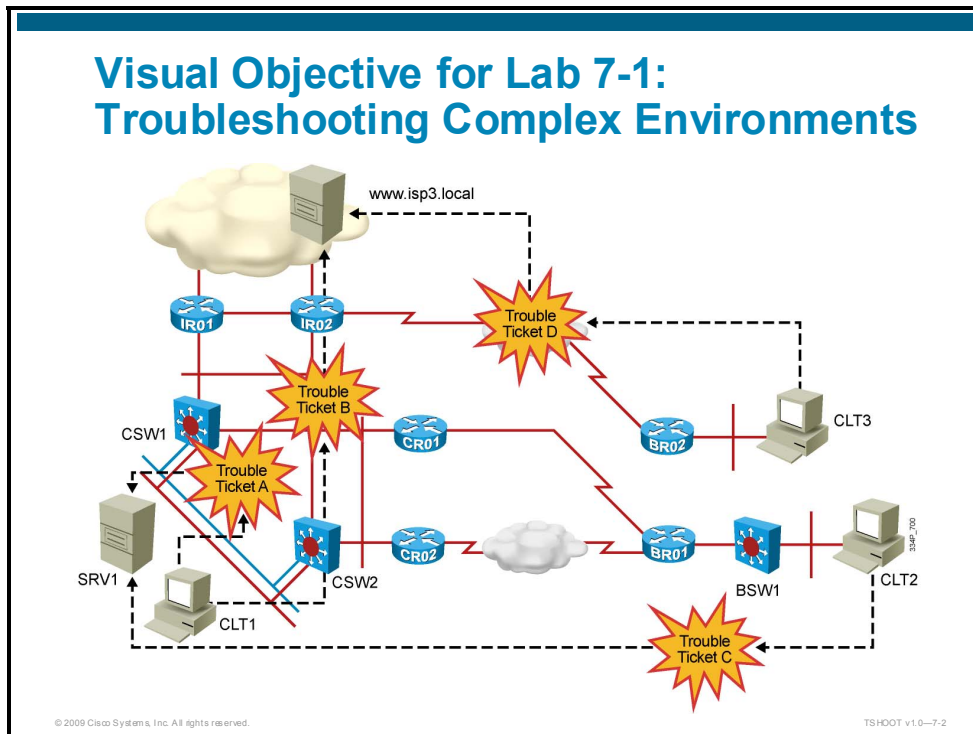
Objectives

Upon completing this lesson, you will be able to diagnose and resolve network problems in a complex environment using a structured, methodical approach. This ability includes being able to meet these objectives:

- Compare your solution, findings, and action log against a set of checkpoints provided by the instructor and identify common and alternate solutions
- Consolidate the lessons that you learned during the review discussions into a set of best practice methods and commands to aid you in future troubleshooting procedures

Review and Verification

This topic describes the problems that were introduced in Lab 7-1, asks how you can verify that you have solved the problems, and gives an example of a troubleshooting process that will allow you to find and resolve the issues.



This lab consisted of five distinct parts: four trouble tickets and a network maintenance task. Each of the trouble tickets revolved around a specific reported connectivity problem that should be diagnosed and resolved, while the maintenance task was more generic and prompted you to verify several aspects of the network operation and proactively find and prevent potential problems.

Each of the trouble tickets has clearly defined completion criteria and after the resolution of a trouble ticket, your results were evaluated and points were based on how well you performed on various aspects of the troubleshooting process. Points could also be scored for successful completion of the maintenance task.

In this topic, solutions to the problems will be discussed, in addition to other aspects of the trouble tickets, such as planning, communication, time management, and documentation. The instructor will also present the final scores of each of the teams.

Your team score gives you an indication of how well your team performed relative to the other teams. The scoring also serves the purpose of introducing the aspect of time pressure to the lab. However, the focus of the discussion in this lesson should not be on the scores themselves, but on what you can learn from your experience and the experience of the other teams. What made the approach of certain teams more effective than other teams? What would you do differently next time? Which tools and commands did you discover that could have allowed you to troubleshoot more efficiently?

Planning Troubleshooting

How did your team approach the lab?

- Did you troubleshoot all tickets in parallel, in sequence, or did you use a combination of methods?
- What was your strategy to optimize your score?
- What process did you use to make optimal use of the knowledge and experience of the individual team members?
- How did you assign problems and coordinate device access among your team members?
- Did you establish an escalation process in your team?
- How did you communicate with your team members?
- How did you manage your time?
- Did you lose any points because of flaws in your plan, team coordination, or communication processes?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-7-3

Note

This lesson provides sample answers and solutions to the questions posed during the debrief discussions. Remember that alternate solutions and methods may be just as valid and that the solutions provided here only highlight a sample approach and solution. The instructor will reward correct alternate solutions and processes in the same manner as the solutions that are presented here. If you did not get the score that you expected for an item, ask your instructor why your solution or process was not considered correct.

The score your team receives for this lab does not depend on just the technical ability of the individual team members. The score also depends greatly on the ability of your team to use the knowledge, skills, and experience of your team members in an effective and efficient manner.

Time management plays an important role in this lab. You specifically gain points for quickly restoring connectivity in each ticket, but you also gain more points by fully completing two tickets, than by working on four, but not completing any of them.

In addition, implementing a last minute change to score an extra point may actually cause you to lose other points because your last minute change could affect the connectivity in other parts of the network. Once you have successfully restored connectivity for one of the trouble tickets, you should ensure that you do not lose the points in a later stage because you made changes in one ticket and you did not verify its effects on other tickets.

Assigning trouble tickets to different team members and troubleshooting the tickets in parallel is likely to be the most efficient approach. However, given the difficulty level of some of the problems in this lab, it is worthwhile to establish escalation procedures within your team, to hand over a problem to a different team member if you are unable to solve the problem and do not know how to proceed. It may be more efficient to hand over a problem to a specialist and start working on a different problem than to keep struggling, especially if some of your team members have particular areas of expertise.

Coordination and communication processes are very important to your success in this lab. Review your team processes with your team members to see how you could have improved your process and learn from the other teams how they optimized their team processes.

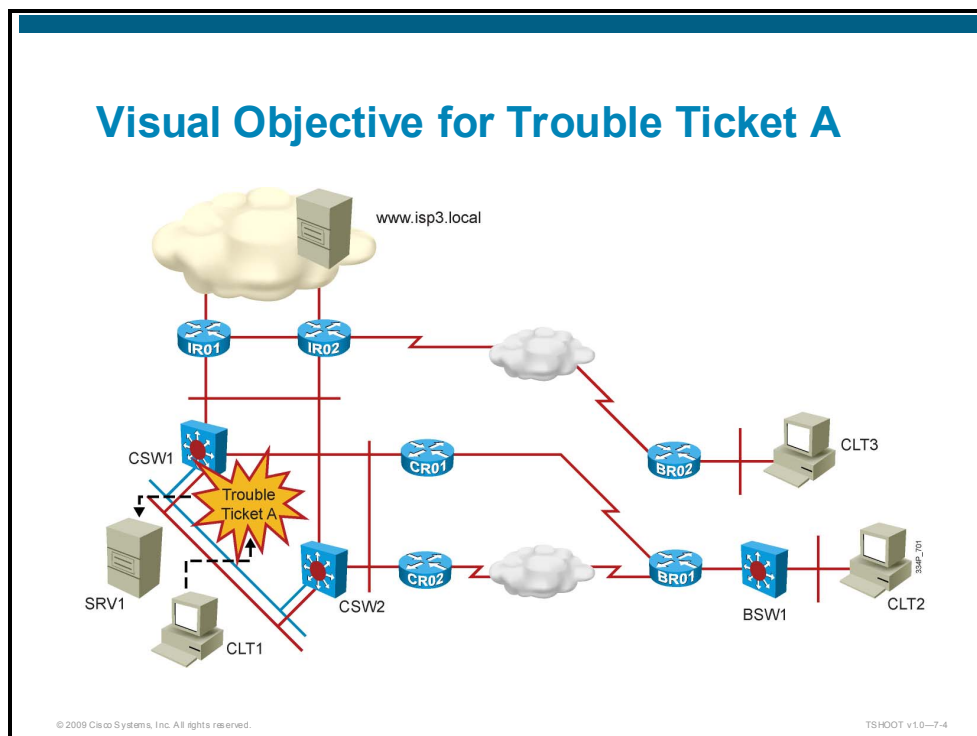
A sample plan to approach this lab for a team of three could be the following:

- Team member 1 will start with Trouble Ticket A. Team member 1 is in control of switches ASW1, CSW1, and CSW2. Any changes or other disruptive actions on these switches by other team members can only be performed with the permission of team member 1.
- Team member 2 will start with Trouble Ticket D. Team member 2 is in control of routers BRO2, IRO1, and IRO2. Any changes or other disruptive actions on these routers by other team members can only be performed with the permission of team member 2.
- Team member 3 will start with Trouble Ticket C. Team member 2 is in control of switch BSW1 and routers BRO1, CRO1, and CRO2. Any changes or other disruptive actions on these devices by other team members can only be performed with the permission of team member 3.
- Any information discovered by one of the team members that may affect a ticket of another team member should be communicated to that team member.
- Any changes made by one of the team members that may affect a ticket of another team member should be coordinated with that team member.
- After one hour, the team will assess the overall progress and adapt the plan if necessary.
- When one of the team members finishes a ticket, that team member will first check to see if it is possible to help the other team members to complete their tickets. If it is not possible for the team member to help other members, then the team member that has finished will start on Trouble Ticket B. Device access is coordinated with the other team members as necessary.
- After another hour, the overall progress will be assessed again and the plan may be adapted.
- When another team member finishes a ticket, that team member will first see if it is possible to help the other team members complete their tickets. If it is not possible for the team member to help other members, then the team member that has finished will start planning the maintenance tasks and work on them.
- After two and a half hours, with half an hour left, the team will again assess the status and establish a plan to optimize the score. From this point on there should be a rollback plan for any change. If a change affects the status of a completed ticket, the change will be rolled back to preserve the points scored for that ticket.

