



Release Notes: CCNA Discovery v4.0 Introducing Routing and Switching in the Enterprise – Release 4.0(1)

Purpose

Release 4.0(1) of Introducing Routing and Switching in the Enterprise is the first maintenance release of the third course in the CCNA Discovery curriculum. These notes provide detailed information about this release, including curriculum content, known issues, updates and fixes, and support information.

Release Content

Component	Description
E-Learning Content	10 chapters
Labs	Hands-on labs involving networking equipment
Discovery Server v2.0	Version 2.0 is required and provides network services to offline classroom labs. Version 2.0 is compatible with all CCNA Discovery courses
Packet Tracer v4.11	Version 4.11 is required and enables students to complete activities in simulated networks. Version 4.11 is compatible with all CCNA Discovery courses
Chapter Quizzes	9 chapter quizzes
Chapter Exams	9 chapter exams
Final Exam	1 final exam covering chapters 1-9

Known Issues and Caveats

Item	Description
Graphic Resolution	This curriculum was designed for viewing with a screen resolution of 1024 X 768 or less. If viewed in a higher resolution, items may not display properly in the media area.
Adobe Flash Player	This curriculum was designed for viewing using Adobe Flash Player 8. Certain versions of Flash Player 8 may produce undesirable side effects. If you experience issues using Flash Player 8, we recommend upgrading to Flash Player 9. Known issues reported with some versions of Flash Player 8: <ul style="list-style-type: none"> • Unreadable text in the course tour • Text missing after the first page of chapter summaries
Glossary	This course includes a glossary with hyperlinked terms. In its current implementation, variations of a particular term, such as access point, AP, and APs, each have glossary entries with the same definition. Enhancements are planned to include a single variant and its acronym, if needed, for each term in the glossary.
Content Delivery	This course may be delivered through different channels. The primary delivery channels for the course are Academy Connection or a local Web server. The recommended method is to deliver the course through a local Web server. Secondary channels for delivery include installing the

	<p>content directly to a workstation or PC.</p> <p>When contemplating the various delivery options, administrators and instructors should consider the diversity of platforms on which the course and its content must operate, and note the following guidelines:</p> <ul style="list-style-type: none"> • Select the download package (Windows or Linux zip file) that corresponds to your server/workstation operating system • When possible, configure the content to be delivered through a local Web server when presenting to a class or over an academy LAN • When installing the course on a standalone workstation or PC, please be aware of the following: <ul style="list-style-type: none"> ○ Disable all popup blocker software, toolbars, and applications ○ Accept any ActiveX warning messages when viewing course content ○ Navigate within the course window to avoid ActiveX pop-ups that can be generated by certain combinations of operating systems and browsers
<p>Linux Operating System Support</p>	<p>This course uses the latest features in Flash technology. An installer was used to aid in the local deployment of this product to Windows users. However, for Linux users, the Flash Player security settings must be set manually to run the course through a browser on a local workstation/PC. Installing a standalone curriculum on a Linux operating system requires additional steps after unzipping the course to the file system. After the course is unzipped, visit the Macromedia's security settings page at: www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager04.html</p> <p>After the page loads, some security options will be displayed. Verify that Always ask is selected. In the drop-down menu, select Add location, and then browse for the course folder. After the directory has been marked as secure, close all browser windows. Navigate to the course folder and click the index.html file to launch the course.</p>
<p>Course Navigation for Local Installation on a Workstation/PC</p>	<p>Under certain conditions, "Allow blocked content" ActiveX popup messages may appear in a yellow bar at the top of the screen. If you receive these messages, select "allow blocked content" to continue. On the launch page for the course, select the launch course button to view the course content. Some users may receive a second "Allow blocked content" ActiveX popup message. Click the yellow bar at the top of the screen and choose "allow blocked content" to begin using the course.</p> <p>Note: To avoid excessive ActiveX popup messages, do not use the launch page chapter drop down menu to move between course chapters. Instead, use features such as the course index, back and next buttons, and location box at the bottom of the course content to navigate within the course browser window. For more information on these navigation features, we recommend reviewing the Course Tour, which can be accessed from the course launch page.</p> <p>To stop the information bar from blocking file and software downloads for Internet Explorer, we recommend the following steps:</p> <ul style="list-style-type: none"> • Open Internet Explorer. • Select Tools > Internet Options • Click the Security tab, and select Custom Level • Do one or both of the following: <ul style="list-style-type: none"> ○ To turn off the Information bar for file downloads, scroll to the Downloads section and enable automatic prompting for file downloads. ○ To turn off the Information bar for ActiveX controls, scroll to the ActiveX controls and plug-ins section, and enable automatic prompting for ActiveX controls. • Click OK, click Yes to confirm that you want to make the change, and then click OK again.

	<p>To stop the information bar from blocking file and software downloads for Mozilla Firefox, we recommend the following steps:</p> <ul style="list-style-type: none"> • To access the Popup Blocker Options, select Tools > Options > Content. From there, you can do the following things: <ul style="list-style-type: none"> ○ Block pop-up windows: Deselect this option to disable the popup blocker altogether. ○ Exceptions: Use this option to specify which sites can display popups. You can allow or remove sites from the list.
<p>Packet Tracer Evaluation Feedback</p>	<p>Due to the evaluative nature of Packet Tracer activity files, all course activities have a “Check Results” button that submits the student’s work for evaluation, and provides feedback. This includes observational activities that do not involve any configuration tasks. Packet Tracer files are evaluated by comparing the network submitted by a student to an “answer network.”</p> <p>Activities that require students to perform configurations have a default feedback message that states: “This activity is incomplete, please try again.” This message will appear until all configuration tasks are properly completed.</p> <p>For activities that require observation only, the state of the network will not change. If the “Check Results” button is selected, the feedback will say: “Congratulations on completing this activity,” even though the activity may not be completed. If this occurs, the student should finish all of the instructions in the observation activity to complete it.</p>

Updates and Fixes

This maintenance release includes the following fixes that address issues reported to the Global Support Desk:

