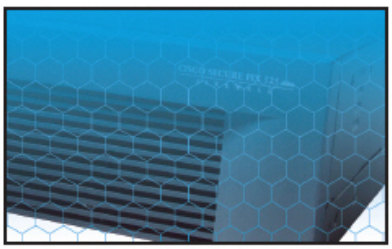
"When will you be an IPexpert?"

IPexpert's Ultimate Lab Preparation Workbook

For the Cisco® CCIE™ Security Labratory Exam (Version 3.1)



ipexpert
powered by PROCTOR LABS

IPexpert's Preparation Workbook for the Cisco® CCIE™ Security Laboratory Exam (Version 3.1)

Before We Begin

Congratulations! **You now possess the ULTIMATE CCIE™ Security Lab preparation resource available today!** This resource was produced by senior engineers, technical instructors, and authors boasting decades of internetworking experience. Although there is no way to guarantee a 100% success rate on the CCIE™ Security Lab exam, we feel **VERY** confident that your chances of passing the Lab will improve dramatically after completing this industry-recognized Workbook!

At the beginning of each section, you will be referred to a diagram of the network topology, as illustrated in Diagram A (located on page 4). All sections utilize the same physical topology, which can be rented at www.ProctorLabs.com.

Each section has been carefully laid-out and will challenge you with a specific technology or protocol. Within each section, there is a baseline overview of the technologies covered in that particular lab scenario, as well as an "Estimated Time to Complete" each scenario. Each lab starts out with a "Configuration Tasks" section that will give you specific tasks or requirements that must be met to complete each lab scenario successfully. If you are unsure of the command or unsure how to complete a required task, a "Technical Tips and Comments" section provides a portion of the IOS commands that you will need to use to complete the task successfully. In this section, you will also find helpful technical pointers from our Instructors.

In addition, for your convenience, ALL technical configurations, diagrams, and documentation are now immediately available via download in your IPexpert Member's Area. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Technical Support

CertificationTalk *(http://www.CertificationTalk.com)*

ONLINE study list *(http://www.OnlineStudyList.com)*

IPexpert is proud to lead the industry with multiple support options at your disposal free of charge. Our online forums (www.CertificationTalk.com) have attracted a membership of nearly 20,000 of your peers from around the world! At www.OnlineStudyList.com, you may subscribe to multiple "SPAM-free" email lists. Also, if you are an IPexpert Elite Member and need support for your IPexpert products, simply open a support ticket at www.IPexpert.com and it will be addressed promptly. In fact, IPexpert *guarantees* a response within one business day.

About IPexpert's Authors

IPexpert employs only the best and brightest CCIE developers and instructors in the industry. Our celebrated team of diverse experts holds multiple CCIE certifications gained from substantial and highly relevant real-world experience. These key attributes give IPexpert the leading edge for delivering the most effective training possible.

Wayne A. Lawson II
CCIE #5244 (R&S), CCNA, CCDA, Nortel NCSE, MCP, MCSE (NT 4.0), MCSE +I, CNA, CNE (4.0), CNX Ethernet, Cisco Wireless LAN Design Specialist, Cisco IP Telephony Design Specialist
Founder & President – IPexpert, Inc.
With 15 years of networking, sales and marketing experience, Mr. Lawson possesses the technical competency, leadership and visionary talent possessed only by the most successful entrepreneurs around the globe. Wayne has served as a highly effective contributing member of five major organizations, including the United States Marine Corps (USMC), International Network Services (INS), Cisco Systems, Vertical Networks and IPexpert, Inc. He has been published on the topics of "Building Cisco Remote Access Networks" (ISBN: 1-928993-13-X) and "Configuring Cisco AVVID" (ISBN: 1-928994-14-8), and has written for various technical and entrepreneurial magazines. Mr. Lawson founded IPexpert in 2001 and continues to revolutionize the way engineers prepare for the coveted CCIE Lab certification. Wayne's unique visionary approach to cutting-edge technologies and enterprise network solutions, coupled with a fanatical dedication to customer satisfaction, propel the engine of success at IPexpert. With a talent for revolutionizing products, services and solutions, and a drive to achieve perfection, his leadership and business ethics have molded IPexpert into the clear leader in CCIE Lab training. In addition to acting as the President and Senior Director of IPexpert, Inc., Wayne is also preparing for his CCIE Voice Lab exam.

Scott Morris
Quad CCIE #4713 (R&S, ISP-Dial, Security and Service Provider), CCDP, CCSP, Cisco Cable Communications Specialist, Cisco IP Telephony Support Specialist, Cisco IP Telephony Design Specialist, CCNA (WAN Switching), MCSE (NT 4.0), Juniper Networks JNCIE (#153) and JCNIS, RiverStone Networks RCNP, NSA/CNSS INFOSEC Professional, TIA Convergence Technology Professional (CTP), and CISSP #37445.
Senior Technical Instructor and Developer – IPexpert, Inc.
Boasting more than 18 years of technical training and consulting experience and a wealth of technical certifications, Scott Morris has proven himself among the elite in the technical training industry. Scott is one of the few people in the world currently holding four separate CCIE certifications, and he is actively preparing for his fifth – the CCIE Voice. Scott has an outstanding track record of success in editing, writing and reviewing training books for Cisco Press, Wylie, Sybex, Que Publishing and McGraw-Hill, and teaching CCIE lab preparation materials. He has served as a contributing author for works including Cisco Press' Managing Cisco Network Security book (ISBN: 1578701031) - Chapters on the PIX Firewall; and Cisco Press' CCIE Practical Studies, Vol. 2 (ISBN: 1587050722) - Chapter on Multicast. Scott has also written various articles for Packet Magazine and TCP Mag.

Vik Malhi
CCIE #13890 Voice, CCVP, Cisco IP Telephony Support Specialist, Cisco IP Telephony Operations Specialist, Cisco IP Telephony Design Specialist and Cisco Wireless LAN Design Specialist.
Sr. Voice Technical Instructor and Developer – IPexpert, Inc.
With nearly 10 years of IP Telephony training and consulting experience and a wealth of technical certifications, Vik Malhi has proven that he? one of the top Cisco voice instructors and consultants in the world! Vik was the first engineer to install CM 3.0 in Europe, Has over 6 years of AVVID consulting and implementation experience and has taught CCIE Voice Lab classes for the past several months. Vik has joined IPexpert's accredited team of experts and will be in charge of updating, supporting and teaching IPexpert's CCIE Voice-related products, services and classes.

Mark Snow
CCIE #14073 Voice, CCVP, CCNP, CCDP, CSE, CQS-CIPCCES, CQS-CIPTDS, CQS-CIPTOS, CQS-CIPTSS, MCSE.
Sr. Voice Technical Instructor and Developer – IPexpert, Inc.
From the age of 5 in his father's (patented inventor) laboratory, Mark passion for technology has never stopped growing. With over 10 years working professionally in the IT industry and over 5 years spent consulting internationally with a focus on large-scale, Cisco IP Telephony, Mark brings a wealth of knowledge to the training arena. Mark holds a CCIE in Voice, as well as many other Cisco and Microsoft certifications. Mark plans to begin working on his next CCIE in Security. Mark is responsible for IPexpert's CCIE Voice training, self-paced product development and support.

Feedback

Do you have a suggestion or other feedback regarding this book or other IPexpert products? At IPexpert, we look to you – our valued clients – for the real world, frontline evaluation that we believe is necessary to improve continually. Please send an email with your thoughts to feedback@ipexpert.com or call 1.866.225.8064 (international callers dial +1.810.326.1444).

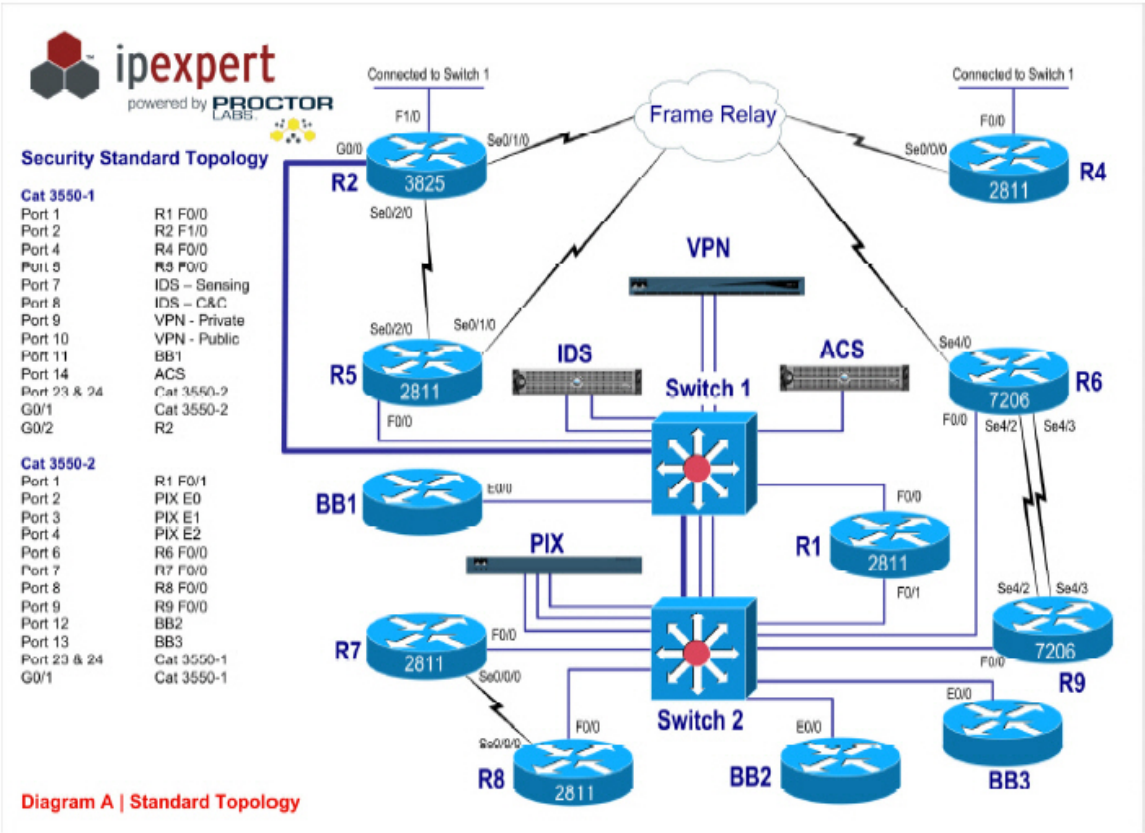
In addition, when you pass the CCIE™ Lab exam, we want to hear about it! Email your CCIE™ number to success@ipexpert.com and let us know how IPexpert helped you succeed. We would like to send you a gift of thanks and congratulations.

Additional CCIE™ Preparation Material

IPexpert, Inc. is committed to developing the most effective Cisco CCIE™ R&S, Security, Service Provider, and Voice Lab certification preparation tools available. Our team of certified networking professionals develops the most up-to-date and comprehensive materials for networking certification, including self-paced workbooks, online Cisco hardware rental, classroom training, online (distance learning) instructor-led training, audio products, and video training materials. Unlike other certification-training providers, we employ the most experienced and accomplished team of experts to create, maintain, and constantly update our products. At IPexpert, we are focused on making your CCIE™ Lab preparation more effective.

IPexpert features a variety of CCIE™ training materials to suit your needs and learning preferences. Please review the IPexpert catalog which can be downloaded from our website at www.ipexpert.com.

Diagram A | Standard Topology



NOTE:

When you download the configurations from your IPexpert Member's Area, please note that base configurations, backbone configurations and ALL diagrams seen in this workbook are included in the download (.zip) file. Please visit the following web site for instructions: http://www.ipexpert.com/configs

IPEXPERT END-USER LICENSE AGREEMENT

END USER LICENSE FOR ONE (1) PERSON ONLY

**IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS,
DO NOT OPEN OR USE THE TRAINING MATERIALS.**

This is a legally binding agreement between you and IPEXPERT, the "Licensor," from whom you have licensed the IPEXPERT training materials (the "Training Materials"). By using the Training Materials, you agree to be bound by the terms of this License, except to the extent these terms have been modified by a written agreement (the "Governing Agreement") signed by you (or the party that has licensed the Training Materials for your use) and an executive officer of Licensor. If you do not agree to the License terms, the Licensor is unwilling to license the Training Materials to you. In this event, you may not use the Training Materials, and you should promptly contact the Licensor for return instructions.

The Training Materials shall be used by only **ONE (1) INDIVIDUAL** who shall be the sole individual authorized to use the Training Materials throughout the term of this License.

Copyright and Proprietary Rights

The Training Materials are the property of IPEXPERT, Inc. ("IPEXPERT") and are protected by United States and International copyright laws. All copyright, trademark, and other proprietary rights in the Training Materials and in the Training Materials, text, graphics, design elements, audio, and all other materials originated by IPEXPERT at its site, in its workbooks, scenarios and courses (the "IPEXPERT Information") are reserved to IPEXPERT.

The Training Materials cannot be used by or transferred to any other person. You may not rent, lease, loan, barter, sell or time-share the Training Materials or accompanying documentation. You may not reverse engineer, decompile, or disassemble the Training Materials. You may not modify, or create derivative works based upon the Training Materials in whole or in part. You may not reproduce, store, upload, post, transmit, download or distribute in any form or by any means, electronic, mechanical, recording or otherwise any part of the Training Materials and IPEXPERT Information other than printing out or downloading portions of the text and images for your own personal, non-commercial use without the prior written permission of IPEXPERT.

You shall observe copyright and other restrictions imposed by IPEXPERT. You may not use the Training Materials or IPEXPERT Information in any manner that infringes the rights of any person or entity.

Exclusions of Warranties

THE TRAINING MATERIALS AND DOCUMENTATION ARE PROVIDED "AS IS." LICENSOR HEREBY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW THE LIMITATION OF INCIDENTAL DAMAGES OR LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. This agreement gives you specific legal rights, and you may have other rights that vary from state to state.

Choice of Law and Jurisdiction

This Agreement shall be governed by and construed in accordance with the laws of the State of Michigan, without reference to any conflict of law principles. You agree that any litigation or other proceeding between you and Licensor in connection with the Training Materials shall be brought in the Michigan state or courts located in Port Huron, Michigan, and you consent to the jurisdiction of such courts to decide the matter. The parties agree that the United Nations Convention on Contracts for the International Sale of Goods shall not apply to this License. If any provision of this Agreement is held invalid, the remainder of this License shall continue in full force and effect.

Limitation of Claims and Liability

ANY ACTION ON ANY CLAIM AGAINST IPEXPERT MUST BE BROUGHT BY THE USER WITHIN ONE (1) YEAR FOLLOWING THE DATE THE CLAIM FIRST ACCRUED, OR SHALL BE DEEMED WAIVED. IN NO EVENT WILL THE LICENSOR'S LIABILITY UNDER, ARISING OUT OF, OR RELATING TO THIS AGREEMENT EXCEED THE AMOUNT PAID TO LICENSOR FOR THE TRAINING MATERIALS. LICENSOR SHALL NOT BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, REGARDLESS OF WHETHER LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. WITHOUT LIMITING THE FOREGOING, LICENSOR WILL NOT BE LIABLE FOR LOST PROFITS, LOSS OF DATA, OR COSTS OF COVER.

Entire Agreement

This is the entire agreement between the parties and may not be modified except in writing signed by both parties.

U.S. Government - Restricted Rights

The Training Materials and accompanying documentation are "commercial computer Training Materials" and "commercial computer Training Materials documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction release, performance, display, or disclosure of the Training Materials and accompanying documentation by the U.S. Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

IF YOU DO NOT AGREE WITH THE ABOVE TERMS AND CONDITIONS, DO NOT OPEN OR USE THE TRAINING MATERIALS AND CONTACT LICENSOR FOR INSTRUCTIONS ON RETURN OF THE TRAINING MATERIALS.

IPexpert's Preparation Workbook for the Cisco® CCIE™ Security Laboratory Exam (3.1)

Table of Contents

NOTE:

You are encouraged to take advantage of the knowledge and support from your peers around the globe. Join www.CertificationTalk.com to participate in online forums along with nearly 20,000 other members! Subscribe to one or more email lists at www.OnlineStudyList.com to stay informed and involved with others who are working to achieve the same goals. CertificationTalk and OnlineStudyList memberships are available to you at no charge!

Section 5: PIX Firewall *(Page 35)*

- Basic PIX Configuration (Global, NAT, NAT 0, Static)
- Configuring VLAN interfaces on the PIX
- Translations and Connections
- Access Lists and Object Groups on a PIX
- Authentication Proxy for Standard and Non-Standard Protocols through the PIX
- Advanced Filtering on the PIX
- Routing RIP and OSPF on the PIX
- Running Routing Protocols through the PIX Firewalls (IGP and BGP)
- Remote Management of the PIX
- DHCP Server on the PIX

Section 6: IPSec *(Page 45)*

- Configuring a Router-to-Router IPSec Tunnel using Pre-Shared Keys
- Configuring a Router-to-Router IPSec Tunnel using a GRE Tunnel through the PIX
- Configuring a Router-to-PIX Tunnel
- Configuring a PIX for PPTP Connections

Section 7: VPN Concentrator *(Page 53)*

- Configuring the VPN Concentrator from the CLI
- Enabling Routing Protocols on the Concentrator
- Configuring a LAN-to-LAN Tunnel from a Router to a Concentrator
- Configuring a Remote Access VPN using PPTP and IPSec
- Configuring Web VPN
- Configuring EZVPN between a Router and a Concentrator

Section 8: Switching *(Page 59)*

- Creating VTP Domains with Authentication
- Trunking
- VLANs and Port Assignment
- Port Security
- Configuring the Switch to Communicate to a VMPS Server
- Dot1x Authentication
- Filtering
- L3

Section 9: IDS *(Page 65)*

- Configuring IDS on a Router
- Configuring IDS on the PIX
- Configuring the IDS Sensor Appliance from the CLI
- Configuring the IDS Sensor Appliance from IDM
- Configuring IEV to Receive Alarms from the Sensor
- Fine Tuning Signatures on the Sensor
- Creating Custom Signature on the Sensor
- Configuring Shun on a PIX

Appendices

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 1: Access Control Lists (ACLs) and Filters for IP

- Named Access Lists
- Time-Based Access Lists
- Dynamic Access Lists
- Reflexive Access Lists
- Context Based Access Lists (CBAC)
- RFC 1918 Filtering
- IP Spoofing Filtering

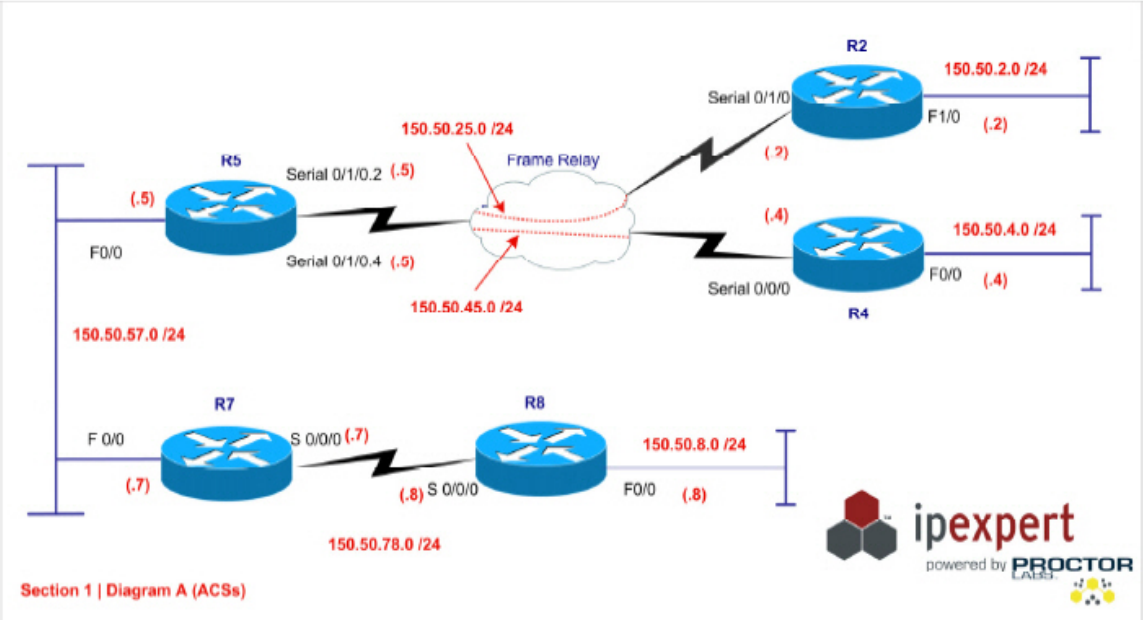
Access Control Lists (ACLs) and Filters for IP Overview

This section will test your understanding and knowledge of TCP/IP ACLs. You will configure various types of ACLs that will affect traffic flow. This section requires you to have knowledge about application ports and IP protocols, and as well as how to configure different types of ACLs.

This lab will use Routers R2, R4, R5, R7 and R8 and the appropriate Catalyst switches.

Estimated Time to Complete: 4 Hours

Diagram 1-A



Section 1 Pre-Lab Setup

- Physically connect and configure your network according to Diagram 1-A.
- The Routers are running the following protocols:
  - RIP – R2, R4 and R5 (Frame Network)
  - OSPF – R5 and R7 (Ethernet Network)
  - EIGRP – R7 and R8 (Serial Connection)
- Redistribution of the Routing protocols will be done on the appropriate Routers (R5 and R7).
- This lab will focus strictly on ACLs. You will need to pre-configure the network with the base Frame Relay, IP Addressing, OSPF, RIP and EIGRP. The pre-configuration will include the Redistribution of the Routing Protocols. Prior to starting this lab, be sure you pre-load the "Initial Configuration" for each router used in this lab scenario. You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 1 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*
- Configure the Clock and Time zone on all the routers based on Local Time. This is required for the Time Based Access Lists to work properly.

Section 1 Configuration Tasks

NOTE:

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

R2 Filtering

1) Allow traffic destined to a Web Server located at 150.50.2.80 from any where coming in through the Frame Relay interface. Traffic Filtering should be done on the Frame Relay interface in the inbound directions for all incoming traffic.

2) Users from the 150.50.2.0 network should be able to go to the outside networks and return. This should be allowed for TCP based traffic.

3) DNS queries will be sent to a DNS Server located at 150.50.57.53. Allow the DNS query replies to come back thru the Frame Relay network. The ACL entry should be as specific as possible.

4) The users on the 150.50.2.0 networks should access the Web. The access list should be created on the Frame Relay interface in the outbound direction. They are only allowed to browse during the following times:

   - 12:00 to 1:00 PM on Weekdays
   - 5:00 PM to Midnight on Weekdays
   - All day on Saturday and Sunday.

5) All the ACLs in this section should be named. You cannot use Reflexive or CBAC to accomplish the tasks in this section. Allow relevant traffic coming in. Make sure Routing is still working after you are done with this section. Be sure to log any traffic that violates these rules.

R4 Filtering

6) Allow users on 150.50.4.0 network to browse the WAN. The users should be able to go out from the following traffic:

   - Telnet
   - SMTP
   - DNS
   - HTTP
   - HTTPS

7) The return entries should be automatically created on the return.

8) The return entries should expire after 3 minutes for TCP based protocols. DNS entries should expire after 1 minute. Use minimum configuration lines to accomplish this.

9) There is a Web Server located at 150.50.4.80. Access should be allowed to this server for regular and secure web traffic.

10) The above mentioned Web Server will be taken down for Maintenance and Backups between 1:00 AM and 3:00 AM every Wednesday. The Maintenance schedule should come into effect from the 1st of next month for a duration of 6 months.

11) CBAC is not allowed to accomplish the objectives of this section. Allow relevant traffic coming in. Make sure Routing is still working after you are done with this section. Be sure to log any traffic that violates these rules

R5 Filtering

12) Allow all TCP and UDP based traffic to go out and return from the Frame Relay network on R5.

13) For web traffic, only allow Java applets to be downloaded from Web servers 150.50.4.80 and 150.50.2.80.

14) Create inbound filter on the Frame Relay interface. Log all the Denies.

15) The router should act as a Firewall and protect the internal network against Syn-floods. It should start deleting half open connections if they are at 800. It should stop deleting half open connections when they reach 600.

16) It should further protect the internal network by starting to delete half-open connections at 600 if there have been 600 new connections created within the last one minute and stop deleting at 400.

17) Configure the Router to delete TCP connections if the connection has been idle for 10 minutes.

18) Do not allow traffic with source IP address from the RFC 1918 address space to come in thru the Frame Relay interface.

19) Also block any address that should never be in the source address field.

20) Turn on an audit trail messages which will be displayed on the console after each CBAC session closes.

21) Globally specify the TCP session will still be managed after the firewall detects a FIN-exchange to be 10 seconds for all TCP sessions.

22) Changes the max-incomplete host number to 35 half-open sessions, and changes the block-time timeout to 3 minutes.

23) Set the global UDP idle timeout to 100 seconds

24) Prevent IP Spoofing using Reverse Path Forwarding.

R7 Filtering

25) Allow users on 150.50.57.0 to go out to R8 using the following protocols:

- ➔ Telnet
- ➔ SMTP
- ➔ DNS
- ➔ HTTP
- ➔ HTTPS

26) The return entries should be automatically created on the return.

27) The return entries should expire after 3 minutes for TCP based protocols. DNS entries should expire after 1 minute. Use minimum configuration lines to accomplish this.

28) Do not allow traffic with source IP address from the RFC 1918 address space to come in thru the Serial interface.

29) Also block any address that should never be in the source address field.

30) Prevent IP Spoofing using Reverse Path Forwarding.

31) Allow R8 users to access the 150.50.57.0 and the Frame Relay networks thru R7 based on successful authentication. They should only be allowed to come in for TCP based protocols.

32) Create an access list entry that is only effective after successful authentication by the host.

33) Create the username as **ipexpert** with a password of **cisco** on the router.

34) The user should use Telnet for the authentication.

35) The dynamic entry created should remain in effect for a maximum of 1 hour and should get deleted after 2 minutes of no activity.

36) Make sure you leave at least 2 lines open for Telnet Management access to the router. The administrators should use 3050 as the telnet port for management.

37) Allow 150.50.78.8 to telnet into R7 for Management access. Allow the appropriate entries in the access list.

38) CBAC is not allowed to accomplish the objectives of this section. Allow relevant traffic coming in. Make sure Routing is still working after you are done with this section. Be sure to log any traffic that violates these rules.

R8 Filtering

39) Create a lock-and-key access-list for R8s Fast Ethernet 0/0 and require users to authentication prior to accessing a web server located at 150.50.57.5

40) The session will be open at most for 100 mins.

41) The session will timeout after 10 mins of idleness.

42) The username and password for the user is **ccie** and **ccie**.

Section 1 Technical Tips and Comments

R2 Filtering

- Use the **ip access-list** command to create the ACL.
- Use the **Time-range** command to create the Time range. Use the **Periodic** command to create the Time range entries.
- Make sure the Clock and Time zone is set correctly.
- Application Ports can be used in the source or destination part of an access list.

R4 Filtering

- Use the **ip access-list** command to create the ACL.
- Use the **Time-range** command to create the Time range. Use the **Periodic** and **Absolute** commands to create the Time range entries.
- Use the **IP reflexive-list** command.
- Make sure the Clock and Time zone is set correctly.
- Use the **Show IP access-list** and **show time-range** command to verify the configurations.
- Make sure the ACL entries are active and inactive based on the correct time.

R5 Filtering

- Use the **Access-list** command to create the ACL.
- Use the **IP inspect** command to create the inspection list.
- Use the **Java-list** option in the **IP Inspect** command to allow or prevent Java applets.
- Use the **IP inspect** command to set the blocking configurations.
- Block address like Multicast, broadcast and Loopback (127.0.0.0) as source addresses.
- Use the **IP verify unicast reverse-path** command to prevent IP Spoofing.
- When the software detects a valid TCP packet that is the first in a session, and if CBAC inspection is configured for the packet's protocol, the software establishes state information for the new session. The FIN-exchange occurs when the TCP session is ready to close.
- An unusually high number of half-open sessions with the same destination host address could indicate that a denial-of-service attack is being launched against the host. For TCP, "half-open" means that the session has not reached the established state. Whenever the number of half-open sessions with the same destination host address rises above a threshold, the software will delete half-open sessions.
- When the software detects a valid UDP packet, if CBAC inspection is configured for the packet's protocol, the software establishes state information for a new UDP "session." Because UDP is a connectionless service, there are no actual sessions, so the software approximates sessions by examining the information in the packet and determining if the packet is similar to other UDP packets and if the packet was detected soon after another similar UDP packet. If the software detects no UDP packets for the UDP session for a period of time defined by the UDP idle timeout, the software will not continue to manage state information for the session.

R7 Filtering

- Use the **ip access-list** command to create the ACL.
- Use the **IP reflexive-list** command.
- Block address like Multicast, broadcast and Loopback (127.0.0.0) as source addresses.
- Use the **IP verify unicast reverse-path** command to prevent IP Spoofing.
- Use the **dynamic** keyword to create the dynamic ACL entry.
- Use the **autocommand** and **login** commands to setup authentication.
- Use the **Username** command to create the username.
- Use the **rotary** command.

R8 Filtering

- In the access-list command, the timeout is the absolute timeout. When a user logs in and enables the access-enable command, a dynamic ACL is created for the amount of timeout. The session is closed afterward, whether or not anyone is using it.
- In the autocommand command, the timeout is the idle timeout. Each time the user logs in or authenticates there is a default of 5-minute session. If there is no activity, the session closes and the user has to reauthenticate. If the user uses the connection, the absolute time takes affect.
- After a user opens a Telnet session into the router, the router will attempt to authenticate the user. If authentication is successful, the autocommand executes and the Telnet session terminates. The autocommand creates a temporary inbound access list entry at the Ethernet 0 interface, based on the second access-list entry (mytestlist). This temporary entry will expire after 5 minutes, as specified by the timeout.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 2: Network Attacks and Advanced Filtering

- Using Route Maps to Prevent Attacks
- Using Access-List to Filter ICMP Smurf Attacks
- Using Mac Address List to Filter Packets
- Using IP TCP Intercept Feature to Prevent Attacks
- Using NBAR to Block Attacks

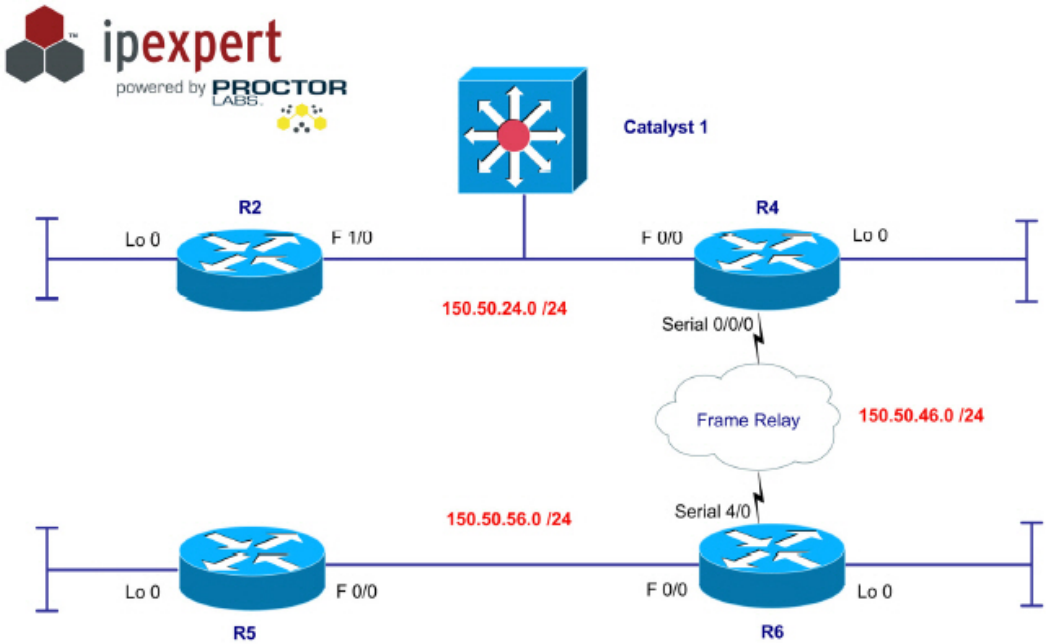
Network Attacks and Advanced Filtering Overview

This section will test your understanding and knowledge of Preventing Network Attacks and applying Advanced Filtering

This lab will use Routers R2, R4, R5, R6 and the appropriate Catalyst switches.

Estimated Time to Complete: 3 Hours

Diagram 2-A



Section 2 Pre-Lab Setup

- Physically connect and configure your network according to Diagram 2-A.
- The Routers are running the following protocols:
  - OSPF as the routing protocol
- This lab will focus strictly on Network attacks and Advanced Filtering. You will need to pre-configure the network with the base Frame Relay, IP Addressing and OSPF configuration. You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 2 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

Section 2 Configurations Tasks

NOTE:

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

Route Maps

1) R2 has detected attacks coming in from the Ethernet segment.
2) All the packets are HTTP packets with a size of 115 bytes.
3) Use Policy Based Routing (PBR) to block this attack by Black Holing the packets.

Smurf Attack

4) You are also the administrator for R5. You wan to block a smurf attack from the Ethernet segment.
5) Using an access-list block this type of attack on R5.

IP Spoofing

6) Remove problems caused by the introduction of malformed or forged IP source addresses into a network by discarding IP packets that lack a verifiable IP source address in R2's F1/0.
7) An application server on the 150.50.56.0/24 network is sending out packets with a source address of 192.168.24.20. Make sure that only spoofed packets from this server are dropped.

Preventing attacks on the Switch

8) You do not want a device with a MAC address of 0015.12AB.BAD0 to send AppleTalk and Vines traffic into port F 0/6 on Switch 1.
9) Filter the preceding traffic coming into port F 0/6 on Switch 1. Allow all other traffic.
10) Use a Mac address list to block this type of traffic.
11) Configure MAC address filtering and only permit ARP from 0000.1111.2222 to 0000.2222.1111 for Vlan 20.

IP TCP Intercept

12) The 150.50.24.0 network is experiencing syn attacks from the Frame cloud to your web servers.
13) R4 should watch the traffic and if it does not complete the TCP handshake in 20 seconds, it should drop the packets.
14) Limit IP TCP intercept to only watch packets coming from 150.50.46.0 or the 150.50.56.0 networks for Web traffic.

15) Configure IP TCP intercept such that the router drops embryonic connections if they reach 1050. It should stop dropping the embryonic connections once the number reaches 850.

16) Set the software to manage the connection for 12 hours after no activity.

17) Configure the router such that it will enter aggressive mode when 1400 connections are made within 60 seconds.

18) Configure the router such that it will leave aggressive mode when the number of connections drop below 850 in a 60 second window.

Network Based Application Recognition

19) You are under the Code Red and Nimda attacks from the Frame Cloud on R4.

20) Using NBAR classify the traffic on the inbound on S 0/0/0.

21) Drop the classified traffic on an outbound ACL on the F 0/0 interface. Use DSCP to classify Code Red traffic.