Note	Some of the problems that were introduced in the lab affect multiple tickets. In this lesson, the tickets are covered sequentially. As a result, some of the suggested changes for one of the tickets may actually have been made in a different ticket during your troubleshooting process. This will not affect the score for any of the individual tickets, because the scores are based on results, not on configuration.

Trouble Ticket A: No Connectivity from CLT1 to SRV1

The following figure shows the visual objective for the trouble ticket.



The text introducing this trouble ticket is as follows:

The user at headquarters who uses client PC CLT1 on VLAN 17 has complained that he cannot use the file services on server SRV1.

Your task is to restore connectivity from client PC CLT1 to server SRV1 and ensure that the user can view the directory “\\SRV1\\Public” and upload a file to it.

Trouble Ticket A: Review and Discuss

How did your team approach Trouble Ticket A?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems, and if so, how?
- Did you accomplish the goal of restoring the connectivity between client PC CLT1 and server SRV1?
- How long did it take to restore the connectivity?
- Did you implement a workaround at any point or did you find and implement the solution directly?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—7-5

The loss of connectivity between client PC CLT1 and server SRV1 is caused by a configuration mismatch between the physical interfaces (FastEthernet 0/3 and FastEthernet 0/4) and the port-channel interface (Port-channel 10) on switch CSW1. The allowed VLAN list is not configured on the physical interfaces, but it is configured on the port-channel interface. This configuration causes the physical interfaces to be suspended on switch CSW1 and, as a result, the EtherChannel between the switches CSW1 and CSW2 is down.

This issue affects the connectivity between client PC CLT1 and server SRV1: Client CLT1 uses switch CSW2 as its default gateway because CSW2 is the active router on VLAN 17 for the Hot Standby Router Protocol (HSRP). However, because of the problem with the EtherChannel to switch CSW1, switch CSW2 cannot forward its packets to CSW1 and on to server SRV1 on VLAN 112.

Although there are many possible methods that you could use to solve this problem, the following list provides an example of a troubleshooting log to show you a methodical approach that can be used to resolve this problem.

Device	Actions and results
CLT1	Verify problem: Ping to SRV1 fails. The name SRV1 cannot be resolved. Ping to IP address 10.1.152.1 also fails.
CLT1	An IP address is successfully acquired via DHCP from 10.1.128.124 (CSW1).
CLT1	A ping to the default gateway 10.1.128.126 succeeds.
CSW1	CSW2 (10.1.128.125) is the active HSRP router for VLAN 17. CSW1 is standby.
SRV1	A ping to the default gateway 10.1.152.254 succeeds.
CSW1	CSW1 is the active HSRP router for VLAN 112. No standby router is recorded.
CSW2	CSW2 is the active HSRP router for VLAN 112. No standby router is recorded.
	Conclusion: HSRP is not operating correctly on VLAN 112.
CSW2	Ping to 10.1.152.252 (CSW1 on VLAN 112) fails.
CSW1 and 2	Verify IP address and mask for interface VLAN 112: Correctly configured.
CSW1 and 2	Verify spanning tree for VLAN 112: Port-channel 10 is not listed on CSW1.
CSW1	Interface Port-channel 10 is down. The associated physical interfaces FastEthernet 0/3 and 0/4 are marked as "down (suspended)."
CSW1	The show etherchannel 10 detail command reveals "Probable reason: vlan mask is different."
CSW1	Compare configuration of interfaces Port-channel 10 and FastEthernet 0/3 and 0/4: An allowed VLAN list is configured on the port-channel interface, but not on the physical interfaces.
CSW2	Compare configuration of interfaces Port-channel 10 and FastEthernet 0/3 and 0/4: An allowed VLAN list that is identical to the list on Port-channel 10 of CSW1 is configured on all interfaces. Conclusion: The policy for the network must be to use an allowed VLAN list to prune VLANs off the trunks.
CSW1	Configuration changed: Added allowed VLAN list to interfaces FastEthernet 0/3 and 0/4. Both pre- and post-change configurations were saved in flash on the switch. Communicated this information to team members.
CLT1	Ping to SRV1 succeeds. File transfer to \\SRV1\\Public succeeds.
	Problem fixed. Documented changes. Backed up configurations.
	Notified instructor and demonstrated successful file copy. Closed ticket.

Primary Clue: show etherchannel detail

- The **show etherchannel detail** command reveals the reason that the physical links in the EtherChannel were suspended.

```
CSW1#show etherchannel 10 detail
Group state = L2
Ports: 2    Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol:    -
Minimum Links: 0
      Ports in the group:
      -----
Port: Fa0/3
-----

Port state      = Up Cnt-bndl Suspend Not-in-Bndl
Channel group = 10          Mode = On          Gchange = -
Port-channel   = null       GC      = -         Pseudo port-channel = Po10
Port index     = 0          Load = 0x00        Protocol = -

Age of the port in the current state: 0d:18h:10m:19s

Probable reason: vlan mask is different
<...further output omitted...>
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-7-6

A straightforward Layer 3 and Layer 2 troubleshooting process should quickly lead you to the conclusion that the connectivity problem between client PC CLT1 and server SRV1 is caused by the failure of the EtherChannel between switches CSW1 and CSW2.

To diagnose the root cause of this failure, the command **show etherchannel detail** provides an important clue. It lists “vlan mask is different” as the probable reason for the suspension of interfaces FastEthernet 0/3 and 0/4.

Even without this clue, you should realize that suspension of an interface that is participating in an EtherChannel is commonly caused by mismatches in configuration, either between the physical interfaces and the port-channel interface on a switch, or between the two switches that participate in the EtherChannel.

Comparing the configuration of the interfaces involved shows that the allowed VLAN list is missing on interfaces FastEthernet 0/3 and 0/4.

Trouble Ticket A: Checkpoints and Scoring

Scores for this ticket are based on the following checkpoints:

- **Result (10 points):** Client PC CLT1 can transfer a file to the directory “\\SRV1\Public”.
- **Solution (5 points):** You have addressed the root cause or causes of the problem, not implemented a workaround.
- **Process (5 points):** You have clearly documented your process, your solution, and any changes that you have made to the device configurations.
- **Timing (5 points):** You have restored connectivity in a timely manner.

Total possible points for this ticket: $25 \times 6 = 150$ points.

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0-7.7

Points for this topic are scored based on the checkpoints shown in the preceding figure.

To prove that connectivity between client PC CLT1 and server SRV1 has been restored, you should demonstrate to the instructor that you can successfully transfer a file to the directory “\\SRV1\Public” from client PC CLT1. It should still be possible to demonstrate the restored connectivity at the end of the lab. If you are not able to demonstrate connectivity, you lose the points for this section.

If the changes that you implemented have restored the EtherChannel between switches CSW1 and CSW2, this restoration is considered a solution, because the root cause of the problem was addressed. If your changes restored connectivity between client PC CLT1 and server SRV1, but the EtherChannel between switches CSW1 and CSW2 is not operational, this fix is considered a workaround and points are scored for the “Result” section, but not for the “Solution” section.

A possible workaround to restore the connectivity between client PC CLT1 and server SRV1 would be to increase the HSRP priority for standby group 17 on switch CSW1. This workaround will cause switch CSW1 to become the default gateway for VLAN 17 and traffic between client CLT1 and server SRV1 will be Layer 3 switched locally on switch CSW1 without having to traverse the EtherChannel between switches CSW1 and CSW2.

The multiplier that indicates the difficulty level and urgency for this ticket was determined to be 6. As a result, the maximum possible score for this ticket is $25 \times 6 = 150$ points.

Suggested Solution

Correcting the configuration of switch CSW1 as follows can restore the connectivity from client PC CLT1 to server SRV1.

Suggested Configuration Changes

- On switch CSW1 configure the same allowed VLAN list on interfaces FastEthernet 0/3 and 0/4 that is also configured on interface Port-channel 10.