Section	Reported Issue/Error	Solution
1.1.2.2	Text: Last paragraph. ECNM not defined before use.	Changed: All data that enters or exits the ECNM passes through an edge device. To: All data that enters or exits the Enterprise Composite Network Model (ECNM) passes through an edge device.
1.1.2.4	Packet Tracer: Corrected grammar, spelling and formatting errors.	
1.1.2.4	Packet Tracer: The objective says “3 hosts and a hub” but the activity uses a switch	Changed reference from hub to switch.
1.1.2.4	Packet Tracer: Step 1 stated "Moving the cursor over the device categories will show options to the right." Doesn't work – you have to click on the icon.	Changed text to read: Moving the cursor over the device categories will display each individual device category. To select a device, first select the device category and then select the device that is required
1.1.2.4	Packet Tracer: Wrong computer identified in Step 3 "Move to PC3"	Changed to "Move to PC2"
1.1.2.4	Packet Tracer: Wrong reference to "PC3" used throughout.	Changed all references of PC3 to PC2.
1.1.2.4	Packet Tracer: Wrong reference to "PC-A" used throughout.	Changed reference of PC-A to PC0
1.1.2.4	Packet Tracer: Reflection - Incorrect reference to "PC2" - "Why is the ARP table for PC2 empty?"	Changed reference to PC1 "Why is the ARP table for PC1 empty?"
1.1.2.4	Packet Tracer: Missing sub step in Step 2.	Added a sub step "e" to Step 2 advising student to click Check Results on the activity.

1.2.1.2	Media: It is not possible to drop an option in the fourth position of either the WAN or External flow pattern bins.	Final position of WAN and External bins eliminated.
1.2.1.2	Media: Inter-campus voice is an option that is accepted under LAN. The term should be intra-campus voice not inter-campus voice.	Inter-campus voice replaced with intra-campus voice.
2.2.1.1	Media: Missing a T1 label on link to cloud.	Added the 5th T1 label on link to the cloud.
2.3.3.2	Packet Tracer: PC0 and PC1 have wrong initial IP address and gateway configuration.	Existing (incorrect) IP addresses removed from PC0 and PC1 and they are pre-configured with 192.168.2.3/24 (gateway 192.168.2.1) and 192.168.3.3/24 (Gateway 192.168.3.1) respectively
2.3.3.2	Packet Tracer: Corrected grammar, spelling and formatting errors.	
2.3.5.3	Text: ip default-gateway is a global config command - it can be issued from config-if and then jumps to config but this may confuse students	Deleted "ip default-gateway" from "Interface settings" Added "ip default-gateway" to "Global Settings"
2.3.5.3	Media: ip default-gateway is a global config command - it can be issued from config-if and then jumps to config but this may confuse students	Changed graphic text prompt From - S1(config-if)#ip default-gateway 192.168.1.1 To - S1(config-if)#exit S1(config)#ip default-gateway 192.168.1.1
2.3.5.4	Packet Tracer: Activity instructions state to "enable secret cisco" but answer config and activity scoring grades "enable password cisco" instead - so if the instructions are followed only 98% max is possible. So scoring needs to be adjusted	Changed activity scoring to grade "enable secret cisco" and remove "enable password cisco" from scoring
2.3.5.4	Packet Tracer: Corrected grammar, spelling and formatting errors.	
2.3.5.4	Packet Tracer: Step 1 e The order of commands to configure the telnet password are reversed.	Changed to: 5. Enter password cisco 6. Enter login
2.3.5.4	Packet Tracer: Step 2 e The order of the commands to configure the telnet password are reversed.	Changed to: 5. Enter password cisco 6. Enter login
2.3.5.4	Packet Tracer: Activity jumps from Step 2 to Step 5.	Change Step 5 to Step 3
3.1.1.5	Media: When the help button is clicked, an empty text box displays.	Help window properly populated with instructions.
3.1.4.2	Lab: Step 19: "Disable unused ports" - does not disable unused ports Fa0/2 and Fa0/3	Changed Step 19 to shutdown interfaces Fa 0/2-3 and Fa 0/5-24
3.1.4.2	Lab: Topology diagram has incorrect graphic for console cable.	Corrected console cable graphic in topology diagram.
3.2.1.4	Packet Tracer: Corrected grammar, spelling and formatting errors.	
3.2.2.2	Text: Bullet "Cost of source path" is misleading	Changed bullet to: "Cumulative cost of path to root bridge"
3.2.2.2	Media: The rollover popup window for "Root ID" has wrong header on the window. The header reads "Root	Added correct header to 'Root ID' popup window.

	IDFlagsMessage Type".	
3.2.2.4	Media: Activity scores correct if all boxes are checked.	Activity changed to score correct only if the correct answers are selected. Extra selections will score the activity as incorrect.
3.2.2.4	Media: Row 1 (Processes BPDUs) columns "Blocking" and "Listening" are correct answers.	Changed activity to accept "Blocking" and "Listening" as correct answers for "Processes BPDUs"
3.2.3.3	Text: Incorrect command provided to set priority.	Changed: To set priority S3(config)#spanning-tree vlan 1 priority 4096 To restore priority to default: S3(config)#no spanning-tree vlan 1 priority
3.2.3.4	Lab: Step 5 uses "interfaces vlan 1" to see the MAC address of the switch for STP. This works on a 2950 or lower switch, but not on 2960 and higher switches	The command to view the MAC address should be "show hardware" which works on all models of switches.
3.2.4.2	Lab: The "show interface vlan 1" command will not display the MAC address on 2960 and newer model switches.	Added "show hardware" command to the following steps- Step 5: Examine interface VLAN 1 information a. On SwitchA, enter the command show interface vlan1 at the privileged EXEC mode prompt. What is the MAC address of SwitchA? b. On SwitchB, enter the command show interface vlan1 at the privileged EXEC mode prompt. What is the MAC address of SwitchB? Which switch should be the root of the spanning tree for this network?
3.3.2.2	Media: Incorrect command prompt in graphic.	Changed: Switch(config)# configure terminal To: Switch# configure terminal
3.3.2.4	Text: The Curriculum states "The removal of VLANs and the reassignment of ports to different VLANs are two separate and distinct functions. When a port is disassociated from a specific VLAN, it returns to VLAN1." This does not explain what happens when a VLAN is deleted.	Added: "When a VLAN is removed any associated ports are deactivated because they are no longer associated with any VLAN."
3.3.2.4	Media: Port Fa0/13 is shown associated with VLAN1 after it's VLAN (VLAN27) is deleted. It should not be listed.	Removed port Fa0/13 from graphic.
3.3.2.5	Lab: Router interface configuration not included in instructions.	Added additional step 2c "Configure the Fa 0/0 interface ip address and mask according to the addressing table."
3.3.2.5	Lab: Incorrect host in Step 6 c. "Ping from Host 1b to R1."	Changed Step 6 c to "Ping from Host 1a to R1."
3.3.2.5	Lab: Missing commands in Step 5c	Modified Step 5c as follows: Assign interfaces to VLANs. Assign S1 port