Section 2 Technical Tips and Comments

Route Maps

- Use the **route-map** command with the **match length** and **match ip address** command to classify traffic.
- Use the **set interface** command to use Null0 to drop the packets.

Smurf Attack

- Use the **Access-list** command to configure an extended Access list on the Router to block the Smurf attack.

IP Spoofing

- Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IP address spoofing. For example, routers at the edge of the network of an ISP are more likely to have symmetrical reverse paths than routers that are in the core of the ISP network. Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router. Hence, it is not recommended that you apply Unicast RPF where there is a chance of asymmetric routing. It is simplest to place Unicast RPF only at the edge of a network or, for an ISP, at the customer edge of the network.

Preventing attacks on the Switch

- Use the **Mac access-list** command to configure a Mac ACL to filter the required traffic.
- First, you create the VLAN access maps for each type of traffic that requires filtering. You select a MAC address for blocking. You also need to identify the ARP traffic in the access list. An ARP frame uses the Ethernet protocol type of value 0x806. You can filter on this protocol type as interesting traffic for the access list.

IP TCP Intercept

- Use the **IP TCP Intercept** command to configure the IP TCP Intercept feature on the Router.
- If the number of connection requests exceeds the number value configured, the TCP intercept feature becomes aggressive. If this is the case, then each new arriving connection causes the oldest partial connection to be deleted. Moreover, the initial retransmission timeout is reduced by half to 0.5 seconds. Lastly, the watch-timeout is cut in half.
- When both connection requests and incomplete connections fall below the values of ip tcp intercept one-minute low and ip tcp intercept max-incomplete low, the TCP intercept feature leaves aggressive mode.

Network Based Application Recognition

- Use the **Class-map** command to specify the url to match for code red.
- Use the **policy-map** command to match the traffic based on the Class map and set the DSCP to 1.
- Use the **service-policy** command to apply the policy map to the interface.
- Use the **access-list** command to define the access-list to drop the packet.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 3: GRE and NAT

- GRE Tunneling
- Static Routes over GRE Tunnels
- Running Routing Protocols over GRE Tunnels
- NAT
- PAT
- Static NAT

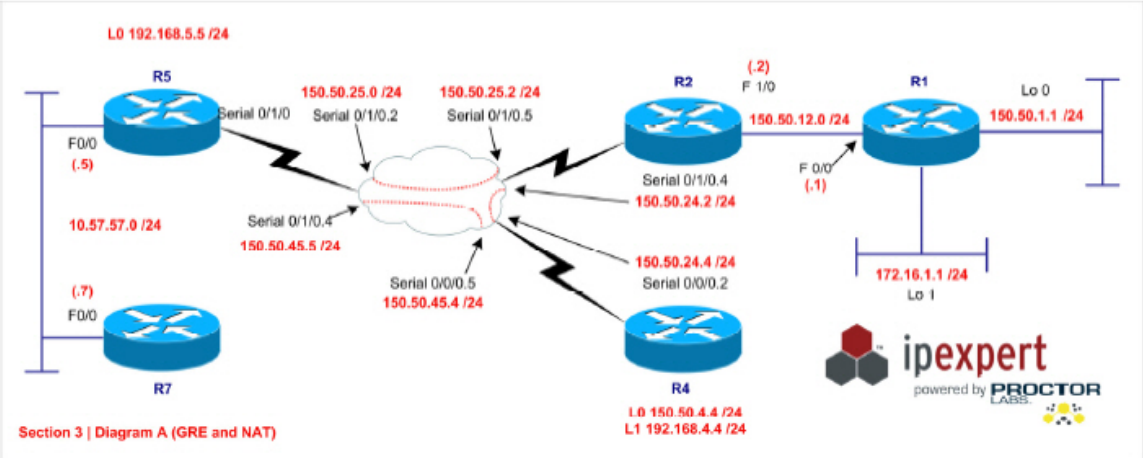
GRE and NAT Overview

This section will test your understanding and knowledge of GRE Tunnel and Address Translations using NAT and PAT. You will configure GRE Tunnels and route private networks over the configured Tunnels. This section will also test your understanding and knowledge of NAT and PAT. This section also requires you to have knowledge about Static Routes and Routing Protocols.

This lab will use Routers R1, R2, R4, R5, R7 and the appropriate Catalyst switches.

Estimated Time to Complete: 3 Hours

Diagram 3-A



Section 3 Pre-Lab Setup

- Physically connect and configure your network according to Diagram 3-A.
- This lab will focus strictly on GRE and NAT. You will need to pre-configure the network with the base Frame Relay, IP Addressing and VLAN configuration. The pre-configuration will not include configuration of Routing Protocols. You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 3 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

Section 3 Configuration Tasks

NOTE:

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

Base Routing Configuration

1) Routers R1, R2, R4 and R5 need to be configured with EIGRP as the routing protocol in AS 1245 with the following networks advertised:

   → R1 – 150.50.1.0/24 and 150.50.12.0/24
   → R2 – 150.50.12.0/24, 150.50.24.0/24 and 150.50.25.0/24
   → R4 – 150.50.4.0/24, 150.50.24.0/24 and 150.50.45.0/24
   → R5 – 150.50.25.0/24 and 150.50.45.0/24.

2) Do not advertise any of the RFC 1918 networks under EIGRP 1245.

Configuring GRE Tunnels

3) Configure a GRE tunnel between R1 and R5. The Tunnel Network should be set to 10.15.15.0/24. Make sure the tunnel is authenticated.

4) Configure a GRE tunnel between R1 and R4. The Tunnel Network should be set to 10.14.14.0/24. Make sure the tunnel is authenticated.

5) Configure a GRE tunnel between R4 and R5. The Tunnel Network should be set to 10.45.45.0/24. Make sure the tunnel is authenticated.

6) Make sure you can ping the Tunnel interfaces of directly connected tunnels. For example, you should be able to ping 10.15.15.1 from R5 and you should also be able to ping 10.14.14.4 from R1.

Routing RFC 1918 using Static Routes

7) R1 should be able to route to the following networks:

   - 10.57.57.0 /24
   - 192.168.5.0 /24
   - 192.168.4.0 /24

8) R4 should be able to route to the following networks:

   - 10.57.57.0 /24
   - 192.168.5.0 /24
   - 172.16.1.0 /24

9) R5 should be able to route to the following networks:

   - 192.168.4.0 /24
   - 172.16.1.0 /24

10) R7 should also be able to connect to any of the RFC 1918 networks. You can only use one **ip route** command to accomplish this.

11) No routing protocols can be used for this section. No configuration should be done on R2 to accomplish this section.

Routing RFC 1918 using RIP

12) Remove all the Static Routes configured in the previous section.

13) R1, R4, R5 and R7 should be able to route to the RFC 1918 networks.

14) Configure RIP V2 as the routing protocols to accomplish this task.

15) Do not use any Static Routes to accomplish this section.

Routing RFC 1918 using OSPF

16) Remove RIP as the Routing protocol on R1, R4, R5 and R7.

17) Run OSPF as the routing protocol to route the RFC 1918 networks.

18) Do not use any Static Routes to accomplish this section.

Routing RFC 1918 using EIGRP

19) Remove OSPF as the Routing protocol on R1, R4, R5 and R7.

20) Run EIGRP 1457 as the routing protocol to route the RFC 1918 networks.

21) Do not use any Static Routes to accomplish this section.

NAT

22) Configure R5 such that the 10.57.57.0/24 network can reach non RFC 1918 networks using a pool of either 150.50.25.0/24 or 150.50.45.0/24.

23) Make sure pools are chosen in an efficient manner. When 10.57.57.0 communicates to 150.50.12.0 it should use the 150.50.25.0 pool and when it communicates to 150.50.4.0 it should use the 150.50.45.0 pool. 150.50.24.0 should be reachable via either pool. Make sure to allow for failover in case of a problem with either PVC going to R2 or R4

24) R7 should be able to connect to the non RFC 1918 networks as well.

25) One static route is allowed for this section.

26) Route Maps are allowed for this section.

27) Make sure when 10.57.57.0 network is communicating to other RFC 1918 networks it does not get translated.

PAT

28) Configure R1 such that the 172.16.1.0/24 network can reach non RFC 1918 networks without configuring a pool.

29) Configure R4 such that the 192.168.4.0/24 network can reach the 150.50.12/24 and 150.50.24/24 networks. You should use a pool to accomplish this. Make sure the address is translated using IP address and Port number combination.

30) Make sure when the RFC 1918 network communicates to other RFC 1918 networks, they do not get translated.

Static NAT

31) There is a Web server at 10.57.57.80. This Web server should be visible to the outside networks as 150.50.25.80.

32) There is a Web server at 172.16.1.80. This web server should be visible to the outside networks as 150.50.12.80.

Section 3 Technical Tips and Comments

Base Routing Configuration

- Use the **Router EIGRP** command to configure EIGRP as the routing protocol.

Configuring GRE Tunnels

- Use the **Interface Tunnel** command to create the GRE Tunnels.

Routing RFC 1918 using Static Routes

- Use the **IP Route** command to create the static and default routes.

Routing RFC 1918 using RIP

- Use the **Router RIP** to configure RIP as the Routing protocol.
- Use the **version** command to set the appropriate RIP version.
- Make sure Subnets are advertised.

Routing RFC 1918 using OSPF

- Use the **Router OSPF** to configure OSPF as the Routing protocol.

Routing RFC 1918 using EIGRP

- Use the **Router EIGRP** to configure EIGRP as the Routing protocol.

NAT

- Use the **IP NAT** command to specify internal and external networks.
- Use the **IP NAT** command to create the pool of addresses.
- Use the **IP NAT** command with an ACL to specify interesting traffic for translation.
- Use **Route Map** command to configure Policy Based Routing (PBR).

PAT

- Use the **IP NAT** command to specify internal and external networks.
- Use the **IP NAT** command with the **Interface** option on R1.
- Use the **IP NAT** command to create the pool on R4.
- Use the **IP NAT** command with the **Overload** option on R4.
- Use the **IP NAT** command with an ACL to specify interesting traffic for translation.

Static NAT

- Use the **IP NAT** command to create static mapping for the Web Server on R5.
- Use the **IP NAT** command to create static mapping for the Web Server on R1.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 4: Authentication, Authorization and Accounting (AAA) on a Router

- Configuring TACACS+ for AAA on a Router
- Configuring RADIUS for AAA on a Router
- Configuring Login Authentication on a Router using TACACS+ and RADIUS
- Configuring Local Authorization on a Router
- Configuring Accounting using TACACS+ and RADIUS

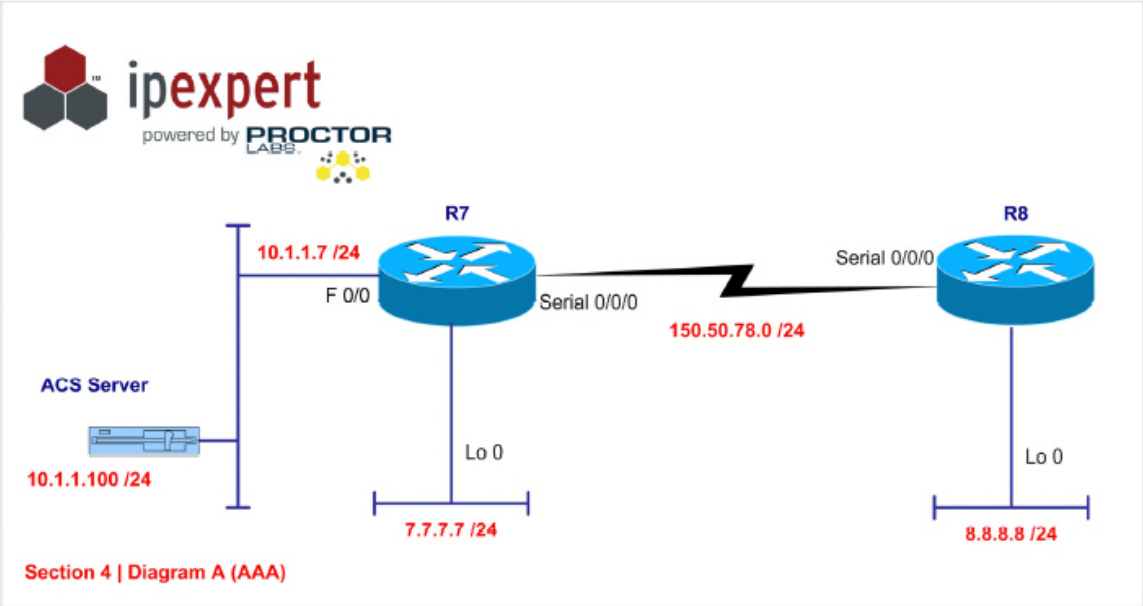
AAA on a Router Overview

This section will test your understanding and knowledge of AAA. You will configure AAA on a router for Authentication, Authorization and Accounting.

This lab will use Routers R7 and R8 and the appropriate Catalyst switches.

Estimated Time to Complete: 3 Hours

Diagram 4-A



Section 4 Pre-Lab Setup

- Physically connect and configure your network according to Diagram 4-A.
- The Routers are running RIP V2 as the routing protocol.
- This lab will focus strictly on AAA You will need to pre-configure the network with the base IP Addressing, HDLC and VLAN configuration. The pre-configuration files will be used to initially configure the router. You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 4 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

Section 4 Configuration Tasks and Objectives

NOTE:

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

Configuring R7 and R8 for AAA

1) AAA Server is located at 10.1.1.100.

2) Configure R7 to communicate to the AAA Server. The AAA Server is configured to communicate to R7 using its Loopback 0 address of 7.7.7.7. The Secret key is **Tipexpert**. Use TACACS+ as the Protocol.

3) Verify connectivity by testing Users U1 with a password of **cisco**.

4) Configure R8 to communicate to the AAA Server. The AAA Server is configured to communicate to R8 using its Loopback 0 address of 8.8.8.8. The Secret key is **Ripexpert**. Use RADIUS as the protocol.

5) Verify connectivity by testing Users U1 with a password of **cisco**.

Configuring Login Authentication for Telnet, Console and Aux ports

6) Configure R7 such that the AUX and Console ports are not authenticated. Make sure of it.

7) Configure R7 such that the Telnet connections are authenticated against the AAA server using TACACS+. Do not use the default list. Provide for a way to authenticate the user locally if the AAA server is unavailable.

8) Create a User for backup authentication as admin with a password of admin.

9) Configure R8 such that the AUX and Console ports are not authenticated. Make sure of it.

10) Configure R8 such that the Telnet connections are authenticated against the AAA server using RADIUS. Do not use the default list. Provide for a way to authenticate the user locally if the AAA server is unavailable.

11) Create a User for backup authentication as admin with a password of admin.

Configuring Local Authorization on R7

12) Allow User **User1** access to all commands.

13) Allow User **User2** access to a user-defined privilege 5. Privilege 5 should have the following capabilities:

- ➔ It should allow users to be able to go into Global Config Mode.
- ➔ It should allow users to be able to configure a hostname
- ➔ It should allow users to be able to configure routing and advertise networks.
- ➔ It should allow users to be able to configure all snmp related commands in global config mode.

14) Authorization should only be done on the Telnet Connections. Make sure of it.

15) The password for both users is **cisco**.

Accounting

16) On R7, Log all logins and logout to track usage for Telnet connections only.

17) On R7, Log all commands typed by users when on the router through Telnet only.

18) On R8, Log all logins and logout to track usage for Telnet connection only.

Section 4 Technical Tips and Comments

Configuring R7 and R8 for AAA

- Use the **aaa new-model** command to turn on AAA services on the router.
- Use the **tacacs-server** to configure information about the TACACS+ server.
- Use the **ip tacacs source-interface** to configure the source IP address of the Router.
- Use the **radius-server** to configure information about the TACACS+ server.
- Use the **ip radius source-interface** to configure the source IP address of the Router.
- Use the **test aaa** command to verify the configuration.

Configuring Login Authentication for Telnet, Console and Aux ports

- Use the **aaa authentication login** command to create the authentication lists for no authentication, TACACS+ authentication and the RADIUS authentication.
- Use the **login authentication** command to apply the authentication list to the Console, AUX and Telnet ports.

Configuring Local Authorization

- Use the **Privilege** command to create privilege level 5.
- Use the **username** with the **privilege** command to assign the privilege level to the User.
- Use the **aaa authorization exec** and **aaa authorization command** to configure the authorization lists.
- Use the **authorization exec** and **authorization command** to apply the authorization list to the appropriate lines.

Accounting

- Use the **aaa accounting exec** and **aaa accounting command** commands to create accounting list.
- Use the **accounting** command to apply the accounting list for the Telnet connections.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 5: PIX Firewall

- Basic PIX Configuration (Global, NAT, NAT 0, Static)
- Configuring VLAN interfaces on the PIX
- Translations and Connections
- Access Lists and Object Groups on a PIX
- Authentication Proxy for Standard and Non-Standard Protocols through the PIX
- Advanced Filtering on the PIX
- Routing RIP and OSPF on the PIX
- Running Routing Protocols through the PIX Firewalls (IGP and BGP)
- Remote Management of the PIX
- DHCP Server on the PIX

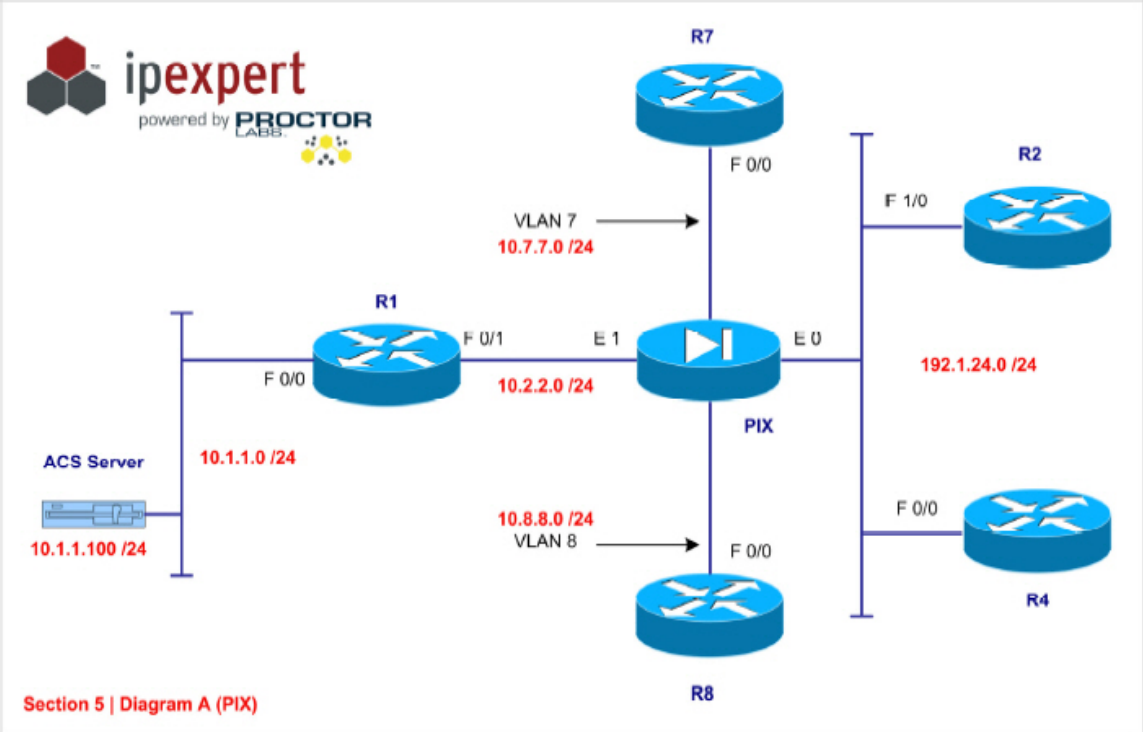
PIX Firewall Overview

This section will test your understanding and knowledge of PIX. You will configure the PIX and its communication with other devices.

This lab will use Routers R1, R2, R4, R7, F8, the appropriate Catalyst switches and the PIX.

Estimated Time to Complete: 3 Hours

Diagram 5-A



Section 5 Pre-Lab Setup

- Physically connect and configure your network according to Diagram 5-A.
- This lab will focus strictly on PIX you will need to pre-configure the network with the base IP Addressing and VLAN configuration. The pre-configuration files will be used to initially configure the routers. You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 5 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

Section 5 Configuration Tasks

NOTE:

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

Basic PIX Configuration

1) Create 2 logical interfaces off of E0, VLAN7 and VLAN8. VLAN20 is the primary untagged VLAN.

2) Assign them names and security levels as follows:

   - VLAN7 – DMZ7 - 25
   - VLAN8 – DMZ8 - 50

3) Also configure the PIX outside port on the switch to allow VLAN7 and VLAN8 to communicate to the rest of the network.

4) Assign the following addresses to the PIX and bring all PIX interfaces up:

   - Inside – 10.2.2.10/24
   - Outside – 192.1.24.10/24
   - DMZ7 – 10.7.7.10/24
   - DMZ8 – 10.8.8.10/24

5) Verify connectivity by pinging the directly connected devices around the PIX.

Translations and Connections

6) Use a NAT/PAT combination to allow inside networks to outside using the following range of address:

   - 192.1.24.51 – 192.1.24.150

7) If more than 100 simultaneous connections are received, the PIX uses PAT to translate. Do not use NAT-ID 1

8) R2 should be able to Manage R7 using Telnet. R2 should see R7 as 192.1.24.7. Allow the appropriate filtering on the PIX. Do not use conduits.

9) R4 should be able to Manage R8 using Telnet. R4 should see R8 as 192.1.24.8. Allow the appropriate filtering on the PIX. Do not use conduits.

10) If an outside user Telnets or HTTPs to 192.1.24.10, he should be redirected to a server at 10.7.7.100. This server is not there. But your company will be putting this server up in the future. Allow the appropriate entries in your filter list.

11) R7 should be able to ping R2 and R4's Loopback addresses using its own IP Address 10.7.7.7. You cannot use the static command to accomplish this. Allow the appropriate entries in the access list. You are allowed to create a single route on both R2 and R4. You may also create a single route on the PIX

Access List and Object Groups on the PIX

12) Your company will be putting in 2 application servers. One of the application servers will be in DMZ7 with an IP Address of 10.7.7.21, and the other will be in DMZ8 with an IP Address of 10.8.8.22.

13) Create a static translation for them on the outside so that 10.7.7.21 is seen as 192.1.24.21 on the outside and 10.8.8.22 is seen as 192.1.24.22 on the outside.

14) These servers are going to be access by partner organizations. The IP Addresses of these partner organizations are as follows:

- 205.15.25.0/24
- 207.215.1.0/24
- 210.208.15.16/28
- 211.0.15.32/27
- 192.1.150.112/28

15) The applications on the servers are as follows:

- TFTP
- FTP
- HTTP
- SMTP
- DNS
- Custom Application at UDP 50000

16) Allow all the partner organizations access to all the applications on the 2 servers. You are allowed 2 lines in the Access List to accomplish this.

Authentication Proxy

17) The AAA server is located at 10.1.1.100. It communicates to the PIX using TACACS+ and a key of **ipexpert**. Create a static route for the AAA server on the PIX pointing towards R1.

18) All outbound Telnet and HTTP Requests have to authenticate against the AAA server. The Username to use is **pixuser** with a password of **ipexpert**. Use the same username and password for all authentication passwords.

19) Enable Telnet on R1 with a password of **ipexpert**.

20) Make R1 appear as 192.1.24.15 on the outside. Allow R4 to telnet into R1 through the PIX.

21) All inbound traffic for Telnet should be authenticated against the AAA server. Allow any networks to telnet into R1's outside address in the Access List.

22) All outbound TFTP and RSH traffic should be authenticated against the AAA server. Use 192.1.24.9 for the virtual address and telnet as the authentication protocol.

23) R2 should be able to Telnet into 192.1.24.15 (R1's translated address). Configure R1 such that it should allow R2 to telnet into port 3025. Allow the appropriate entries in the access-list.

24) Authenticate all Telnet traffic to port 3025 from R2 to R1 using the AAA Server.

NOTE:

Please use *Clear uauth* on the PIX after every authentication step to clear the authentication.

Advanced Filtering on the PIX

25) You want to block Java and ActiveX applets from 2.2.2.2.

26) Configure the Firewall to support Microsoft's SMTP server

27) There is a WebSense server located at 10.1.1.101.

28) Before a HTTP request is allowed to go out, the PIX should verify with the WebSense server if the website is allowed or not. Configure the PIX such that traffic will be allowed to pass if the WebSense server is down.

Running RIP as the Routing Protocol on the PIX

29) Remove all static routes from R1, R7, R8 and the PIX.

30) Run RIP V2 as your routing protocol on R1, R2, R4, R7 and R8. Advertise all networks on each router.

31) Configure routing protocol authentication using a key of 1 and key-string of **ipexpert**.

32) Run RIP V2 on the PIX to inject a default route to R1, R7 and R8. Make sure to use RIP authentication to match the Routers.

33) Run RIP to receive routes from all the routers. Make sure to use RIP authentication to match the Routers.

34) Verify that the appropriate routes are propagating in the routing tables of all routers and the PIX Firewall.

Running OSPF as the Routing Protocol on the PIX

35) Remove RIP from all Routers and the PIX Firewall.

36) Run OSPF as your routing protocol on R1, R2, R4, R7 and R8. Advertise all networks on each router.

37) Configure routing protocol authentication using a key of 1 and key-string of **ipexpert**. Do not use the AREA authentication command under the ospf process.

38) Run OSPF in Process ID 1 for the outside network. Make sure to use OSPF authentication to match the Routers on the outside.

39) Run OSPF in Process ID 2 for the inside and the 2 DMZ networks. Make sure to use OSPF authentication to match the Routers on the inside and the DMZ networks.

40) Verify that the appropriate routes are propagating in the routing tables of all routers and the PIX Firewall.

41) You want routes from the outside routers to propagate to R1, R7 and R8 and vice versa.

Running OSPF thru the PIX

42) Remove OSPF process ID 1 from the PIX Firewall.

43) You want R2 to peer with R1 for OSPF.

44) Configure a GRE Tunnel to accomplish this. Make sure the 192.1.24.0 network is advertised to R1 and the 10.2.2.0 network is advertised to R2.

45) Allow the appropriate entries in the Access List.

46) You cannot use Static routes to accomplish this task.

47) You should see all routes in R2's routing table, including the 10.1.1.0 and 10.2.2.0.

Running BGP thru the PIX

48) This lab will start with a fresh config. Erase the configs and reload R1, R2, R4, the switches and the PIX.

49) Load the initial configs for R1, R2, R4 and the switches.

50) Bring the E0 and E1 interfaces up on the PIX. Configure them with the following IP addresses:

- Outside: 192.1.24.10 /24
- 10.2.2.10 /24

51) Run RIP v2 as the routing protocol on R1, R2 and R4. Advertise all directly connected networks.

52) Run RIP on the PIX to receive the RIP routes on the inside and outside interfaces.

53) Configure the following loopbacks on R1, R2 and R4:

- R1 Loopback 55: 55.1.1.1 /24
- R2 Loopback 55: 55.2.2.2 /24
- R4 Loopback 55: 55.4.4.4 /24

54) Run IBGP between R1 and R2. They should be in AS 12. Peer R2 with 1.1.1.1. Peer R1 with 2.2.2.2. Configure the PIX with the appropriate statics and access-lists. Create host routes on R1 and R2 for each other.

55) Run EBGP between R1 and R4. R4 is in AS4. Peer R4 with 10.2.2.1. Peer R1 with 192.1.24.4. Configure the PIX with the appropriate statics and access-lists. Create host routes on R1 and R4 for each other.

56) Advertise the new loopbacks in BGP.

57) Authenticate the EBGP neighbors.

Remote Management of the PIX

58) Allow the ACS Server to Manage the PIX Firewall.

59) The ACS Server should be able to use either ssh or telnet for management.

60) The user authentication should be done based on TACACS+.

61) The ACS Server should already been setup for this communication.

62) The username for management is **pixuser** with a password of **ipexpert**.

Enabling the PIX firewall as a DHCP Server

63) Configure the PIX firewall as a DHCP Server.

64) It should assign IP configuration on the inside interface based on the following information:

- ➔ IP ADDRESS : 10.2.2.51 – 10.2.2.100
- ➔ WINS ADDRESS : 10.2.2.135
- ➔ DNS ADDRESS : 150.50.24.53
- ➔ DEFAULT GATEWAY : 10.2.2.10
- ➔ LEASE TIME : 3 Days 12 hours
- ➔ Excluded Addresses : 10.2.2.1 – 10.2.2.50

Section 5 Technical Tips and Comments

Basic PIX Configuration

- Use the **interface** command to create VLAN interfaces.
- Use the **name-if** to assign names and security levels.
- Use the **VLAN** command to create VLANs on the switch.
- Use the **IP Address** command to assign IP Addresses to the interfaces

Translations and Connections

- Use the **Global** command to create the address pool and the **NAT** command to link the addresses to the pool.
- Use the **Static** command to create a static mapping.
- Use the **access-list** and **access-group** command to allow access thru the PIX.
- Use the **Static** command to configure port redirection.
- Use the **NAT 0** command with an access-list to configure **no-translation.**

Access List and Object Groups on the PIX

- Use the **Object-group Network** command to network or host object-groups.
- Use the **Object-group Service** command to object-groups for TCP and UDP applications.
- Use the **static** command to create the static translations for the Application servers.
- Use the **access-list** command with the **object-group** option to create the access-list entries.

Authentication Proxy

- Use the **aaa-server** command to configure the PIX to communicate to the TACACS+ server.
- Use the **aaa authentication** command to configure authentication proxy for Telnet and HTTP requests.
- Use the **Virtual Telnet** or **Virtual HTTP** command to enable non-standard protocols to authenticate before going thru the PIX.

Advanced Filtering on the PIX

- Use the **Filter Java** and **Filter ActiveX** commands to filter Java and ActiveX applets.
- Use the **no fixup protocol smtp** command to disable SMTP Fixup.
- Use the **url-server** and **filter url** commands to enable url filtering on the PIX.
- Use the **no fixup protocol ftp** command to disable Standard FTP.
- Use the **access-list** command to allow Passive FTP to come thru the PIX.

Running RIP as the Routing Protocol on the PIX

- Use the **Router RIP** command to enable RIP on the Routers.
- Use the **Key Chain** command to create the Keys on the Routers.
- Use the **IP rip authentication** command to enable RIP authentication on the Routers.
- Use the **rip** command to enable RIP on the PIX.
- Use the **access-list** command to allow Passive FTP to come thru the PIX.

Running OSPF as the Routing Protocol on the PIX

- Use the **no RIP** command on the PIX to disable RIP.
- Use the **Router OSPF** command to enable OSPF on the Routers and the PIX.
- Use the **IP OSPF Authentication** and **IP OSPF Message-digest-key** commands to enable OSPF authentication on the Routers.
- Use the **OSPF Authentication** and **OSPF Message-digest-key** commands to OSPF authentication on the PIX. OSPF Authentication is done under the **routing interface** sub-configuration mode.

Running OSPF and BGP thru the PIX

- Use the **Interface Tunnel** command on the Routers to create the GRE Tunnel.
- Use the **Access-list** command to allow the GRE Tunnel thru the PIX Firewall.
- Use the **Router BGP** command to enable BGP authentication on the Routers.
- Use the **Neighbor** command with the **EBGP-Multihop** option to configure EBGP relationships.
- Use the **Access-list** command to allow BGP traffic thru the PIX.
- **Hint:** You might to change an existing static for BGP Authentication to work.

Remote Management of the PIX

- Use the **hostname** and **domain-name** commands to configure a hostname and Domain-name on the PIX. This is required to generate a RSA Key.
- Use the **ca generate rsa key** command to generate a RSA Key.
- Use the **Telnet** command to allow the ACS Server IP Address to telnet into the PIX from the Inside interface.

- Use the **ssh** command to allow the ACS Server IP Address to ssh into the PIX from the Inside interface.
- Use the **aaa authentication** command to specify the AAA as the authentication mechanism for ssh and Telnet.

Enabling the PIX firewall as a DHCP Server

- Use the **dhcpd** command and its subcommands to configure the PIX as a DHCP Server.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 6: IPSec

- Configuring a Router-to-Router IPSec Tunnel using Pre-Shared Keys
- Configuring a Router-to-Router IPSec Tunnel using a GRE Tunnel through the PIX
- Configuring a Router-to-PIX Tunnel
- Configuring a PIX for PPTP Connections
- Configuring DMVPN with EasyVPN Server

IPSec Overview

This section will test your understanding and knowledge of IPSec. You will configure IPSec tunnels from the Router to another Router and PIX Firewalls. You will also configure an IPSec tunnel over a GRE Tunnel. This section will also have you configure the PIX Firewall as a PPTP Server.

This lab will use Routers R1, R2, R4, R5, and R6. It will also use the PIX and the appropriate Catalyst switches.