```
CSW1 (config) #interface range FastEthernet 0/3 - 4
CSW1 (config-if-range) #switchport trunk allowed vlan 17-19,21-23,25-27,33-35,37-39
CSW1 (config-if-range) #switchport trunk allowed vlan add 41-43,111,112,128-130
```

© 2009 Cisco Systems, Inc. All rights reserved.

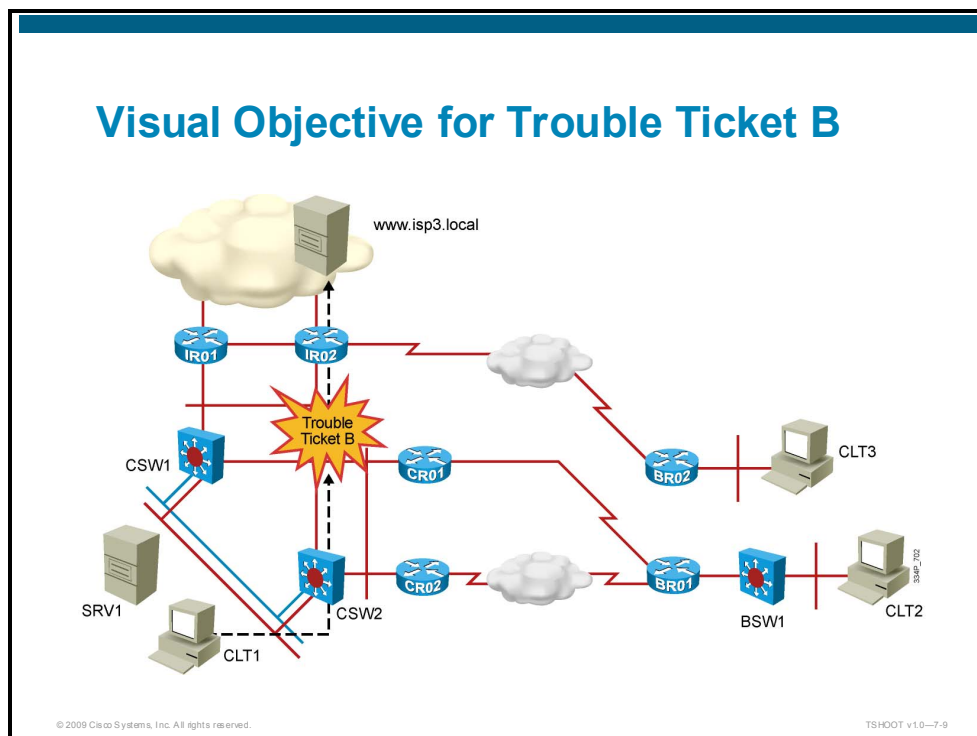
TSHOOT v1.0-7-8

To address the root cause of this problem you should restore the EtherChannel between switches CSW1 and CSW2. This restoration can be achieved by adding the allowed VLAN list to the interfaces FastEthernet 0/3 and 0/4 on switch CSW1.

If you have removed the allowed VLAN list from interface Port-channel 10 on switch CSW1 to restore the EtherChannel, this change is also considered a solution, because the root cause is addressed. However, this change does not comply with the established policies on the network because allowed VLAN lists are configured on all other trunks between the switches. As a result, you will lose points for policy compliance in the Network Maintenance section of this lab.

Trouble Ticket B: No Internet Access from CLT1

The following figure shows the visual objective for the trouble ticket.



The text introducing this trouble ticket is as follows:

Many users on the network are experiencing problems when accessing the Internet. You have a report from an office user, who uses client PC CLT1, claiming that he cannot browse to <http://www.isp3.local> (172.34.224.1).

Your task is to restore the connectivity from client PC CLT1 to the Internet and ensure that the user can connect to the site <http://www.isp3.local> using a web browser.

Trouble Ticket B: Review and Discuss

How did your team approach Trouble Ticket B?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems, and if so, how?
- Did you accomplish the goal of restoring the connectivity between client PC CLT1 and the Internet?
- How long did it take to restore the connectivity?
- Did you implement a workaround at any point during the resolution of this ticket?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--7-10

Two main problems cause the loss of connectivity in this lab.

One problem is that the system maximum transmission unit (MTU) and the routing system MTU on switch CSW2 have been increased to a value of 1512 instead of the default of 1500 bytes. This setting prevents establishment of Open Shortest Path First (OSPF) adjacencies between switch CSW2 and its neighbors. Because switch CSW2 is the HSRP active router for VLAN 112 and VLAN 17, this issue causes any traffic from server SRV1 and client PC CLT1 that needs to be routed to other routers to fail.

After this problem has been resolved, a second issue causes traffic to the Internet to fail. Router CRO2 has been configured with the same OSPF router ID as router IRO2. Because these routers are not in the same area (router IRO2 is in area 10.1.192.0 and router CRO2 is in area 0.0.0.0) this issue does not cause an immediate conflict. The problem with the Internet connectivity is caused by the two routers engaging in an “OSPF flood war” over the external link-state advertisement (LSA) for the default route.

Router IRO2 generates a type-5 external LSA for the default route and floods this to all other routers. When router CRO2 receives this LSA, it recognizes its own router ID as the originator of the LSA and, because it is not generating a default route itself, it concludes that this is old information and it sends out an LSA for the default route set to the maximum age to flush it out of the database. When router IRO2 receives this LSA, it regenerates the LSA because it thinks that the default route should be advertised, not flushed. The cycle repeats itself and this causes the default route to flap continually in the routing tables of the other routers. Secondly, even when the default route is present, traffic will be sent to both router IRO2 and router CRO2 because both routers claim to be the router with router ID 10.1.220.4. As a result, occasional packets may be routed to the Internet, but a very large part of the traffic is dropped and connectivity is only possible intermittently, if at all.

This ticket is hard to troubleshoot, because the network is not stable and the results of **show** commands will be different depending on the state of the network when the commands are executed. The following list provides an example of a troubleshooting log to show you a methodical approach that can be used to resolve this problem. Be aware that you may not be able to reproduce the exact results of this log because of the instability on the network.

Device	Actions and results
CLT1	Confirm problem: Cannot browse or ping to www.isp3.local. Name resolution fails.
CLT1	Ping to 172.34.224.1 fails: "Reply from 10.1.128.125: destination host unreachable."
CSW2	No default route present in the routing table.
CSW2	No other routes than directly connected routes available in routing table.
CSW2	No fully established OSPF neighbors are presented. All neighbors are in state DOWN, INIT or EXSTART.
CSW2	The debug ip ospf adj command shows "Nbr 10.1.220.252 has smaller interface MTU" and "Killing nbr 10.1.220.252 on Vlan130 due to excessive (25) retransmissions."
CSW2	MTU is 1512 bytes on all interfaces (?). Attempt to change MTU or IP MTU on VLAN interface fails. Attempt to change MTU on physical interfaces also fails.
	Research MTU on Cisco Catalyst 3560 Switches: MTU can only be configured systemwide.
CSW2	The show system mtu command reveals that the system MTU is set to 1512.
CSW1 and ASW1	System MTU is 1500 bytes. Review implementation guidelines: MTU is not mentioned. Conclusion: System MTU should be 1500 on all switches.
CSW2	Configuration changed: Changed system MTU to 1500. Communicated this information to team members and coordinated necessary reload. Reloaded CSW2.
CSW2	After the reload, all OSPF neighbors are fully established and the default route is present in the routing table.
CLT1	Browsing to http://www.isp3.local still fails. Ping to 172.34.224.1: Requests alternately fail and succeed.
CSW2	Default route flaps in routing table. The debug ip routing command reveals that the route is added and then deleted after approximately five seconds and then added again after approximately five seconds, and then deleted again, and so on.
CSW2	Sequence number of the external LSA for the default route generated by 10.1.220.4 (IRO2) rapidly increases. The LSA seems to be alternately aged out and then regenerated.
IRO2	The debug ip ospf lsa-generation command reveals that LSA for the default route is regenerated every 10 seconds. It also reveals that the LSA for 10.1.94.8 is flushed (age set to 3600) every 10 seconds. In addition, the log shows "%OSPF-4-FLOOD_WAR: Process 1 re-originates LSA ID 0.0.0.0 type-5 adv-rtr 10.1.220.4 in area 10.1.192.0."
	Research OSPF Flood War: Would a duplicate router ID cause this?
	Subnet 10.1.94.8 is the link between CRO2 and BRO1.
CRO2	The log on CRO2 also contains %OSPF-4-FLOOD_WAR messages. This router does the opposite of what router IRO2 does: it flushes the default route and reoriginates 10.1.194.8.
CRO2	Verify router ID: Router ID is configured as 10.1.220.4, which is the same as IRO2. This IP address belongs to the loopback interface of IRO2. Need to change router ID on this router.
CRO2	Configuration changed: Changed router ID to loopback IP address 10.1.220.2 and reset OSPF process. Both pre- and post-change configurations were saved in flash on the switch. Communicated this information to team members.
CSW2	Default route is stable now.
CLT1	Ping to 172.34.224.1 succeeds.
CLT1	Browsing to http://www.isp3.local succeeds.
	Problem fixed. Documented changes. Backed up configurations.
	Notified instructor and demonstrated successful browsing to http://www.isp3.local. Closed ticket.

Primary Clue: MTU Mismatch Causing DBD Retransmissions

- Running the **debug ip ospf adj** command on switch CSW2 reveals that a smaller MTU is used by router CSW1.

```
*Feb 28 17:11:07.222 PST: OSPF: Rcv DBD from 10.1.220.252 on Vlan130 seq
0x17C6 opt 0x52 flag 0x7 len 32 mtu 1500 state EXSTART
*Feb 28 17:11:07.222 PST: OSPF: Nbr 10.1.220.252 has smaller interface MTU
*Feb 28 17:11:07.230 PST: OSPF: Send DBD to 10.1.220.252 on Vlan130 seq
0x1DE3 opt 0x52 flag 0x7 len 32
*Feb 28 17:11:07.230 PST: OSPF: Retransmitting DBD to 10.1.220.252 on Vlan130
[25]
*Feb 28 17:11:12.239 PST: OSPF: Killing nbr 10.1.220.252 on Vlan130 due to
excessive (25) retransmissions
*Feb 28 17:11:12.239 PST: OSPF: 10.1.220.252 address 10.1.192.25 on Vlan130
is dead, state DOWN
*Feb 28 17:11:12 PST: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.220.252 on Vlan130
from EXSTART to DOWN, Neighbor Down: Too many retransmissions
```

- The same debug command also reveals that this issue apparently causes excessive DBD retransmissions.
- As a result, the adjacency never transitions beyond the EXSTART state.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—7-11

The clearest hint that you can get that the failing OSPF adjacencies on switch CSW2 are caused by an MTU mismatch is found by enabling the command **debug ip ospf adj** on switch CSW2. This command reveals clearly that the neighbors, such as switch CSW1 in the example shown in the figure, are using a smaller MTU than switch CSW2. It further shows that the adjacencies with the other neighbors do not transition beyond the EXSTART state, because the database description (DBD) packets are apparently not properly exchanged and need to be retransmitted. Although the debug command does not explicitly state that the retransmissions are caused by the MTU mismatch, there is a strong suggestion that there is at least a correlation between these two facts, and this correlation makes it worthwhile to investigate further.

Primary Clue: Default Route Is Flapping

- The sequence number for the LSA associated with the default route is steadily increasing and the LSA is alternately advertised and deleted.