		<p>Fa0/2 to VLAN 20 and ports Fa0/3 through Fa0/8 to VLAN 30. Observe that the switchport access command was applied to ports Fa0/2 through Fa0/8.</p> <pre>S1(config)#interface fastethernet 0/2 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 20 S1(config-if)#exit S1(config)#interface range fastethernet 0/3 - 8 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 30 S1(config-if-range)#end S1#show running-config</pre>
3.3.3.2	Media: Ethernet frame headers "SA" and "DA" are reversed in graphic.	"DA" moved ahead of "SA" in Ethernet frame.
3.3.3.2	Media: Frame field name "CFID" disagrees with ieee802.1q 9.6 nomenclature	Changed dot1Q field labeled "CFID" to "CFI" as per ieee802.1q 9.6 nomenclature
3.3.3.2	Text: The text: "Devices with ports that are not 802.1Q-compatible view a tagged Ethernet frame as too large. They drop the frame and log it as an error, called a baby giant." disagrees with the CCNP 3 text which states: "If a non-802.1Q-enabled device or an access port receives an 802.1Q frame, the tag data is ignored, and the packet is switched at Layer 2 as a standard Ethernet frame. This allows for the placement of Layer 2 intermediate devices, such as other switches or bridges, along the 802.1Q trunk path. To process an 802.1Q tagged frame, a device must allow an MTU of 1522 or higher."	Newer versions of the IOS support the ability to accept baby giant frames. In this case they will switch the 802.1Q tagged frame at layer 2, ignoring the tag. Older versions of the IOS may discard the frame. Curriculum has been updated to agree with CCNP.
3.3.3.3	Media: Activity appears to always produce a frame that is not deliverable.	This activity does score correctly but the probability of obtaining a frame that is delivered is low.
3.4.1.3	Text: Text assumes students recognize that the Cisco 2960 is a switch.	Changed: The 2960 does not require that statement because it only supports 802.1Q. To: The 2960 switch does not require that statement because it only supports 802.1Q.
3.4.2.2	Text: Incorrect command provided for setting native VLAN	Change "Switch(config-if)#dot1q native vlan 3" To "Switch(config-if)#switchport trunk native vlan 3"
3.4.2.2	Text: Spanning-tree loops do not exist as stated in the text.	Change "If they are different, spanning-tree loops might result." To: "if they are different, bridging loops may result."

3.4.2.2	Text: Incorrect command provided for setting nateive VLAN.	Change "Switch(config-if)#dot1q native vlan vlan-id" to "Switch(config-if)#switchport trunk native vlan vlan-id" To "Switch(config-if)#switchport trunk native vlan vlan-id"
3.4.2.2	Media: Incorrect commands provided in graphic for setting native VLAN.	Change "Switch(config-if)#dot1q native vlan vlan 3" To "Switch(config-if)#switchport trunk native vlan 3"
3.5.1.3	Text: Incorrec information provided about how to reset the VTP revision number.	Deleted the statements: "Rebooting the switch also resets the revision number to zero." and:: "When adding a new switch to an existing network, always reboot the switch just prior to adding it to the network to reset the revision number." Added text: The 2 ways to reset the VTP config revision number are: 1) Set the new switch to transparent mode and then switch it back to client or server . 2) Change the domain name to something else then change it back.
3.5.1.4	Text: Inaccurate information provided about VTP advertisement requests.	Change "VTP clients use advertisement requests to ask for VLAN information." To: "Catalyst switches use advertisement requests to ask for VLAN information."
3.5.2.1	Text: Incorrect VTP version specified.	Changed "Step 1 Configure VTP off-line (version 1)" to "Configure VTP off-line"
3.5.2.1	Text: Remove reference to rebooting switch to reset VTP revision number. This will not work.	Change "Step 3: Reboot the switch." To "Step 3: Ensure the VTP configuration version is reset by setting the switch to transparent mode then changing it back to client or server; or by changing the domain name to something else, such "test" then changing it back to required name."
3.5.2.1	Media: Graphic does not match text.	Changed the commands in Step 3 of the graphic to match Step 3 in the text.
3.5.2.2	Packet Tracer: Corrected grammar, spelling and formatting errors.	
3.5.2.3	Packet Tracer: Activity only scores to 92% - scoring criteria require amendment.	Removed reference to rebooting switch to clear VTP revision number and verify scoring.
3.5.2.3	Packet Tracer: Corrected grammar, spelling and formatting errors.	
3.5.2.3	Packet Tracer: Word and pdf files show diff question for Reflection question 'a' then contained in pka file.	Updated .pka so that Reflection a. has same question as word docs.
3.5.2.3	Packet Tracer: Activity does not score correctly.	The .pka was scoring incorrectly, included the trunk link on the 1st_Floor2 switch to get activity to score correctly.