Estimated Time to Complete: 3 Hours

Diagram 6-A

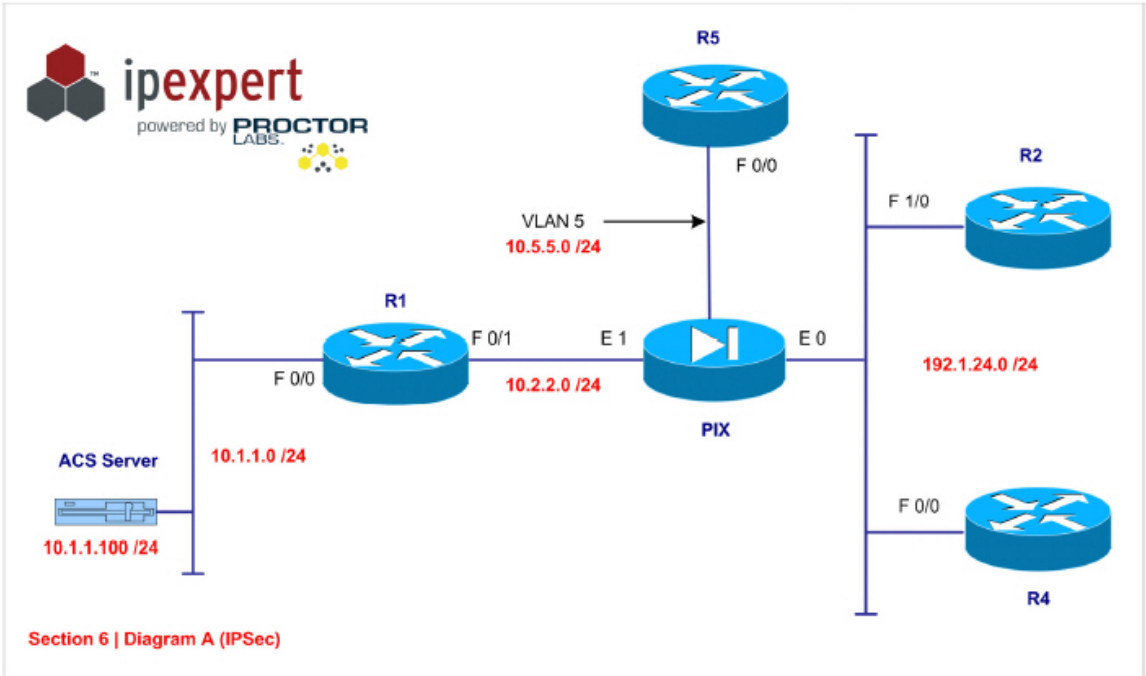
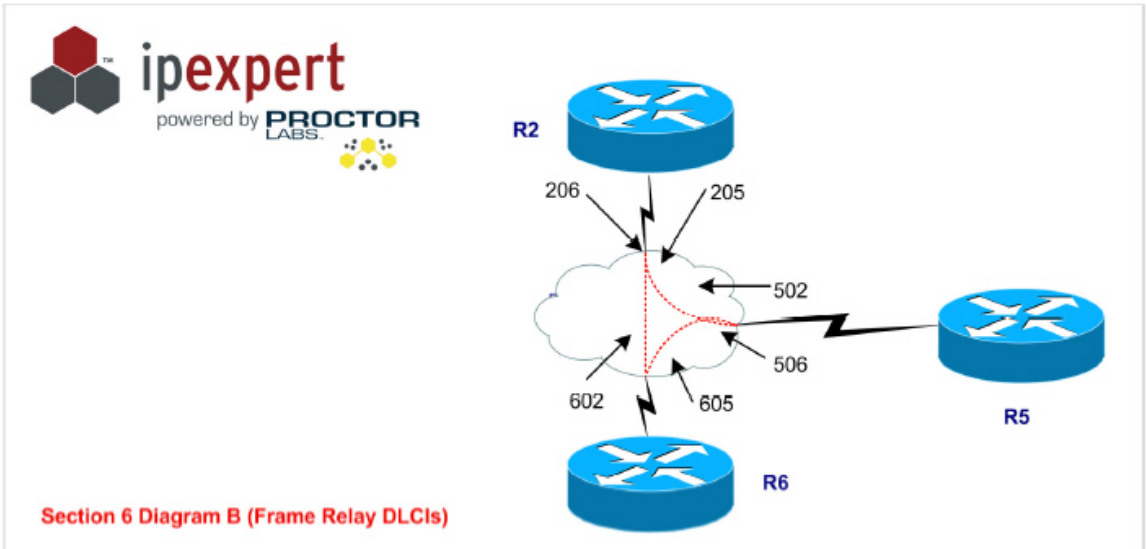


Diagram 6-B



Section 6 Pre-Lab Setup

- Physically connect and configure your network according to Diagram 6-A.
- This lab will focus strictly on IPSec. You will need to pre-configure the network with the base IP Addressing, VLAN and PIX configuration. You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 6 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

Section 6 Configuration Tasks

NOTE:

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

Router-to-Router IPSec Tunnel

1) Create a static mapping for R5 as 192.1.24.5.

2) You are allowed a static route on R2.
3) Configure an IPSec tunnel encrypting traffic from the Loopbacks behind R2 and R5.

4) Use R2 E 0/0 and the static translation of R5 as the Tunnel Endpoints.

5) Use the following Parameters for the Tunnel:

   → Authentication – Pre-shared
   → Group – 2
   → Key – ccie
   → Transform-set – esp-des and esp-md5-hmac
   → Interesting Traffic – Network 2.0.0.0 to Network 5.0.0.0 and vice versa.

6) Allow the appropriate entries through the PIX Firewall. Use minimum number of entries in the PIX access-list.

Router-to-Router using a GRE Tunnel

7) Create a GRE tunnel from R2 to R4. Use 10.24.24.0 /24 as the tunnel address.

8) Create a loopback on R2 and R4 as follows:

   → R2 Loopback: 22.2.2.2 /8
   → R4 Loopback: 44.4.4.4 /8

9) Run EIGRP in AS 24 as the routing protocol to route the GRE networks. Advertise the new loopbacks on R2 and R4 in EIGRP 24.

10) Configure a IPSec tunnel between R2 and R4 using the following parameters:

- Authentication: Pre-shared
- Group: 2
- Key: ccie
- Transform-set: esp-des
- Mode: transport
- Interesting Traffic: Any traffic that goes over the GRE tunnel between R2 and R4 including the EIGRP traffic.

Router-to-PIX Firewall Tunnel

11) Configure an IPSec tunnel encrypting traffic from the 10.2.2.0 network to the 4.0.0.0 network.

12) Use the PIX outside and the R4 E 0/0 as the Tunnel endpoints.

13) Use the following Parameters for the Tunnel:

- Authentication – Pre-shared
- Group – 2
- Key – ccie
- Transform-set – esp-des and ah-md5-hmac
- Interesting Traffic – Network 10.2.2.0 to Network 4.0.0.0 and vice versa.

14) You are allowed a static route on R4 to accomplish this task.

Configure the PIX Firewall as a PPTP Server

15) Configure the PIX Firewall as a VPN Server for PPTP Clients.

16) Use a Local Pool with a range of 192.168.1.1-192.168.1.254.

17) Use MS-CHAP for authentication and MPPE for Encryption.

18) Use Local Authentication and create a user pptpuser with a password of ccie.

19) Allow users on the outside to connect to the PIX using PPTP.

DMVPN for R2, R5, R6

20) Create a tunnel with the network of 100.0.0.x/24 where x is the router number.

21) Activate the Frame Relay interfaces should have IP address 150.50.99.x/24.

22) Running a separate EIGRP process for the tunnel interface.

23) Use XAUTH for local configuration, with username and password is ccie.

24) The default pre-shared key should be ccie.

25) Easy VPN Clients should use Diffie-Hellman group 2.

26) The dynamic address pool should be 60.0.0.10 to 60.0.0.20.

27) Client should response to the address.

28) Create a VPN client group that uses DNS at 60.0.0.1, 60.0.0.2 and WINS at 60.0.0.3 and 60.0.0.4.

29) Phase 2 policy should be esp-3des esp-md5-hmac.

30) NHRP authentication should use ccie.

31) Reverse route injection should be used to provide the DMVPN networks access to any Easy VPN Client network.

32) R6 will be the hub.

Section 6 Technical Tips and Comments

Router-to-Router IPSec Tunnel

- Use the **Static** command on the PIX to configure a static route for R5.
- Use the **IP Route** command to create a static route on R2.
- Use the **Crypto ISAKMP** commands to define the ISAKMP parameters and the Pre-shared key.
- Use the **Crypto IPSec** command to define the IPSec parameters.
- Use the **Access List** command to define interesting traffic.
- Use the **Crypto Map** command to configure the Crypto Map and assign it to the Interface.
- Use the **Access-list** and **Access-group** commands to configure and apply an Access List on the PIX for the IPSec traffic.

Router-to-Router using a GRE Tunnel

- Use the **Interface Tunnel** command to create the GRE Tunnels.
- Use **Router RIP** command to configure RIP as the routing protocol over the GRE networks.
- Allow the appropriate entries thru the PIX to accomplish this.
- Use the **Crypto ISAKMP** commands to define the ISAKMP parameters and the Pre-shared key.
- Use the **Crypto IPSec** command to define the IPSec parameters.
- Use the **Access List** command to define interesting traffic.
- Use the **Crypto Map** command to configure the Crypto Map and assign it to the Interface.
- Use the **Access-list** and **Access-group** commands to configure and apply an Access List on the PIX for the IPSec traffic.

Router-to-PIX Firewall Tunnel

- Use the **Crypto ISAKMP** commands to define the ISAKMP parameters and the Pre-shared key on the Router.
- Use the **Crypto IPSec** command to define the IPSec parameters on the Router.
- Use the **Access List** command to define interesting traffic on the Router.

- Use the **Crypto Map** command to configure the Crypto Map and assign it to the Interface on the Router.
- Use the **ISAKMP** commands to define the ISAKMP parameters and the Pre-shared key on the PIX.
- Use the **Crypto IPSec** command to define the IPSec parameters on the PIX.
- Use the **Access List** command to define interesting traffic on the PIX.
- Use the **Crypto Map** command to configure the Crypto Map and assign it to the Interface on the PIX.
- Use the **Sysopt Connection** command to bypass the ASA Security for the IPSec tunnel on the PIX.
- Use the **Access-list** and **Nat 0** commands to configure bypassing NAT for IPSec traffic on the PIX.

Configure the PIX Firewall as a PPTP Server

- Use the **IP local pool** to configure a pool of address to assign to the PPTP clients.
- Use the **Sysopt Connection** command to bypass the ASA Security for the PPTP traffic on the PIX.
- Use the **Access-list** and **Nat 0** commands to configure bypassing NAT for PPTP traffic on the PIX.
- Use the **vpdn group** commands to enable and configure PPTP parameters for authentication, encryption and client configuration parameters on the PIX.
- Use the **vpdn username** command to create the local user on the PIX Firewall.
- Use the **vpdn enable** command to enable vpdn on the PIX Firewall.

DMVPN for R2, R5, R6

- All routers configured with NHRP within one logical NBMA network must share the same authentication string.
- The **NHRP map multicast** command is useful for supporting broadcasts over a tunnel network when the underlying network does not support IP multicast. If the underlying network does support IP multicast, you should use the **tunnel destination** command to configure a multicast destination for transmission of tunnel broadcasts or multicasts. When multiple NBMA addresses are configured, the system replicates the broadcast packet for each address.
- In general, all NHRP stations within one logical NBMA network must be configured with the same network identifier.
- The **ip nhrp holdtime** command affects authoritative responses only. The advertised holding time is the length of time the Cisco IOS software tells other routers to keep information that it is providing in authoritative NHRP responses. The cached IP-to-NBMA address mapping entries are discarded after the holding time expires.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 7: VPN Concentrator

- Configuring the VPN Concentrator from the CLI
- Enabling Routing Protocols on the Concentrator
- Configuring a LAN-to-LAN Tunnel from a Router to a Concentrator
- Configuring a Remote Access VPN using PPTP and IPSec
- Configuring Web VPN
- Configuring EZVPN between a Router and a Concentrator

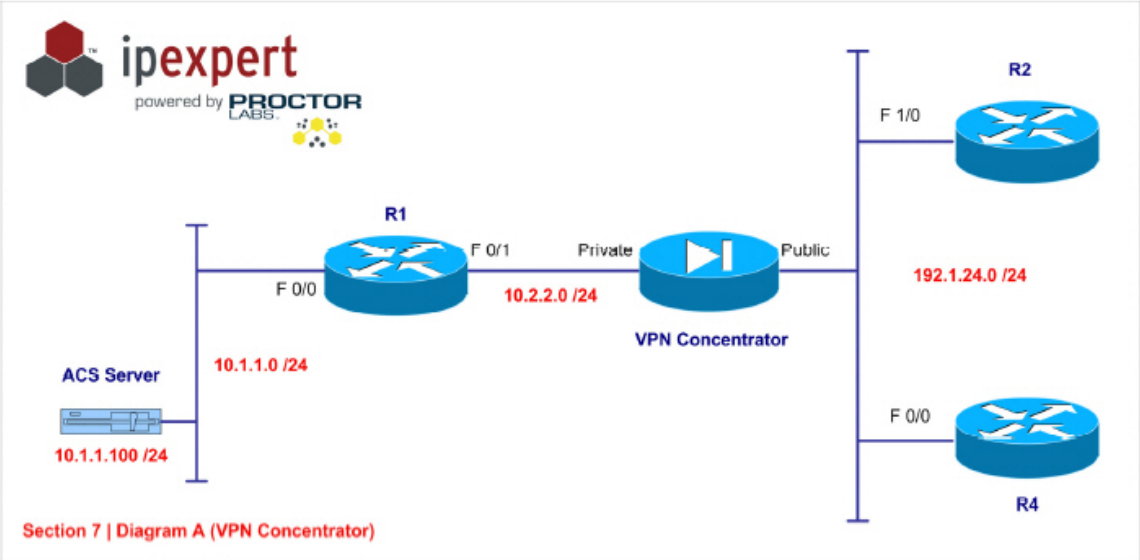
VPN Concentrator Overview

This section will test your understanding and knowledge of the VPN Concentrator. You will configure the Concentrator using the CLI and the Graphical Interface. You will be configuring Remote Access and LAN-to-LAN tunnels. You will also configure Web VPN and EZVPN on the Concentrator.

This lab will use Routers R1, R2, R4 and the appropriate Catalyst switches in addition to the Concentrator.

Estimated Time to Complete: 3 Hours

Diagram 7-A



Section 7 Pre-Lab Setup

- Physically connect and configure your network according to the Diagram 7-A.
- This lab will focus strictly on the Concentrator. You will need to pre-configure the network with the base IP Addressing on the Routers. The pre-configuration files will be used to initially configure the routers. You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 7 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

Section 7 Configuration Tasks

NOTE:

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

Basic Configuration of the VPN Concentrator from the CLI and the Graphical Interface

1) Configure the VPN Concentrator from the CLI. Assign it an IP Address on the Private interface of 10.2.2.5 with a Mask of 255.255.255.0.

2) Allow the Inside PC to connect to the VPN Concentrator for Administrator from the inside address.

3) You are allowed a single static route on the VPN Concentrator.

4) Configure the Public interface of the Concentrator using the Graphical Interface.

5) Assign it an IP Address of 192.1.24.5 with a mask of 255.255.255.0.

Configuring RIP and OSPF on the Concentrator

6) Configure OSPF on R2 and R4 in Area 0. Advertise all directly connected networks.

7) Configure OSPF on the Public Interface of the Concentrator in Area 0.

8) Configure RIP V2 on R1. Advertise all directly connected networks.

9) Configure RIP V2 on the Private interface of the Concentrator.

10) Redistribute the OSPF Routes into RIP and vice versa.

Concentrator Administration

11) Admin access should be restricted to the inside PC.

12) Also allow HTTP management from the Public Interface using HTTPS. This should be limited to network 192.1.24.0.

LAN-to-LAN IPSec Tunnel to a Router

13) Configure an IPSec tunnel between R2 and the Concentrator using the following information:

- ISAKMP Hash – MD5
- ISAKMP Authentication – Pre-shared
- IPSec – ESP-DES, ESP-MD5-HMAC
- Interesting Traffic – 10.2.2.0 to 2.0.0.0

Remote Access Tunnel Using IPSec and PPTP

14) Create a Group called RA with a password of **abcd.**

15) Allow IPSec and PPTP as the Access Protocol.

16) Create a Pool of IP Address 192.168.1.1-192.168.1.254. This pool should be specific to this group.

17) Make sure this network gets propagated to R1.

18) Allow users of this group to also connect to the 4.0.0.0 network when they are connected to the VPN Concentrator.

19) Create a user **RAUser** with a password of **RAUser12.** Assign the user to the **RA** group.

Web VPN

20) Enable HTTP Services on R1.

21) Create a Telnet Password of **telnet** on R1.

22) Create a Group called **WebVPN** with a password of **abcd.**

23) Allow WebVPN as the protocol for this group.

24) Create a Pool of IP Address 192.168.2.1-192.168.2.254. This pool should be specific to this group.

25) Make sure this network gets propagated to R1.

26) Enable the Concentrator to redirect HTTP requests to HTTPS.

27) Disable the ability of the users to enter a URL.

28) Create a URL Link for the HTTP Server on R1 such that when a user part of this group logs in, he has the ability to click on a Link to connect to the HTTP server on R1.

29) Create a custom application that allows the user to telnet into R1 using port 20000.

30) Create a user **webvpnuser** with a password of **webvpn12.** Assign the user to the **WebVPN** group.

31) Verify the config by logging on and verifying the configuration.

EZVPN

32) Configure an IPSec tunnel between R4 and the Concentrator using EZVPN.

33) The Concentrator should act as the EZVPN Server and R4 should be the client.

34) Create a separate group for the EZVPN Configuration called EZVPN with a password of **abcd**.

35) Create a Pool of IP Address 192.168.3.1-192.168.3.254. This pool should be specific to this group.

36) Make sure this network gets propagated to R1.

37) Create a User **EZ** with a password of **ezvpn123**.

38) Make this user a member of the EZVPN group.

39) Configure R4 to act as the EZVPN Client with the following parameters:

- Peer: 192.1.24.5
- Connect: Auto
- Mode: client
- Group: EZVPN
- Key: abcd
- Outside Interface: F 0/0
- Inside Interface: Loopback 0

40) Connect from R4 to the Concentrator to verify the configuration.

Section 7 Technical Tips and Comments

Basic Configuration of the VPN Concentrator from the CLI and the Graphical Interface

- Once you have configured the Private Interface thru the CLI, continue with the setup and disable all protocols at this time.
- Static Routes are configured under **Configuration**.
- Once the Private interface has been configured, connect in using your Browser.
- Configure the Public Interface. It is under the **Configuration** link.

Configuring RIP and OSPF on the Concentrator

- Enable OSPF globally under the **Configuration – System** link.
- Enable OSPF on the Public Interface under the interface configuration.
- Allow OSPF on the Public Interface by modifying the Filter List for the Public Interface. This is done under the **Traffic Management** Link.
- Enable RIP on the Private Interface under the interface configuration.
- Enable Redistribution by making the Concentrator into a ASBR for OSPF. This is done under the Global configuration of OSPF under the **Configuration – System** link.

Concentrator Administration

- Control Admin access by specifying who is allowed to access the Concentrator for Management under the **Administration – Access Control List** link.
- Allow Management from the Public Interface by allowing admin access under the Interface. This is done under the Interface configuration tab.

LAN-to-LAN IPSec Tunnel to a Router

- Configure an LAN to LAN tunnel on the Concentrator under the **Tunneling and Security – IPSec** Link.
- Configure IPSec on the Router pointing towards the Concentrator.
- Use the Parameters specified in the Task Objectives.

Remote Access Tunnel Using IPSec and PPTP

- Create the Group under the **User Management** Link.
- Only allow IPSec and PPTP for this group.
- Create an Address Pool specific to this group.
- Enable Address Assignment Globally under the **System – Address Management** link.
- Enable Reverse Route Injection under the **System – IP Routing** Link.
- Create a Network List under the **Traffic Management** Link for the 4.0.0.0.
- Use the Network List under the Group to configure Split Tunneling.
- Create a User and Assign it to the configured group. This is done under the **User Management** Link.

Web VPN

- Create the Group under the **User Management** Link.
- Only allow WebVPN for this group.
- Create an Address Pool specific to this group.
- Enable Address Assignment Globally under the **System – Address Management** link.
- Make sure Reverse Route Injection is enabled from the previous task and the route is propagating to R1.
- Enable HTTP to be redirected to HTTPS. This is done under the **Interface** Configuration Link. Also allow WebVPN on the Interface.
- Disabling the ability to enter a URL is done under the Group Configuration.
- Create an Application Link for the Group by using **Application Servers** button for the Group.
- Configure Port Forwarding for the Group to allow the Telnet Application.

EZVPN

- Create the Group under the **User Management** Link.
- Only allow IPSec for this group.
- Create an Address Pool specific to this group.
- Enable Address Assignment Globally under the **System – Address Management** link.
- Enable Reverse Route Injection under the **System – IP Routing** Link.
- Create a User and Assign it to the configured group. This is done under the **User Management** Link.
- Configure EZVPN in Client mode on R4 using the **Crypto IPSec client** command.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 8: Switching

- Creating VTP Domains with Authentication
- Trunking
- VLANs and Port Assignment
- Port Security
- Configuring the Switch to Communicate to a VMPS Server
- Dot1x Authentication
- Filtering
- L3

Switching Overview

This section will test your understanding and knowledge of the 3550 Switches. You will configure the Switch for Basic and Advanced Security functions.

This lab will use Routers R1, R6 and both Catalyst switches.

Estimated Time to Complete: 2 Hours

Diagram 8-A

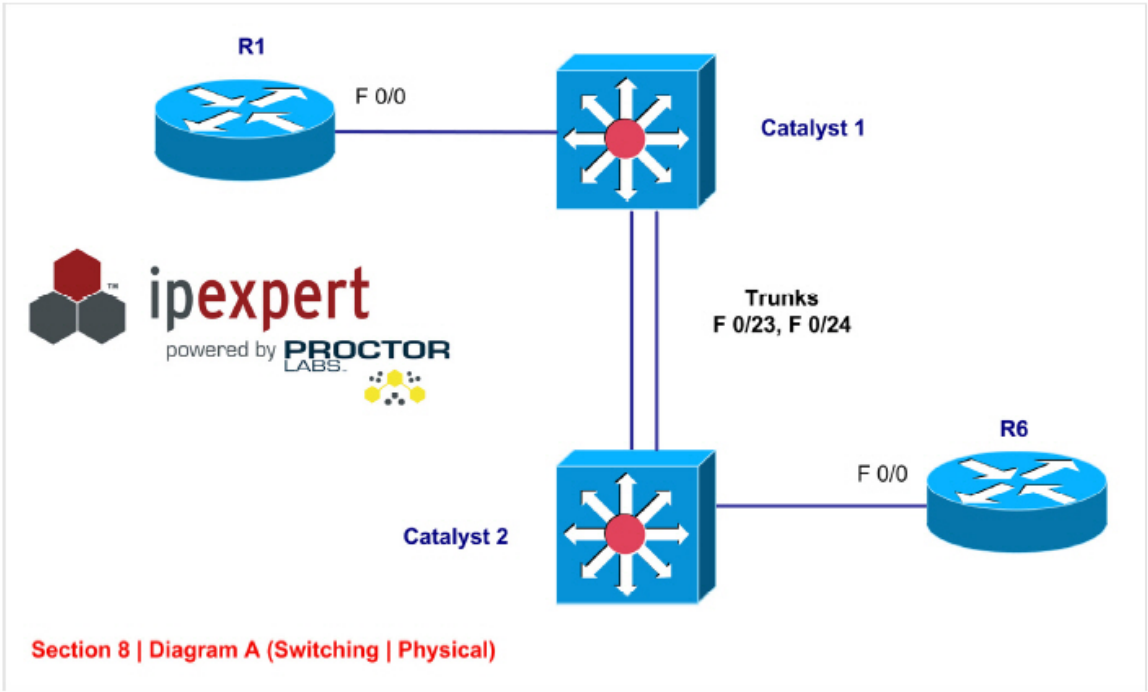
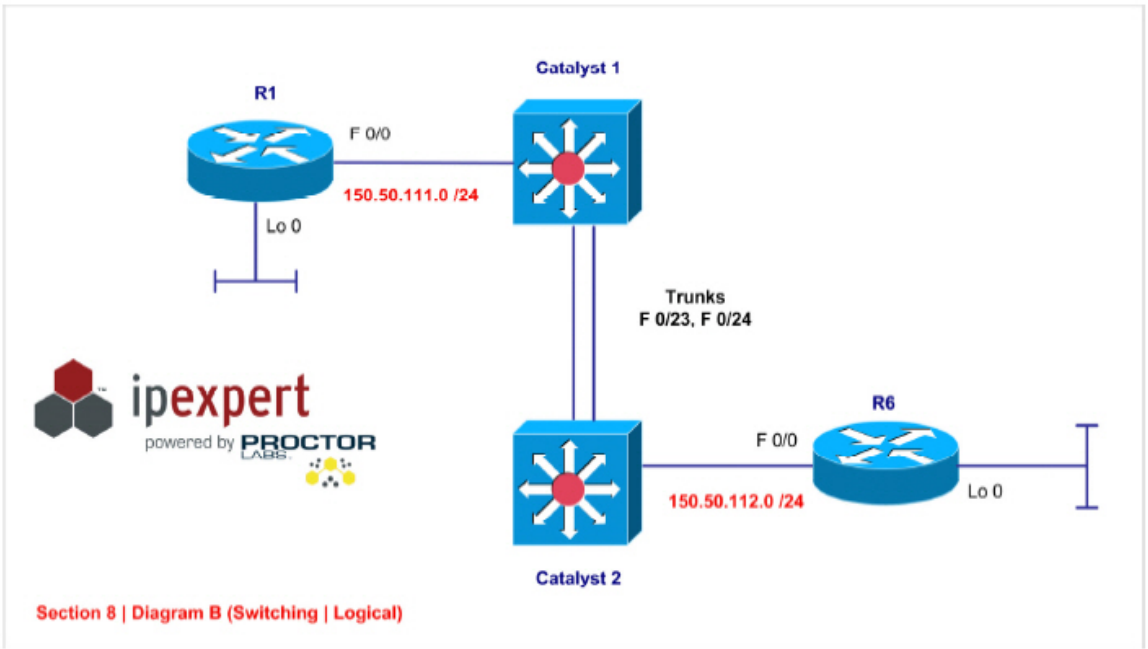


Diagram 8-B



Section 8 Pre-Lab Setup

- Physically connect and configure your network according to the Lab Topology provided above.
- This lab will focus on the Switches. You will need to pre-configure the network with the base IP Addressing using the pre-configuration files. You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 8 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

Section 8 Configuration Tasks

NOTE:

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

Configuring a Trunk and VTP Domains

1) F 0/23 and F 0/24 are connected to each other on both switches. Configure both these links as trunk links. Set the encapsulation as ISL. Make sure the switches do not negotiate the trunk.

2) Configure a VTP Domain as **ipexpert** with a password of **ipexpert**. Do not use the VLAN database to accomplish this. Set Switch 1 as the Server and Switch 2 as the Client.

Creating VLANs and Assigning them Ports

3) Create the following three VLANs on Switch 1:

   → 111 with a name of VLAN_Sales.
   → 112 with a name of VLAN_Finance.
   → 100 with a name of Trunk_VLAN.

4) Make sure the VLANs are propagating to Switch 2 using VTP.

5) Assign R1 to VLAN 111 and R6 to VLAN 112.

Creating VLAN Interfaces on the Switches

6) Create a VLAN Interface on Switch 1 to connect to R1. Assign it an IP Address of 150.50.111.100/24.

7) Create a VLAN Interface on Switch 2 to connect to R6. Assign it an IP Address of 150.50.112.100/24.

8) Create a VLAN interface on both switches to connect to each other over VLAN 100. Assign it an IP Address of 150.50.100.1/24 for Switch 1 and 150.50.100.2/24 for Switch.

9) Make sure you can ping all directly connected devices.

Port Security

10) An Application server connects to port 6 on Switch 1.

11) You want to make sure that no other device connects into that port. If another device connects into the port, you should shut the port down.

12) The MAC address of the port is 002A.115C.13DA.

VMPS Server Configuration

13) There is a VMPS server at 150.50.111.150.

14) You would like to get VLAN assignment for all ports on switch 1 in dynamic mode from the VMPS server.

15) You would like to reconfirm the assignment every 20 minutes.

16) Configure Switch 1 for VMPS.

Dot1x Authentication

17) Configure Port 8 on Switch 1 for Dot1x authentication.

18) Any device that connects to Port 8 should be authenticated by a RADIUS server located at 150.50.111.175.

19) The RADIUS server uses **ipexpert** as the key and 1645 as the Authentication port.

20) The Switch should re-authenticate every 2 hours.

Routing on the Switch

21) Configure EIGRP in AS 1 as the routing protocol between R6, Sw2 and Sw1.

22) Advertise the Loopback on R6 in EIGRP 1.

23) Authenticate all EIGRP devices using MD5 authentication and key of ipexpert.

24) Run BGP between R1 and Sw1. Sw1 should be AS 100 and R1 should be is AS 1.

25) Advertise the Loopback on R1 in BGP.

26) Configure mutual redistribution on Sw1 between EIGRP in AS 1 and BGP.

27) All devices should see all routes in their routing tables.

Section 8 Technical Tips and Comments

Configuring a Trunk and VTP Domains

- Use the **Switchport trunk** command under the Interface to configure the interface as a Trunk.
- Use the **VTP Domain** command to specify VTP Domain.
- Use the **VTP Password** command to specify VTP Password
- Use the **VTP Mode** command to specify VTP mode.

Creating VLANs and Assigning Ports to them

- Use the **VLAN** command to create VLANs.
- Use the **Name** command to assign VLAN names.
- Use the **Switchport Access** command to assign ports to VLANs.

Creating VLAN Interfaces on the Switches

- Use the **Interface VLAN** command to configure a VLAN interface.

Port Security

- Use the **Switchport Port-security** command set to specify various Port Security commands.
- **Hint :** The port has to be an Access Port before Port Security will work.

VMPS Server Configuration

- Use the **VMPS Server** command to specify the IP Address of the VMPS Server.
- Use the **VMPS reconfirm** command to specify the reconfirm time.

Dot1x Authentication

- Use the **Radius-server** command to define the IP Address, key and authentication port for the RADIUS server.
- Use the **aaa authentication dot1x** command to define the default authentication list for dot1x.
- Use the **dot1x system-auth-control** global command to turn dot1x on globally.
- Use the **dot1x port-control** command to turn on dot1x authentication on a port.
- Use the **dot1x re-authentication** command to enable re-authentication.
- Use the **dot1x timeout** command to specify the re-authentication time.
- **Hint:** The port has to be an Access Port before dot1x authentication will work.

Routing on the Switch

- Use the **IP routing** command to turn on routing on a Switch.
- Use the **Router OSPF** command to configure OSPF on a Switch.
- Use **IP OSPF message-digest-key** command to specify the authentication key for OSPF.
- Use the **Router BGP** command to configure BGP on a Switch.
- Use the **Redistribute** command to configure mutual redistribution of the routing protocols.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 9: IDS

- Configuring IDS on a Router
- Configuring IDS on the PIX
- Configuring the IDS Sensor Appliance from the CLI
- Configuring the IDS Sensor Appliance from IDM
- Configuring IEV to Receive Alarms from the Sensor
- Fine Tuning Signatures on the Sensor
- Creating Custom Signature on the Sensor
- Configuring Shun on a PIX

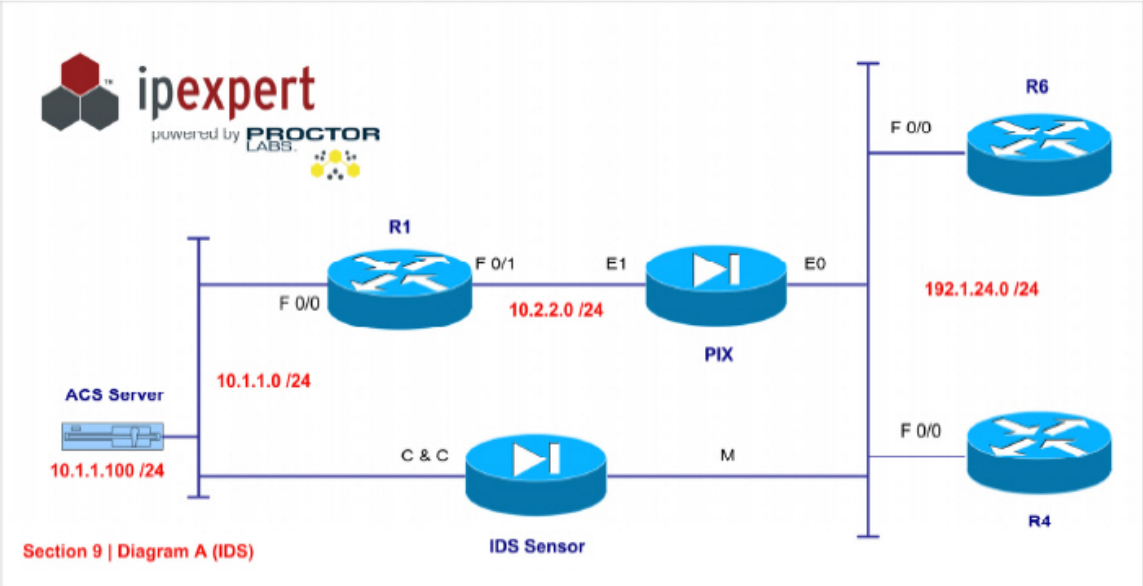
IDS Overview

This section will test your understanding and knowledge of IDS on the Routers, IDS on the PIX, and the IDS Sensor Appliance.

This lab will use Routers R1, R4, R6, the appropriate Catalyst switches, the PIX and the IDS Sensor.

Estimated Time to Complete: 4 Hours

Diagram 9-A



Section 9 Pre-Lab Setup

- Physically connect and configure your network according to Diagram 9-A.
- This lab will focus strictly on IDS. You will need to pre-configure the network with the base IP Addressing and VLAN configuration. The pre-configuration files will be used to initially configure the routers and the PIX. You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 9 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

Section 9 Configuration Tasks

NOTE:

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

IDS on a PIX

1) Configure a Syslog Server at 10.1.1.100. Configure the PIX to send message to the Syslog server.

2) Configure Console Logging to level 4. Configure Trap logging level to debugging.

3) Configure the PIX IDS with the following parameters:

   - ➔ Send an alarm for Info signatures
   - ➔ Send an alarm and drop packets for Attack signatures

4) You do not want signature 2004 to fire at all.

5) Protect the PIX from the outside interface.

IDS on a Router

6) On R6, Protect traffic coming in thru the E 0/0 interface.

7) Configure the IOS IDS with the following parameters:

   - ➔ Send an alarm for Info signatures
   - ➔ Send an alarm and drop packets for Attack signatures
   - ➔ Send the alarm to both the nr-director and a syslog server
   - ➔ Configure the router with the syslog server's translation address.

8) The nr-director is located at 10.1.1.100. Translate that address to 192.1.24.100 for the outside networks on the PIX. Allow appropriate entries in the Access List of the PIX.

9) Use the following parameters for the Post Office Protocol (POP) parameters.

   - ➔ Sensor HostID = 20
   - ➔ Director HostID = 10
   - ➔ Org ID = 100
   - ➔ Local IP Address = 192.1.24.6
   - ➔ Remote Director IP Address = 192.1.24.100
   - ➔ Port # = 45000

10) You do not want signatures to fire from 192.1.24.10 for the IOS-IDS Rule Set.

11) You do not want signatures 2150 to fire from 192.1.24.4.

12) You do not want signature 2004 to fire at all

Basic configuration and IDS Sensor Configuration from the CLI

13) Configure RSPAN on the Switch to copy all traffic from R6, R4 and PIX outside to the Monitoring Interface on the IDS Sensor.

14) Configure Telnet on R1.

15) Create a Static for R1 on the PIX to 192.1.24.11. Allow the outside network to Telnet into R1.

16) Allow the Inside Network to Telnet into the PIX.

17) IDS Sensor C & C interface is seen as 192.1.24.50 on the outside networks.

18) Configure the IDS Sensor with an IP Address of 10.1.1.15 and a default gateway of 10.1.1.1 (PIX) from the CLI.

19) Linking the IEV to the IDS Sensor for alarms

Signature and Sensor Tuning

20) Enable the ICMP Echo Signature 2004.

21) Configure the Alarm severity to Medium.

22) You don't want the 2004 signature to fire from R6.

23) Configure IDS for NT reassembly for 2000 and one minute values.

24) Apply the Signature to the Sensor.

Configuring a Custom Signature

25) Create a custom signature to fire if a packet is received for Telnet or shell with the word "attack" in it.

26) Set the Severity level to high.

27) Configure it send an alarm if the signature is detected.

28) Telnet into R1 from the outside to test it by typing in the word "attack".

Configuring the IDS to shun the connection on the PIX

29) Configure IP Blocking on the IDS Sensor.

30) Configure the PIX firewall as a Managed Device under IDS Sensor. Use the Telnet password as **cisco.**

31) Change the Signature action for ICMP 2004 to shun.

32) Verify by pinging the outside interface of the PIX.