```
CSW2#show ip ospf database external 0.0.0.0
<... output omitted ...>
LS age: 6
Options: (No TOS-capability, DC)
LS Type: AS External Link
Link State ID: 0.0.0.0 (External Network Number )
Advertising Router: 10.1.220.4
LS Seq Number: 800001FF
<... output omitted ...>

CSW2#show ip ospf database external 0.0.0.0
<... output omitted ...>
Delete flag is set for this LSA
LS age: MAXAGE(3600)
Options: (No TOS-capability, DC)
LS Type: AS External Link
Link State ID: 0.0.0.0 (External Network Number )
Advertising Router: 10.1.220.4
LS Seq Number: 80000200
<... output omitted ...>
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--7-12

The problem of the duplicate OSPF router IDs on routers IRO2 and CRO2 is hard to find. The first clue that you get is the fact that the routing table is not stable. The default route is continually disappearing and reappearing from the routing tables in all routers. The default route is generated based on an OSPF type-5 external LSA generated by router IRO2. For this LSA the same behavior is observed. The sequence number of this LSA is steadily increasing and alternately the LSA is generated and deleted.

One explanation for this behavior would be that the default route on router IRO2, which is learned via the Border Gateway Protocol (BGP), is flapping. Therefore, you should connect to router IRO2, which is the source of the LSA, to investigate this problem further.

Primary Clue: OSPF Flood War

- Running the **debug ip ospf lsa-generation** command on router IRO2 reveals that the LSA for the default route is re-originated every ten seconds, while the LSA for 10.1.194.8/30 is repeatedly flushed.

```
May 14 07:47:12 PDT: %OSPF-4-FLOOD_WAR: Process 1 re-originates LSA ID
0.0.0.0 type-5 adv-rtr 10.1.220.4 in area 10.1.192.0
May 14 07:47:12.200 PDT: OSPF: Generate external LSA 0.0.0.0, mask 0.0.0.0,
type 5, age 0, metric 1, tag 1, metric-type 2, seq 0x80000255
May 14 07:47:12.224 PDT: OSPF: Generate external LSA 10.1.194.8, mask
255.255.255.252, type 5, age 3600, metric 16777215, tag 0, metric-type 2, seq
0x80000300
May 14 07:47:21.708 PDT: OSPF: Generate external LSA 0.0.0.0, mask 0.0.0.0,
type 5, age 0, metric 1, tag 1, metric-type 2, seq 0x80000257
May 14 07:47:22.036 PDT: OSPF: Generate external LSA 10.1.194.8, mask
255.255.255.252, type 5, age 3600, metric 16777215, tag 0, metric-type 2, seq
0x80000302
May 14 07:47:31.232 PDT: OSPF: Generate external LSA 0.0.0.0, mask 0.0.0.0,
type 5, age 0, metric 1, tag 1, metric-type 2, seq 0x80000259
May 14 07:47:31.260 PDT: OSPF: Generate external LSA 10.1.194.8, mask
255.255.255.252, type 5, age 3600, metric 16777215, tag 0, metric-type 2, seq
0x80000304
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-7-13

As it turns out, the default route on IRO2 itself is stable in the routing table and does not flap. Therefore, there must be another reason that causes the LSA to be continually regenerated and flushed by router IRO2. The command **debug ip ospf lsa-generation** can be used to monitor the generation of LSAs and in this case, it yields a number of useful clues regarding what happens. Even without the debug command enabled, there is a log message that states “%OSPF-4-FLOOD_WAR: Process 1 re-originates LSA ID 0.0.0.0 type-5 adv-rtr 10.1.220.4 in area 10.1.192.0.” To begin with, this message confirms that this router is repeatedly regenerating the LSA for the default route. Secondly, the term “flood war” hints that there is some sort of race condition on the network. The output of the debug shows more clearly what is happening. It shows that the LSA for the default route is regenerated approximately every 10 seconds.

This command also yields an important hint, which points to the source of the problem. While this router is regenerating the LSA for the default route, at the same time, it is flushing a different LSA every 10 seconds. This is the LSA for network 10.1.194.8/30. This subnet is associated with the link between router CRO2 and router BRO1 (which is not running OSPF). This strongly suggests that router CRO2 may be the other party engaged in the “OSPF flood war.” Researching the “%OSPF-4-FLOOD_WAR” system message should give you an indication that a duplicate router ID may be causing the symptoms observed. After verification of the router ID on router CRO2, the root cause of the problem is revealed: router CRO2 has the same configured router ID as router IRO2.

Trouble Ticket B: Checkpoints and Scoring

Scores for this ticket are based on the following checkpoints:

- **Result (6 points):** Client PC CLT1 can ping IP address 172.34.224.1.
- **Result (4 points):** Client PC CLT1 can browse to `http://www.isp3.local`.
- **Solution (5 points):** You have addressed the root cause or causes of the problem, not implemented a workaround.
- **Process (5 points):** You have clearly documented your process, your solution, and any changes that you have made to the device configurations.
- **Timing (5 points):** You have restored connectivity in a timely manner.

Total possible points for this ticket: $25 \times 10 = 250$ points.

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0-7-14

Points for this topic are scored based on the checkpoints shown in the preceding figure.

To prove that connectivity between client PC CLT1 and the Internet has been restored, you should demonstrate to the instructor that you can browse to `http://www.isp3.local`. However, because DNS problems may prevent this, even if there is IP connectivity from client PC CLT1 to the IP address of `www.isp3.local` 172.34.224.1, partial points are awarded for being able to ping to IP address 172.34.224.1. For both “Result” items, it should still be possible to demonstrate this result at the end of the lab. If you are not able to demonstrate this result at that time, you lose the points for this section.

If the changes that you implemented have eliminated the MTU mismatch between switch CSW2 and its neighbors and you have ensured that all routers in the OSPF network have unique router IDs, your changes would be considered a solution because the root causes of the problems were addressed. If your changes restored connectivity between client PC CLT1 and server `www.isp3.local` without addressing the MTU mismatch or the duplicate router IDs, your changes would be considered a workaround and points are scored for the “Result” section, but not for the “Solution” section.

A possible workaround for the MTU problem is to make switch CSW1 the active HSRP router for all VLANs by increasing the HSRP priority or shutting down all VLAN interfaces on switch CSW2.

In the same manner, a possible workaround for the duplicate router ID issue is to disable OSPF entirely on router IRO2 and route all Internet traffic from the office networks via router IRO1. (The guest traffic from the branch office coming from router BRO2 can still be routed via IRO2 because the connectivity between these routers is based on static routing instead of OSPF).

The multiplier that indicates the difficulty level and urgency for this ticket was determined to be 10. As a result, the maximum possible score for this ticket is $25 \times 10 = 250$ points.

Suggested Solution

Correcting the configurations of switch CSW2 and router CRO2 as follows can restore the connectivity from client PC CLT1 to server www.isp3.local.

Suggested Configuration Changes

- On switch CSW2, reset the system MTU to 1500 bytes and reload the switch.

```
CSW2(config)#system mtu 1500
Changes to the system MTU will not take effect until the next reload is done
Warning : Configured system MTU is less than routing MTU
          On next reload, routing MTU value will change
          to configured system MTU
CSW2(config)#^Z
CSW2#reload

System configuration has been modified. Save? [yes/no]: yes
Building configuration...
[OK]
Proceed with reload? [confirm]
```

- On router CRO2, change the OSPF router ID to the IP address of its loopback 0 interface and reset the OSPF process.

```
CRO2(config)#router ospf 1
CRO2(config-router)#router-id 10.1.220.2
Reload or use "clear ip ospf process" command, for this to take effect
CRO2(config-router)#^Z
CRO2#clear ip ospf process
Reset ALL OSPF processes? [no]: yes
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—7-15

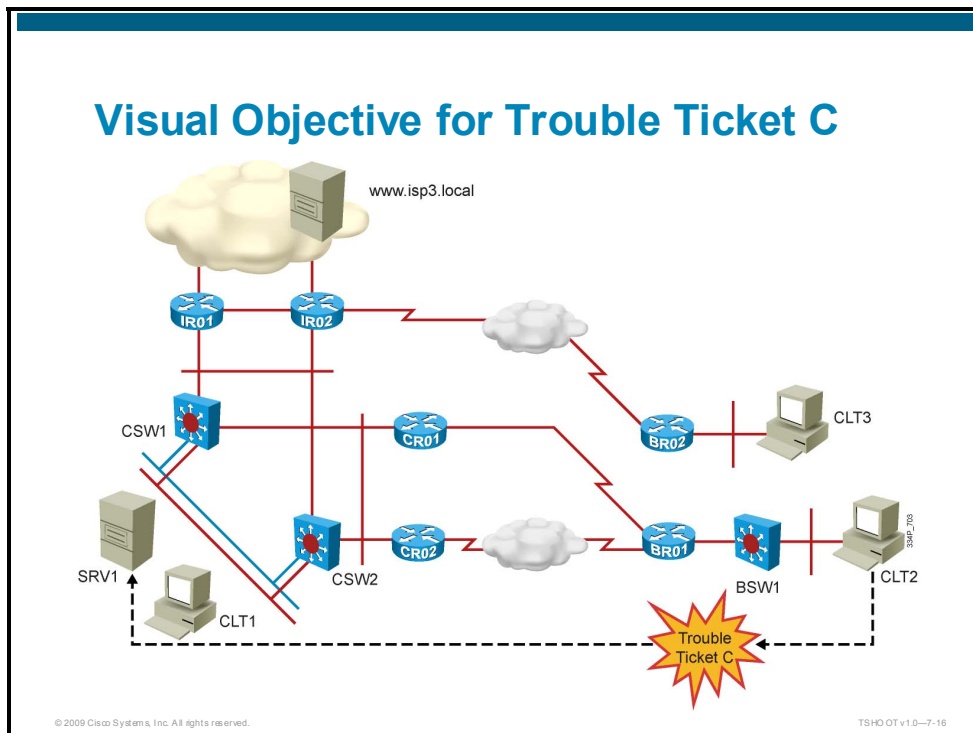
To address the MTU mismatch between switch CSW2 and its neighbors, the system MTU of switch CSW2 should be reset to the default value of 1500 to match the MTU of its neighbors. As an alternative, the MTU on all neighbors could be changed to match the MTU of 1512 configured on switch CSW2, but clearly this change is more work and you will even need to change the MTU on routers IRO1 and IRO2, because otherwise a similar problem will be created on switch CSW1.