3.5.2.3.	Packet Tracer: Slow convergence on activity.	<p>Reworked activity to improve convergence time.</p> <p>In the initial network and answer networks for the activity, removed the switchport mode trunk configuration for the giga interfaces on both switches.</p> <p>Reordered the sub steps in step 3 to speed up conversion of VTP. Also, added a new step 3b advising that the trunk link between 1_st Floor3 switch and 1st_Floor2 switch needs to be green prior to configuring the VTP commands on the switch.</p>
3.5.3.3	Packet Tracer: Corrected grammar, spelling and formatting errors.	
3.5.4.1	Text: Incorrect information about power cycling a Catalyst switch to zero VTP revision number.	<p>Deleted second bullet under "VTP Revision Number"</p> <p>Added new bullet: Reset the revision number by either of the following: 1) set the new switch to transparent mode then switch it back to client or server . 2) Change the domain name to something else, change it back</p>
3.5.4.2	Lab: Incorrect Switch prompts on commands in Step 7a.	<p>Changed step 7a of lab to:</p> <pre>Switch3(config)#int fa0/2 Switch3(config-if)#switchport access vlan 30 Switch3(config-if)#int fa0/3 Switch3(config-if)#switchport access vlan 30 Switch3(config-if)#int fa0/4 Switch3(config-if)#switchport access vlan 10 Switch3(config-if)#int fa0/5 Switch3(config-if)#switchport access vlan 40</pre>
3.5.4.2	Packet Tracer: Corrected grammar, spelling and formatting errors.	
3.5.4.2	Packet Tracer: First bullet in Background / Preparation is incorrectly worded. It sounds like only one switch was purchased when actually three were.	<p>Changed bullet from: One Cisco 2960 switch has been purchased for each of the 3 floors. To: Three Cisco 2960 switches have been purchased, one for each of the three floors.</p>
4.2.2.1	Media: The mark used to indicate the length of each 8-bit number does not match the actual length of the bit pattern.	<p>Realigned markers to coincide with ends of 8-bit values.</p>
4.3.1.2	Media: The labels on R2 and R3 do not agree with text. They are reversed.	<p>R2 and R3 labels swapped to agree with text in graphic.</p>
4.3.1.4	Text: Ambiguous text in third bullet.	<p>Changed: The sending router, by default, summarizes all of the subnets and advertises the major classful network. To: The sending router, by default, summarizes all of the subnets and advertises the major classful network along with the summarized subnet mask</p>

		information.
4.3.3.2	Media: There is no correct answer to the third group of addresses. The summary address should be 10.3.5.0/24	All choices in question 3 should have a base IP address of 10.3.5.0 with a mask of /24, /25, /26 and /28 respectively. The correct summary address for the group is 10.3.5.0/24.
4.3.3.3	Lab: Background/Preparation reverses routers B and C.	Changed to: After completing the table for RouterC, calculate the summarization for RouterB (it only advertises one route).
4.3.4.3	Lab: Incorrect Router prompts in Steps 5b, 6b, 7b and 7d.	In steps 5b, 6b, 7b, and 7d, the output shown should be Router1# (first line 5b, and 6b and 7b outputs). 2nd line of commands in 5b should be Router2. 3rd line of commands in step 5b should be Router3.
4.3.5.1	Media: Extra address in bottom right portion of expanded network graphic.	Removed extra network address from bottom right area of expanded network graphic. Removed 10.4.80.0/20 and relocated 10.4.64.0/20 to proper location.
4.4.3.3	Lab: Wrong address used for NAT translation in Step 13b	Changed Step 13b command and step to the following: Gateway(config)#ip nat inside source static 10.10.10.2 209.165.200.225 This permanently maps 209.165.200.225 to the inside address 10.10.10.2.
4.4.3.3	Packet Tracer: Corrected grammar, spelling and formatting errors.	
4.4.3.3	Packet Tracer: Step 3 and Reflection a both refer to the R&D_1 workstation and then just Rmt_Wks	Changed instructions to refer to both devices as workstations: Rmt_Wks workstation.
4.4.3.4	Packet Tracer: Corrected grammar, spelling and formatting errors.	
5.1.3.3	Packet Tracer: Corrected grammar, spelling and formatting errors.	
5.1.4.4	Packet Tracer: Corrected grammar, spelling and formatting errors.	
5.1.5.1	Media: Incorrect network address in graphic. The ip route output shows Fa0/0 connected 172.16.3.0 but the graphic shows the address as 172.16.2.0.	Changed network address in graphic to 172.16.3.0/24 to agree with output.
5.1.5.2	Packet Tracer: Corrected grammar, spelling and formatting errors.	
5.1.5.2	Packet Tracer: Step 4 b - modified note.	Changed the note to reflect no IP address being shown as the gateway of last resort: The routing table now contains routing information for the two locally connected networks and a default route setting the Gateway of last resort.
5.2.2.1	Text: Current text is ambiguous.	Replaced page text with: "Routing Information Protocol (RIP) was the first IP distance vector routing protocol to be standardized in a RFC (RFC1058 in

		<p>1988). The first version of RIP is now often called RIPv1 to distinguish it from the later improved version, RIPv2; and from the IPv6 version, RIPv6.</p> <p>By default RIPv1 broadcasts its routing updates out all active interfaces every 30 seconds.</p> <p>RIPv1 is a classful routing protocol. It automatically summarizes subnets to the classful network boundary and does not send subnet mask information in the update. Therefore RIPv1 does not support VLSM and CIDR. A router configured with RIPv1 either uses the subnet mask configured on a local interface, or applies the default subnet mask based on the address class. Due to this limitation, the subnets of the networks that RIPv1 advertises should not be discontinuous if correct routing is to occur.</p> <p>For example, a router configured with interfaces as the gateways for the 172.16.1.0/24 and 172.16.4.0/24 subnets will advertise only the 172.16.0.0 Class B network with RIPv1. Another router receiving this update will therefore list the 172.16.0.0 network in its routing table. This means packets with an actual destination subnet address of 172.16.3.0 could mistakenly be forwarded to the advertising router and therefore not arrive at the correct destination subnet.</p> <p>The graphic shows that even if the subnets are configured to be advertised by RIPv1 separately, only the classful network is used."</p>
<p>5.2.2.1</p>	<p>Current diagram does not show automatic summarization by RIPv1.</p>	<p>Graphic to be changed to reflect automatic summarization by RIPv1: Amended graphic: On R2 delete text "Fa0/0" and "192.168.3.0/24" On R2 delete text "Fa0/1" and "192.168.4.0/24" Delete two dashed lines connecting R2 with two PCs Delete the two PCs attached to R2 Replace text "192.168.1.0/24" with "172.16.1.0/24" Replace text "192.168.2.0/24" with "172.16.4.0/24"</p> <p>Deleted all graphic output text (show ip protocols o/p) Replaced with: ----- ---- Attempt to configure RIPv1 to advertise subnets - R1(config)#router rip</p>