Section 9 Technical Tips and Comments

IDS on a PIX

- Use the **logging** command to configure logging parameters.
- Use the **IP audit info** command to define the action for the info signatures.
- Use the **IP audit attack** command to define the action for the attack signatures.
- Use the **IP audit name** command to configure the rule name for the info and attack signatures.
- Use the **IP audit interface** command to apply the rule name to the outside interface.
- Use the **IP audit signature** command to disable a signature.

IDS on a Router

- Use the **Static** command on the PIX to create a static mapping for the Syslog and nr-director server.
- Use the **Access-List** and the **Access-group** command to allow appropriate entries for the Syslog and nr-director services thru the PIX.
- Use the **logging** command to configure logging parameters.
- Use the **IP audit notify** command to specify the destination of alarms.
- Use the **IP audit info** command to define the action for the info signatures.
- Use the **IP audit attack** command to define the action for the attack signatures.
- Use the **IP audit po** command to configure the parameters for the nr-director.
- Use the **IP audit name** command to configure the rule name for the info and attack signatures.
- Use the **IP audit** command to apply the rule to the interface.
- Use the **IP audit signature** command to tune or disable a signature.

Basic configuration and IDS Sensor Configuration from the CLI

- Use the **Monitor session** command on the switch to configure SPAN or RSPAN.
- Use the **Static** command on the PIX to create a static mapping for R1.
- Use the **Telnet** command to specify the network that can Telnet into the PIX for management.
- Use the **Static** command on the PIX to create a static mapping for the IDS Sensor.
- Use the **Setup** command to configure the Network Parameters for the IDS Sensor.
- Create an entry for the IDS Sensor in IEV by using the IP Address and Username and Password for the IDS Sensor.

Signature and Sensor Tuning

- Enable the ICMP Echo Signature by clicking the **Configuration** tab, the **Sensing Engine** Link and the **Signature Configuration Mode** TOC link.
- Enable Event Filtering by clicking the **Configuration** tab, the **Sensing Engine** Link and the **Event Filters** TOC link.
- Enable reassembly for NT by clicking the **Configuration** tab, the **Sensing Engine** Link and the **IP Fragment Reassembly** TOC link.

Configuring a Custom Signature

- Configure a Custom Signature by clicking the **Configuration** tab, the **Sensing Engine** Link and the **Signature Wizard** TOC link.

Configuring the IDS to shun the connection on the PIX

- Configure Blocking properties by clicking the **Configuration** tab, the **Blocking** Link.
- Change the action for the ICMP Echo Signature by clicking the **Configuration** tab, the **Sensing Engine** Link and the **Signature Configuration Mode** TOC link.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 10: Routing | IGP

- RIP
- EIGRP
- OSPF
- Configure Routing Protocol Authentication on RIP, EIGRP and OSPF
- Route Redistribution
- Route Filtering

Routing | IGP Overview

This section will test your understanding and knowledge of Routing Protocols (RIP, EIGRP and OSPF). You will configure RIP, EIGRP and OSPF as your Routing Protocols. This section will have 2 lab scenarios. The first lab will have Individual Routing protocols with Authentication. The second lab will contain all routing in one single lab with Route Redistribution and Route Filtering.

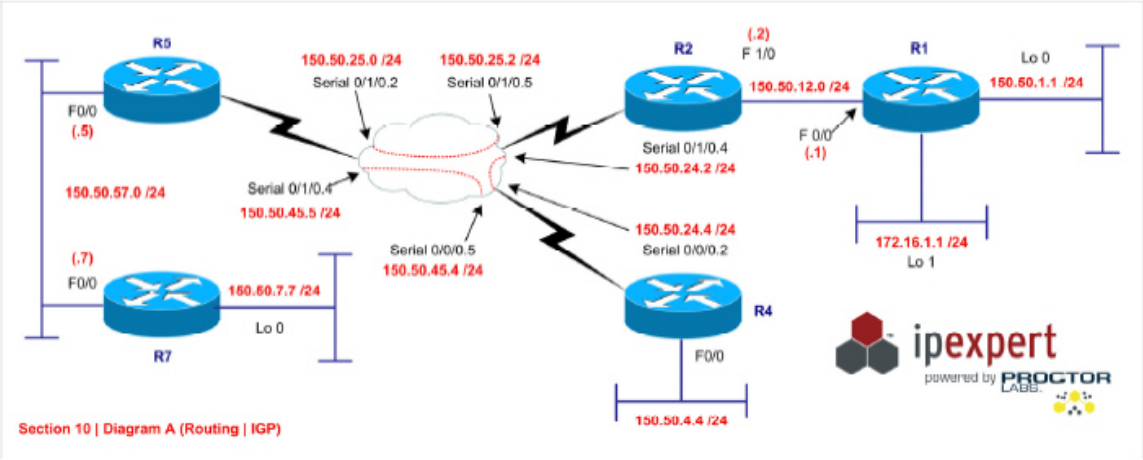
This lab will use Routers R1, R2, R4, R5, R7 and the appropriate Catalyst switches.

Estimated Time to Complete: 7 Hours

NOTE:

This section is broken into 2 lab scenarios each focusing on various, yet fundamentally important IGP topics. The first being IGP configuration, the second being redistribution. The first lab in this section should take you approximately 4 hours to complete. The second lab scenario in this section should take approximately 3 hours to complete.

Diagram 10-A



Section 10 – Scenario 1 (Routing Protocols) Pre-Lab Setup

- Physically connect and configure your network according to Diagram 10-A.
- This lab will focus strictly on IGP. You will need to pre-configure the network with the base Frame Relay, IP Addressing and VLAN configuration. The pre-configuration will not include configuration of Routing Protocols. You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 10 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

Section 10 – Scenario 1 Configuration Tasks

NOTE:

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

RIP Routing Protocol

1) Routers R1, R2, R4, R5 and R7 need to be configured with RIP V2 as the routing protocol with the following networks advertised:

   → R1 - 150.50.1.0/24, 150.50.12.0/24 and 172.16.1.0/24
   → R2 – 150.50.12.0/24, 150.50.24.0/24 and 150.50.25.0/24
   → R4 – 150.50.4.0/24, 150.50.24.0/24 and 150.50.45.0/24
   → R5 – 150.50.25.0/24, 150.50.57.0/24 and 150.50.45.0/24.
   → R7 – 150.50.7.0/24 and 150.50.57.0/24

2) Make sure all routers see all routes.

3) Configure RIP authentication on all routers using a key id of **1** and key of **cisco**. Use the most secure authentication mechanism.

4) Configure the following loopbacks on R1:

   - Interface Loopback 11 – 150.5.111.11 / 24
   - Interface Loopback 12 – 150.5.112.12 / 24
   - Interface Loopback 13 – 150.5.113.13 / 24
   - Interface Loopback 14 – 150.5.114.14 / 24
   - Interface Loopback 15 – 150.5.115.15 / 24

5) Inject the newly configured networks into RIP with the exception of 150.5.115.0 network. Do not use the Network command to accomplish this.

6) Make sure that the 150.5.115.0 network does not get injected into RIP.

7) Verify that all the routers are receiving the newly configured routes.

8) R2 should not send the 150.5.112.0 and 150.5.113.0 networks to R4 and R5. Use the minimum number of lines to configure this.

9) R7 should block the 150.5.111.0 network from coming in thru RIP.

EIGRP Routing Protocol

NOTE:

Reload the routers and start with the base Frame Relay, IP Addressing and VLAN configuration

Please read the entire list in each section before starting.

---

10) Routers R1, R2, R4, R5 and R7 need to be configured with EIGRP is AS 12457 as the routing protocol with the following networks advertised:

    - R1 – 150.50.1.0/24, 150.50.12.0 /24 and 172.16.1.0 /24
    - R2 – 150.50.12.0/24, 150.50.24.0/24 and 150.50.25.0/24
    - R4 – 150.50.4.0/24, 150.50.24.0/24 and 150.50.45.0/24
    - R5 – 150.50.25.0/24, 150.50.57.0/24 and 150.50.45.0/24
    - R7 – 150.50.7.0/24 and 150.50.57.0/24

11) Make sure all routers see all routes.

12) Configure EIGRP authentication on all routers using a key id of **1** and key of **cisco**. Use the most secure authentication mechanism.

13) Configure the following loopbacks on R1:

- Interface Loopback 11 – 150.5.111.11 / 24
- Interface Loopback 12 – 150.5.112.12 / 24
- Interface Loopback 13 – 150.5.113.13 / 24
- Interface Loopback 14 – 150.5.114.14 / 24
- Interface Loopback 15 – 150.5.115.15 / 24

14) Inject the newly configured networks into EIGRP with the exception of 150.5.115.0 network. Do not use the Network command to accomplish this.

15) Make sure that the 150.5.115.0 network does not get injected into EIGRP.

16) Verify that all the routers are receiving the newly configured routes.

17) R2 should not send the 150.5.112.0 and 150.5.113.0 networks to R4 and R5. Use the minimum number of lines to configure this.

18) R7 should block the 150.5.111.0 network from coming in thru EIGRP.

OSPF Routing Protocol

NOTE:

Reload the routers and start with the base Frame Relay, IP Addressing and VLAN configuration

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

---

19) Routers R1, R2, R4 and R5 need to be configured with OSPF as the routing protocol with the following networks advertised in Area 0:

- R1 – 150.50.1.0/24, 150.50.12.0 /24 and 172.16.1.0 /24
- R2 – 150.50.12.0/24, 150.50.24.0/24 and 150.50.25.0/24
- R4 – 150.50.4.0/24, 150.50.24.0/24 and 150.50.45.0/24
- R5 – 150.50.25.0/24 and 150.50.45.0/24

20) Configure a separate routing process on R5 to communicate to R7. Routers R5 and R7 need to be configured with OSPF as the routing protocol with the following networks advertised:

- R5 – 150.50.57.0/24.
- R7 – 150.50.57.0/24 and 150.50.7.0/24

21) Make sure R5 sees all the routes. R1, R2 and R4 should not see the 150.50.57.0 and the 150.50.7.0 networks.

22) Configure Mutual Route Redistribution on R5 between the 2 OSPF processes. All Routers should see all routes.

23) Configure OSPF authentication on all routers using a key id of **1** and key of **cisco**. You are not allowed to use the Area command on R2 to accomplish this. Use the most secure authentication mechanism.

24) Configure the following loopbacks on R1:

- ➔ Interface Loopback 11 – 150.5.111.11 / 24
- ➔ Interface Loopback 12 – 150.5.112.12 / 24
- ➔ Interface Loopback 13 – 150.5.113.13 / 24
- ➔ Interface Loopback 14 – 150.5.114.14 / 24
- ➔ Interface Loopback 15 – 150.5.115.15 / 24

25) Inject the newly configured networks into OSPF with the exception of 150.5.115.0 network. Do not use the Network command to accomplish this.

26) Make sure that the 150.5.115.0 network does not get injected into OSPF.

27) Verify that all the routers are receiving the newly configured routes.

28) R4, R5 and R7 should not see the 150.5.111.0 and 150.5.112.0 networks. Use the minimum number of lines to configure this.

29) Do not make any configuration changes on R7 to accomplish this step.

OSPF Routing Protocol with Virtual Links

NOTE:

Reload the routers and start with the base Frame Relay, IP Addressing and VLAN configuration

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

---

30) Routers R1, R2, R4, R5 and R7 need to be configured with OSPF as the routing protocol with the following networks advertised in the appropriate Areas:

- ➔ Area 0 – R1 Loopback 0, R1 Loopback 1, R1 F 0/0, R2 F 1/0
- ➔ Area 10 – R2 S 0/1/0.4, R2 S 0/1/0.5, R4 S 0/0/0.2, R4 S 0/0/0.5, R4 F 0/0, R5 S 0/1/0.2 and R5 S 0/1/0.4
- ➔ Area 100 – R5 F 0/0 , R7 E 0/0 and R7 Loopback 0

31) Configure a Virtual Link to allow Area 100 to communicate to the Backbone Area.

32) Make sure R7 sees all the routes.

33) Configure all routers to authenticate using the most secure authentication mechanism. The Virtual Link should also be authenticated. You cannot use the Area 0 command to enable authentication on R5.

34) Configure the following loopbacks on R1:

- ➔ Interface Loopback 11 – 150.5.111.11 / 24
- ➔ Interface Loopback 12 – 150.5.112.12 / 24

35) Configure the following loopbacks on R7:

- ➔ Interface Loopback 13 – 150.5.113.13 / 24
- ➔ Interface Loopback 14 – 150.5.114.14 / 24
- ➔ Interface Loopback 15 – 150.5.115.15 / 24

36) Inject the newly configured networks into OSPF on R1 and R7 respectively using the Redistribute connected command.

37) Verify that all the routers are receiving the newly configured routes.

38) Configure area 100 in such a way that it does not receive any external routes from the backbone but the routers in Area 100 should still have reachability to them. The external routes from R7 should still be seen in Area 100. Also, R7 should not see the routes from outside area 100. It should still have reachability to them. Do not use an access-list to accomplish this.

Section 10 – Scenario 2 (Redistribution) Pre-Lab Setup

- Physically connect and configure your network according to the Lab Topology provided at the beginning of this section.

- This lab will focus strictly on IGP Redistribution. You will need to pre-configure the network with the base Frame Relay, IP Addressing and VLAN configuration. The pre-configuration will not include configuration of Routing Protocols. **Reload the routers and start with the base Frame Relay, IP Addressing and VLAN configuration.** You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 10 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

Section 10 – Scenario 2 Configuration Tasks

NOTE:

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

---

39) Configure the following loopbacks on R1:

- ➔ Interface Loopback 11 – 150.5.11.11 / 24
- ➔ Interface Loopback 12 – 150.5.12.12 / 24
- ➔ Interface Loopback 13 – 150.5.13.13 / 24
- ➔ Interface Loopback 14 – 150.5.14.14 / 24
- ➔ Interface Loopback 15 – 150.5.15.15 / 24

40) Configure RIP as the routing protocol between R1 and R2. Advertise all the networks on R1 including the newly created loopbacks. On R2, advertise the F 1/0 interface in RIP. Make sure R2 does not send RIP updates over S 0/1/0.4 and S 0/1/0.5 and that R2 does not send any routes to R1 at this stage.

41) Configure OSPF as the routing protocol between R2, R4 and R5. Use Area 0. Advertise the S 0//0/0.2, S 0/0/0.5, and the F 0/0 interface on R4. Only advertise the serial links on R2 and R5 in OSPF.

42) Configure the following loopbacks on R7:

- Interface Loopback 21 – 150.5.21.21 / 24
- Interface Loopback 22 – 150.5.22.22 / 24
- Interface Loopback 23 – 150.5.23.23 / 24
- Interface Loopback 24 – 150.5.24.24 / 24
- Interface Loopback 25 – 150.5.25.25 / 24

43) Configure EIGRP in AS 57 between R5 and R7. Advertise all the networks on R7 including the newly created loopbacks. On R5, advertise the F 0/0 interface in EIGRP.

44) On R2, Mutually redistribute RIP and OSPF with the following parameters:

- Redistribute RIP into OSPF
- Do not inject networks from the 150.5.x.0 range that have an even number in the third octet. All the other networks should be redistributed. Use the minimum number of lines in your access-list. You cannot use distribute lists in this task
- Redistribute OSPF into RIP. R1 should see the R4 networks with a hop count of 4 and the R5 networks with a hop count of 5
- You cannot use the offset-list command to accomplish this
- You can use the neighbor command under RIP to accomplish this task.

45) On R5, Mutually redistribute EIGRP and OSPF with the following parameters:

- Redistribute EIGRP into OSPF
- Set a tag of 100 for all the networks in the 150.5.x.0 range that have an even number in the third octet. This tag will be used later to filter routes at appropriate routers.
- Make sure you do not set the tag on the other networks
- Redistribute OSPF into EIGRP

46) R2 should ONLY pass any routes from R5 with a tag of 100 to RIP. You can add one more line of code to the existing configuration to accomplish this. R1 should see the following routes thru RIP:

- 150.50.45.0 with a metric of 4
- 150.50.4.0 with a metric of 4
- 150.50.24.0 with a metric of 1
- 150.50.25.0 with a metric of 1
- 150.5.22.0 with a metric of 5
- 150.5.24.0 with a metric of 5

Section 10 Technical Tips and Comments

RIP Routing Protocol

- Use the **Router RIP** command to configure RIP as the routing protocol.
- Use the **Key Chain** global configuration command to create the Key chain.
- Use the **IP RIP authentication** interface configuration command to setup RIP Authentication.
- Use **Route Redistribution** command with **Route-Maps** to selectively advertise Loopback networks.
- Use **Distribute List** to configure route filtering.

EIGRP Routing Protocol

- Use the **Router EIGRP** command to configure EIGRP as the routing protocol.
- Use the **Key Chain** global configuration command to create the Key chain.
- Use the **IP authentication** interface configuration command to setup EIGRP Authentication.
- Use **Route Redistribution** command with **Route-Maps** to selectively advertise Loopback networks.
- Use **Distribute List** to configure route filtering.

OSPF Routing Protocol

- Use the **Router OSPF** command to configure OSPF as the routing protocol.
- Use the **Area** command to enable authentication.
- Use the **IP OSPF** interface configuration command to setup OSPF Authentication.
- Use **Route Redistribution** command with **Route-Maps** to selectively advertise Loopback networks.
- Use **Distribute List** to configure route filtering.

OSPF Routing Protocol – Virtual Link

- Use the **Router OSPF** command to configure OSPF as the routing protocol.
- Use the **Area** command to configure the virtual link.
- Use the **Area** and **IP OSPF** commands to enable authentication.
- Use the **IP OSPF** interface configuration command to setup OSPF Authentication.
- Use **Route Redistribution** command to redistribute the Loopback networks.
- Use **Area** to configure area 10 as a NSSA Area.

Redistribution

- Use the **Router RIP** command to configure RIP as the routing protocol.
- Use the **Router OSPF** command to configure OSPF as the routing protocol.
- Use the **Router EIGRP** command to configure OSPF as the routing protocol.
- Use **Route Map** and **Access Lists** to filter redistribution between RIP and OSPF.
- Use **Route Map, Access Lists** and **Set/Match Tags** to filter redistribution between EIGRP and OSPF.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 11: Routing | BGP

- IBGP
- EBGP
- BGP Authentication between IBGP and EBGP Neighbors
- BGP Route Filtering using Prefix-List, Distribute-List, Route-Maps and Suppress-Maps
- Route Reflectors

Routing | BGP Overview

This section will test your understanding and knowledge of BGP topics. This section will have 2 lab scenarios.

This lab will use Routers R1, R2, R4, R5, R6 and the appropriate Catalyst switches.

Estimated Time to Complete: 6 Hours

NOTE:

This section has 2 lab scenarios each focusing on various, yet fundamentally important BGP topics. Each lab scenario within this section should take you approximately 3 hours to complete.

Diagram 11-A

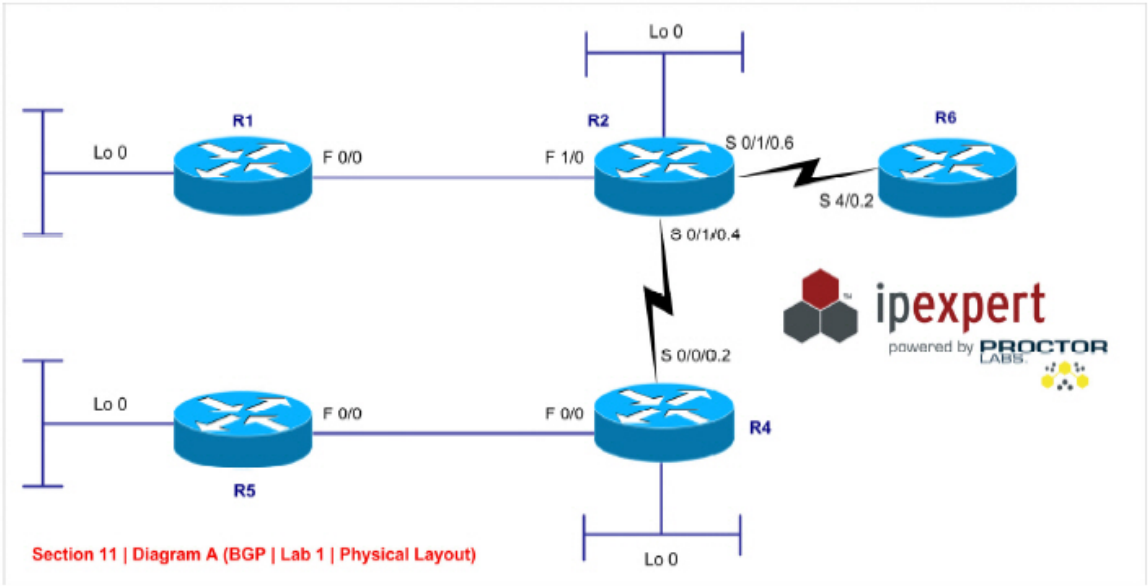
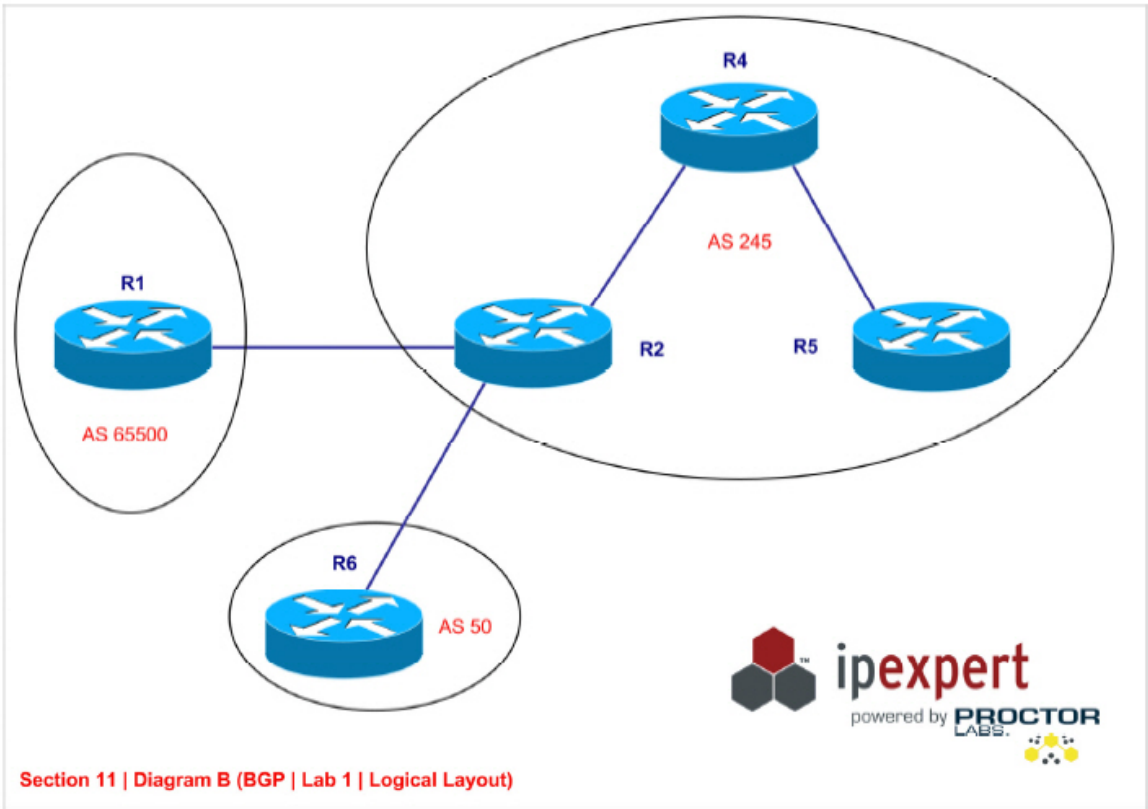


Diagram 11-B



Section 11 – Scenario 1 Pre-Lab Setup

- Physically connect and configure your network according to Diagrams 11-A and 11-B.
- This lab will focus strictly on BGP. You will need to pre-configure the network with the base Frame Relay, IP Addressing and VLAN configuration. The pre-configuration will not include configuration of Routing Protocols. You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 11 → Initial Configurations Lab 1 → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

Section 11 – Scenario 1 Configuration Tasks

NOTE:

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

OSPF

1) Setup OSPF between R1, R2, R4, R5 and R6. All interfaces should be in Area 0. Advertise Loopback 0 on all routers in OSPF.
2) Authenticate all routers using area-based authentication. Use the most secure method for authentication.

IBGP

3) Create a Loopback 11 on all Routers. (R1, R2, R4 and R5) using the following format:

   → 11.X.X.X/24 (where X is your router #)

4) Hard Code the Router ID on all the routers to Loopback 0.
5) Setup R2, R4 and R5 in AS 245 using a method that can allow for redundancy in case of link failure.
6) Do not setup a neighbor relationship between R2 and R5. Do not use Confederations.
7) Advertise Loopback 11 under BGP on R2, R4 and R5.
8) Setup authentication between all IBGP Peers. Use the most secure authentication method.

EBGP

9) Setup a neighbor relationship between AS 245 and AS 65500. Use the most logical routers to set this relationship up.
10) Authenticate the neighbors with the most secure authentication possible.

11) Advertise Loopback 11 in AS 65500. Do not use the Network Command to accomplish this.

12) Setup a neighbor relationship between AS 245 and AS 50.

13) Advertise all the loopbacks on R6 except Loopback 0.

14) Use R2 in AS 245 to set this relationship up.

Route Aggregation with Filtering

15) R6 should not see the AS 65500 in the AS-Path attribute. You can only use 1 line to accomplish this.

16) Send a single summary route towards AS 65500 and AS 245 for all the routes learned from R6.

17) The Routes should not be seen as suppressed on R2.

18) Specific routes should not be sent to AS 65500 and AS 245.

19) R1, R4 and R5 should be able to Ping all R6 routes.

Section 11 – Scenario 1 Technical Tips and Comments

OSPF

- Use the **Router OSPF** command to configure OSPF as the IGP routing protocol.
- Use the **Area** and **IP OSPF message-digest-key** command to configure authentication.

IBGP

- Use the **Router BGP** command to configure IBGP between the IBGP neighbors.
- Use the **Neighbor** command with the **password** option to configure authentication.
- Use the **Neighbor** command with the **update-source** option to provide a fault tolerant neighbor relationship.
- Use the **Neighbor** command with the **route-reflector-client** option to configure the route reflector relationship between the routers.

EBGP

- Use the **Router BGP** command to configure EBGP between the IBGP neighbors.
- Use the **Neighbor** command with the **password** option to configure authentication.
- Use a **Route-map** and an **Access-List** to advertise the Loopback network without using the network statement.

Route Aggregation with Filtering

- Use the **Neighbor** command with the **remove-private-as** option to filtering the Private AS.
- Use the **aggregate-address** command to aggregate the required networks.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 11 – Scenario 2

This lab will use Routers R1, R2, R4, R5, R6 and the appropriate Catalyst switches.

Diagram 11-C

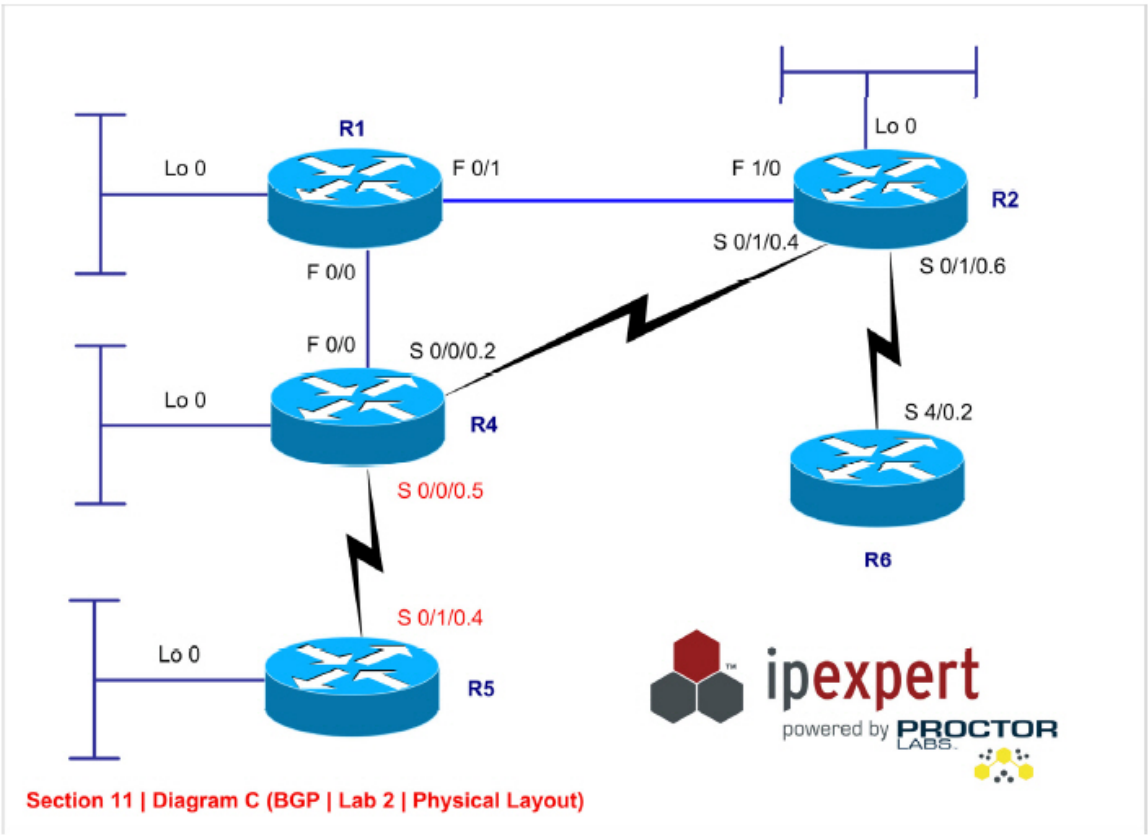
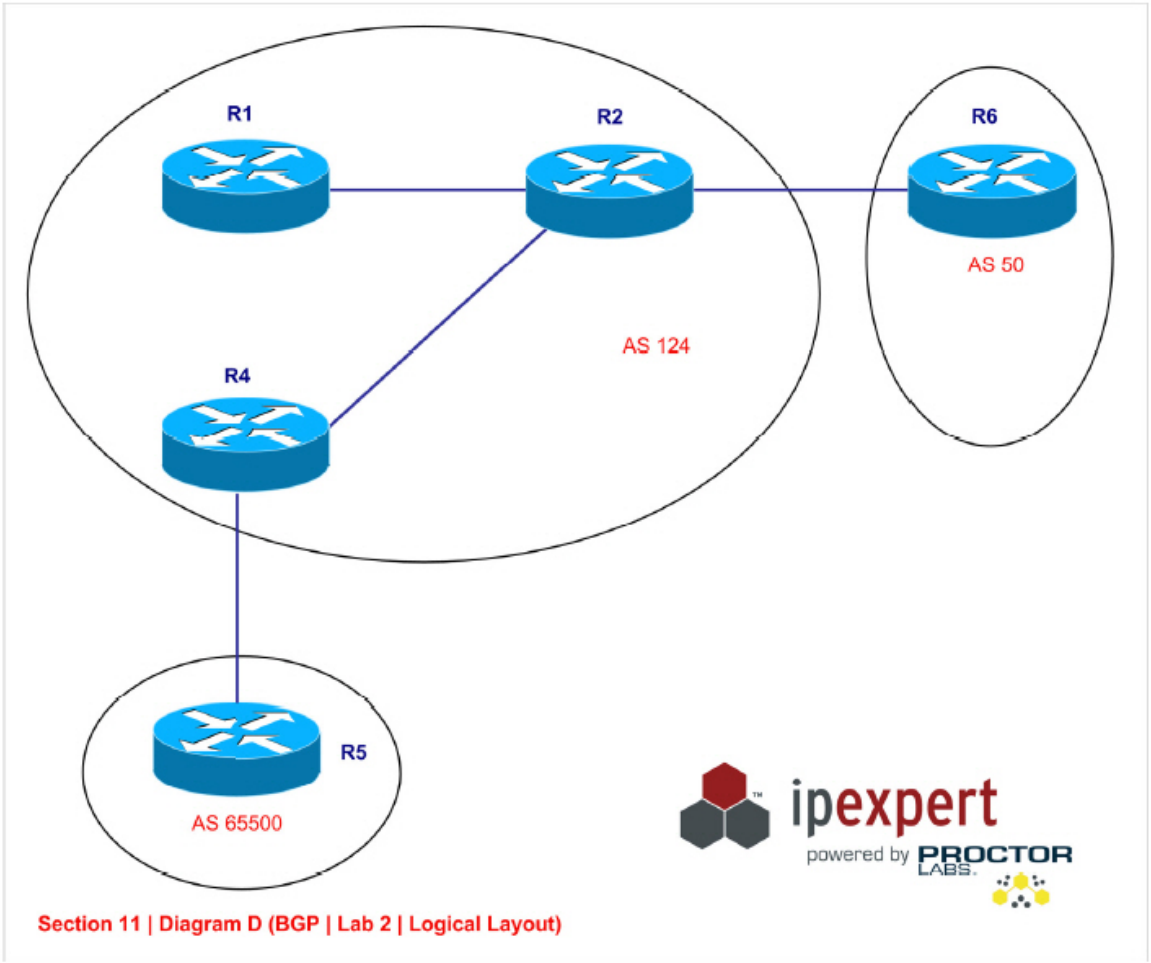


Diagram 11-D



Section 11 – Scenario 2 Pre-Lab Setup

- Physically connect and configure your network according to Diagrams 11-C and 11-D.
- This lab will focus strictly on BGP. You will need to pre-configure the network with the base Frame Relay, IP Addressing and VLAN configuration. The pre-configuration will not include configuration of Routing Protocols. You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 11 → Initial Configurations Lab 2 → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

Section 11 – Scenario 2 Configuration Tasks

NOTE:

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

IGP

20) Run OSPF in Area 0 between R2 and R4.

21) Run EIGRP in AS 12 between R1 and R2.

22) Advertise Loopback 0 on R1 in EIGRP, Loopback 0 on R2 in EIGRP and Loopback 0 on R4 in OSPF.

23) Create a Loopback 11 on R1, R4 and R5 using the following format:

- 11.X.X.X / 24. (where X is your router number)

24) Run RIPv2 between on R1, R4 and R5.

25) Advertise Loopback 11 in RIP on those 3 routers.

26) Perform Redistribution on R1 and R4 as follows:

- Redistribute EIGRP into RIP on R1.
- Redistribute OSPF into RIP on R4.
- Redistribute RIP into EIGRP with Filtering on R1 by sending only RIP originated routes into EIGRP.

IBGP

27) Create a Loopback 12 on all Routers. (R1, R2, R4 and R5) using the following format:

- 12.X.X.X / 24. (where X is your router number)

28) Setup R1, R2 and R4 in AS 124.

29) You cannot have a neighbor relationship between R1 and R4. Do not use Confederations.

30) Advertise Loopback 12 under BGP on R1, R2 and R4. **Configure the BGP neighbors such that Traffic destined to BGP learned routes between the peers will flow through R2.**

31) Setup authentication between all IBGP Peers. Use the most secure authentication method.

EBGP

32) Setup a neighbor relationship between AS 124 and AS 50.

33) Use R2 in AS 124 to set this relationship up.