For the change to take effect, switch CSW2 needs to be reloaded after you change the configuration.

To address the problem caused by the duplicate router ID on router IRO2 and CRO2, you should change the router ID on router CRO2 to 10.1.220.2, which is the IP address of its loopback interface. Choosing a different unique IP address or changing the router ID of router IRO2 will also solve the problem. However, this change does not comply with the policies on the network because all other routers that run OSPF use the IP address of their Loopback 0 interface as their OSPF router ID. As a result, using this solution will cause you to lose points for policy compliance in the Network Maintenance section of this lab.

Trouble Ticket C: No Connectivity Between Headquarters and Branch Office

The following figure shows the visual objective for the trouble ticket.



The text introducing this trouble ticket is as follows:

The office users in the branch office have complained that they cannot connect to server SRV1 at headquarters and they cannot browse the Internet. Additionally, the core WAN routers CRO1 and CRO2 cannot be reached via Telnet or SSH from the branch office. You can use client PC CLT2 in VLAN 17 for testing purposes.

Your task is to restore connectivity between headquarters and the branch office. This task includes ensuring that you can use Telnet to connect to routers CRO1 and CRO2 and ensuring that the user on client PC CLT2 can view the directory “\\SRV1\\Public” and upload a file to it.

Trouble Ticket C: Review and Discuss

How did your team approach Trouble Ticket C?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you accomplish the goal of restoring the connectivity between headquarters and the branch office?
- How long did it take to restore the connectivity?
- Did you implement a workaround at any point during the resolution of this ticket?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—7-17

Two major problems cause the loss of connectivity in this lab. You only have to solve one of the two issues to regain connectivity between the headquarters and branch office.

The only assumption is that you have solved the problems in the other tickets, because some of these issues may also affect the connectivity in this ticket. Specifically, the OSPF problems covered in Trouble Tickets A and B affect the connectivity to server SRV1.

One of the two problems introduced in this ticket is that the serial interface between routers BRO1 and CRO1 is down. This problem is caused by the failure of the Challenge Handshake Authentication Protocol (CHAP) on router BRO1. On routers BRO1 and CRO1 authentication, authorization and accounting (AAA) has been configured to authenticate against RADIUS, but use locally defined user names and passwords if no RADIUS server is available. A RADIUS server is not present on the network and no RADIUS server has been configured on the routers. Therefore, the authentication process should fall back to local user names and passwords. However, on router BRO1, authentication has not been correctly configured for PPP authentication. The keyword **local** is missing and as a result, the local user name and password database are not used for the CHAP authentication. As a result, the authentication fails and the serial link stays down.

The second problem is that routers CRO2 and BRO1 are not correctly establishing an EIGRP neighbor relationship across the Frame Relay link. On all routers, control plane policing has been configured to drop all traffic to the router control plane except for specifically configured protocols. In the access list that defines the routing protocol traffic on router CRO2, EIGRP is not explicitly permitted. This causes the router to drop incoming EIGRP packet and prevents it from establishing any EIGRP neighbor relationships.

Although there are many possible methods that you could use to solve this problem, the following list provides an example of a troubleshooting log to show you a methodical approach that could be used to resolve this problem. For completeness, this log shows how to troubleshoot and resolve both described problems, even though only one of the two needs to be resolved to restore connectivity.

Device	Actions and results
CLT2	Verify problem: Cannot ping to 10.1.152.1 (SRV1), 10.1.220.1 (CRO1) and 10.1.220.2 (CRO2): "Reply from 10.1.160.126: Destination host unreachable." Conclusion: Default gateway 10.1.160.126 (BSW1) is correctly configured and reachable.
BSW1	No route to 10.1.152.0/24, 10.1.220.1/32 or 10.1.220.2/32. Only two EIGRP routes are in the routing table.
BRO1	No EIGRP routes are learned across the WAN.
BRO1	The show ip eigrp neighbors command lists only 10.1.194.9 (CRO2), not CRO1.
BRO1	"Serial0/0/1 is up, line protocol is down." Likely cause is a Layer 2 problem.
	Note: Troubleshoot this problem first. Investigate why EIGRP routes are not learned from router CRO2 later.
BRO1	The debug ppp negotiation command shows that PPP frames are sent to and received from CRO1. Authentication fails with message "Unable to authenticate for peer."
BRO1 and CRO1	Verify configured user names and passwords: User names are correct and passwords seem to match.
CRO1	The debug ppp negotiation command shows "Using password from AAA".
CRO1	The debug aaa subsystems command reveals that authentication is passed based on local authentication.
BRO1	The debug aaa subsystems command reveals that authentication fails with "No methods left to try". Local authentication is not used.
BRO1 and CRO1	Compare AAA configuration: On BRO1 authentication for PPP is missing the keyword "local."
BRO1	Configuration changed: Changed authentication for PPP to fall back to local authentication if RADIUS fails. Both pre- and post-change configurations were saved in flash on the switch. Communicated this information to team members.
BRO1	Routes are now learned from router CRO1.
CLT2	Telnet connection to CRO1, Telnet connection to CRO2, and file transfer to SRV1 work.
	Problem fixed. Documented changes. Backed up configurations.
	Notified instructor and demonstrated that file could be successfully copied to the server and Telnet connection was achieved.
	Note: Resolve other tickets first. Troubleshoot EIGRP issue between CRO2 and BRO1 during the maintenance tasks.
BRO1	The debug eigrp packets command (limited to neighbor 10.1.194.9) reveals that EIGRP hello packets are sent and received. Update packets are sent, but not acknowledged.
BRO1	Ping to 10.1.194.9 succeeds.
CRO2	No EIGRP neighbors are listed.
CRO2	The debug eigrp packets command shows only sent packets. No packets seem to be received. Incoming EIGRP packets are not received or dropped.
CRO2	Configure the access list that permits EIGRP specifically and then permits all other IP packets. Apply this access list to interface Serial 0/0/0.121 in the incoming direction. (Verified that no other access lists were present on the interface).
CRO2	Packet counters for EIGRP increase on the configured access list. Conclusion: Packets are received on the interface, but somehow not passed to the EIGRP process. Remove access list.
CRO2	Discovered more access lists: Used for control plane policing.

Device	Actions and results
	Research control plane policing.
CRO2	Access list that permits routing traffic does not match EIGRP.
CRO2	Configuration changed: Added EIGRP to access-list "ROUTING-PROTOCOLS". Both pre- and post-change configurations were saved in flash on the switch. Communicated this information to team members.
CRO2	Neighbor relationship with BRO1 is now established.
BRO1	Paths via CRO1 are preferred, but topology table also lists the alternative path via CRO2.
BRO1	Execute failover test: Shutdown interface Serial 0/0/1. Result: Traffic between branch and office is rerouted via CRO1. Re-enable interface Serial 0/0/1.
	Closed ticket.

Primary Clue: AAA Authentication Fails

- Executing the **debug aaa subsystems** command on router CRO1 shows that local authentication is used after RADIUS fails.

```
May 15 02:14:37.179 PDT: AAA SRV(0000832A): process authen req
May 15 02:14:37.179 PDT: AAA SRV(0000832A): Authen method=SERVER_GROUP radius
May 15 02:14:37.179 PDT: AAA/SRV (0000832A): No server group radius defined
May 15 02:14:37.183 PDT: AAA SRV(0000832A): protocol reply BEGIN for
Authentication
May 15 02:14:37.183 PDT: AAA SRV(0000832A): Authen method=LOCAL
May 15 02:14:37.183 PDT: AAA SRV(0000832A): protocol reply PASS for
Authentication
May 15 02:14:37.183 PDT: AAA SRV(0000832A): Return Authentication status=PASS
```

- Executing the same **debug** command on router BRO1 shows that authentication fails by lack of options other than RADIUS.

```
*May 15 02:13:19.288 PDT: AAA SRV(00007750): process authen req
*May 15 02:13:19.288 PDT: AAA SRV(00007750): Authen method=SERVER_GROUP radius
*May 15 02:13:19.288 PDT: AAA/SRV (00007750): No server group radius defined
*May 15 02:13:19.288 PDT: AAA SRV(00007750): protocol reply BEGIN for
Authentication
*May 15 02:13:19.288 PDT: AAA SRV(00007750): Authen method=NOT_SET - No methods
left to try
*May 15 02:13:19.288 PDT: AAA SRV(00007750): Return Authentication status=FAIL
```

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0--7-18

Although the **debug ppp negotiation** command shows some minor hints about the cause of the problem, the clearest clue about the cause of the CHAP authentication failure is revealed by the **debug aaa subsystems** command. When this command is executed on router CRO1, it shows that RADIUS authentication is tried and fails. Subsequently, local authentication is tried and succeeds, resulting in a “PASS” from the authentication process.