		<pre>R1(config-router)#network 172.16.1.0 R1(config-router)#network 172.16.4.0 Actual configuration showing summarized network to be advertised - R1#show running-config < output omitted > ! interface FastEthernet0/0 ip address 172.16.1.1 255.255.255.0 ! < output omitted > ! interface Serial0/0/0 ip address 172.16.4.1 255.255.255.0 shutdown ! < output omitted > ! router rip network 172.16.0.0 <--- Summarized Class B network only, not separate subnets, advertised ! -----</pre>
5.2.2.3	Tables missing headers.	Added Network, Interface and Hop column headers to each table.
5.2.4.5	Packet Tracer: Corrected grammar, spelling and formatting errors.	
5.2.5.2	Packet Tracer: Corrected grammar, spelling and formatting errors.	
5.3.2.3	Media: Incorrect interface in R2 table.	Changed interface in last row of R2 table from 's/0/0/0' to 's0/0/1'.
5.3.3.2	Media: Missing close feature on popup box.	Added close capability to popup box.
5.3.5.4	Media: Links between routers show as arrows not lines.	Changed arrows between routers to lines to indicate links.
5.4.1.4	Lab: Lab introduction incorrect.	<p>Changed to :</p> <p>This lab presents a three router corporate network using variably subnetted private IP addressing. On Branch1 and Branch2, loopback interfaces simulate LANs attached to those routers. The design creates discontinuous subnets on the routers which will be "hidden" when EIGRP is configured with automatic summarization as the default. You will enable EIGRP MD5 authentication to protect your routing updates.</p> <p>The following resources are required:</p> <ul style="list-style-type: none"> • Three Cisco 1841 routers or comparable routers • At least one PC with a terminal emulation program • At least one RJ-45-to-DB-9 connector console cable • Three serial cables to connect R1 to both R2 and R3, and to connect R2 to R3

5.4.1.4	Lab: Lab uses wrong keychain name and is missing commands.	<p>Changed to:</p> <p>Create a keychain named discchain. Configure a key that has a key string of san-fran. Enable the Branch1 router to utilize EIGRP MD5 authentication with each of your EIGRP neighbors and to use the keychain discchain.</p> <pre>Branch1(config)#key chain discchain Branch1(config-keychain)#key 1 Branch1(config-keychain-key)#key-string san-fran Branch1(config-keychain-key)#end Branch1#configure terminal Branch1(config)#interface serial 0/0/0 Branch1(config-if)#ip authentication mode eigrp 100 md5 Branch1(config-if)#ip authentication key-chain eigrp 100 discchain Branch1(config-if)#exit Branch1(config)#interface serial 0/0/1 Branch1(config-if)#ip authentication mode eigrp 100 md5 Branch1(config-if)#ip authentication key-chain eigrp 100 discchain</pre> <p>b. Repeat the MD5 authentication configuration for the Branch2 and Gateway routers.</p> <p>c. View the contents of the Gateway, Branch1, and Branch2 routing tables to ensure all routing updates are still being accepted.</p> <pre>Gateway#show ip route</pre> <p>List the routes that are shown on the Gateway router.</p>
5.4.2.3	Corrected grammar, spelling and formatting errors.	
5.4.2.3	Incorrect command in Step 1 b3.	<p>Changed from: Enter no auto summary To Enter the no auto-summary command.</p>
5.4.2.3	Packet Tracer: Reworked the activity to remove the manual summarization.	
5.4.3.1	Media: Improper command labels on media buttons.	<p>Changed flash activity buttons to be consistent with router output:</p> <p>From: show ip eigrp neighbors details To: show ip eigrp neighbors detail</p> <p>From: show ip eigrp interfaces details To: show ip eigrp interface detail</p>
5.4.3.4	Packet Tracer: Corrected grammar, spelling and formatting errors.	
6.1.2.2	Media: Activity is confusing. It is hard to tell which paths are identified as the Least Cost Path.	<p>Removed confusion by identifying the Least Cost Path added to each of the orange boxes and removing extra arrows.</p>
6.2.1.3	Media: Activity provides incorrect answers and scoring.	<p>Corrected activity logic to provide and score correct answers.</p>

6.2.3.5	Lab: Step 5a has an incorrect command -- bandwith should be bandwidth.	Corrected spelling on "bandwidth"
6.2.4.2	Media: Incorrect IP addresses in show ip protocols popup box.	Changed: 172.168.10.0 and 172.168.10.4 To: 192.168.10.0 and 192.168.10.4
6.2.4.4	Lab: Step 9f has an incorrect command in the wording.	The first line should be Use the show ip ospf neighbor (not neighbors) command Changed Step 9f to "Use the show ip ospf neighbor command"
6.3.4.4	Media: The bottom routing table has several incorrect ip addresses,	Changed: Destination 172.168.0.10 Router 1 172.168.0.0/12[110/65]via 172.168.0.1 serial0/0/0 Router 2 172.168.0.0/18[110/65]via 172.168.1.1 serial0/0/1 Router 3 172.168.0.0/26[110/65]via 172.168.1.1 serial0/1/0 To: Destination 172.168.0.10 Router 1 172.16.0.0/12[110/65]via 192.168.0.1 serial0/0/0 Router 2 172.16.0.0/18[110/65]via 192.168.1.1 serial0/0/1 Router 3 172.16.0.0/26[110/65]via 192.168.1.1 serial0/0/1
6.3.4.5	Media: Option 2 on question 5 refers to a FastSerial port. This does not exist.	Option 2 on question 5 changed to 'FastEthernet'.
7.2.1.1	Packet Tracer: Corrected grammar, spelling and formatting errors.	
7.2.3.3	Lab: Steps 4, 5, 8, 9 and 11 use wrong command "show interface".	Changed all occurrences to "show interfaces"
7.2.3.3	Lab: Step 7a uses wrong interface.	Changed interface in Step 7a to S0/0/0
8.1.3.2	Media: When you get the activity all correct, it marks everything correct but provides feedback that you are incorrect.	Changed scoring so that when activity is correct the proper feedback is provided.
8.3.1.4	Media: R2 s0/0/1 label in wrong location.	Relocated R2 s0/0/1 label above link between R2 and ISP.
8.3.3.4	Lab: Step 10 is missing. It goes from Step 9 to Step 11.	Lab steps renumbered.
8.3.3.4	Lab: Diagram and loopback masks are not correct.	Main graphic changed: (1) Loopback 1 becomes Loopback 0, (2) Loopback 2 becomes Loopback 1, (3) Fa0/0 needs to be closer (down) to the R1 Fa0/0 interface line. Main table needs to have the mask on the loopback interface addresses: Lo0 192.168.1.1/32 and Lo1 192.168.2.1/32 to be consistent with other labs and interface addressing schemes.
8.3.3.4	Lab: Missing instruction in step 8.	Added step 8i to display ACL again using show access-list command.