34) Advertise all Loopback networks on R6 in AS 50. Make R6 routes show up as valid routes on R1 and R4.

35) Setup a neighbor relationship between AS 124 and AS 65500. Use R4 in AS 124 and R5 in 65500.

36) Advertise Loopback 12 in AS 65500. Do not use the Network Command to accomplish this.

37) Make sure R2 can see R5's Loopback 12 through BGP.

Route Filtering

38) On R2, aggregate the 200.1.0.0 networks received from R6.

39) Send a summary route using the most specific mask. In addition to the summary route, the specific routes for 200.1.5.0/24 and 200.1.6.0/24 should also be sent.

40) Do not use Prefix-list or distribute-list to accomplish this.

41) AS 124 should not allow AS 65500 and AS 50 to use AS 124 to get to each others routes.

42) Do not send any routes learned from AS 50 to AS 65500 and vice-versa.

43) Do not use the distribute-list or prefix-list commands to accomplish this task.

Section 11 – Scenario 2 Technical Tips and Comments

IGP

- Use the **Router RIP** command to configure RIP as the routing protocol.
- Use the **Router OSPF** command to configure OSPF as the routing protocol.
- Use the **Router EIGRP** command to configure RIP as the routing protocol.
- Use the **Redistribute** command with the **Route-map** option to configure Redistribution with Filtering.

IBGP

- Use the **Router BGP** command to configure IBGP between the IBGP neighbors.
- Use the **Neighbor** command with the **password** option to configure authentication.
- Use the **Neighbor** command with the **route-reflector-client** option to configure the route reflector relationship between the routers.

EBGP

- Use the **Router BGP** command to configure EBGP between the IBGP neighbors.
- Use the **Neighbor** command with the **password** option to configure authentication.
- Use a **Route-map** and an **Access-List** to advertise the Loopback network without using the network statement.

Route Aggregation with Filtering

- Use the **suppress-map** and **route-map** commands to aggregate and send specific routes.
- Use the **IP AS-Path** command to make the AS a non-transit AS. The Regular expression **^$** will accomplish this.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 12: Router Management | IOS Services

- Configuring Telnet Parameters
- Configuring DHCP Server Parameters
- Configuring NTP
- Configuring IP Accounting
- Configuring Core Dumps

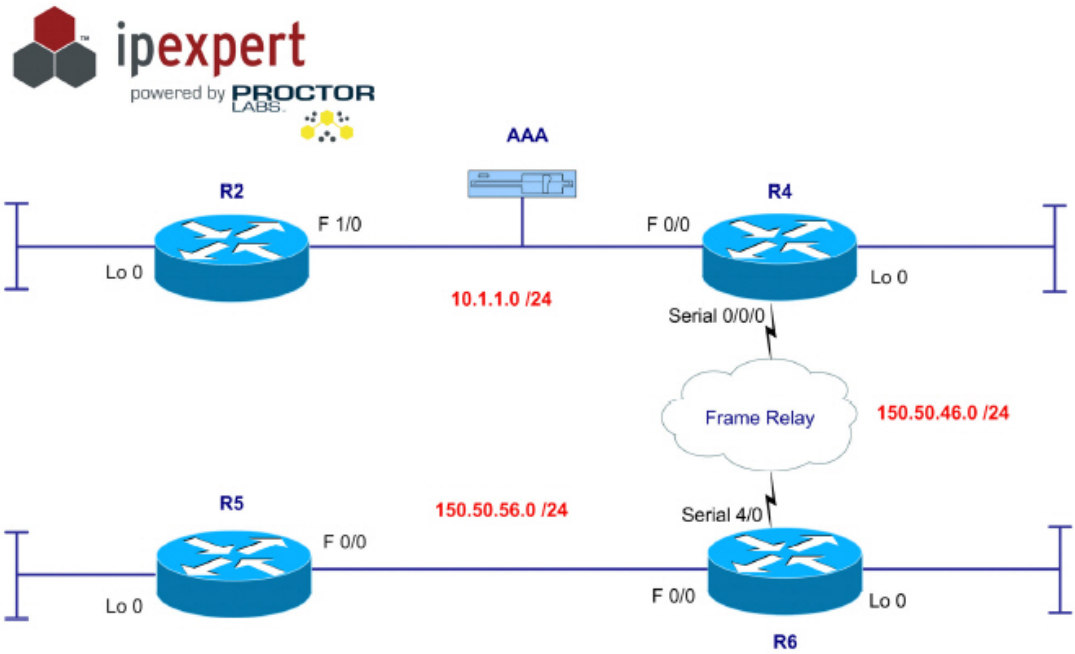
Router Management | IOS Services Overview

This section will test your understanding and knowledge of various IOS Services.

This lab will use Routers R2, R4, R5, R6 and the appropriate Catalyst switches.

Estimated Time to Complete: 2 Hours

Diagram 12-A



Section 12 | Diagram A (Router Management | IOS Services)

Section 12 Pre-Lab Setup

- Physically connect and configure your network according to Diagram 12-A.
- The Routers are running the following protocols:
  - OSPF as the routing protocol
- This lab will focus strictly on IOS Services. You will need to pre-configure the network with the base Frame Relay, IP Addressing and OSPF configuration. You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 12 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

Section 12 Configuration Tasks

NOTE:

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

Telnet Configurations

1) The administrator of R2 wants to reserve a Telnet line for himself.

2) Accomplish this by changing the telnet port for the last vty line to 3045.

3) The administrator of R2 does not want anybody to telnet from R2. Disable the Telnet client on R2. You cannot use an Access List to accomplish this task.

4) When users Telnet into the normal Telnet port on R2, they should not have the ability to access the command prompt. Instead, they should receive a menu that only allows them the ability to perform the following commands:

   - SH IP INT BRIEF
   - SH IP ROUTE
   - SH IP OSPF NEIGHBOR
   - EXIT

DHCP Server

5) Enable R4 as a DHCP Server with the following information:

   - IP ADDRESS : 10.1.1.0 255.255.255.0
   - WINS ADDRESS : 10.1.1.135
   - DNS ADDRESS : 10.1.1.53
   - DEFAULT GATEWAY : 10.1.1.4
   - LEASE TIME : 3 Days 12 hours
   - Excluded Addresses: 10.1.1.1 – 10.1.1.20, 10.1.1.53 – 10.1.1.100, 10.1.1.135

6) Disable any DHCP Related services on R2.

7) Enable conflict logging on R4

8) Configure option 19 to tell the client should configure its IP layer for packet forwarding.

9) Specifies five ping attempts by the DHCP server before ceasing any further ping attempts

NTP

10) Configure the timezone on R2 as PST -8. Set the clock to the current time on R2.

11) Set R2 as the NTP Master with a stratum of 2. NTP should require MD5 authentication with a key 1.

12) Configure R6 as the client for R2. R6 should point to R2 using the NTP Server command. Configure the timezone to PST -8 on R6.

13) Configure R4 to peer with R6. R4 should get its clock from R6. Use the Peer command to accomplish this. Configure the timezone to PST -8 on R4.

14) Configure R6 to periodically update the hardware clock from NTP time source.

15) Configure a Trimble Palisade NTP Synchronization Kit as the GPS clock source connected to the Aux0 port

IP Accounting

16) You would like to gather traffic statistics about the traffic that transits thru R6. Configure R6 for IP accounting on both interfaces.

17) The maximum number of accounting entries to be created should be 500.

18) IP accounting should be based on IP precedence for received and transmitted packets

Privilege

19) Configure a user (username = "user"/password = none) in R2 that can set the clock.

20) Configure a user (username = "manager"/password = "manager") in R2 such that he inherit the privilege of user "user" but he can also set the ip address and shut down any interface.

Core Dump to a RCP Server

21) Configure R5 to send a Core Dump to a RCP Server located at 10.1.1.15.

22) The router logs into the RCP Server using a username of **ipexpert**.

23) Set the Dump size to 32768.

24) The router should use the source address of 5.5.5.5, the Loopback address on R5.

Section 12 Technical Tips and Comments

Telnet Configurations

- Use the **rotary** command to specify a non-default port for Telnet.
- Use the **transport output none** command to disable the Telnet client on a router.
- User the **Menu** command to define the menu options for the menu.
- Use the **autocommand** to enable the menu automatically when a user telnets into the router's default port.

DHCP Server

- Use the **IP DHCP** command to configure the DHCP parameters.
- Use the **No service** command to disable DHCP services on a router.

- Cisco recommends using a DHCP server database agent to store automatic bindings. By default, the Cisco IOS DHCP Server records DHCP address conflicts in a log file.
- The DHCP server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the DHCP server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client.

NTP

- Use the **NTP Master** command to configure NTP Stratum.
- Use the **NTP Authenticate** command to configure the authentication parameters.
- Use the **NTP Server** command on R6 to point to the NTP Server.
- If the software clock is synchronized to an outside time source via NTP, it is a good practice to periodically update the hardware clock with the time learned from NTP. Otherwise, the hardware clock will tend to gradually lose or gain time (drift), and the software clock and hardware clock may become out of synchronization with each other. The hardware clock will be updated only if NTP has synchronized to an authoritative time server.
- Use the **NTP Peer** command on R4 to point to R6.

IP Accounting

- Use the **IP Accounting** command to record traffic that transits thru R6.

Privilege

- Users can override the privilege level you set using this command by logging in to the line and enabling a different privilege level. When you set the privilege level for a command with multiple words, note that the commands starting with the first word will also have the specified access level. For example, if you set the show ip route command to level 15, the show commands and show ip commands are automatically set to privilege level 15—unless you set them individually to different levels. This is necessary because you can not execute, for example, the show ip command unless you have access to show commands.

Core Dump to a RCP Server

- Use the **IP RCMD Remote-username** command to configure the username to connect to the RCP Server.
- Use the **Exception** command to specify the Core dump parameters.
- The accounting threshold defines the maximum number of entries (source and destination address pairs) that the software accumulates, preventing IP accounting from possibly consuming all available free memory. This level of memory consumption could occur in a router that is switching traffic for many hosts. Overflows will be recorded; see the monitoring commands for display formats. The default accounting threshold of 512 entries results in a maximum table size of 12,928 bytes. Active and checkpointed tables can reach this size independently.
- The precedence accounting feature provides accounting information for IP traffic, summarized by IP precedence values. This feature calculates the total packet and byte counts for an interface that receives or sends IP packets and sorts the results based on IP precedence. This feature is supported on all interfaces and subinterfaces and supports CEF, dCEF, flow, and optimum switching.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 13: WAN | Layer 2

- Frame Relay using Regular Multipoint Interfaces
- Frame Relay using Sub-interfaces
- Routing Protocols (EIGRP and OSPF) over Frame
- QoS over Frame Relay

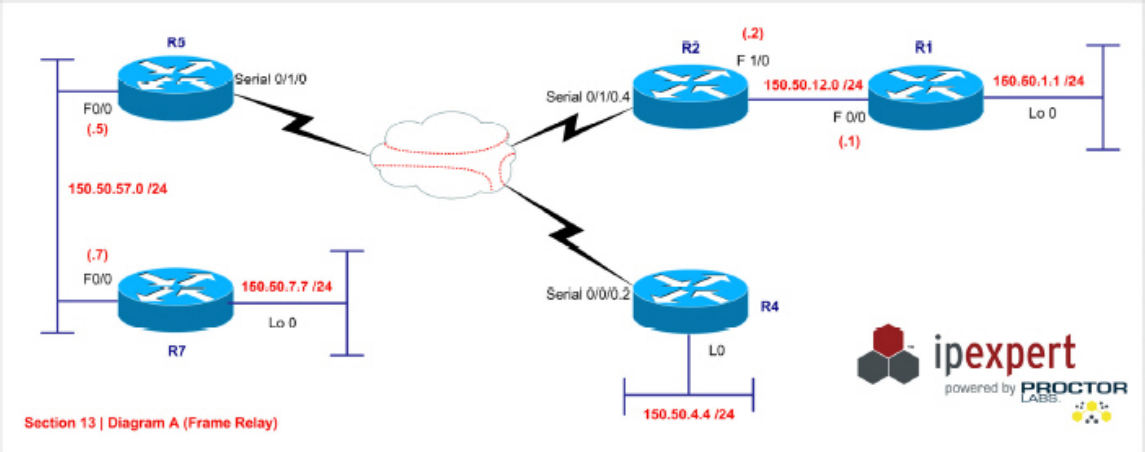
WAN | Layer 2 Overview

This section will test your understanding and knowledge of Frame Relay. You will configure Frame Relay using various configurations. This section will have 2 lab scenarios. The first will test your understanding of Frame Relay. The second will contain the Routing and QoS configurations over Frame Relay.

This lab will use Routers R1, R2, R4, R5, R7 and the appropriate Catalyst switches.

Estimated Time to Complete: 5 Hours

Diagram 13-A



Section 13 – Scenario 1 (Frame Relay) Pre-Lab Setup

- Physically connect and configure your network according to Diagram 13-A. The Frame Relay DLCI information is provided on the Physical Setup of the Lab.
- The Serial interfaces are not set. You will need to assign IP Address based on the Sections.
- This lab will focus on Frame Relay. You will need to pre-configure the network with IP Addressing and VLAN configuration use the pre-configuration files. You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 13 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

Section 13 – Scenario 1 Configuration Tasks

NOTE:

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

Full Mesh Frame Relay Using Regular Interfaces

1) Configure Frame Relay between R2, R4 and R5.
2) You cannot use Sub-Interfaces.
3) The Frame Mappings should not be learned thru Inverse-ARP.

4) Use 150.50.246.0/24 as your network for all 3 routers. The Interface IP address for the Individual Routers are as follows:

   - R2 – S0/1/0 – 150.50.245.2 / 24
   - R4 – S0/0/0 – 150.50.245.4 / 24
   - R5 – S0/1/0 – 150.50.245.6 / 24

5) All the routers should use a single hop to get to each other.

6) All routers should be able to ping each other and their own IPs.

Hub-n-Spoke Frame Relay Using Regular Interfaces

NOTE:

Reload R2, R4 and R5 and use the pre-configuration file to load the IP address on the non-frame interfaces.

Please read the entire list in each section before starting.

---

7) Configure Frame Relay between R2, R4 and R5.

8) You cannot use Sub-Interfaces.

9) The Frame Mappings should not be learned thru Inverse-ARP.

10) Use 150.50.245.0/24 as your network for all 3 routers. The Interface IP address for the Individual Routers are as follows:

    - R2 – S0/1/0 – 150.50.245.2 / 24
    - R4 – S0/0/0 – 150.50.245.4 / 24
    - R5 – S0/1/0 – 150.50.245.6 / 24

11) Do not configure any PVC between R4 and R5.

12) All routers should be able to ping each other and their own IPs.

13) Configure TCP header compression for all PVC's

Hub-n-Spoke Frame Relay Using Sub-interfaces

NOTE:

Reload R2, R4 and R5 and use the pre-configuration file to load the IP address on the non-frame interfaces.

Please read the entire list in each section before starting.

---

14) Configure Frame Relay between R2, R4 and R5.

15) The Frame Mappings should not be learned thru Inverse-ARP.

16) Use 150.50.24.0/24 as your network for the link between R2 and R4 and 150.50.25.0/24 for the link between R2 and R5. The Interface IP address for the Individual Routers will be the router numbers. For example, R2 will be 150.50.24.2 and 150.50.25.2.

17) Do not configure any PVC between R4 and R5.

18) You cannot use the **Frame-Relay map** command.

19) R2 should be able to ping R4 and R5. R4 and R5 should only be able to ping the Hub.

20) Enable Frame-relay end-to-end keepalives for bi-directional mode between R2 and R5.

21) configure the PVC between R2 and R5 to be in the priority DLCI group

Hub-n-Spoke Frame Relay Using Sub-interfaces and Regular Interfaces

---

NOTE:

Reload R2, R4 and R5 and use the pre-configuration file to load the IP address on the non-frame interfaces.

Please read the entire list in each section before starting.

---

22) Configure Frame Relay between R2, R4 and R5.

23) The Frame Mappings should not be learned thru Inverse-ARP on R4 and R5.

24) Use 150.50.245.0 /24 as your network for the 3 routers. The interface IP addresses for the individual routers are as follows:

- ➔ R2 s 0/1/0: 150.50.245.2
- ➔ R4 s 0/0/0: 150.50.245.4
- ➔ R5 s 0/1/0: 150.50.245.5

25) Do not configure any PVC between R4 and R5.

26) You cannot use the **Frame-Relay map** command on R2.

27) You cannot create Sub-interfaces on R4 and R5.

28) R2 should be able to ping R4 and R5. R4 and R5 should only be able to ping the Hub.

Hub-n-Spoke Frame Relay Using Sub-interfaces and Regular Interfaces II

NOTE:

Reload R2, R4 and R5 and use the pre-configuration file to load the IP address on the non-frame interfaces.

Please read the entire list in each section before starting.

---

29) Configure Frame Relay between R2, R4 and R5.

30) The Frame Mappings should not be learned thru Inverse-ARP

31) Use 150.50.24.0/24 as your network for the link between R2 and R4 and 150.50.25.0/24 for the link between R2 and R5. The Interface IP address for the Individual Routers will be the router numbers. For example, R2 will be 150.50.24.2 and 150.50.25.2.

32) Do not configure any PVC between R4 and R5.

33) On R2, you cannot specify IP Address or Frame-Relay Mappings on the regular interface. You must create sub-interfaces on R2. You are allowed to use the **Frame Relay interface-dlci** command under the sub-interface's on R2.

34) You cannot create sub-interfaces on R4 and R5.

35) R2 should be able to ping R4 and R5 and its own IPs. R4 and R5 should be able to ping R2 as well as their own IPs.

Section 13 – Scenario 2 (Routing over Frame Relay and QoS on Frame Relay) Pre-Lab Setup

- Physically connect and configure your network according to Diagram 13-A. The Frame Relay DLCI information is provided on the Physical Setup of the Lab.
- The Serial interfaces are not set. You will need to assign IP Address based on the Sections.
- This lab will focus on Frame Relay. You will need to pre-configure the network with IP Addressing and VLAN configuration use the pre-configuration files. You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 12 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

Section 13 – Scenario 2 Configuration Tasks

NOTE:

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

Hub-n-Spoke Frame Relay Using Sub-interfaces and Regular Interfaces

36) Configure Frame Relay between R2, R4 and R5.

37) The Frame Mappings should not be learned thru Inverse-ARP.

38) Use 150.50.24.0/24 as your network for the link between R2 and R4 and 150.50.25.0/24 for the link between R2 and R5. The Interface IP address for the Individual Routers will be the router numbers. For example, R2 will be 150.50.24.2 and 150.50.25.2.

39) Do not configure any PVC between R4 and R5.

40) You cannot use the **Frame-Relay map** command on R2.

41) You cannot create Sub-interfaces on R4 and R5.

42) R2 should be able to ping R4 and R5. R4 and R5 should only be able to ping the Hub.

OSPF Routing Protocol

NOTE:

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

---

43) Routers R1, R2, R4, R5 and R7 need to be configured with OSPF as the routing protocol with the following networks advertised in Area 0:

- → R1 – 150.50.1.0/24 and 150.50.12.0/24
- → R2 – 150.50.12.0/24, 150.50.24.0/24 and 150.50.25.0/24
- → R4 – 150.50.4.0/24, 150.50.24.0/24
- → R5 – 150.50.25.0/24, 150.50.57.0 /24
- → R7 – 150.50.57.0/24 and 150.50.7.0/24

44) Make sure you can ping all OSPF networks from all routers.

45) You cannot use the Neighbor command under OSPF.

46) You cannot change the Hello Interval.

QoS over Frame Relay

47) The PVC between R2 and R5 is used more heavily than the PVC between R2 and R4.

48) The PVC between R2 and R5 should be allocated 65% of the Bandwidth and PVC between R2 and R4 should be allocated 35% of the bandwidth.

49) Use Class Maps and Service Policy to implement QoS on the Frame Relay Links.

50) For R4, Enable congestion management function on all switched PVC with ECN BE=0, ECN BC=20 and DE=40.

51) For R4, Enable policing on all switched PVCs on the interface.

Hub-n-Spoke Frame Relay Using Regular Interfaces

NOTE:

Reload R2, R4 and R5 and use the pre-configuration file to load the IP address on the non-frame interfaces.

Disable OSPF on all Routers.

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

---

52) Configure Frame Relay between R2, R4 and R5.

53) You cannot use Sub-Interfaces.

54) The Frame Mappings should not be learned thru Inverse-ARP.

55) Use 150.50.245.0/24 as your network for all 3 routers. The Interface IP address for the Individual Routers are as follows:

- ➔ R2 – S0/1/0 – 150.50.245.2 / 24
- ➔ R4 – S0/0/0 – 150.50.245.4 / 24
- ➔ R5 – S0/1/0 – 150.50.245.6 / 24

56) Do not configure any PVC between R4 and R5.

57) All routers should be able to ping each other and their own IPs.

EIGRP Routing Protocol

NOTE:

As a general rule of thumb, we recommend that you read the ENTIRE lab prior to beginning.

---

58) Routers R1, R2, R4, R5 and R7 need to be configured with EIGRP as the routing protocol in AS 12457. All interfaces on all routers need to be advertised in EIGRP.

59) Make sure you can ping all EIGRP networks from all routers.

Section 13 Technical Tips and Comments

Full Mesh Frame Relay Using Regular Interfaces

- Use the **No Frame-Relay inverse-arp** command to disable inverse-arp on the interface.
- Use the **Frame-relay Map** command to configure static Frame relay mapping.

Hub-n-Spoke Frame Relay Using Regular Interfaces

- Use the **No Frame-Relay inverse-arp** command to disable inverse-arp on the interface.
- Use the **Frame-relay Map** command to configure static Frame relay mapping.
- When you use this command to enable TCP/IP header compression, every IP map inherits the compression characteristics of the interface, unless header compression is explicitly rejected or modified by use of the frame-relay map ip tcp header compression command.

Hub-n-Spoke Frame Relay Using Sub-interfaces

- Use the **No Frame-Relay inverse-arp** command to disable inverse-arp on the interface.
- Use the **Frame-relay Interface-dlci** command to configure the appropriate DLCI for the Sub-interface.
- A map-class must be associated and a DLCI is assigned. In bidirectional mode, both ends of a virtual circuit send keepalive requests and respond to keepalive requests. If one end of the VC is configured in the bidirectional mode, the other end must also be configured in the bidirectional mode.
- To prioritize multiple data-link connection identifiers (DLCIs) according to the type of Frame Relay traffic, use the frame-relay priority-dlci-group interface configuration command.

Hub-n-Spoke Frame Relay Using Sub-interfaces and Regular Interfaces

- Use the **No Frame-Relay inverse-arp** command to disable inverse-arp on the interface.
- Use the **Frame-relay Interface-dlci** command to configure the appropriate DLCI for the Sub-interface.
- Use the **Frame-relay Map** command to configure static Frame relay mapping.

Hub-n-Spoke Frame Relay Using Sub-interfaces and Regular Interfaces

- Use the **No Frame-Relay inverse-arp** command to disable inverse-arp on the interface.
- Use the **Multipoint** Sub-interface for the Hub.
- Use the **Frame-relay Map** command to configure static Frame relay mapping.

OSPF over Frame Relay

- Use the **No Frame-Relay inverse-arp** command to disable inverse-arp on the interface.
- Use the **Frame-relay Interface-dlci** command to configure the appropriate DLCI for the Sub-interface.
- Use the **Frame-relay Map** command to configure static Frame relay mapping.
- Use the **Router OSPF** command to configure OSPF as the routing protocol.
- Use the **IP OSPF Network** interface configuration command to configure Network types to allow OSPF to run over Frame Relay.

QoS

- Use a class-map to define your DLCI.
- Use a policy map to specify the bandwidth percent based on the class-map.
- Apply the Policy to the interface.
- Frame Relay congestion management is supported only when the interface is configured with FIFO queueing, weighted fair queueing (WFQ), or PVC interface priority queueing (PIPQ).
- You must enable Frame Relay policing on the incoming interface before you can configure traffic-policing parameters.

EIGRP over Frame Relay

- Use the **No Frame-Relay inverse-arp** command to disable inverse-arp on the interface.
- Use the **Frame-relay Map** command to configure static Frame relay mapping.
- Use the **Router EIGRP** command to configure OSPF as the routing protocol.
- Use the **IP Split-horizon** interface configuration command to disable Split Horizon.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 14: Multiprotocol Challenge A (One Day Lab Experience)

This Lab is intended to assess your readiness to attempt the actual CCIE Security lab exam. During this section you will be utilizing the entire topology and all topics listed on the CCIE Security Lab Blueprint are fair game.

Estimated Time to Complete: 8 Hours

MUST DO:

Read the ENTIRE lab prior to beginning.

Diagram 14-A

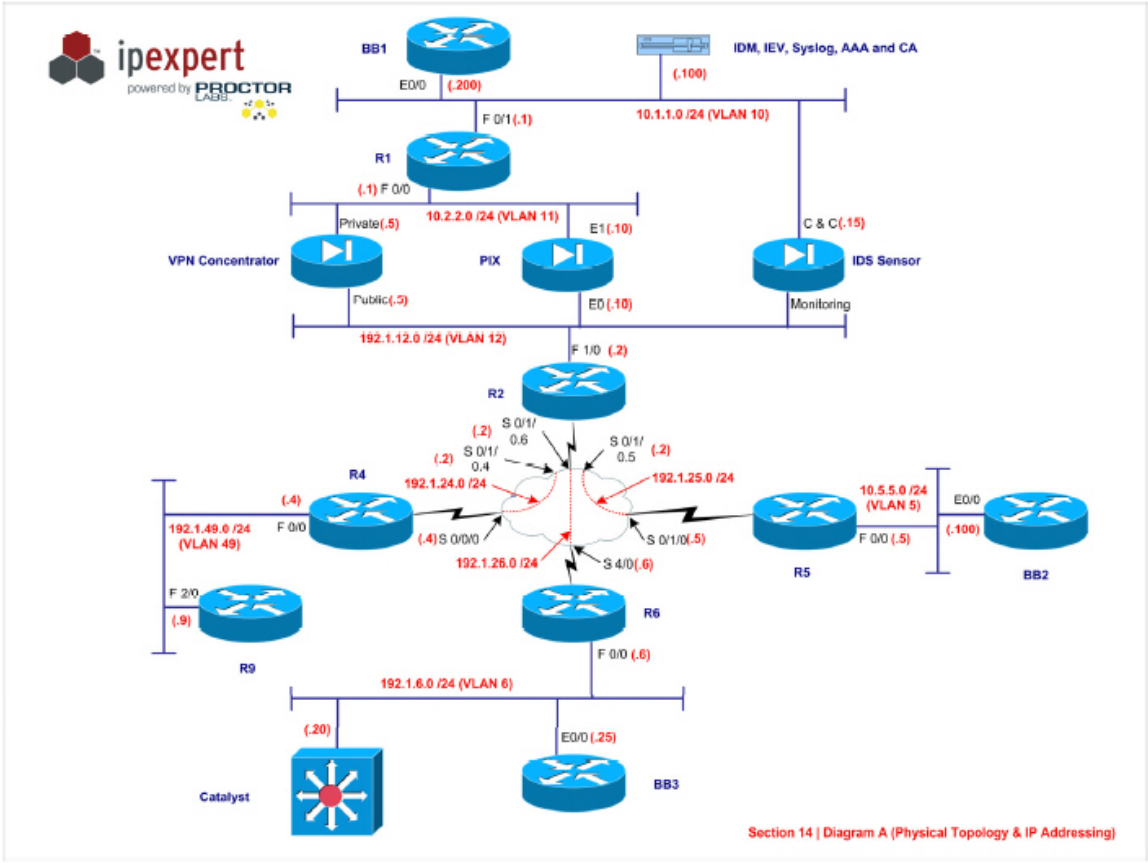
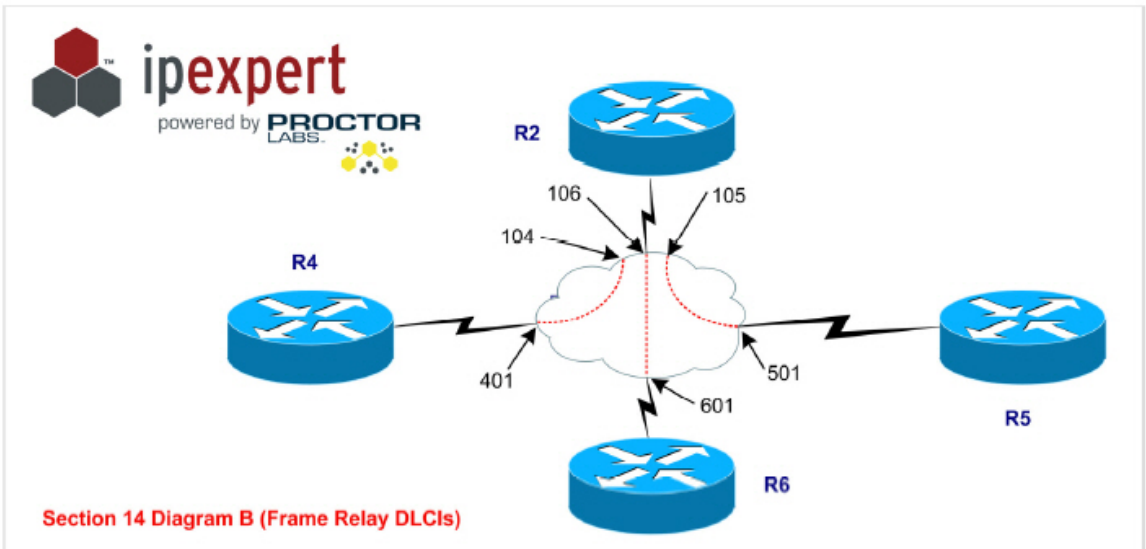


Diagram 14-B



Section 14 IP Addressing

Device	Port	IP Address
R1	F 0/0	10.2.2.1/24
	F 0/1	10.1.1.1/24
	Loopback 0	1.1.1.1 / 8
R2	F 1/0	192.1.12.2/24
	S 0/1/0.4	192.1.24.2/24
	S 0/1/0.5	192.1.25.2/24
	S 0/1/0.6	192.1.26.2/24
	Loopback 0	2.2.2.2 / 8
R4	F 0/0	192.1.49.4/24
	S 0/0/0	192.1.24.4/24
	Loopback 0	4.4.4.4/8
R5	F 0/0	10.5.5.5/24
	S 0/1/0	192.1.25.5/24
	Loopback 0	5.5.5.5 / 8
R6	F 0/0	192.1.6.6/24
	S 4/0	192.1.26.6/24
	Loopback 0	6.6.6.6/8
R9	F 0/0	192.1.49.9/24
	Loopback 0	9.9.9.9/8
PIX	E 0 (outside)	192.1.12.10/24
	E 1 (inside)	10.2.2.10/24
Concentrator	Private	10.2.2.5/24
	Public	192.1.12.5/24
IDS Sensor	Command & Control	10.1.1.15/24
BB1	Ethernet	10.1.1.200 /24
BB2	Ethernet	10.5.5.100 /24
BB2	Ethernet	192.1.6.25 /24

Diagram 14-C (RIP)

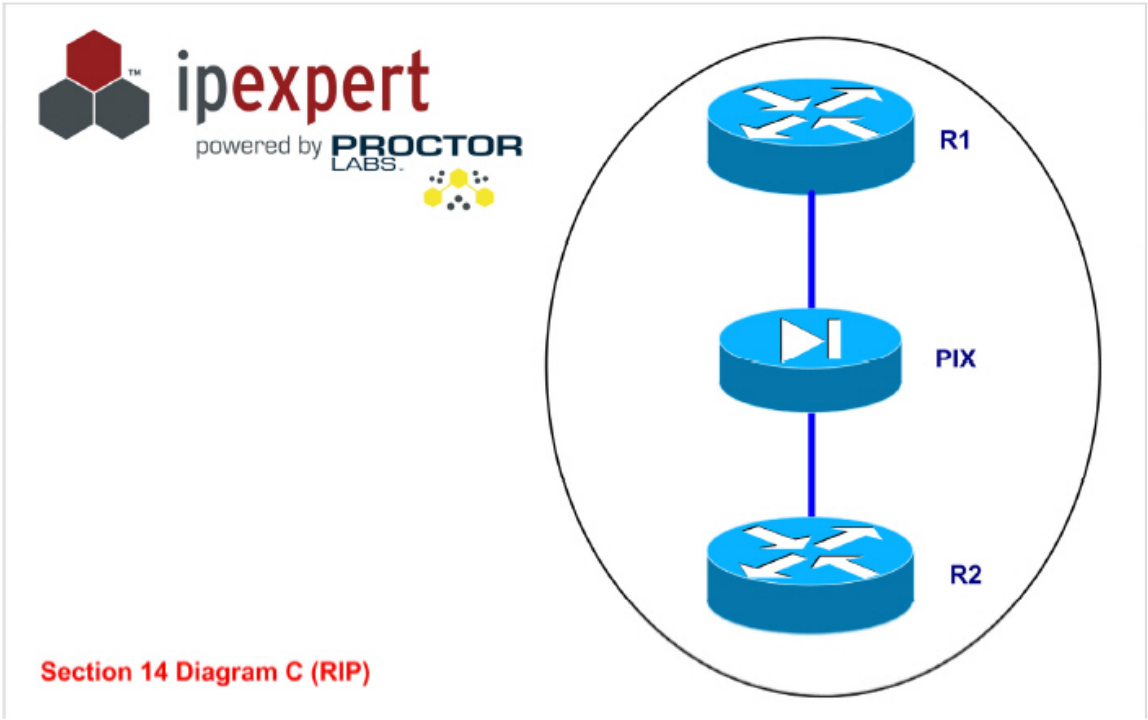
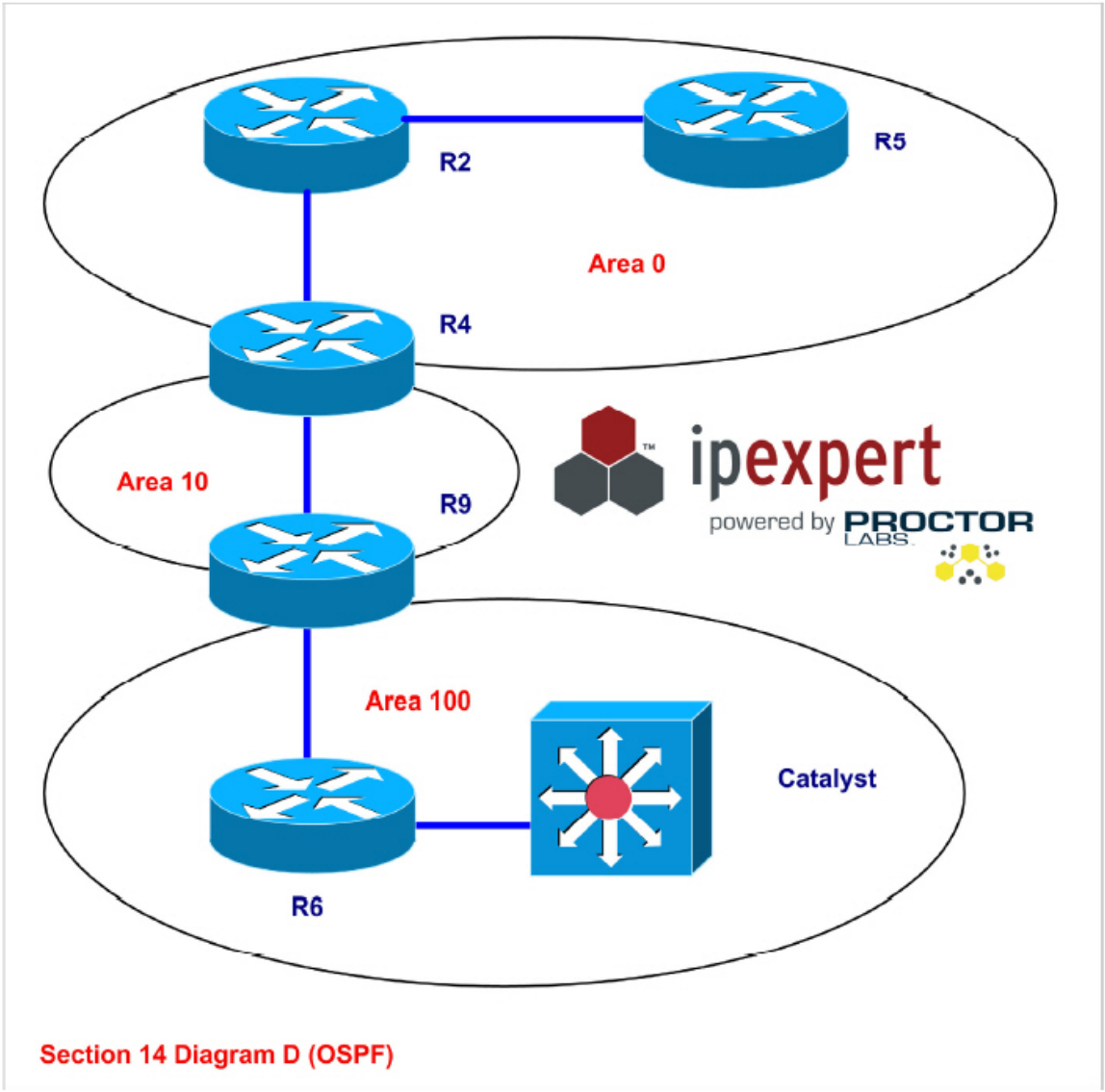