When the same **debug** command is used on router BRO1, the RADIUS authentication also fails by lack of a defined RADIUS server, similar to what happens on router CRO1. However, after the RADIUS authentication fails, no other methods are tried and the authentication fails.

After comparing the AAA configuration between routers CRO1 and BRO1, you should quickly see that the local keyword is missing from the **aaa authentication ppp default group radius** command on router BRO1.

For the second problem, the failing EIGRP neighbor relationship between routers CRO2 and BRO1, there are no commands that show the problem clearly. Through interpretation of various **show** and **debug** commands, such as **show ip eigrp neighbors** and **debug eigrp packets**, you should eventually reach the conclusion that router CRO2 sends EIGRP packets, but does not seem to receive the packets that are sent by router BRO1. Because a ping between routers BRO1 and CRO2 succeeds, which confirms that there is IP connectivity between BRO1 and CRO2, you have to start thinking of access lists as the possible cause of the problem. This thinking should lead you to the discovery of the control plane policy on the router and eventually you should see that EIGRP is not permitted by the access list named ROUTING-PROTOCOLS, which should match all routing protocol traffic.

Trouble Ticket C: Checkpoints and Scoring

Scores for this ticket are based on the following checkpoints:

- **Result (3 points):** Telnet can be used from client PC CLT2 to connect to the loopback IP address 10.1.220.1 of router CRO1.
- **Result (3 points):** Telnet can be used from client PC CLT2 to connect to the loopback IP address 10.1.220.2 of router CRO2.
- **Result (4 points):** Client PC CLT2 can transfer a file to the directory \\SRV1\Public.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—7-19

Points for this topic are scored based on the checkpoints shown in the preceding figure.

To prove that connectivity between headquarters and the branch office has been restored you should demonstrate three separate types of connections: using Telnet from client PC CLT2 to connect to the loopback IP addresses of router CRO1 and router CRO2, and transferring a file from client PC CLT2 to server SRV1. If the previous tickets have been successfully resolved, you should have no problem demonstrating all three items after you resolve one of the two problems that were introduced in this trouble ticket. However, if previous tickets were not resolved or were only partially resolved, this partial resolution may affect the connectivity from the branch office to the headquarters. Because there are three separate types of connections, three separate “Result” items are scored for this ticket. This scoring allows you to score partial points for the ticket, even if you did not manage to resolve the problems in Trouble Tickets A and B.

Trouble Ticket C: Checkpoints and Scoring (Cont.)

Scores for this ticket are based on the following checkpoints:

- **Solution (5 points):** You have addressed the root cause or causes of the problem, not implemented a workaround.
- **Process (5 points):** You have clearly documented your process, your solution, and any changes that you have made to the device configurations.
- **Timing (5 points):** You have restored connectivity in a timely manner.

Total possible points for this ticket: $25 \times 8 = 200$ points.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0-7-20

If you have changed the AAA configuration on router BRO1 in such a way that the CHAP authentication succeeds, or if you have adapted the control plane policy on router CRO2 to allow routers CRO2 and BRO1 to become EIGRP neighbors, then your changes would be considered a solution because the root causes of the problems were addressed. If your changes restored connectivity between the headquarters and branch office by removing CHAP from routers CRO1 and BRO1 or by removing the control plane policy from router CRO2, your changes would be considered to be a workaround and points are scored for the “Result” section, but not for the “Solution” section.

Only one of the two problems needs to be addressed to score the points for this ticket. However, if you leave one of the two issues unresolved, you will lose points for the redundancy and failover section of the network maintenance task in this lab.

The multiplier that indicates the difficulty level and urgency for this ticket was determined to be 8. As a result, the maximum possible score for this ticket is $25 \times 8 = 200$ points.

Suggested Solution

Correcting the configurations of routers BRO1 and CRO2 as follows can restore the connectivity between the headquarters and the branch office.

Suggested Configuration Changes

- On router BRO1 add local authentication as a fallback method to the AAA authentication for PPP.

```
BRO1(config)#aaa authentication ppp default group radius local
```

- On router CRO2 permit EIGRP in the access list that matches the routing protocol traffic.

```
CRO2(config)#ip access-list extended ROUTING-PROTOCOLS  
CRO2(config-ext-nacl)#permit eigrp any any
```

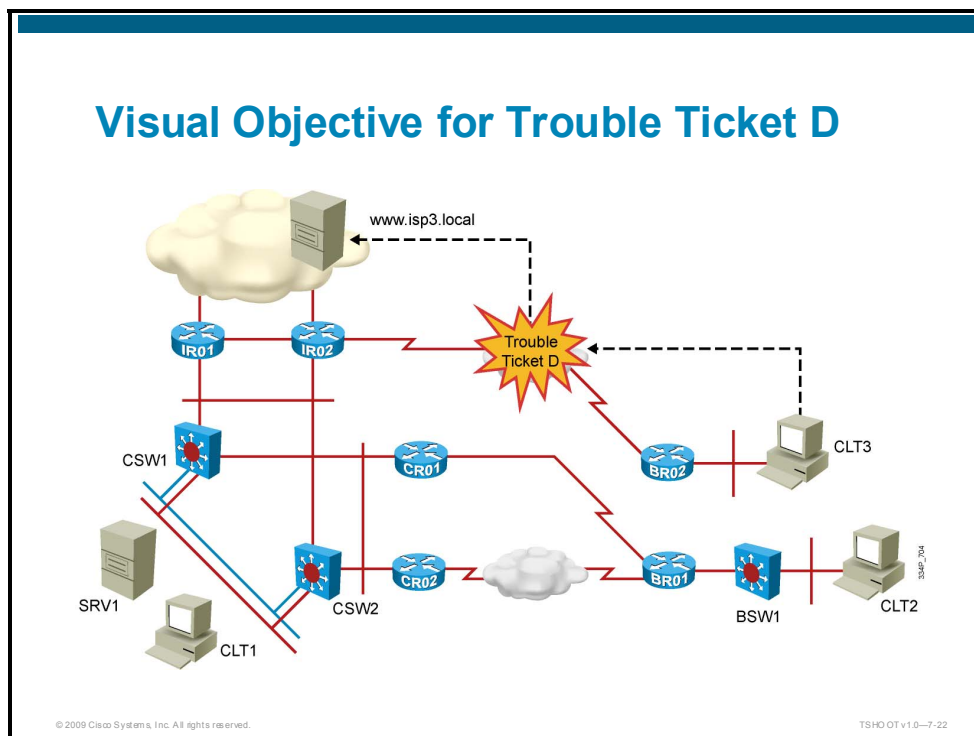
© 2009 Cisco Systems, Inc. All rights reserved.TSHO OT v1.0—7-21

To resolve the AAA problem that causes the CHAP authentication to fail, the AAA method for PPP authentication should be changed to include the local method as an option on router BRO1. To keep the configuration consistent across the routers, the best solution is simply to add the local authentication method as a fallback option to RADIUS on router BRO1, similar to the configuration of router CRO1. RADIUS could also be removed from the configuration entirely, because no RADIUS server is currently configured; however, if you decide to make this change, you should adapt the configuration of router CRO1 in a similar manner to keep the configurations consistent.

To address the problem that the EIGRP neighbor relationship between routers CRO2 and BRO1 fails, you should adapt the control plane policy on router CRO2 to include EIGRP in the ROUTING-TRAFFIC class. The easiest and most consistent manner to do this is to add a line to the extended access-list ROUTING-PROTOCOLS to permit EIGRP. There are various other ways that the result can be achieved. However, if your solution enables the EIGRP neighbor relationship, but alters the policy significantly or removes it entirely, you may lose points in the network maintenance section of this lab.

Trouble Ticket D: No Internet Access for Guest Users

The following figure shows the visual objective for the trouble ticket.



The text introducing this trouble ticket is as follows:

A guest user in the branch office who uses PC CLT3 on VLAN 19 has complained that he cannot browse to the website `www.isp3.local`.

Your task is to restore connectivity from client PC CLT3 to the Internet and ensure that the user can connect to the site `http://www.isp3.local` using a web browser.

Trouble Ticket D: Review and Discuss

How did your team approach Trouble Ticket D?

- What method did you use to solve this ticket?
- Which tools did you use?
- Which problems did you find?
- Did you solve these problems and if so, how?
- Did you accomplish the goal of restoring the connectivity from the guest VLAN to the Internet?
- How long did it take to restore the connectivity?
- Did you implement a workaround at any point during the resolution of this ticket?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—7-23

Two main problems cause the loss of connectivity in this lab and both need to be resolved to restore the connectivity from client PC CLT3 to the Internet.

The first problem is that the configuration-register on router BRO2 has been changed to the value 0x2100, which causes it to boot to ROM monitor mode instead of booting the Cisco IOS Software. To get out of this situation the router can be booted manually. To ensure that the same problem does not occur on the next reboot of the router, the configuration register needs to be reset to the default value of 0x2102.

The second problem is harder to find. VLAN 19, the guest VLAN, has been configured as a remote Switched Port Analyzer (SPAN) VLAN. This type of VLAN is not intended for use as an access VLAN, but as a transport mechanism to carry traffic that is captured on one switch to a port on another switch. Spanning tree and MAC address learning are disabled for this type of VLAN. If a remote span VLAN is configured as an access VLAN on a port, the interface is rendered inactive. To resolve this problem, the VLAN should be reconfigured as a standard (nonremote SPAN) VLAN.

The following list provides an example of a troubleshooting log to show you a methodical approach that could be used to resolve this problem.