8.3.5.2	Media: When selecting "Insert" the line numbers on the new ACL are incorrect.	Changed line number '30' to '25' and changed line number '40' to '30'
8.3.5.3	Packet Tracer: Corrected grammar, spelling and formatting errors.	
8.3.5.3	Packet Tracer: Step 3 subheading refers to ACLs, there is only one ACL	Changed the sub-heading from: Verify ACLs are working properly To: Verify the ACL is working properly
8.3.5.4	Lab: Step 10a and 10c use improper command "show access-list"	Changed command in Step 10a and 10c to "show access-lists"
8.3.6.3	Packet Tracer: ACL 160 is filtering tcp on each line, should filter tcp only on the line pertaining to www access (http)	Change the ACL in the answer network from: access-list 160 permit tcp 172.16.10.0 0.0.0.255 172.16.30.0 0.0.0.255 access-list 160 permit tcp 172.16.100.0 0.0.0.255 host 172.16.30.100 eq www access-list 160 deny tcp 172.16.100.0 0.0.0.255 host 172.16.30.100 access-list 160 deny icmp 172.16.100.0 0.0.0.255 172.16.30.0 0.0.0.255 access-list 160 permit tcp any any To: access-list 160 permit ip 172.16.10.0 0.0.0.255 172.16.30.0 0.0.0.255 access-list 160 permit tcp 172.16.100.0 0.0.0.255 host 172.16.30.100 eq www access-list 160 deny icmp 172.16.100.0 0.0.0.255 172.16.30.0 0.0.0.255 Remove the permit tcp any any as the scenario states all other access should be denied.
8.3.6.4	Packet Tracer: Corrected grammar, spelling and formatting errors.	
8.3.6.4	Packet Tracer: Incorrect subnet masks on servers in first table.	The servers show subnet masks of, 255.255.255.255, in the table. Change this to the actual subnet masks of 255.255.255.0
8.3.6.4	Packet Tracer: Background states London clients need access to the London Server, all other access should be denied and the DC clients need access to the DC Server and that all other access to the DC server should be denied. The table and testing does not follow this. The table shows London Clients being granted access to the DC server for http, and the DC Clients granted access to the London server.	Background statements changed to match the table configuration.

8.3.6.4	Packet Tracer: ACL 150 is filtering tcp on each line, should filter tcp only on the line pertaining to www access (http)	<p>Changed the ACL in the answer network from: access-list 150 permit tcp 172.16.100.0 0.0.0.255 172.16.20.0 0.0.0.255</p> <pre>access-list 150 permit tcp 172.16.10.0 0.0.0.255 host 172.16.20.100 eq www access-list 150 deny tcp 172.16.10.0 0.0.0.255 host 172.16.20.100 access-list 150 deny icmp 172.16.10.0 0.0.0.255 172.16.20.0 0.0.0.255 access-list 150 permit tcp any any To: access-list 150 permit ip 172.16.100.0 0.0.0.255 172.16.20.0 0.0.0.255 access-list 150 permit tcp 172.16.10.0 0.0.0.255 host 172.16.20.100 eq www access-list 150 deny icmp 172.16.10.0 0.0.0.255 172.16.20.0 0.0.0.255</pre> <p>Remove the permit tcp any any as the scenario states all other access should be denied.</p>
8.3.6.4	Packet Tracer: The named ACL on the London router in Step 3 is blocking tcp. Should block ip from the DC clients, not tcp.	<p>Change:</p> <pre>ip access-list extended ICMP permit icmp 172.16.10.0 0.0.0.255 172.16.100.0 0.0.0.255 deny tcp 172.16.10.0 0.0.0.255 172.16.100.0 0.0.0.255 permit tcp any any</pre> <p>To:</p> <pre>ip access-list extended ICMP permit icmp 172.16.10.0 0.0.0.255 172.16.100.0 0.0.0.255 deny ip 172.16.10.0 0.0.0.255 172.16.100.0 0.0.0.255 permit ip any any</pre>
8.3.6.4	Packet Tracer: Missing/Ambiguous information in Step 4b	<p>There is a problem here. The PC2 should be able to browse and ping the DC server, for DC clients in the table have full access to the DC resources and this includes the DC server. Add information instructing the PC2 to browse the London server and ping the London server and advise that the ping should fail.</p> <p>The PC1 should be able to browse and ping the London server as the table states that the London clients have full access to all London resources and this includes access to the London server. Add steps here to have PC1 browse the DC server and this will succeed and then ping the DC server and this should fail.</p>
8.3.6.4	Packet Tracer: Incorrect server address in Step 4b4	The address for the London Server is 172.16.20.100, not 172.16.30.100.
8.4.1.3	Packet Tracer: Corrected grammar, spelling and formatting errors.	
8.4.5.3	Packet Tracer: Corrected grammar, spelling and formatting errors.	