Diagram 14-D (OSPF)



Section 14 Diagram D (OSPF)

Diagram 14-E (EIGRP)

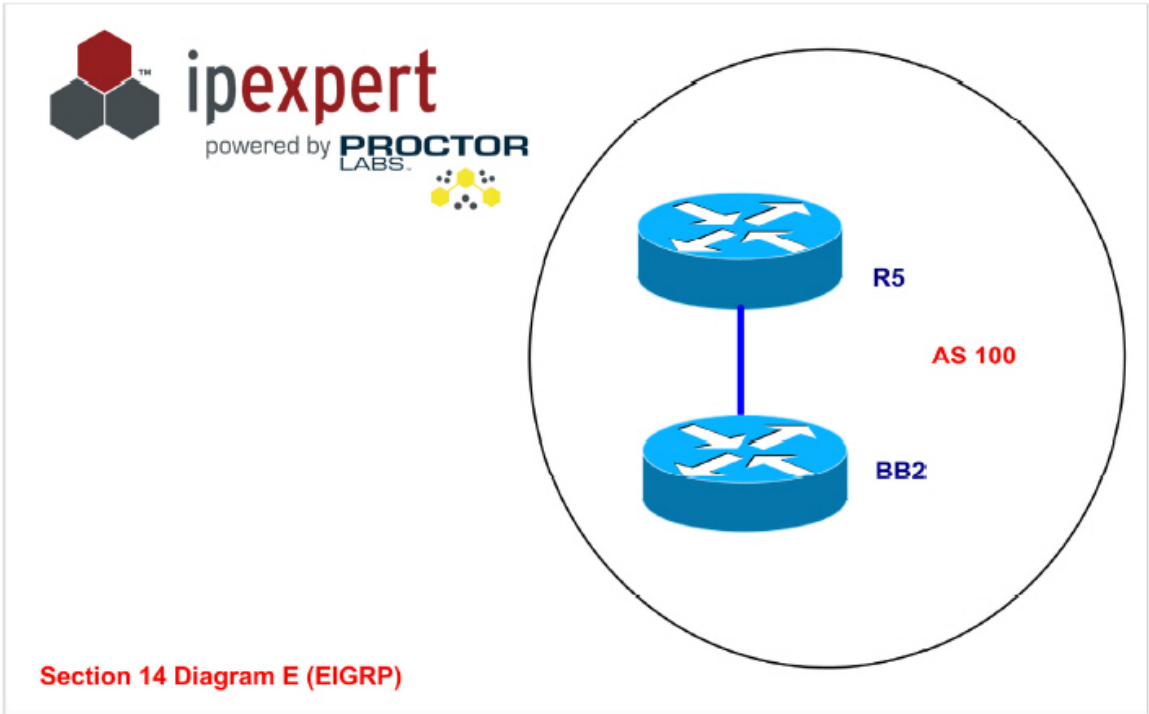
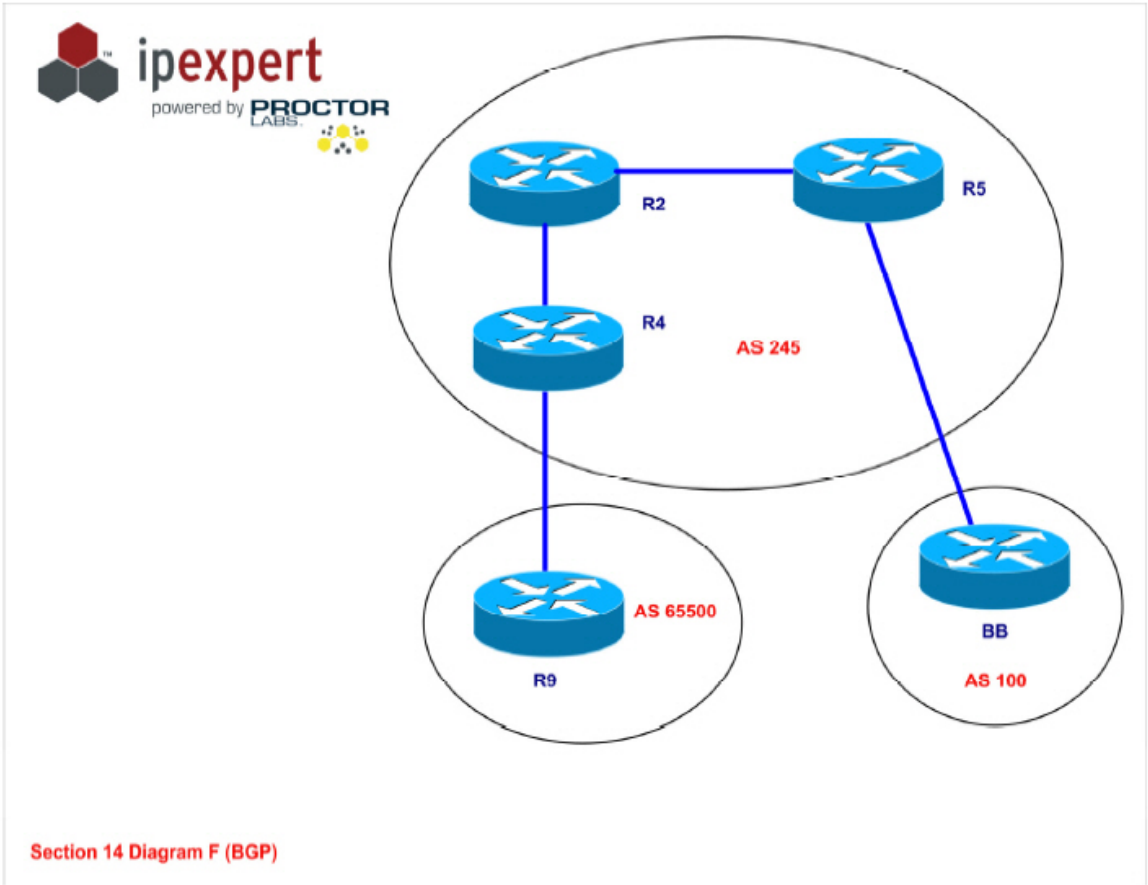


Diagram 14-F (BGP)



Section 14 Pre-Lab Setup

- **Pre-load the Initial Configurations for all the devices.** You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 14 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

1 - Layer 2 Configuration (7 Points)

1.1 - Switch Management (2 Points)

a) Create a Management interface on the Switch1 belonging to VLAN 6.

b) Set the IP Address as .20 on that network.

c) Allow Management access to this switch from VLAN 6 only.

1.2 - Catalyst Traffic Control (2 Points)

a) Port F 0/15 on the Switch1 is experiencing Broadcast and Multicast problems.

b) Configure it so that broadcasts do not take more than 30% of the bandwidth and Multicast does not take more than 20% of the bandwidth.

c) Set the Port to Access Mode so that it does not negotiate the Port mode.

1.3 - Catalyst Security (2 Points)

a) Assume that there is a VLAN 123. Configure MAC address filtering and only permit MAC address from 0000.1234.4321 to 0000.4321.1234 for Vlan 123.

1.4 - Frame Relay QoS (1 Point)

a) Configure TCP header compression for PVC between R2 and R4 (2 points).

2 - Basic PIX Firewall Configuration (10 Points)

2.1 - PIX IP Address (2 Points)

a) Assign IP Addresses to the PIX Firewall interfaces.

2.2 - Routing (2 Points)

a) Run RIP as the routing protocol on the PIX Firewall.

b) Configure RIP such that it only receives routes from the outside interface.

c) Configure RIP such that it receives routes from the inside interface and also injects a default route from the inside interface.

2.3 - Static Translation (4 Points)

a) There is a Web/SMTP/DNS Server at 10.1.1.55. Create a Static Mapping to 192.1.12.55. Allow the appropriate entries in the access-list.

b) Also create a static mapping to R1. Create a Static Mapping to 192.1.12.15. Allow Telnet access to R1 from R2 only in the access-list.

c) Create a Static entry for the AAA server at 10.1.1.100. Translate it to 192.1.12.100. Allow the appropriate entries in the access-list for TACACS+. Only allow R2 to communicate to the TACACS+ server.

2.4 - Advanced Protocol Handling on the PIX (2 Points)

a) The SMTP server is having problems with connections. Upon further investigations, it was found that is running Microsoft Exchange Server. Configure the PIX firewall to fix the problem. You can only use 1 command for this.

3 - Routing Using Interior Gateway Protocols Configuration (7 Points)

3.1 - RIP V2 Authentication (2 Points)

a) R2 and PIX outside should authenticate to each other using the highest level of authentication with a password of ccie.

3.2 - OSPF Authentication (2 Points)

a) All OSPF routers should exchange packets based on the most secure Authentication method.

b) The password should be set to **ccie**.

c) You cannot use **Area x authentication message-digest** command.

3.3 - EIGRP Authentication (2 Points)

a) All routers in EIGRP should authentication with each other.

b) The password should be set to **ccie** with a key id of 1.

3.4 - Redistribution of IGP (1 Point)

a) Redistribute at all appropriate routers. Make sure that all routes are visible and there are no routing loops.

4 - BGP Routing Configuration (7 Points)

4.1 - Authentication (2 Points)

a) Authenticate all IBGP Peerings using MD5 authentication with a password of **ccie**.

4.2 - BGP Filtering (3 Points)

a) AS 245 is receiving routes from AS 100 (BB2) and AS 65000.

b) AS 245 should not pass the routes learned from AS 100 to AS 65000.

c) You can only make configuration changes to R4.

d) You cannot use communities to accomplish this task.

4.3 - Redistribution of BGP (2 Points)

a) Redistribute routes learned through BGP in such a way that the PIX can see all the BGP routes.

5 - Access Management Configuration (6 Points)

5.1 - Management of R2 using Telnet (4 Points)

a) Setup R2 with AAA access.

b) No Authentication or authorization should be done on the Console or AUX lines.

c) Setup Authentication based on TACACS+ for the VTY lines.

d) There are 2 users created on the AAA server, User 1 and User2. Both the users have **cisco** as their password.

e) Setup Authorization based on Local Privilege Levels defined as follows:

- ➔ Setup authorization for User1 such that the user can type all commands. User1 should be in Privilege Exec mode when logged in.
- ➔ Setup authorization for User2 such that the user can type all commands specified in Privilege Level 7. Privilege Level 7 should allow the user to type all commands for snmp-server in global configuration mode. This privilege level should also allow the user to change the hostname of the Router.

f) Configure Accounting for all commands typed by users from Telnet. You should be able to charge the users based on usage times.

g) Only allow VLAN 6 to be able to telnet into R2.

5.2 - HTTP Management (2 Points)

a) Configure HTTP Management on R2.

b) Only Users from the VLAN 49 should be able to manage this router through HTTP.

c) HTTP should authenticate to the already configured AAA.

6 - IP Services Configuration (9 Points)

6.1 - Creating Core Dumps (3 Points)

a) Configure R5 to send a Core Dump to a TFTP Server located at 192.1.12.100.

b) Set the Dump size to 32768.

c) The router should use the source address of 5.5.5.5, the Loopback address on R5.

6.2 - DHCP Server (4 Points)

a) Enable R4 as a DHCP Server with the following information:

- IP ADDRESS : 192.1.49.0/24
- WINS ADDRESS : 192.1.49.135
- DNS ADDRESS : 192.1.49.53
- DEFAULT GATEWAY : 192.1.49.4
- LEASE TIME : 6 Days

b) Enable conflict logging on R4.

c) Configure option 19 to tell the client should configure its IP layer for packet forwarding.

d) Specifies four ping attempts by the DHCP server before ceasing any further ping attempts.

6.3 - NTP (2 Points)

a) Configure R2 as the NTP clock master.

b) Configure R4 to use NTP clock from R2 in a secured way. Key should be **cisco**.

7 - Virtual Private Networks Configuration (18 Points)

7.1 - Basic Concentrator Configuration (3 Points)

a) Configure the IP Address of the Private Interface through the CLI.

b) The Public interface should be configured from the Graphical interface.

c) Make sure the PC can access the Concentrator. You are allowed a static route on the Concentrator to accomplish this.

d) Configure the concentrator to send routes using RIP on the private interface.

e) Configure a Default Route on the Public Interface pointing towards R2.

7.2 - Setup a Site-to-Site IPSec VPN between the Concentrator and R5 (4 Points)

a) Encrypt traffic between the 10.2.2.0/24 and 10.5.5.0/24 networks using the following parameters:

- ➔ Authentication is based on Pre-shared key of **ccie**.
- ➔ Use MD5 for the Hashing algorithm. Use defaults for the rest of the ISAKMP parameters.
- ➔ For IPSec, use ESP-DES for encryption and ESP-SHA-HMAC for Data Authentication in Tunnel Mode.

b) You can use static routes on R5 and R1 to accomplish this.

7.3 - Setup a Remote Access VPN from the Cisco Secure Client and the Concentrator (4 points)

a) Use the following parameters to setup Concentrator with the following options:

- ➔ Assign IP Address in the range of 10.3.3.1 – 10.3.3.254. The pool should be created on the Concentrator.
- ➔ Set the username as VPNUser with a password of **ccie1234**.
- ➔ Create a group called Remote with a password of **ccie**.

b) The network 10.3.3.0 should be propagated to R1 through RIP.

7.4 - Configure the PIX as a PPTP Server (3 Points)

a) Use the following parameters to setup PPTP on the PIX.

- ➔ Allow PPTP access to the 10.1.1.0/24 network only.
- ➔ Create a pool name "pptp-pool" with the range of 192.168.1.1-192.168.1.254.
- ➔ Authentication should be based on MS-CHAP and Encryption MPPE 40.
- ➔ User Authentication should be based on the local database.
- ➔ Create a Username pptpuser with a password of **ccie**.

7.5 - Setup a Site-to-Site IPSec VPN between the R2 and R6 (4 Points)

a) Create the following loopbacks on R2 and R6:

- ➔ **R2** - Int loo 10 : 192.168.102.2/24
- ➔ **R6** - Int loo 10 : 192.168.106.6/24

b) Create a GRE tunnel from R2 S 0/1/0.6 to R6 S 4/0. Route the newly created loopbacks over the tunnel using EIGRP in AS 26.

c) Encrypt traffic going on the GRE tunnel including the EIGRP traffic using the following parameters:

- ➔ Authentication is based on Pre-shared key of **ccie**.
- ➔ Use MD5 for the Hashing algorithm and Group 2 for the Diffie-Hellman key exchange. Use defaults for the rest of the parameters.
- ➔ For IPSec, use ESP-DES for encryption and ESP-MD5-HMAC for Authentication in Transport Mode.

8 - IOS Firewall Configuration (8 Points)

8.1 - Cisco IOS Firewall on R4 (4 Points)

a) Inspect all tcp, udp and icmp traffic from the Ethernet segment going towards the Frame networks.

b) Only allow relevant traffic coming in.

c) ACL should be set to inbound on the Serial interface.

8.2 - Cisco IOS Firewall on R4 (2 Points)

a) Set the IOS Firewall such that it blocks half-open connections if they exceed 1000 and stop deleting the connections if the reach 800.

b) Also set it for a one-minute high.

c) Set the TCP idle time to 30 Minutes.

8.3 - Cisco IOS Firewall on R4 (2 points)

a) Set the global UDP idle timeout to 110 seconds.

b) Changes the max-incomplete host number to 32 half-open sessions, and changes the block-time timeout to 1 minute.

c) Turn on an audit trail messages which will be displayed on the console after each CBAC session closes.

d) Globally specify the TCP session will still be managed after the firewall detects a FIN-exchange to be 15 seconds for all TCP sessions.

9 - Advanced Security and Attacks Configuration (12 Points)

9.1 - Filtering Java and ActiveX applets (2 Points)

a) Setup the PIX to block the downloading of Java and ActiveX applets from anywhere.

9.2 - Allow Remote Management of the PIX (2 Points)

a) Setup the PIX firewall so that the PC at 10.1.1.100 can telnet into the PIX for remote management. Change the default Telnet password to **ccie**.

9.3 - Time-Based Access List (2 Points)

a) You do not want users on R6 Ethernet Network access a special application that uses TCP port 25000, during the Weekdays between 9:00 AM to 4:00 PM.

b) It is OK for them to use the application at other times.

9.4 - Time-Based Access List (2 Points)

a) You do not want users on R6 Ethernet Network to use a customized application that uses UDP port 20000, on the Weekend between 10:00 AM to 3:00 PM.

b) It is OK for them to use the application at other times.

9.5 - Disable Unnecessary Services (2 Points)

a) Disable the DHCP Service on R6.

b) Verify that it is disabled by typing **Show ip socket** output.

9.6 - Spoofing (2 Points)

a) Remove problems caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address in R2's F1/0. Only packets with a source address of 10.5.5.100 arriving at interface FastEthernet0/0 are verified and dropped if needed.

10 - IDS Configuration (16 Points)

10.1 - Basic Configuration of IDS through IDS, IDM and IEV (2 Points)

a) Configure the IDS Sensor's Command and Control Interface through the CLI to allow access to the Sensor from the IDM PC based on the Network Diagram.

b) Add the Sensor to the IEV Console.

10.2 - Switch Configuration (2 Points)

a) You would like to monitor all traffic received in the outside VLAN of the PIX.

b) Configure the Switch to copy all relevant traffic to the monitoring port.

10.3 - Enabling and Fine tuning the ICMP Echo Request Signature (3 Points)

a) Enable the ICMP Echo Request Signature.

b) Set the Alarm Severity to **High**.

c) Verify the Alarm by pinging the outside Interface of the PIX from R2.

10.4 - Creating a Custom Signature (4 Points)

a) Create a custom string signature

b) Set the Alarm Severity to **High**.

c) If sensor detects telnet traffic with a string of "admin", it should fire this alarm.

d) Enable telnet on R1 by assigning it a password of telnet. Configure a static route on R1 for the 192.1.12.0 network via the PIX. It is learning this route through the concentrator.

e) Verify the Alarm by connecting into R1 for Telnet and typing the work "admin" after you are connected.

10.5 - IOS IDS (5 Points)

a) Configure IDS on R6 for attacks from the Frame Relay clouds.

b) Configure the IOS IDS with the following parameters:

- ➔ Send an alarm for Info signatures.
- ➔ Send an alarm and drop packets for Attack signatures.
- ➔ Send the alarm to both the nr-director and a syslog server.
- ➔ Configure the Router with the Syslog Server's Address at 192.1.12.65.
- ➔ Use the following parameters for the Post Office Protocol (POP) parameters:
  - Sensor HostID = 20
  - Director HostID = 10
  - Org ID = 100
  - Local IP Address = 6.6.6.6
  - Remote Director IP Address = 192.1.12.66
  - Port # = 45000

c) Configure Static mappings and access-list entries on the PIX to allow this type of traffic. The syslog is at 10.1.1.65 and the director is at 10.1.1.66.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 15: Multiprotocol Challenge B (One Day Lab Experience)

This Lab is intended to assess your readiness to attempt the actual CCIE Security lab exam. During this section you will be utilizing the entire topology and all topics listed on the CCIE Security Lab Blueprint are fair game.

Estimated Time to Complete: 8 Hours

MUST DO:

Read the ENTIRE lab prior to beginning.

Diagram 15-A

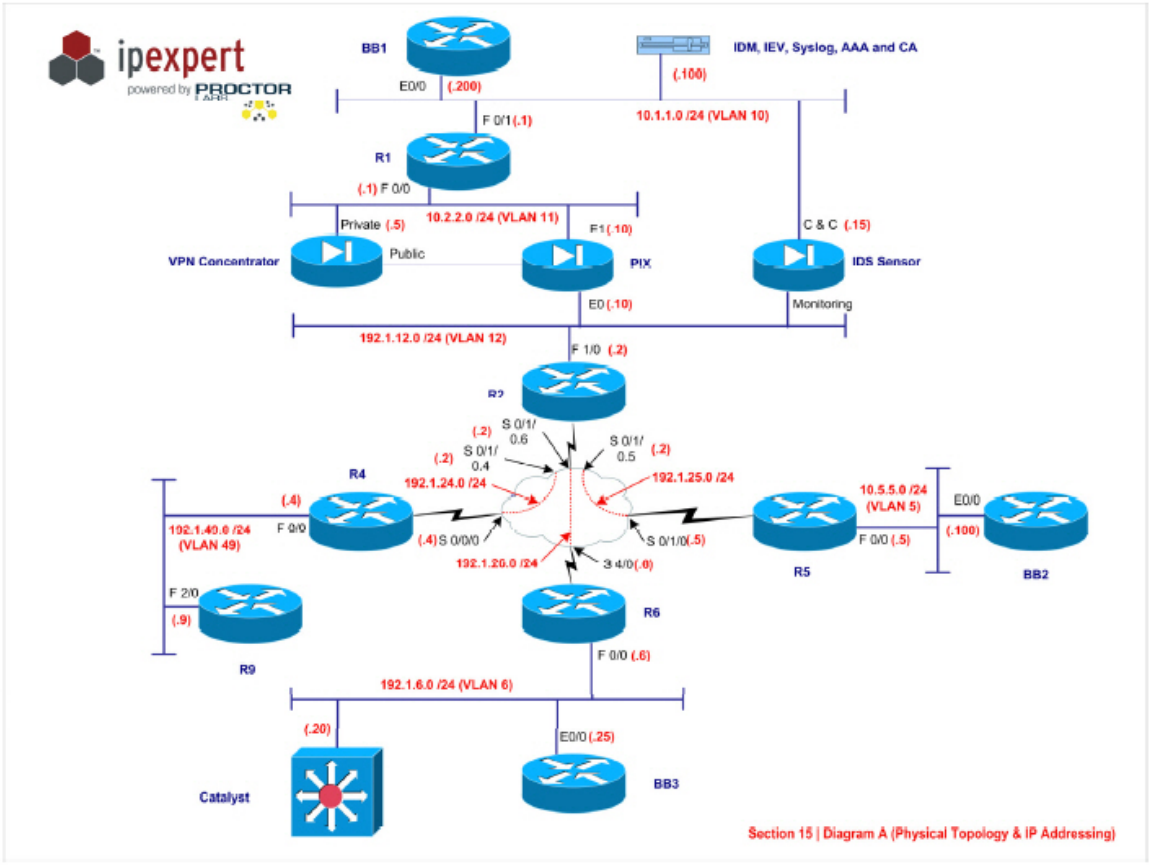
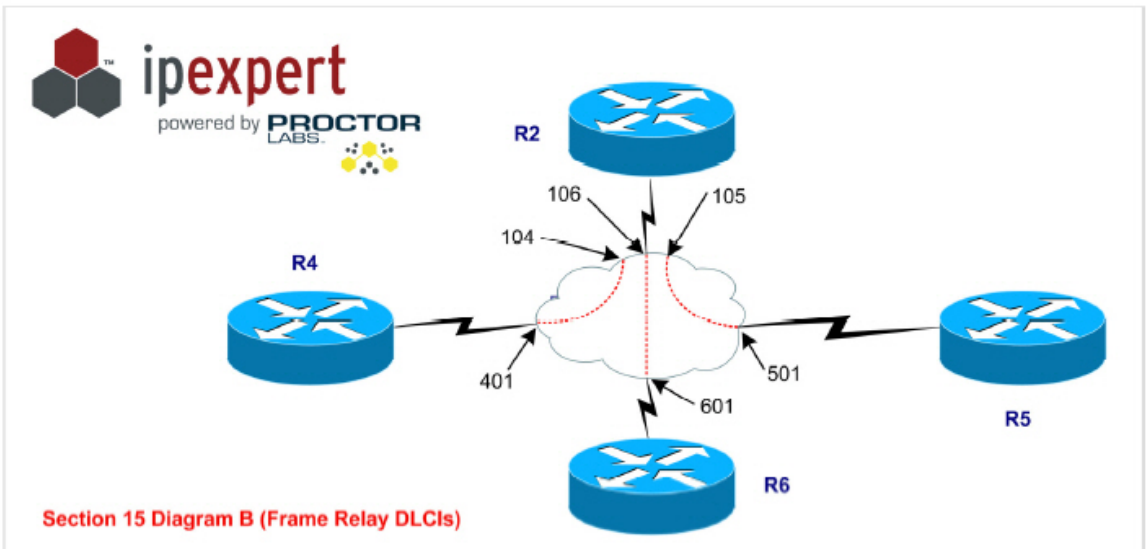


Diagram 15-B



Section 15 IP Addressing

Device	Port	IP Address
R1	F 0/0	10.2.2.1/24
	F 0/1	10.1.1.1/24
	Loopback 0	1.1.1.1 / 8
R2	F 1/0	192.1.12.2/24
	S 0/1/0.4	192.1.24.2/24
	S 0/1/0.5	192.1.25.2/24
	S 0/1/0.6	192.1.26.2/24
	Loopback 0	2.2.2.2 / 8
R4	F 0/0	192.1.49.4/24
	S 0/0/0	192.1.24.4/24
	Loopback 0	4.4.4.4/8
R5	F 0/0	10.5.5.5/24
	S 0/1/0	192.1.25.5/24
	Loopback 0	5.5.5.5 / 8
R6	F 0/0	192.1.6.6/24
	S 4/0	192.1.26.6/24
	Loopback 0	6.6.6.6/8
R9	F 0/0	192.1.49.9/24
	Loopback 0	9.9.9.9/8
PIX	E 0 (outside)	192.1.12.10/24
	E 1 (inside)	10.2.2.10/24
Concentrator	Private	10.2.2.5/24
	Public	192.168.5.5/24
IDS Sensor	Command & Control	10.1.1.15/24
BB1	Ethernet	10.1.1.200 /24
BB2	Ethernet	10.5.5.100 /24
BB2	Ethernet	192.1.6.25 /24

Diagram 15-C (RIP)

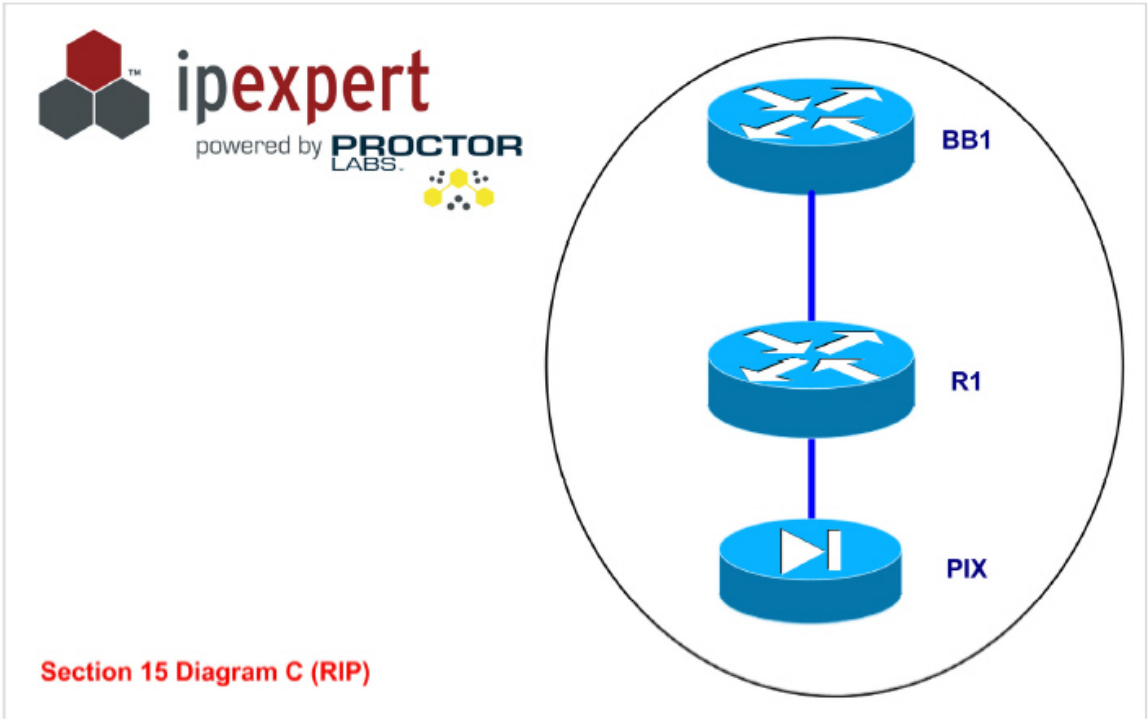
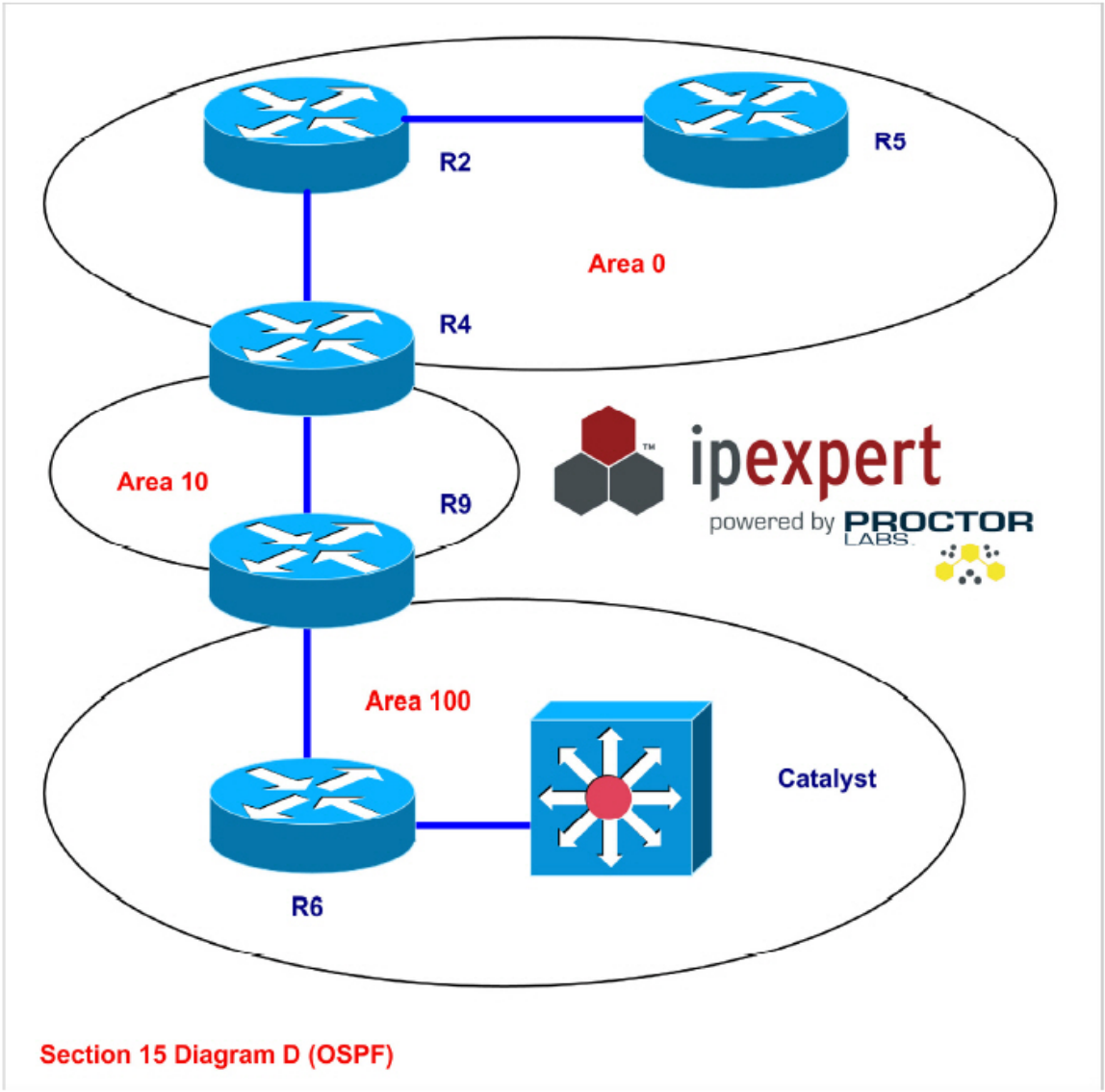


Diagram 15-D (OSPF)



Section 15 Diagram D (OSPF)

Diagram 15-E (EIGRP)