Device	Actions and results
CLT3	No IP address is obtained via DHCP.
	Check design and implementation guidelines: Router BRO2 should provide DHCP service for VLAN 19.
BRO2	Router has not booted: Stuck in ROM monitor mode.
BRO2	Attempt to boot manually from Cisco IOS Software in flash: Succeeds.
BRO2	Examine boot variables: No boot system commands are present in configuration.
BRO2	Examine configuration register: Set to 0x2100, instead of the default of 0x2102. Hypothesis: This setting is the cause of the router being stuck in ROM monitor mode.
BRO2	Change configuration register to 0x2102.
BRO2	Reload to confirm hypothesis: Router boots successfully.
CLT3	Problem is not resolved: Still no IP address is obtained via DHCP.
BSW1	Interface FastEthernet 0/8 is in state “up, line protocol is up (inactive).”
	Research interface state “up (inactive)”: No details found.
BSW1	Verify configuration for interface FastEthernet 0/8: Looks normal and complies with templates.
BSW1	Interface FastEthernet 0/4, which connects to router BRO2 is in the same state. Problem may be VLAN-related.
BSW1	Change access VLAN on interface FastEthernet 0/8 to VLAN 17 (B1S1-OFFICE): Interface state changes to UP.
CLT3	IP address is obtained and browsing to http://www.isp3.local succeeds.
BSW1	Change access VLAN on interface FastEthernet 0/8 back to VLAN 19. Interface goes back to state “up (inactive).”
BSW1	Log reveals “%PM-4-INACTIVE: putting Fa0/8 in inactive state because access VLAN is remote SPAN VLAN.”
BSW1	Verify configuration for VLAN 19: Configured as remote SPAN VLAN.
BSW1	Verify configuration: No other commands related to SPAN are present.
BSW1	Configuration changed: Removed remote SPAN configuration from VLAN 19. Both pre- and post-change configurations were saved in flash on the switch. Communicated this information to team members.
CLT3	IP address is obtained via DHCP.
CLT3	Ping to 172.34.224.1 and browsing to http://www.isp3.local succeed.
	Problem fixed. Documented changes. Backed up configurations.
	Notified instructor and demonstrated successful browsing to http://www.isp3.local. Closed ticket.

Primary Clue: System Log Message

- The log messages on router BRO2 contain an important hint about the reason that the interfaces FastEthernet 0/4 and FastEthernet 0/8 are marked as “up (inactive).”

```
BSW1#show logging | include 0/4|0/8
*Feb 28 16:00:30 PST: %PM-4-INACTIVE: putting Fa0/4 in inactive
state because access VLAN is remote SPAN VLAN
*Feb 28 16:00:31 PST: %PM-4-INACTIVE: putting Fa0/8 in inactive
state because access VLAN is remote SPAN VLAN
```

Although the problem of the router booting to ROM monitor mode instead of booting the Cisco IOS Software immediately reveals itself when you connect to the router, the root cause of this problem is not as easy to find. There is no **show** command that clearly states that the boot to ROM monitor is caused by the value of the configuration register. To solve this problem, you have to know the factors that affect the boot sequence of the router, such as the configuration register and **boot system** commands.

An important clue about the problem of the inactive interfaces in VLAN 19 on switch BSW1, which is caused by the VLAN being configured as a remote SPAN VLAN, can be gathered from the log of the router. Messages state that “%PM-4-INACTIVE: putting Fa0/8 in inactive state because access VLAN is remote SPAN VLAN” for both interfaces FastEthernet 0/8 and FastEthernet 0/4. If you do not scan the logs, this problem is harder to troubleshoot. One of the actions you could have taken during your diagnostics is to change the access VLAN on interface FastEthernet 0/8. Choosing another VLAN, such as VLAN 17, enables the port, which should lead you to the conclusion that the problem is related to the VLAN.

Trouble Ticket D: Checkpoints and Scoring

Scores for this ticket are based on the following checkpoints:

- **Result (8 points):** Client PC CLT3 can ping IP address 172.34.224.1.
- **Result (2 points):** Client PC CLT3 can browse to <http://www.isp3.local>.
- **Solution (5 points):** You have addressed the root cause or causes of the problem, not implemented a workaround.
- **Process (5 points):** You have clearly documented your process, your solution, and any changes that you have made to the device configurations.
- **Timing (5 points):** You have restored connectivity in a timely manner.

Total possible points for this ticket: $25 \times 6 = 150$ points.

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0—7-25

Points for this topic are scored based on the checkpoints shown in the preceding figure.

To prove that connectivity between client PC CLT3 and the Internet has been restored you should demonstrate to the instructor that you can browse to <http://www.isp3.local>. However, because DNS problems may prevent this, even if there is IP connectivity from client PC CLT3 to the IP address of www.isp3.local 172.34.224.1, partial points are awarded for being able to ping to IP address 172.34.224.1. For both “Result” items, it should still be possible to demonstrate this result at the end of the lab. If you are not able to demonstrate this result at that time, you lose the points for this section.

If you have booted router BRO2 and changed the configuration register to the correct value to prevent a similar problem from occurring on the next reload, your change would be considered a solution. If you booted the router, but did not change the configuration register, your change would be considered a workaround, because it addresses the symptoms, but not the cause.

For the problem caused by VLAN 19 being configured as a remote SPAN VLAN, the only real solution is to remove the **remote-span** command from the VLAN on switch BSW1. As a workaround, you could implement a new VLAN and assign both interfaces FastEthernet 0/4 and FastEthernet 0/8 to it.

The multiplier that indicates the difficulty level and urgency for this ticket was determined to be 6. As a result, the maximum possible score for this ticket is $25 \times 6 = 150$ points.

Suggested Solution

Correcting the configurations of router BRO2 and switch BSW1 as follows can restore the connectivity from client PC CLT3 to server www.isp3.local.

Suggested Configuration Changes

- Boot router BRO2 manually from ROM monitor mode by issuing the following command.

```
rommon 2 > boot flash:c1841-advipservicesk9-mz.124-23.bin
```

- Next, change the configuration register to its default value of 0x2102.

```
BRO2(config)#config-register 0x2102
```

- On switch BSW1, remove the remote SPAN configuration from VLAN 19.

```
BSW1(config)#vlan 19  
BSW1(config-vlan)#no remote-span
```

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0—7-26

To boot router BRO2 using the Cisco IOS Software in flash, you can issue the **boot flash:filename** command from ROM monitor mode. You can use the **dir flash:** command to find the correct name of the Cisco IOS Software in flash. After booting the router, the configuration register needs to be changed to prevent this issue from happening again in the future. This change can be done from Cisco IOS global configuration mode using the **config-register** command or alternatively it can be done before booting the router from ROM monitor by use of the **confreg** command.

To resolve the problem with the inactive interfaces in VLAN 19 on switch BSW1, you should remove the remote SPAN configuration from VLAN 19.

Network Maintenance: Verify Network Operation

The text introducing this task is as follows:

After resolving the problems reported by the users, you should verify the operational state of the network and look for unreported problems or issues that might cause problems in the future. At least the following areas should be investigated:

- **Redundancy and failover:** Analyze which redundant paths are available in the network and ensure that the network reconverges after a component or link failure if possible.
- **Security policy compliance:** Verify that implemented security mechanisms were not disabled during the troubleshooting process and verify that the implemented security features have been deployed in a consistent manner across devices.
- **Network management:** Verify that all network management features and protocols that are implemented on the devices are operating correctly.

Network Maintenance: Review and Discuss

How did your team approach the Network Maintenance task?

- What method did you use to approach this task?
- Which tools did you use?
- Did you find any unresolved problems?
- Did you solve these problems and if so, how?
- How did you verify redundancy and test failover?
- How did you verify security compliance?
- How did you verify the operation of network management protocols and features?

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—7-27

This final task in the lab complements the troubleshooting tasks by ensuring that after you have implemented your changes you do not only have an operational network, but also a network that complies with the established policies, that is implemented in a consistent manner, and that is manageable.

The methods used for verification and testing are different from the methods used for the trouble tickets and dependent on the amount of time you had left at the end of the lab to do your verifications. How much time you had left also strongly depended on how you approached the trouble tickets.

If your team used a highly structured and well-coordinated approach during the trouble tickets, you will likely have little work left to do as part of the maintenance task. If you made verification of your solutions against the security policies, verification of redundancy and failover, and verification of network management operation a standard step in your troubleshooting process, then you only needed to consolidate your results from the individual tickets during this task. If you purely focused on restoring connectivity during the troubleshooting process, then you will need to do all verification during this task and you may actually need to go back to adapt your earlier solutions.

In this section, the major points that have not already been addressed in earlier tickets are discussed.

An additional problem exists in the lab that was not specifically reported in any of the trouble tickets and that does not need to be resolved to regain connectivity in any of the tickets. However, it does affect the redundancy of the network and therefore it should be addressed during this task. The problem is that the BGP peering between routers IRO and ISP1 is continually flapping and, as a result, the connection to ISP1 will not be used as a backup path if the connection to ISP2 is down. In order to score the points for the redundancy section, this problem needs to be resolved.

The following list provides an example of a troubleshooting log to show you a methodical approach that could be used to resolve this problem.

Device	Actions and results
IRO2	Maintenance task: Reload router IRO2 to test redundancy to Internet and failover to ISP1.
CLT1, CLT2 and CLT3	Continuous ping to www.isp3.local: Connectivity is lost until router IRO2 has finished rebooting.
IRO1	BGP peering to router ISP1 is in state "Idle (PfxCt)."
IRO1	Log includes messages that state "%BGP-3-MAXPFEXCEED: No. of prefix received from 192.168.224.254 (afi 0): 6 exceed limit 5."
IRO1	Verify configuration: Maximum number of prefixes from neighbor ISP1 set to 5.
IRO2	Compare configuration: Similar configuration in place.
	Verify design and implementation guidelines: Only default route should be accepted from both ISP routers. All other prefixes should be filtered.
IRO1	Examine route map that filters routes from ISP1: Route map ends with a line (number 20) that implicitly permits all other routes.
IRO1	Configuration changed: Removed line 20 from route map. Both pre- and post-change configurations were saved in flash on the switch. Communicated this information to team members.
IRO1	Reset peering to router ISP1: Peering comes up and only default route is learned.
IRO2	Repeat failover test by reloading router IRO2.
CLT1, CLT2 & CLT3	Continuous ping to www.isp3.local: On client PCs CLT1 and CLT2 connectivity is restored during reboot of IRO2 with minimal packet loss. CLT3 loses connectivity during the reboot of IRO2, as was to be expected.
IRO2	Shut down FastEthernet connection from IRO2 to ISP2.
CLT1, CLT2 & CLT3	Continuous ping to www.isp3.local: No packet loss on any of the clients during failover.
IRO2	Re-enable connection to ISP2.
	Problem fixed. Documented changes. Backed up configurations.
	Notified instructor and demonstrated failover behavior from clients to the Internet.