8.4.5.3	Packet Tracer: Instructions do not match the ACL configured for the answer network	<p>ACL 110 is written to permit http and DNS to specific servers. The instructions read that we are going to permit http and DNS access to the server farm. This alludes to broader access i.e. permitting http and dns to the entire server farm subnet, vs permitting access to a specific host. Modify the instructions to match the answer network.</p> <p>Changed the Background/Preparation second and third sentences from: The server farm consist of both web and DNS servers. The Senior Network Engineer only wants to allow web and DNS traffic into the server farm.</p> <p>To: The server farm consists of a Web Server and a DNS Server. The Senior Network Engineer only wants to allow web access to the Web Server and DNS traffic into the server farm using the DNS Server. Also changed Step 2 c from: Create an ACL numbered 110 which permits the HTTP and DNS protocols for any host, but denies all other IP traffic into the server farm.</p> <p>To: Create an ACL numbered 110 which permits the HTTP and DNS protocols for any host, but denies all other IP traffic to the Web Server and DNS Server.</p>
8.4.5.3	Packet Tracer: Missing information in Step 1.	Added additional information that all attempts to ping, telnet and browse should be successful.
8.4.5.3	Packet Tracer: Unclear statements in Step 4f.	<p>Changed: The pings should be unsuccessful, while browsing should be successful.</p> <p>To: The attempts to ping and telnet should be unsuccessful, while browsing should be successful.</p>
8.4.5.3	Packet Tracer: Missing Note in Step 2c.	Added note here that the students should create ACLs using the protocol and not port numbers or scoring will be off on the activity. Add: Note: Create the ACL to filter traffic using protocols instead of port numbers.
8.4.5.3	Packet Tracer: Missing information from note in Step 3c.	Added information to note: "Create the ACL to filter using protocols instead of port numbers."
8.4.5.3	Packet Tracer: Answer network has a PC3, but no PC2	Changed the name of the PC in the answer network from PC3 to PC2 (The PC is correct in the initial network.)
8.4.5.3	Packet Tracer: Reflection d question is wrong.	Question asks: d. Since PC1 and PC2 can both telnet to the Border1 router, should PC1 and PC2 be able telnet to each other's VLAN gateway address? However ... PC1 cannot telnet to Border1 because of the ACL. Changed the question to read: d. Since PC2 can telnet to the Border1 router, should PC1 and PC2 be able telnet to each other's default gateway address?
9.1.2.5	Packet Tracer: Corrected grammar, spelling and formatting errors.	

9.1.2.5	Packet Tracer: Incorrect device name and command in Background/Preparation.	Changed second and third sentences. First sentence to make name of device match the .pka - from Router 0 to Router0 and boldface Router0. Last sentence-curriculum refers to tracert, not trace route in LI 9.1.2.4.
9.1.2.5	Packet Tracer: Wrong command in Step 1b.	Changed trace route to tracert: b. "Select PC2 and execute a ping and tracert to each of the devices in the chart below."
9.2.1.5	Packet Tracer: Corrected grammar, spelling and formatting errors.	
9.2.1.5	Packet Tracer: Student is asked to verify that link between PC and switch is connected to correct switch port. If incorrect, the student cannot move cable, activity has this blocked.	Removed lock on Create new devices, connect, and disconnect links so the activity can be completed.
9.2.1.5	Packet Tracer: Wording in Step 2 is ambiguous from Step 2b onwards.	<p>Changed Step 2 to: b. Using your notes from Step 1, ensure all PC links connect to the correct switch port.</p> <p>3. Adjust any links between the PCs and the switch that are incorrect.</p> <p>4. From the Switch CLI, what additional commands are necessary to resolve the problems with the network? Enter the commands so that each PC can successfully ping all other PCs in the activity.</p>
9.2.2.4	Packet Tracer: Corrected grammar, spelling and formatting errors.	
9.2.2.4	Packet Tracer: Activity has students looking at switch configurations before looking at the router. To troubleshoot when VLANs are not documented, it would make more sense to look at the router configuration first for VLAN info that is trunked, versus looking at the switches.	Moved the router verification to Step 2 and have the switch verification as Step 3.
9.2.3.3	Packet Tracer: Corrected grammar, spelling and formatting errors.	
9.3.1.2	Media: For the "R1 debug ip rip" button, some output is not visible. There is more output after the orange line, but the scrollbar cannot go further down.	Output resized to allow viewing of the entire command output.
9.3.1.3	Packet Tracer: Corrected grammar, spelling and formatting errors.	
9.3.1.3	Packet Tracer: Step 1 duplicates previous instructions.	Refers to Router0 and Router1, we already performed steps on Router1, change the instruction to: Repeat steps c-g for Router0 and Router2 .
9.3.1.3	Packet Tracer: Incorrect reference to button in Step 1 c 1	There is no such button in Simulation as Auto / Capture Forward and the mode is Simulation (mode should not be capitalized, Simulation should be boldfaced.). Change instruction to: Switch to Simulation mode

		and click the Auto Capture / Play button.
9.3.1.4	Lab: There are two Step 4 and two Step 5 in this lab.	Lab steps correctly renumbered.
9.3.1.4	Lab: Page 5 Step 4b and Step 4e use incorrect command "show ip protocol"	Changed command for Step 4b and Step 4e to "show ip protocols"
9.3.2.3	Packet Tracer: Corrected grammar, spelling and formatting errors.	
9.3.3.1	Media: For the "show ip ospf" button output, the orange box is cut off at the bottom.	Output resized to allow viewing of the entire command output.
9.3.3.2	Media: The "3" button command output is cut off.	Output resized to allow viewing of the entire command output.
9.4.1.5	Packet Tracer: Network issues in this troubleshooting PT center around R4 not R1 - also newly added router would usually be #4 not #1	In Instructions: Background / Preparation Replaced "R1" with "R4" in these two sentences - "The extension of the WAN included the installation of router R1. The R1 router has two Point to Point serial connections to the R2 and R3 routers and an Ethernet LAN segment."
9.4.1.5	Packet Tracer: Corrected grammar, spelling and formatting errors.	
9.4.2.3	Packet Tracer: Corrected grammar, spelling and formatting errors.	
9.5.1.3	Media: The command output from the "1" button is truncated.	Output resized to allow viewing of the entire command output.
9.5.1.4	Packet Tracer: Corrected grammar, spelling and formatting errors.	
9.5.1.4	Packet Tracer: Incorrect type of ACL identified in Step 2 c.	To deny Telnet and the other protocols requires an extended ACL, not a standard ACL. Change from: Examine the standard access-list. To: Examine the ACL configured on the router.
9.5.1.4	Packet Tracer: Incorrect instruction provided in Step 3 a.	Correct the instruction by changing: Verify that PC0 and PC1 are unable to Telnet to and R3. To: Verify that PC0 and PC1 are unable to Telnet to R0, R1, R2 and R3.
9.5.2.3	Packet Tracer: Corrected grammar, spelling and formatting errors.	
9.6.2.1	Media: Insufficient information provided to answer question number 4.	Graphic replaced to provide all information required to answer question.