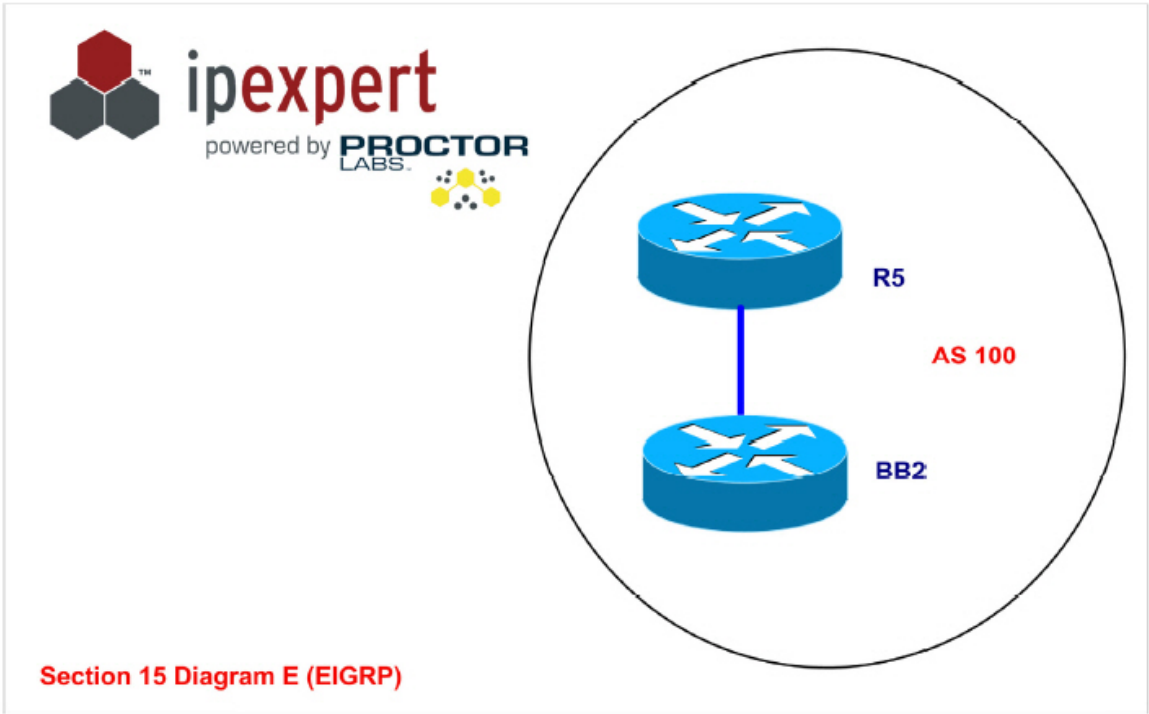
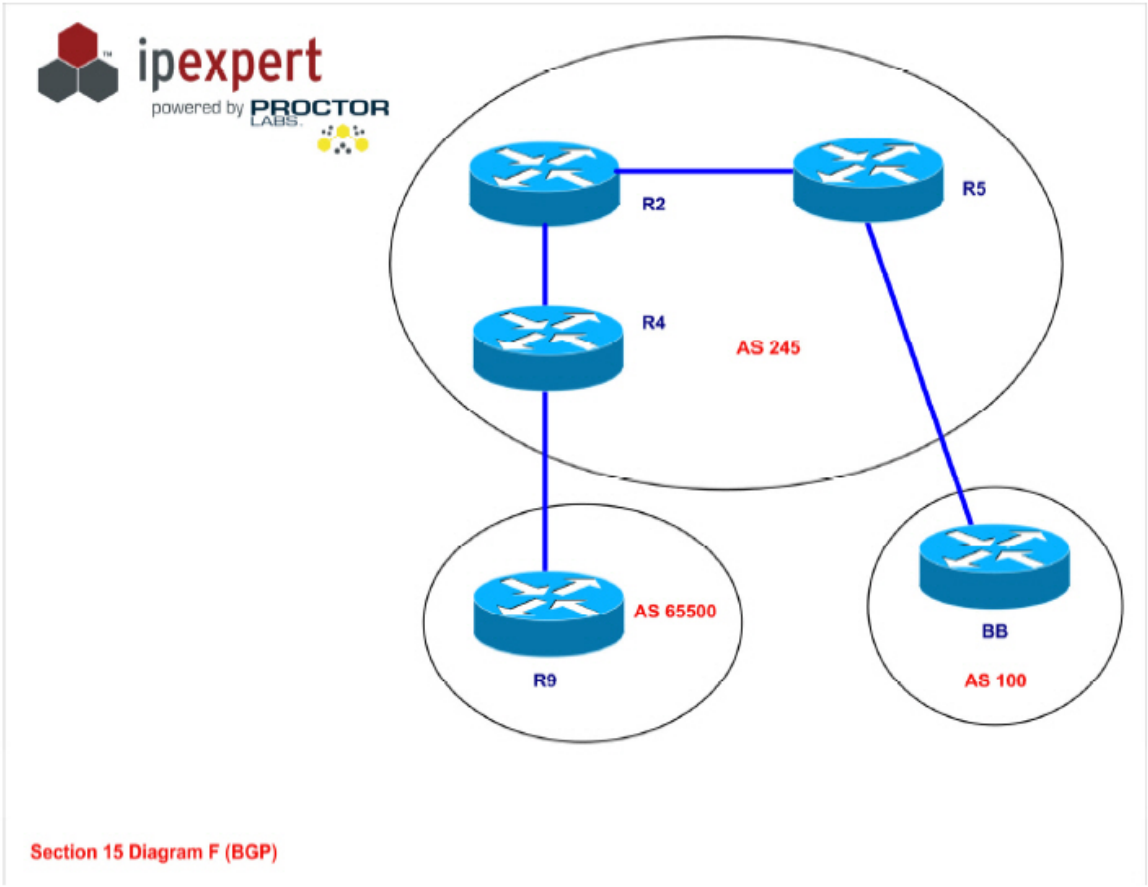


Diagram 15-F (BGP)



Section 15 Pre-Lab Setup

- **Pre-load the Initial Configurations for all the devices.** You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 15 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

1 – Layer 2 Configuration (4 Points)

1.1 – Switch Management (2 Points)

a) Create a Management interface on the Switch1 belonging to VLAN 6.

b) Set the IP Address as .20 on that network.

c) Allow Management access to this switch from VLAN 6 only.

d) Reserve the 15 Telnet Line for the administrator using Port number 3005.

1.2 – Catalyst Security (2 Points)

a) You want to make sure that only the PIX inside interface can connect to port F 0/3 on Switch 2.

b) Configure the Switch to send a trap if a violation is detected.

2 – Basic PIX Firewall Configuration (12 Points)

2.1 – PIX IP Address (4 Points)

a) Create a Logical Interface off of E0 interface on the PIX.

b) The logical interface should belong to VLAN 55.

c) The physical interface belongs to the outside VLAN. Assign the new VLAN interface a name of DMZ55 and a security level of 50.

d) Configure the switch to allow the PIX to communicate to the rest of the network.

e) Assign IP Addresses to the PIX Interfaces.

2.2 – Routing (2 Points)

a) Run RIP as the routing protocol on the PIX Firewall.

b) Configure RIP such that it receives routes from the inside interface and also injects a default route from the inside interface.

c) PIX should be able to reach the rest of the network on the outside interface.

d) You are allowed a single **route** command to accomplish this task.

2.3 – Static Translation (4 Points)

a) Create a static mapping to R1. Create a Static Mapping to 192.1.12.15. Allow Web Access to R1 from R6 Loopback 0 address.

b) Allow R1 Loopback 0 to ping R2 using its own IP Address. You are allowed a static route on R2.

c) Create a Static entry for the AAA server at 10.1.1.100. Translate it to 192.1.12.100. Allow R4 Loopback 0 to communicate to the TACACS+ server. Also allow R2 F 1/0 interface to communicate to the TACACS+ server.

2.4 – Advanced Protocol Handling on the PIX (2 Points)

a) There is a FTP Server at a Partner Network that uses 2020 for the Data port and 2021 for the command port. The inside users should be able to connect to this server using Standard FTP.

b) You are allowed one command to accomplish this.

3 – Routing Using Interior Gateway Protocols Configuration (7 Points)

3.1 – RIP V2 Authentication (2 Points)

a) R1 and BB1 should authenticate to each other using the highest level of authentication with a password of ccie.

3.2 – OSPF Authentication (2 Points)

a) All OSPF routers should exchange packets based on the most secure Authentication method.

b) The password should be set to **ccie**.

c) You cannot use **Area x authentication message-digest** command.

d) OSPF should also be running for the FR link between R2 and R6 for Area 0.

3.3 – EIGRP Authentication (2 Points)

a) All routers in EIGRP should authentication with each other.

b) The password should be set to **ccie** with a key id of 1.

3.4 – Redistribution of IGP (1 Point)

a) Redistribute at all appropriate routers. Make sure that all routes are visible and there are no routing loops. Make sure that all routes including the 192.1.12.0 /24 route is visible on R4, R5, R6, R9 and switch1.

4 – BGP Routing Configuration (6 Points)

4.1 – Authentication (2 Points)

a) Authenticate all IBGP Peerings using MD5 authentication with a password of **ccie**.

4.2 – BGP Filtering - I (2 Points)

a) R5 is receiving routes from BB2 thru EBGP. It should pass these routes to R2.

b) R4 should not receive any routes that originated from AS 100.

c) No configuration change is allowed on R2 to accomplish this task.

4.3 – BGP Filtering - II (2 Points)

a) When AS 245 sends routes from Private AS to the backbone, it should not include the Private AS number in the AS Path List.

5 – Access Management Configuration (6 Points)

5.1 – Configuring AAA Authentication on R4 for Telnet (3 Points)

a) Configure R4 with AAA access. TACACS+ server sees R4 with its Loopback 0 address. The secret key is **ccie**.

b) No Authentication should be done on the Console or AUX lines.

c) Setup Authentication based on TACACS+ for the VTY lines.

d) There are 2 users created on the AAA server, User 1 and User2. Both the users have **cisco** as their password.

5.2 – Configuring AAA Authorization on R4 for Telnet (3 Points)

a) Setup Authorization based on Local Privilege Levels defined as follows:

b) Setup authorization for User1 such that the user can type all commands. User1 should be in Privilege Exec mode when logged in.

c) Setup authorization for User2 such that the user can type all commands specified in Privilege Level 5. Privilege Level 5 should allow the user to type the following commands:

- ➔ Configure or change IP Addresses for the Interfaces.
- ➔ Configure a Routing Protocol. Allow the user to advertise and redistribute networks.
- ➔ Set the Clock and configure the time zone for the router.

d) Configure Accounting for all commands typed by users from Telnet. You should be able to charge the users based on usage times.

6 – IP Services Configuration (6 points)

6.1 – Configuring NTP between R5 and R2 (3 Points)

a) Configure the timezone on R5 as PST -8. Set the clock to the current time on R5.

b) Set R5 as the NTP Master with a stratum of 2. NTP should require MD5 authentication with a key 1.

c) Configure the timezone on R2 as PST -8. Configure R2 as the client for R5. R2 should point to R5 using the NTP Server command.

d) R5 should only allow R2 to get the clock from it.

6.2 – NAT (3 Points)

a) Configure a loopback 15 interface on R6. Assign it an IP Address of 192.168.15.1/24.

b) Configure NAT such that if loopback 15 network wants to go to 9.0.0.0 or 4.0.0.0 networks, it should use the interface IP address of the Serial4/0 interface as the translated address. Configure PAT for this entry.

c) Configure NAT such that if loopback 15 network wants to go to 2.0.0.0 or 5.0.0.0 networks, it should use 192.1.26.15 as the translated address. Configure PAT for this entry.

7 –Virtual Private Networks Configuration (18 Points)

7.1 – Basic Concentrator Configuration (2 Points)

a) Configure the IP Address of the Private Interface thru the CLI.

b) The Public interface should be configured from the Graphical interface.

c) Make sure the PC can access the Concentrator. You are allowed a static route on the Concentrator to accomplish this.

7.2 – Routing Protocols on the Concentrator (2 Points)

a) Disable RIP on the private interface.

b) Configure the Concentrator to run RIP V2 on the Public Interface.

c) Configure the PIX to send a default route to the Concentrator on the DMZ55 interface using RIP V2.

7.3 – Setup a Site-to-Site IPSec VPN between the Concentrator and R5 (5 Points)

a) The concentrator should be seen as 192.1.12.5 on the outside network. Configure the PIX to accomplish this.

b) Encrypt traffic between the 10.2.2.0/24 and 10.5.5.0/24 networks using the following parameters:

- ➔ Authentication is based on Pre-shared key of **ccie**.
- ➔ Use MD5 for the Hashing algorithm. Use defaults for the rest of the ISAKMP parameters.
- ➔ For IPSec, use ESP-DES for encryption and ESP-SHA-HMAC for Data Authentication in Tunnel Mode.

c) You can use static routes on R5 and R1 to accomplish this.

d) Create the appropriate entries in the PIX firewall to accomplish this.

7.4 – Setup a Remote Access VPN from the Cisco Secure Client and the Concentrator (4 points)

a) Use the following parameters to setup Concentrator with the following options:

- ➔ Assign IP Address in the range of 10.3.3.1 – 10.3.3.254. The pool should be created specific to the group **Remote**.
- ➔ Set the username as VPNUser with a password of **ccie1234**.
- ➔ Create a group called Remote with a password of **ccie**.
- ➔ When the user connects in, he should also be allowed to connect to the 192.1.49.0/24 networks.

b) The network 10.3.3.0 should be propagated to R1 thru RIP.

7.5 – Configure a Remote Access VPN using IOS Easy VPN (R2) and Cisco Secure VPN Client (5 Points)

a) Configure R2 as the Easy VPN Server using the following parameters:

- ➔ Group name and password : Name : **EZGroup** Password : **abcd1234**
- ➔ DNS and WINS Address : 192.1.12.175
- ➔ Domain Name : ipexpert.com
- ➔ Address Pool (Local) : 192.168.22.1 192.168.22.16
- ➔ The Address should be assigned to the client from the pool above. This network should be propagated to all the other routers.
- ➔ The Authentication and Authorization should be done locally.
- ➔ Hashing for the ISAKMP Policy should be done based on MD5.
- ➔ Authentication for the ISAKMP Policy should be done based on Pre-shared keys.
- ➔ Set the authentication to XAUTH.
- ➔ Use ESP-DES and ESP-MD5-HMAC for your transform set.

8 - DMVPN, Easy VPN for R4 and R9's LAN Configuration (4 Points)

8.1 – Configure a DMVPN and Easy VPN (4 Points)

a) Configure DMVPN and Easy VPN with XAUTH on the same router. The DMVPN spokes should be dynamically addressed.

b) Create a tunnel with the network of 49.0.0.x/24 with x is the router number.

c) Running a separate EIGRP process for the tunnel interface.

d) Use XAUTH for local configuration, with username and password is **ccie**.

e) The default pre-shared key should be **ccie**.

f) Easy VPN Clients should use Diffie-Hellman group 2.

g) The dynamic address pool should be 123.0.0.10 to 123.0.0.20.

h) Client should respond to the address.

i) Create a VPN client group that uses DNS at 123.1.1.1 and WINS at 123.1.1.2.

j) Phase 2 policy should be esp-3des esp-md5-hmac.

k) NHRP authentication should use **ccie**.

l) Reverse route injection should be used to provide the DMVPN networks access to any Easy VPN Client network.

9 – IOS Firewall Configuration (10 Points)

9.1 – Cisco IOS Firewall on R4 (4 Points)

a) Inspect the following traffic from the Ethernet segment going towards the Frame networks:

- ➔ All TCP Based traffic.
- ➔ All UDP Based traffic.
- ➔ Netmeeting Traffic.
- ➔ SMTP traffic should be inspected so that only a limited number of SMTP commands are allowed in.

b) Only allow Java applets from 2.0.0.0 to be downloaded.

c) Only allow relevant traffic coming in.

d) ACL should be set to inbound on the Serial interface.

9.2 – Cisco IOS Firewall on R4 (3 Points)

a) Set the IOS Firewall such that it blocks half-open connections if they exceed 800 and stop deleting the connections if the reach 600.

b) Also set it for a one-minute high.

c) Configure the Router such that it waits for 10 seconds for a connection to complete before tearing it down.

d) Configure the dns-timeout to 30 seconds.

e) Configure the udp idle timeout to 25 seconds.

9.3 - TCP Intercept (3 points)

a) The 9.9.9.0 network is experiencing syn attacks. R9 should watch the traffic and if it does not complete the TCP handshake in 15 seconds, it should drop the packets.

b) Limit IP TCP intercept to only watch packets coming from 9.9.9.0.

c) Configure IP TCP intercept such that the router drops embryonic connections if they reach 1250. It should stop dropping the embryonic connections once the number reaches 800.

d) Set the software to manage the connection for 12 hours after no activity.

e) Allows 1450 connection requests before the software enters aggressive mode.

f) Sets the software to leave aggressive mode when the number of connection requests falls below 1050.

10 – Advanced Security and Attacks Configuration (12 Points)

10.1 – Allow Remote Management of the PIX (3 Points)

a) Setup the PIX firewall so that the PC at 10.1.1.100 can Telnet into the PIX for remote management.

b) Have the TACACS Server authenticate Telnet Requests.

c) The PIX communicates to the PIX Firewall using TACACS+ with a secret key of **ipexpert**.

10.2 – Reflexive Access List (3 Points)

a) You should allow HTTP, Telnet, SMTP, ICMP Pings and DNS traffic from VLAN 5 to go out of R5 and return back.

b) Do not allow any other traffic into VLAN 5 from outside of R5.

c) Allow relevant traffic in.

d) Use a Reflexive Access List to accomplish it.

10.3 – Black Holing (3 Points)

a) R9 has detected attacks coming in from the Ethernet segment.

b) All the packets are HTTP packets with a size ranging from 40 bytes to 100 bytes.

c) Use Policy Based Routing (PBR) to block this attack by Black Holing the packets.

10.4 - IP Accounting (3 points)

a) You would like to gather traffic statistics about the traffic that transits thru R9. Configure R9 for IP accounting on both interfaces.

b) The maximum number of accounting entries to be created should be 500.

c) IP accounting should be based on IP precedence for received and transmitted packets.

11 – IDS Configuration (15 Points)

11.1 – Basic Configuration of IDS through IDS, IDM and IEV (2 Points)

a) Configure the IDS Sensor's Command and Control Interface through the CLI to allow access to the Sensor from the IDM PC based on the Network Diagram.

b) Add the Sensor to the IEV Console.

11.2 – Switch Configuration (2 Points)

a) You would like to monitor all traffic received in the outside VLAN of the PIX.

b) Configure the Switch to copy all relevant traffic to the monitoring port.

11.3 – Enabling and Fine tuning the ICMP (3 Points)

a) Enable the ICMP Echo Request and ICMP Echo Reply Signatures.

b) Set the Alarm Severity to **Medium**.

c) The alarms should not fire when they are sent by R2. They should fire from any other device.

d) Verify the Alarm by pinging the outside Interface of the PIX from R2 and R5.

11.4 – Creating a Custom Signature (4 Points)

a) Create a custom string signature. The alarm should fire if a telnet connection types the words "admin" or "Admin".

b) Set the Alarm Severity to **High**.

c) Enable telnet on R1 by assigning it a password of telnet. Allow telnet from R2 to R1 thru the PIX. The static for R1 should have been done in an earlier step.

d) Verify the Alarm by telnetting into R1 from R2 and typing the word "Admin" after you have connected.

e) You are only allowed to create one alarm.

11.5 – PIX IDS (4 Points)

a) Configure a Syslog Server at 10.1.1.100. Configure the PIX to send message to the Syslog server.

b) Configure Console Logging to level 4. Configure Trap logging level to debugging.

c) Configure the PIX IDS with the following parameters:

- ➔ Send an alarm for Info signatures.
- ➔ Send an alarm and drop packets for Attack signatures.

d) You do not want signature 2004 to fire at all.

e) Enable IDS on the outside interface.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 16: Multiprotocol Challenge C (One Day Lab Experience)

This Lab is intended to assess your readiness to attempt the actual CCIE Security lab exam. During this section you will be utilizing the entire topology and all topics listed on the CCIE Security Lab Blueprint are fair game.

Estimated Time to Complete: 8 Hours

MUST DO:

Read the ENTIRE lab prior to beginning.

Diagram 16-A

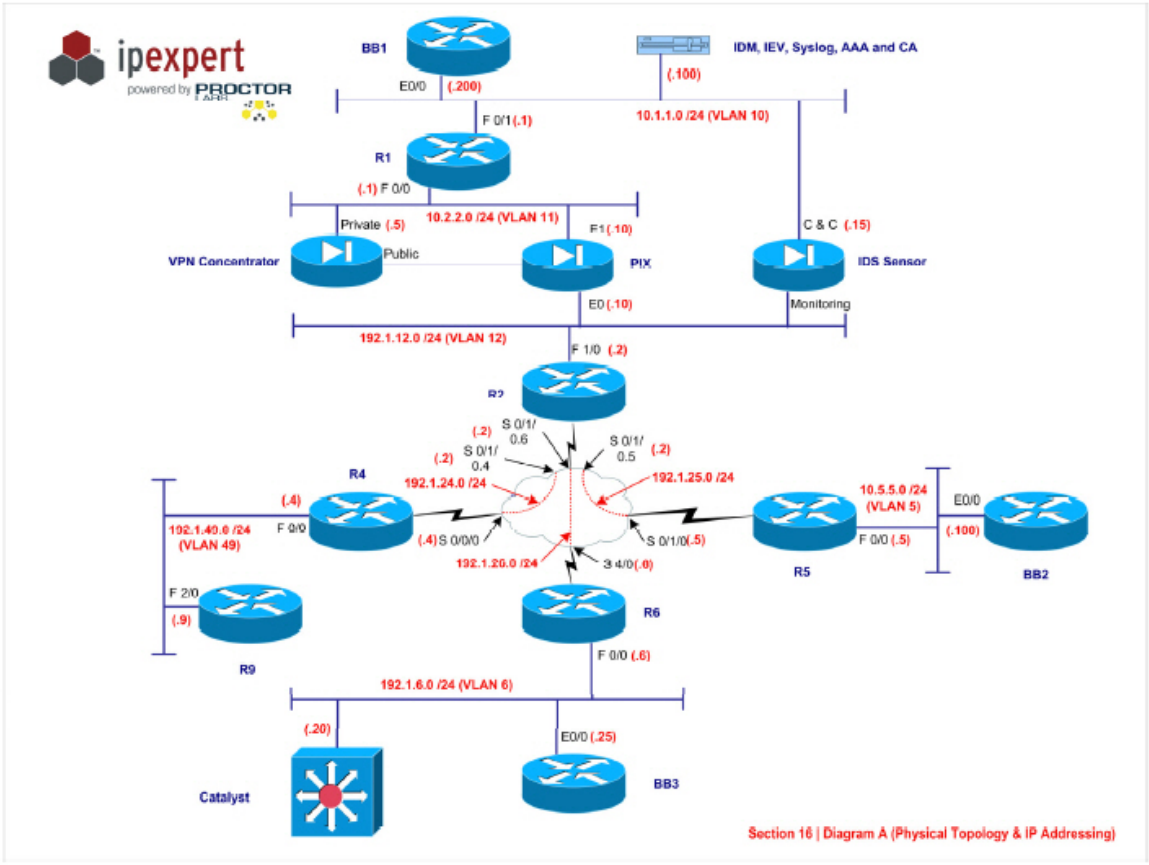
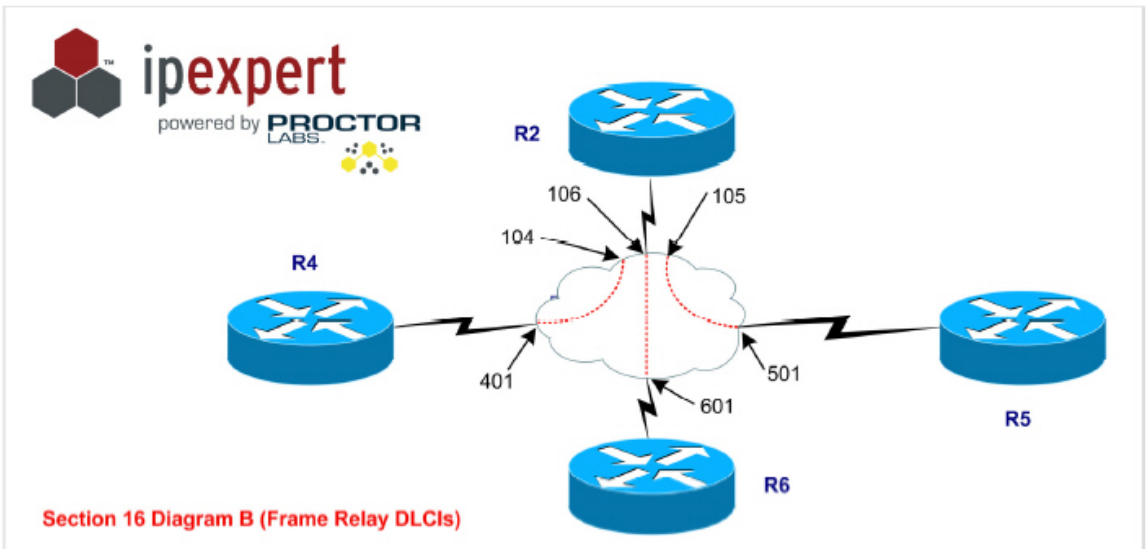


Diagram 16-B



Section 16 IP Addressing

Device	Port	IP Address
R1	F 0/0	10.2.2.1/24
	F 0/1	10.1.1.1/24
	Loopback 0	1.1.1.1 / 8
R2	F 1/0	192.1.12.2/24
	S 0/1/0.4	192.1.24.2/24
	S 0/1/0.5	192.1.25.2/24
	S 0/1/0.6	192.1.26.2/24
	Loopback 0	2.2.2.2 / 8
R4	F 0/0	192.1.49.4/24
	S 0/0/0	192.1.24.4/24
	Loopback 0	4.4.4.4/8
R5	F 0/0	10.5.5.5/24
	S 0/1/0	192.1.25.5/24
	Loopback 0	5.5.5.5 / 8
R6	F 0/0	192.1.6.6/24
	S 4/0	192.1.26.6/24
	Loopback 0	6.6.6.6/8
R9	F 0/0	192.1.49.9/24
	Loopback 0	9.9.9.9/8
PIX	E 0 (outside)	192.1.12.10/24
	E 1 (inside)	10.2.2.10/24
Concentrator	Private	10.2.2.5/24
	Public	192.168.5.5/24
IDS Sensor	Command & Control	10.1.1.15/24
BB1	Ethernet	10.1.1.200 /24
BB2	Ethernet	10.5.5.100 /24
BB2	Ethernet	192.1.6.25 /24
PIX	VLAN 55 (DMZ55)	192.168.5.10 /24

Diagram 16-C (RIP)

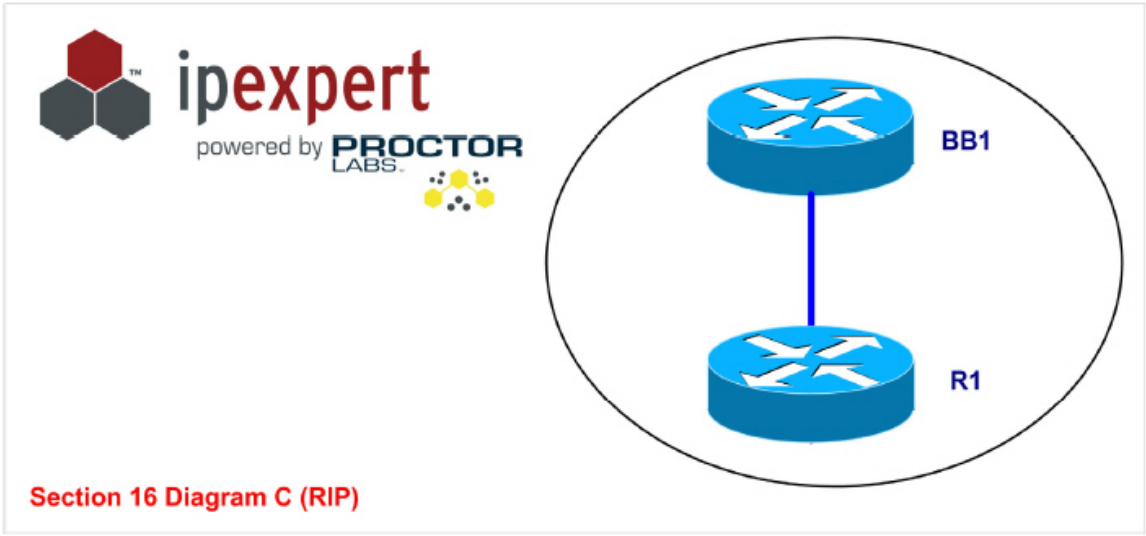


Diagram 16-D (OSPF)

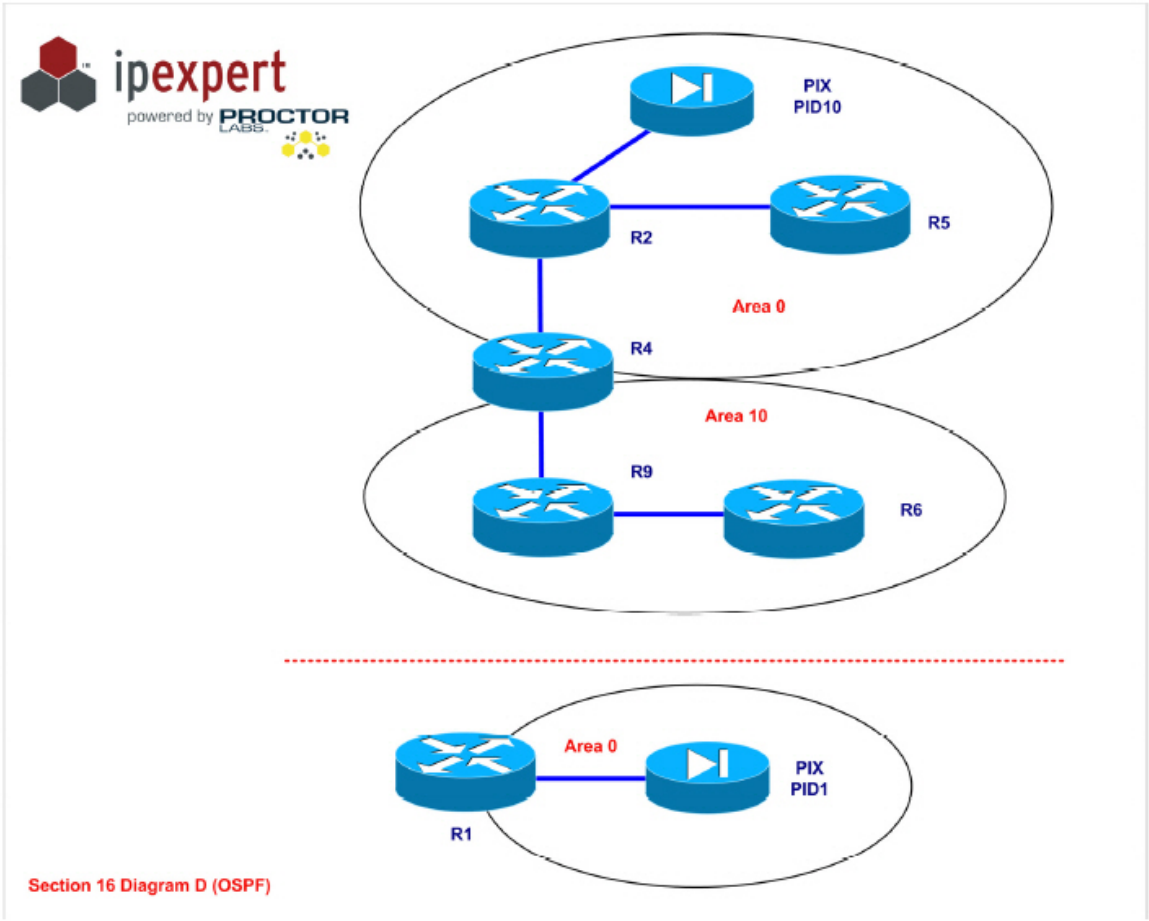


Diagram 16-E (EIGRP)

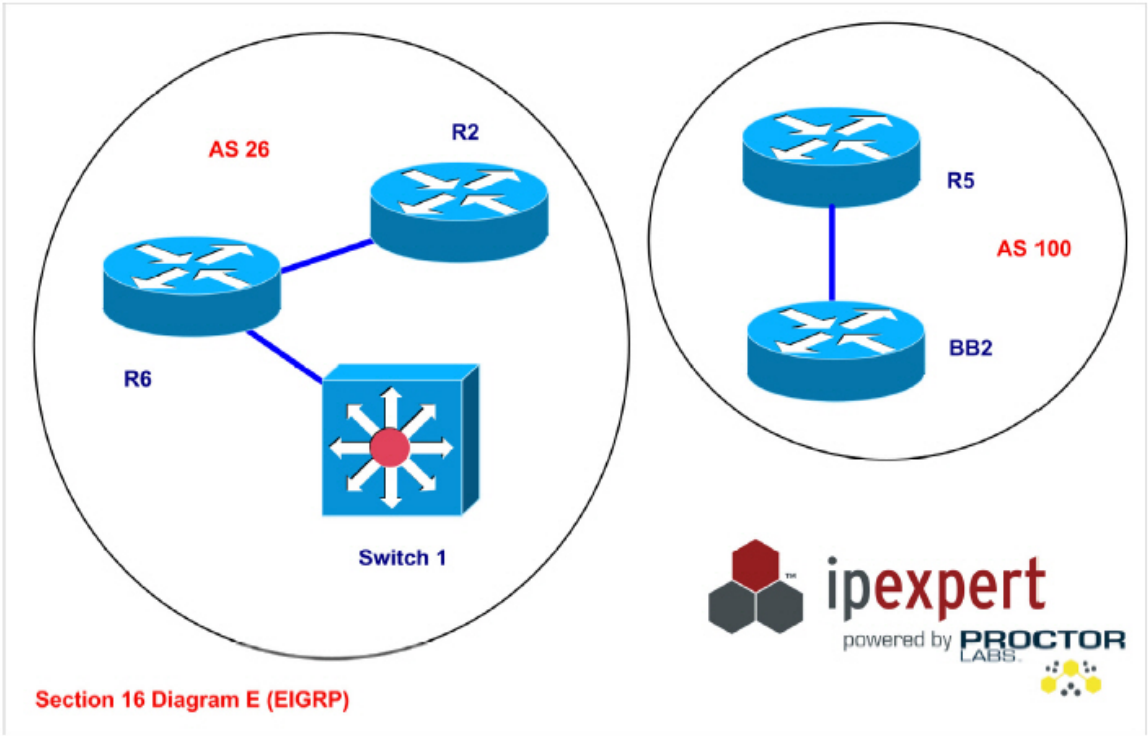
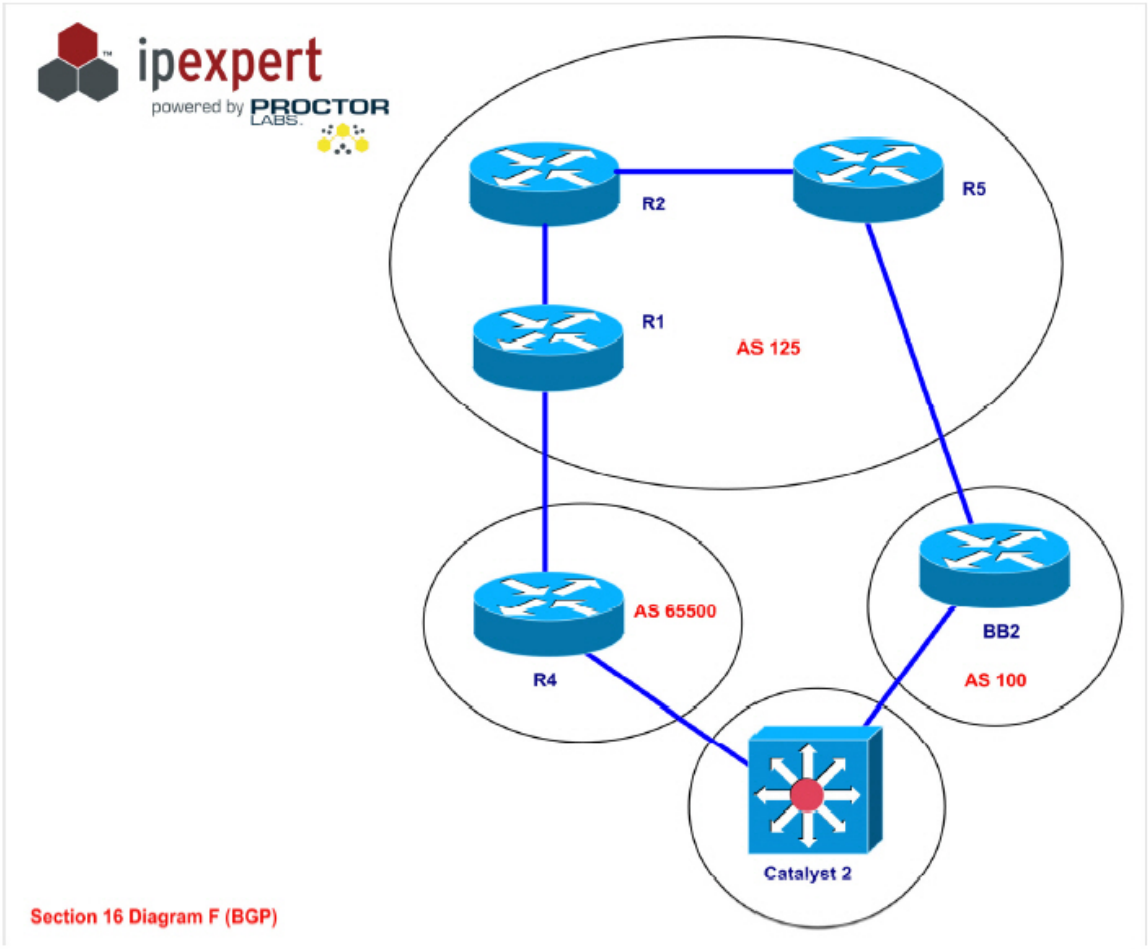


Diagram 16-F (BGP)



Section 16 Pre-Lab Setup

- **Pre-load the Initial Configurations for all the devices.** You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 16 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

1 – Layer 2 (4 Points)

1.1 – Switch Management (2 Points)

a) Create a Management interface on Switch1 belonging to VLAN 6.

b) Set the IP Address as .20 on that network.

c) Allow Management access to this switch from VLAN 6 only.