Primary Clue: System Log Message

- The log messages on router IRO1 reveal an important hint about the reason that the peering to router ISP1 is flapping.

```
IRO1#show logging | include BGP
May 18 00:48:02 PDT: %BGP-5-ADJCHANGE: neighbor 192.168.224.254 Up
May 18 00:48:02 PDT: %BGP-4-MAXPFX: No. of prefix received from
192.168.224.254 (afi 0) reaches 3, max 5
May 18 00:48:02 PDT: %BGP-3-MAXPFXEXCEED: No. of prefix received from
192.168.224.254 (afi 0): 6 exceed limit 5
May 18 00:48:02 PDT: %BGP-5-ADJCHANGE: neighbor 192.168.224.254 Down BGP
Notification sent
May 18 00:48:02 PDT: %BGP-3-NOTIFICATION: sent to neighbor
192.168.224.254 3/1 (update malformed) 0 bytes FFFF FFFF FFFF FFFF FFFF
FFFF FFFF FFFF 0033 0200 0000 1440 0101 0040 0206 0202 FFF5 FFCE 4003
04C0 A8E0 FE18 C0A8 6413 AC22 E0
```

When you have determined that there is a problem with the peering between router IRO1 and router ISP1, it is not too hard to find out what is causing the problem. The indication “Idle (PfxCt)” in the output of the **show ip bgp summary** command already gives a hint about the cause of the problem and the messages in the system log give even better clues: The log messages state that the maximum allowable number of prefixes is exceeded, and router IRO1 closes the BGP session to router ISP1.

When you consult the design and implementation guidelines at the beginning of the trouble ticket you find that only the default route should be accepted from routers ISP1 and ISP2. After you verify the route map that is configured on router IRO1 and that filters the routes from router ISP1 (and comparing it to the route map configured on router IRO2 if necessary), you see that the route map has an extra line that permits all routes. After removing this line, the maximum prefix count will not be exceeded when the session is established and the path via router ISP1 to the Internet can be used.

Network Maintenance: Checkpoints and Scoring

Scores for this task are based on the following checkpoints:

- **Result (5 points):** The connectivity to the Internet should be regained after failure of a redundant connection or component.
- **Result (5 points):** The connectivity from between the branch and headquarters should be regained after failure of a redundant connection or component.
- **Result (5 points):** You have discovered and addressed additional issues that were not part of the reported problems.
- **Solution (5 points):** The changes that you have made are in compliance with the policies implemented on the network.
- **Process (5 points):** You have clearly documented your verification process and any changes made to the device configurations.

Total possible points for this ticket: 25 x 10 = 250 points.

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0—7-29

Points for this topic are scored based on the checkpoints shown in the preceding figure.

To prove that either of the connections to the Internet can be used when the other fails, you should execute failover tests. You need to test two main scenarios.

One scenario is to reload each of two routers, IRO1 and IRO2, and observe possible packet loss from client PCs CLT1, CLT2, and CLT3 to the Internet (www.isp3.local). It is not necessary to minimize the amount of packet loss, but connectivity should be restored while the selected router reloads. The exception is that client PC CLT3 will lose connectivity, because it is physically connected via router IRO2. Therefore, this client is expected to lose connectivity when router IRO2 is reloaded.

The second scenario to test is to disable the FastEthernet interface on router IRO2 that leads to router ISP2. In this instance, client PC CLT3 should still be able to connect to www.isp3.local via the path going through routers IRO2, IRO1, and ISP1.

To score the points for the first item, you should not only have resolved Trouble Tickets B, C, and D, but you should also have discovered and resolved the BGP problem between routers IRO1 and ISP1.

To score the points for the second item you should have resolved both the PPP problem and the EIGRP problem in Trouble Ticket C. If you have only solved one of these problems, it will become apparent during failover tests that you have not solved both problems, because the alternative path is not used.

To score the points for the third item you should have discovered and solved the BGP problem between routers IRO1 and ISP1. There are no other problems that are unrelated to the problems reported in Trouble Tickets A through D.

In the description of the network that introduces the trouble tickets the following statements about policies are made:

- Any routing policies that are implemented should stay in effect.
- Where redundant connections are present, the network should reconverge when a link or device failure occurs.
- Any security mechanisms and policies that are implemented should stay in effect.

The instructor will judge if the changes that you implemented comply with these policies. Several of these items have already been mentioned in the suggested solution section of the individual trouble tickets. The following items are some possible violations of these policies:

- **Trouble Ticket A:** Removing the allowed VLAN list from the EtherChannel between switches CSW1 and CSW2
- **Trouble Ticket B:** Changing the OSPF router ID of router IRO2 or changing the OSPF router ID of router CRO2 to something other than the IP address of its Loopback 0 interface
- **Trouble Ticket C:** Disabling control plane policing on router CRO2 or removing CHAP authentication from routers BRO1 and CRO1.
- **Trouble Ticket D:** Using a different VLAN than VLAN 19 as the guest VLAN.
- **Network maintenance:** Removing the maximum allowed number of prefixes from the peering between routers IRO1 and ISP1.

It is impossible to list all possible reasons that may cause you to lose points for this item. Ask your instructor for details about your score for this section.

The multiplier that indicates the difficulty level and urgency for this task was determined to be 10. As a result, the maximum possible score for this ticket is $25 \times 10 = 250$ points.

The maximum total number of points that could be scored for this lab is 1000 points. In practice, this number is virtually impossible to attain because you would need to complete the full lab within half an hour without making any mistakes.

Although the score is a measure of your performance, it is important to realize that this score depends on many factors. Review your score and, for each of the sections that you lost points for, analyze why you lost the points and determine if optimizing your process could have prevented this problem.

Suggested Solution

Correcting the configuration of router IRO1 as follows can restore the BGP session between routers IRO1 and ISP1.

Suggested Configuration Changes

- Change the route map on router IRO1 that filters the routes received from router ISP1 to only allow the default route by removing the second line that allows all routes.

```
IRO1(config)#no route-map FROM-AS-65525 permit 20
```

- No other changes need to be made as part of this task.

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0—7-30

The only problem left in this ticket is the failing BGP peering between routers IRO1 and ISP1. To resolve this problem, the route map that filters the routes that are received from router ISP1 should be changed to block any route other than the default route. The simplest way to achieve this change is by removing line 20 of the route map, which permits any route.

Technically the problem could also be solved by removing the prefix limitation of five prefixes from the peering to router ISP1. Although this would allow you to score the points for the redundancy and failover section of this task, you will lose points for policy compliance.

Consolidation

This topic describes the primary lessons that could be learned from the lab exercise.

Discussion: Lessons Learned

Method and process:

- How could you improve your troubleshooting methods?
- What alternative methods did you discover?

Communication and procedures:

- How could the troubleshooting process be made more effective?
- What kind of procedures would be useful and why?

Technology and tools:

- Which tools were most useful during troubleshooting?
- Which tools could have improved the effectiveness of your process?
- Which useful Cisco IOS Software commands did you discover?

© 2009 Cisco Systems, Inc. All rights reserved.TSHOOT v1.0—7-31

Think about all the things that you learned during the lab itself and during the debrief discussions.

In addition to thinking of the methods, processes, and tools as they were used in the lab, reflect on how these things would apply to your own organization. Think about all the things that you learned during the lab itself and during the debrief discussions. There is room to write down the important learning points in the Lab Debrief Notes section of the lab guide.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- You have reviewed and verified your lab results.
- You have consolidated the experiences and discoveries that all students got from the lab and have derived a number of key learning points from these experiences.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—7-32

Module Summary

This topic summarizes the key points that were discussed in this module.

Module Summary

- You have summarized and consolidated the lessons that were learned during this course.
- You have practiced and assessed your network maintenance and troubleshooting skills in a complex lab environment.

© 2009 Cisco Systems, Inc. All rights reserved.

TSHOOT v1.0—7-4

To troubleshoot and maintain integrated, complex enterprise networks, you need to have a good understanding of the individual technologies, protocols, devices, and features that are used in the network. In addition, you need to understand the relations and interactions between the various technologies. In this module, the knowledge and skills that were acquired in earlier lessons and labs were summarized and consolidated.

You had an opportunity to further practice and improve your skills in a complex capstone lab. The lab was scored to assess your performance and provide you with an opportunity to reflect on the processes that you and your team used during the lab.

Your lab results, solutions, methods, and tools were discussed during a comprehensive lab debrief session.

References

For additional information, refer to these resources:

- Cisco Systems, Inc. *Catalyst 3560 Switch Software Configuration Guide, Rel. 12.2 (25)SE*: Configuring Interface Characteristics, Configuring the System MTU. San Jose, California, November 2004:
http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_25_se/configuration/guide/swint.html#wp1154596
- Cisco Systems, Inc. *Use of the Configuration Register on All Cisco Routers*: San Jose, California, April 3, 2006:
http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a008022493f.shtml