<p>10.0.1.2</p>	<p>Lab: Mistakes in INSTRUCTOR GUIDE</p>	<p>(1) Task 5 Step 2 INSTRUCTOR GUIDE has a duplicate of the permit icmp 172.20.1.64 0.0.0.63 any command line. (2) Task 5 Step 3 INSTRUCTOR GUIDE steps a and b should be access-list 2 and access-class 2 because access-list 1 has already been used to define what gets natted. (3) Instructor Guide page 34 of 44 HQ router access-list 1 should be access-list 1 permit 172.20.0.0 0.0.1.255 instead of access-list 1 permit 172.20.0.130 because access-list 1 is used for ip nat inside source list 1 in the line above this. Add an access-list 2 permit 172.20.0.130 to control telnet to HQ. (4) Instructor Guide page 35 of 44 does not need the ip route line. This network is directly connected to the ISP. (5) Instructor Guide page 40 of 44 is missing the port-security commands for int fa0/15. Add the following lines to Fa0/15: switchport port-security; switchport port-security mac-address sticky (there will be a third line in the show run once you ping from a workstation...the MAC address will be different, but the line is as follows for example switchport port-security mac-address-sticky 0012.3f0b.1224) (6) Instructor Guide page 43 of 44 is missing the port security commands for int fa0/20. Add the following lines to Fa0/20: switchport port-security; switchport port-security mac-address sticky (there will be a third line in the show run once you ping from a workstation...the MAC address will be different, but the line is as follows for example switchport port-security mac-address-sticky 0011.1179.4112)</p>
<p>10.0.1.3</p>	<p>Packet Tracer: Corrected grammar, spelling and formatting errors.</p>	
<p>10.0.1.3</p>	<p>Packet Tracer: Background/Preparation section ambiguous.</p>	<p>Change from: AnyCompany1 has been a victim of a hacking attack. This hackers intent was to disrupt communication versus destroy data. The attack was focused the companies routers and switches. Identify the configuration changes that the hacker made. Once identified resolve and test connectivity. To: AnyCompany1 has been a victim of a hacking attack. This focus of the attack was on disrupting communication versus destroying data. The attack focused on the company routers and switches. Identify any configuration changes that the hacker made. All passwords should be set to cisco. Once errors are identified, correct the configuration and test connectivity.</p>
<p>10.0.1.3</p>	<p>Packet Tracer: Missing step at beginning of Step 1.</p>	<p>Add a step to the start: "Use ping to identify any potential connectivity problems."</p>

10.0.1.3	Packet Tracer: Additional information required in Step 4 a.	Add more information to advise students of what the ACL is filtering for. Change from: a. View the R2 access list configuration. To: a. The company routing policy allows the following activities: All users are allowed web access to any destination. All users are allowed to use ping to test connectivity. Users working in Dept 2 are allowed to use Telnet. Users working in Dept 3 are allowed to use FTP. All other user traffic is blocked. View the R2 ACL configuration.
10.0.1.3	Packet Tracer: Incorrect subnet mask on PC H3.	Changed H3 subnet mask from 255.255.255.128 to 255.255.255.192
10.0.1.3	Packet Tracer: Last error difficult to detect.	The last error students are to find is on HQ. It has a correct username for the PPP connection to the ISP, but it has an incorrect password: username ISP password class should be username ISP password cisco. The problem is that the interface is up, even with the incorrect password. It appears that PT does not check this. Changing the last error. Since one of the errors is using an incorrect subnet for the serial interface connected to R2 in the OSPF configuration, I am changing the address for HQ interface to match the incorrect subnet address advertised in OSPF.
Glossary	Glossary: Term VMPS shows "VLAN policy server", but it should be "VLAN management policy server."	VMPS glossary term corrected to "VLAN Management Policy Server".
Glossary	Glossary: Definition for native VLAN ambiguous.	Changed: Trunk links carry the untagged over the native VLAN. To: Trunk links carry the untagged traffic over the native VLAN.
Glossary	Glossary: Ambiguous definition for 'Private Addresses' in glossary.	Changed glossary definition for 'Private Addresses' to: "Type of addresses reserved for internal use and are not routed across the public Internet. In IPv4, there are three ranges of private addresses. These include 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255."
Glossary	Glossary: "per VLAN Rapid Spanning Tree Plus" points user to "PVRST". It should be "PVRST+"	Relocated link on 'per VLAN Rapid Spanning Tree Plus' to 'PVRST+'
Glossary	Glossary: Made numerous corrections to grammar and definitions. Linked all terms to acronym and removed links to plural terms.	
Lab	Lab: Made numerous corrections to grammar and formatting.	

Support

For general assistance with curricula, classroom, or program issues, please contact the Global Support desk through the Academy Support site. To access this site, log into Academy Connection and click **Help** at the top of the page, then select **Academy Support**.

Curriculum or assessment bugs and errors should be submitted through the Curriculum and Assessment Quality Support site. To access this site, log into Academy Connection and click **Help** at the top of the page, then select **Curriculum and Assessment Quality Support**. Select the **Contact Assessment Team** or **Contact Curriculum Team** tab, depending on the nature of the problem you are reporting. Provide as much detail as possible and then click **Submit**.