1.2 – VLAN Interfaces (2 Points)

a) Create a couple of Management interfaces on Sw2. It should be able to communicate to VLAN 49 and VLAN 5.

b) Set the IP Address as .20 on both networks.

2 – Basic PIX Firewall (12 Points)

2.1 – PIX IP Address (4 Points)

a) Create a Logical Interface off of E0 interface on the PIX.

b) The logical interface should belong to VLAN 55.

c) The Physical interface belongs to the outside VLAN. Assign the new VLAN interface a name of DMZ55 and a security level of 50.

d) Configure the Switch to allow the PIX to communicate to the rest of the network.

e) Assign IP Addresses to the PIX Interfaces.

2.2 – Routing (2 Points)

a) Run OSPF as the routing protocol on the PIX Firewall.

b) Configure Process ID 1 and advertise the inside network in area 0.

c) Configure Process ID 10 and advertise the outside network in area 0.

2.3 – Static Translation (2 Points)

a) Allow R1 Loopback 0 to ping R2 using its own IP Address. Do not use an access-list to accomplish this. You might have to wait until a later step to verify this step. You are not allowed any static routes.

b) Create a Static entry for the AAA server at 10.1.1.100. Translate it to 192.1.12.100. Allow R4 Loopback 0 to communicate to the TACACS+ server. Also allow R2 F 1/0 interface to communicate to the TACACS+ server.

2.4 – Advanced Access Lists (4 Points)

a) Your company will be putting in 2 application servers. One of the application servers will be in DMZ55 with IP Addresses of 192.168.5.21 and 192.168.5.22.

b) Create a static translation for them on the outside so that 192.168.5.21 is seen as 192.1.12.21 on the outside and 192.168.5.22 is seen as 192.1.12.22 on the outside. You might have to wait until a later step to verify this step. You are not allowed any static routes.

c) These servers are going to be access by partner organizations. The IP Addresses of these partner organizations are as follows:

- 205.15.25.0/24
- 207.215.1.0/24
- 210.208.15.16/28
- 211.0.15.32/27
- 192.1.150.112/28

d) The applications on the servers are as follows:

- TFTP
- FTP
- HTTP
- SMTP
- DNS
- Custom Application at UDP 50000

e) Allow all the partner organizations access to all the applications on the 2 servers. You are allowed 2 lines in the Access List to accomplish this.

3 – Routing Using Interior Gateway Protocols (12 Points)

3.1 – RIP V2 Authentication (2 Points)

a) R1 and BB1 should authenticate to each other using the highest level of Authentication with a password of **ccie**.

3.2 – OSPF Authentication (3 Points)

a) All OSPF routers should exchange packets based on the most secure Authentication method.

b) The password should be set to **ccie**.

c) You cannot use **Area x authentication message-digest** command.

3.3 – EIGRP Authentication (3 Points)

a) All routers in EIGRP should authentication with each other.

b) The password should be set to **ccie** with a key id of 1.

3.4 – Redistribution of IGP (4 Points)

a) Redistribute at all appropriate routers. Make sure that all routes are visible and there are no routing loops.

b) Redistribute OSPF into EIGRP on R2. Perform mutual redistribution on R6. Make sure R4 and R9 do not see the 2.0.0.0 /8 network in their routing table.

4 – BGP Routing (12 Points)

4.1 – IBGP and EBGP through the PIX (4 Points)

a) Configure IBGP peering between R1 and R2 thru the PIX. R1 sees R2 as 192.1.12.2 and R2 should see R1 as 10.2.2.1. Create the Static Mapping on the PIX to accomplish this.

b) Configure EBGP peering between R1 and R4 thru the PIX. R1 sees R4 as 192.1.24.4 and R4 should see R1 as 10.2.2.1. The Static should have been created in the previous step.

4.2 – EBGP on a Switch (3 Points)

a) Sw2 in AS 55. Configure the following Loopbacks on Sw2:

- ➔ Loopback 101 – 155.55.1.1/24
- ➔ Loopback 102 – 155.55.2.1/24

b) Advertise these loopbacks in BGP without using the network command.

c) Configure a neighbor relationship between R4 and the Sw2. R4 is in AS 65000. R4 sees Sw2 in AS 51.

d) Configure a neighbor relationship between BB2 and the Sw2. BB2 is in AS 100. BB2 sees Sw2 in AS 52.

4.3 – Authentication (2 Points)

a) Authenticate all IBGP peerings using MD5 authentication with a password of **ccie**.

4.4 – BGP Filtering (3 Points)

a) Sw2 should only send 155.55.1.0 to R4 and 155.55.2.0 to BB2.

b) R4 and BB2 should not send the 155.55.1.0 and 155.55.2.0 routes to any other AS.

c) Configuration should only be done on Sw2.

d) When AS 125 sends routes from Private AS to the backbone, it should not include the Private AS number in the AS Path List.

5 – Access Management (6 Points)

5.1 – Configuring AAA Authentication on R4 for Telnet (2 Points)

a) Configure R4 with AAA access. TACACS+ server sees R4 with its Loopback 0 address. The secret key is **cisco**.

b) No Authentication should be done on the Console or AUX lines.

c) Setup Authentication based on TACACS+ for the VTY lines.

d) There are 2 users created on the AAA server, User 1 and User2. Both the users have **ccie** as their password.

5.2 – Configuring Controlled Telnet Access (4 Points)

a) Configure Telnet such that when Users login, they see a menu that only allows them the ability to execute the following commands by using a menu:

- ➔ Show IP interface Brief
- ➔ Show IP Route
- ➔ Show IP Protocol
- ➔ Show Run
- ➔ Exit

b) The Users should not to able to get a command prompt if they login using the default port (23).

c) Configure local authorization for exec, command 1 and command 15 privilege levels. Assign User1 and User2 to privilege level 15.

d) The administrator should be given the ability to login and get a prompt without the menu. The administrator to connect using port 3099. Set aside one Telnet line for the Administrator.

6 – IP Services (5 Points)

6.1 – HSRP between R4 and R9 (5 Points)

a) Configure the Switch2 to use 192.1.49.49 as a default gateway.

b) Configure HSRP between R4 and R9.

c) R4 should be the Active Router. R9 should be the standby router.

d) If R4 is up, it should always be the active router.

e) Configure HSRP to authenticate to each other. Use text authentication.

f) HSRP should also look for Serial link failures behind R4 and R9.

7 –Virtual Private Networks (18 Points)

7.1 – Basic Concentrator Configuration (2 Points)

a) Configure the IP Address of the Private Interface thru the CLI.

b) The Public interface should be configured from the Graphical interface.

c) Make sure the PC can access the Concentrator. You are allowed a static route on the Concentrator to accomplish this.

7.2 – Static Routes on the Concentrator (2 Points)

a) Configure a Default Route on the Concentrator pointing towards the DMZ55 interface on the PIX.

7.3 – Setup a Site-to-Site IPSec VPN between the PIX and R5 (5 Points)

a) Configure a LAN to LAN tunnel between the PIX and R5 to encrypt traffic from 10.2.2.0/24 to 10.5.5.0/24.

b) Use the following parameters:

- ➔ Authentication is based on Pre-shared key of **ccie**.
- ➔ Use MD5 for the Hashing algorithm. Use defaults for the rest of the ISAKMP parameters.
- ➔ For IPSec, use ESP-DES for encryption and ESP-SHA-HMAC for Data Authentication in Tunnel Mode.

7.4 – Setup a Remote Access VPN from the Cisco Secure Client and the Concentrator (4 points)

a) Use the following parameters to setup the Concentrator with the following options:

- ➔ Assign IP Address in the range of 10.3.3.1 – 10.3.3.254. The pool should be created specific to the group **Remote**.
- ➔ Set the username as VPNUser with a password of **ccie1234**.
- ➔ Create a group called Remote with a password of **ccie**.
- ➔ Only allow PPTP and IPSec for the group. Configure it such that only MSCHAP V2 is allowed as the authentication protocol for PPTP.

7.5 – Configure a Remote Access VPN using Easy VPN Concentrator and R4 (5 Points)

a) Configure the Concentrator as the Easy VPN Server using the following parameters:

- ➔ Group name and password : Name : **EZGroup** Password : **abcd1234**
- ➔ Domain Name : ipexpert.com
- ➔ Address Pool (Local) : 192.168.22.1 192.168.22.16
- ➔ The Address should be assigned to the client from the pool above. Create a static route on R1 for this network. The Authentication should be done locally.
- ➔ Create a User called **EZUser** with a password of **ccie1234**. Make this user a member of the **EZGROUP**.

b) Configure R4 as the EZVPN Client:

- ➔ Create a Loopback 100 on R4. Assign it an IP address of 172.16.0.1 255.255.0.0.
- ➔ Configure R4 such that when this Loopback connects to the Network, it is translated to the Serial interface of R4 except when it tries to connect to 10.2.2.0/24.
- ➔ When Loopback 100 tries to connect to 10.2.2.0/24 network, the Router should initiate an EZVPN session with the Concentrator.
- ➔ It should match the group name and username of the Concentrator.
- ➔ Configure it in client mode.

8 – IOS Firewall (8 Points)

8.1 – Cisco IOS Firewall on R4 with non-standard ports (4 Points)

a) Inspect the following traffic from the Ethernet segment going towards the Frame networks:

- ➔ All TCP Based traffic
- ➔ All UDP Based traffic
- ➔ Netmeeting Traffic
- ➔ SMTP traffic should be inspected so that only a limited number of SMTP commands are allowed in.

b) FTP should be inspected on the Standard port and also on port 2021.

c) HTTP should also be inspected for a non-standard port of 8000.

d) Only allow relevant traffic coming in.

e) ACL should be set to inbound on the Serial interface.

8.2 – URL Filtering (4 Points)

a) Configure R4 to inspect all HTTP traffic from the Ethernet segment towards the Frame networks for urls.

b) The url server is a Web Sense server located at 192.1.49.52.

c) Configure the Router to point to the Web Sense server.

d) The router should always block requests going towards xxx.com. The router should always permit requests to cisco.com.

e) If the Web Sense server is down, the HTTP requests should be allowed to go out.

9 – Advanced Security and Attacks (7 Points)

9.1 – SSH into PIX (3 Points)

a) Setup the PIX firewall so that the PC at 10.1.1.100 can ssh into the PIX for remote management.

b) Have the TACACS Server authenticate ssh Requests.

c) The PIX communicates to the TACACS Server using TACACS+ with a secret key of **ipexpert**.

9.2 – Dynamic Access Lists (4 Points)

a) R5 should allow access from the frame networks only if users are authenticated.

b) Once Authenticated, the user should be allowed full access.

c) The authentication should be done locally.

d) Allow Administrator to Manage the Router from the Frame Relay interface. They should use a non-default port for this. Dedicated only one Telnet line for this.

e) Apply the ACL on the Frame Relay Interface.

f) Allow relevant traffic to come in including return traffic. You are also allowed to create a reflexive ACL for this task.

g) Create a couple of local users to test the config (U1 with a password of u1 and U2 with a password of U2).

10 – IDS (16 Points)

10.1 – Basic Configuration of IDS through IDS, IDM and IEV (2 Points)

a) Configure the IDS Sensor's Command and Control Interface through the CLI to allow access to the Sensor from the IDM PC based on the Network Diagram.

b) Add the Sensor to the IEV Console.

10.2 – Switch Configuration (2 Points)

a) You would like to monitor all traffic received in the outside VLAN of the PIX.

b) Configure the Switch to copy all relevant traffic to the monitoring port.

10.3 – Fine tuning the ICMP Signature (4 Points)

a) Enable the ICMP Echo Request and ICMP Echo Reply Signatures.

b) Set the Alarm Severity to **Medium**.

c) The alarms should not fire when they are sent by R2. They should fire from any other device.

d) Verify the Alarm by pinging the outside Interface of the PIX from R2 and R5.

10.4 – IP Blocking on the PIX (4 Points)

a) Configure the IDS Sensor to block the Connection if the ICMP Echo Request or Reply signature is detected.

b) The Blocking should be done on the PIX firewall.

c) Configure the PIX to allow the IDS Sensor to Telnet into it.

d) Authenticate the Telnet connection using AAA server. The AAA Configuration should have been done in an earlier step.

e) Configure the Sensor with the appropriate information to Telnet into the PIX. Use User1 as the username and cisco as the password to allow the IDS to connect into the PIX.

f) Set the Block time to 20 Minutes.

10.5 – IOS IDS on R6 (4 Points)

a) Configure the router to send alarms to a Syslog Server. Configure the PIX to allow the alarms from R6 to the Syslog Server at 10.1.1.100. The Syslog server is seen as 192.1.12.100 on the outside of the PIX. This static translation should have been done in an earlier step.

b) Configure the IDS with the following parameters:

- ➔ Send an alarm for Info signatures
- ➔ Send an alarm and drop packets for Attack signatures

c) You do not want signatures to fire from a specific address. (200.0.0.2) for this IDS Rule Set.

d) Any e-mail messages received with more than 50 recipients should be dropped.

e) Attacks should be detected from the Frame cloud and serial link.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 17: Multiprotocol Challenge D (One Day Lab Experience)

This Lab is intended to assess your readiness to attempt the actual CCIE Security lab exam. During this section you will be utilizing the entire topology and all topics listed on the CCIE Security Lab Blueprint are fair game.

Estimated Time to Complete: 8 Hours

MUST DO:

Read the ENTIRE lab prior to beginning.

Diagram 17-A

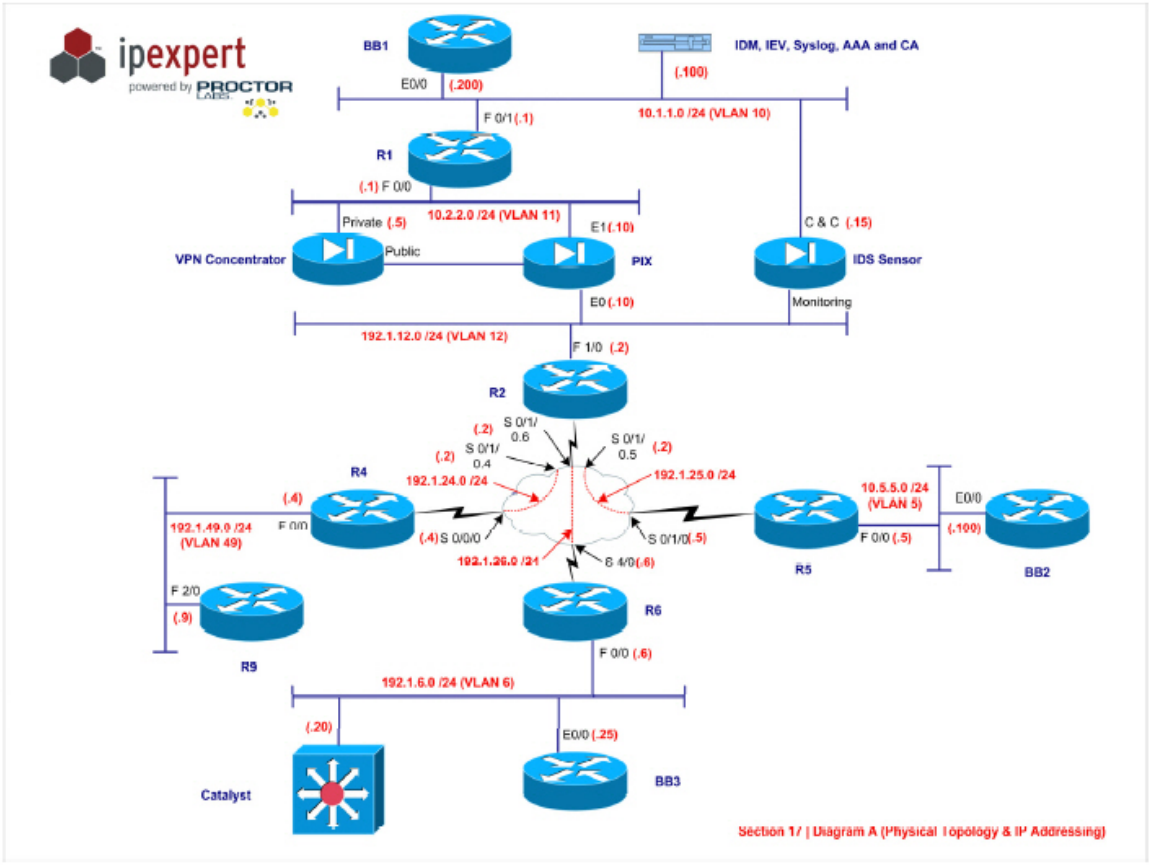
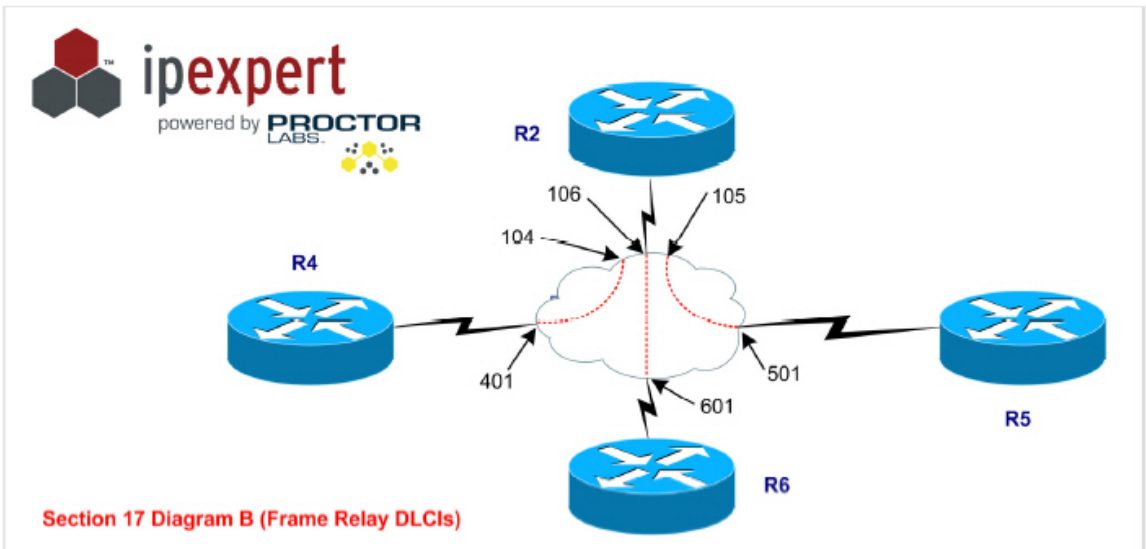


Diagram 17-B



Section 17 IP Addressing

Device	Port	IP Address
R1	F 0/0	10.2.2.1/24
	F 0/1	10.1.1.1/24
	Loopback 0	1.1.1.1 / 8
R2	F 1/0	192.1.12.2/24
	S 0/1/0.4	192.1.24.2/24
	S 0/1/0.5	192.1.25.2/24
	S 0/1/0.6	192.1.26.2/24
	Loopback 0	2.2.2.2 / 8
R4	F 0/0	192.1.49.4/24
	S 0/0/0	192.1.24.4/24
	Loopback 0	4.4.4.4/8
R5	F 0/0	10.5.5.5/24
	S 0/1/0	192.1.25.5/24
	Loopback 0	5.5.5.5 / 8
R6	F 0/0	192.1.6.6/24
	S 4/0	192.1.26.6/24
	Loopback 0	6.6.6.6/8
R9	F 0/0	192.1.49.9/24
	Loopback 0	9.9.9.9/8
PIX	E 0 (outside)	192.1.12.10/24
	E 1 (inside)	10.2.2.10/24
Concentrator	Private	10.2.2.5/24
	Public	192.168.5.5/24
IDS Sensor	Command & Control	10.1.1.15/24
BB1	Ethernet	10.1.1.200 /24
BB2	Ethernet	10.5.5.100 /24
BB2	Ethernet	192.1.6.25 /24
PIX	VLAN 55 (DMZ55)	192.168.5.10 /24

Diagram 17-C (RIP)

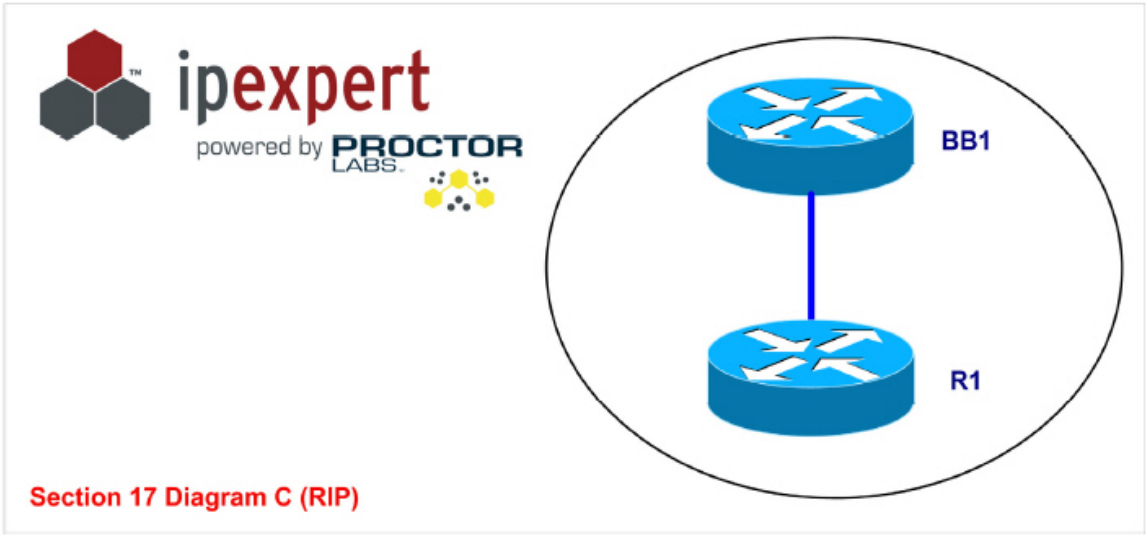


Diagram 17-D (OSPF)

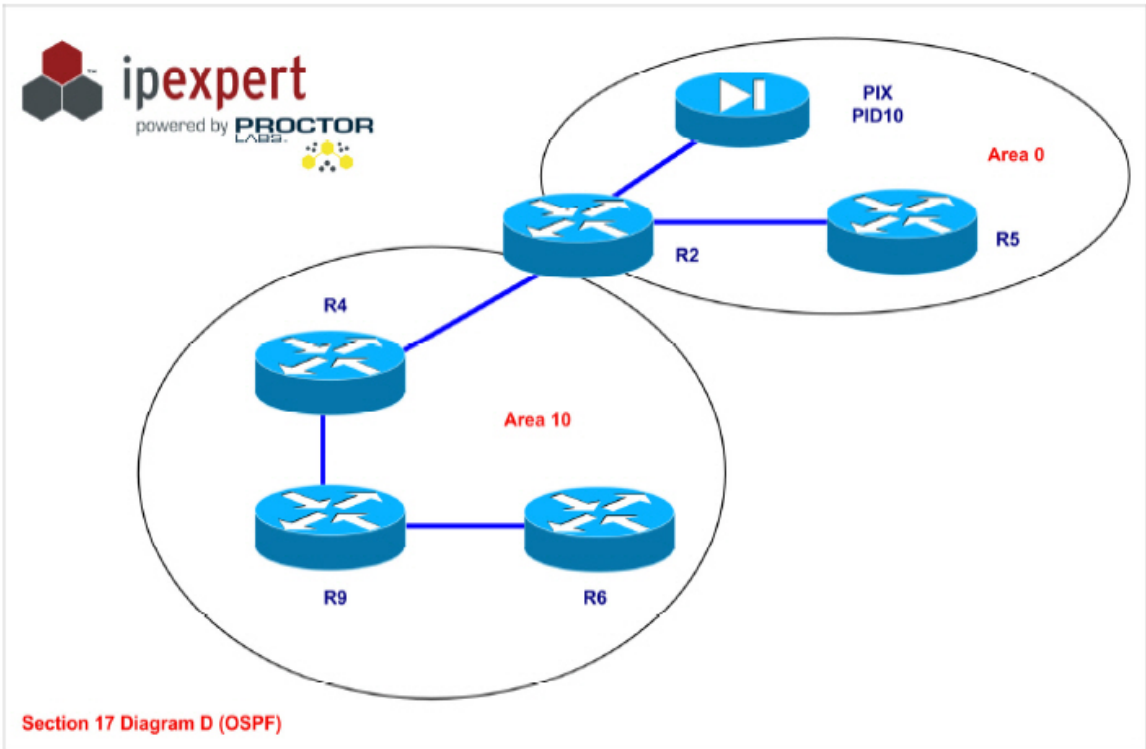


Diagram 17-E (EIGRP)

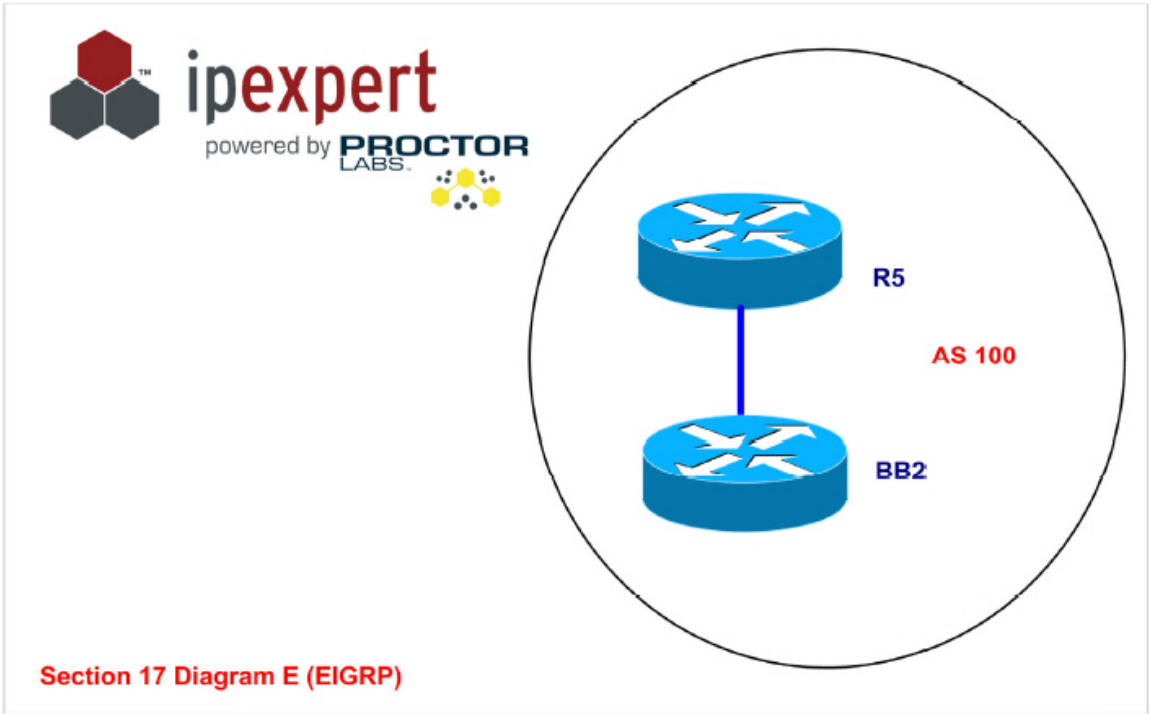
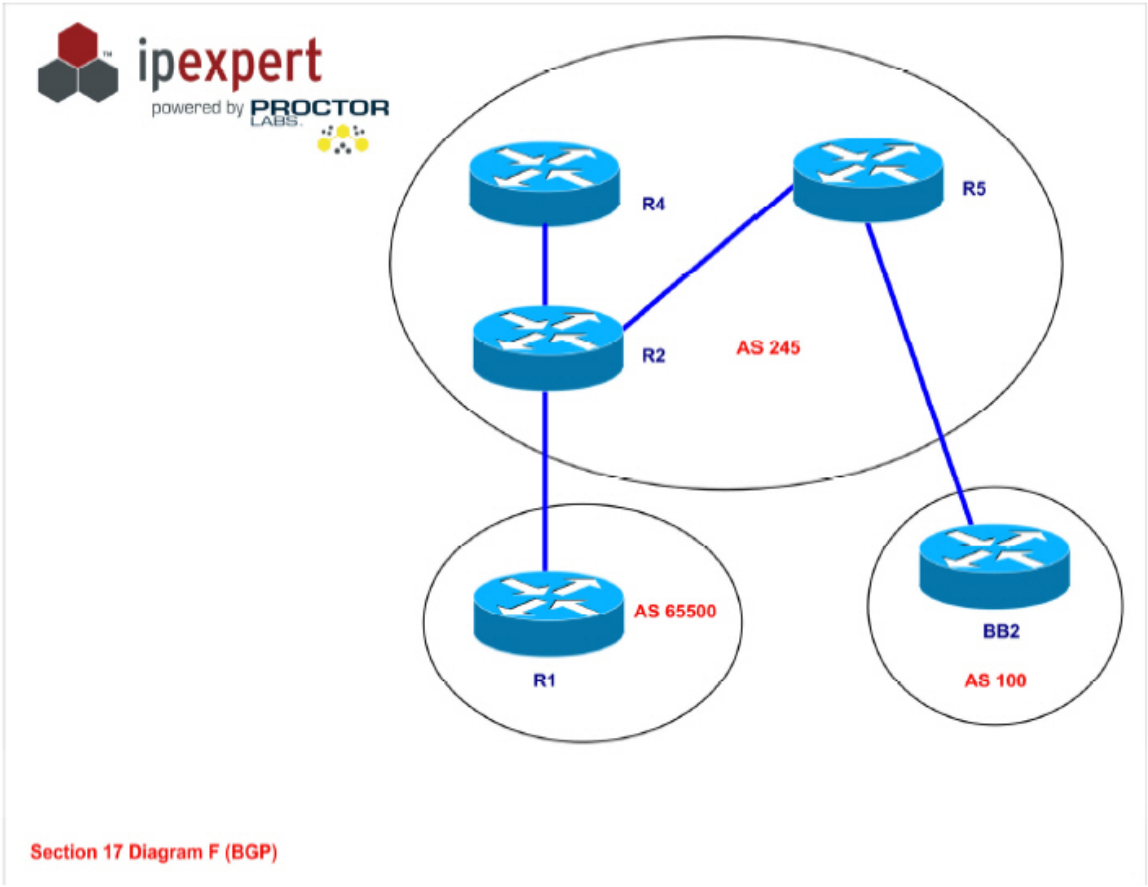


Diagram 17-F (BGP)



Section 17 Pre-Lab Setup

- **Pre-load the Initial Configurations for all the devices.** You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 17 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

1 – Layer 2 (4 Points)

1.1 – Switch Management (2 Points)

a) Create a Management interface on the Switch1 belonging to VLAN 6.

b) Set the IP Address as .20 on that network.

c) Allow Management access to this switch from VLAN 6 only.

1.2 – Port Security (2 Points)

a) You want to make sure that only PIX Inside interface can connect to the respective port on Switch 2.

b) Make sure only PIX inside MAC with an IP Address of 10.2.2.10 can communicate on that port.

2 – Basic PIX Firewall (12 Points)

2.1 – PIX IP Address (4 Points)

a) Create a Logical Interface off of E0 interface on the PIX.

b) The logical interface should belong to VLAN 55.

c) The Physical interface belongs to the outside VLAN. Assign the new VLAN interface a name of DMZ55 and a security level of 50.

d) Configure the Switch to allow the PIX to communicate to the rest of the network.

e) Assign IP Addresses to the PIX Interfaces.

2.2 – Routing (2 Points)

a) Run OSPF as the routing protocol on the outside interface of the PIX Firewall.

b) Configure Process ID 10 and advertise the outside network in area 0.

c) Configure static routes for the 10.1.1.0 and 1.0.0.0 networks on the PIX.

2.3 – Static Translation (3 Points)

a) Allow all networks behind the PIX to get out with translation.

b) Use PAT without using any unused address.

c) Create a Static entry for the AAA server at 10.1.1.100. Translate it to 192.1.12.100. Allow R4 Loopback 0 to communicate to the TACACS+ server. Also allow R2 F 1/0 interface to communicate to the TACACS+ server.

d) Create a Static entry for R1 F 0/0 at 10.2.2.1. Translate it to 192.1.12.15.

2.4 – Advanced Filtering (3 Points)

a) Configure URL Filtering on the PIX. The url server is a Web Sense server located at 10.2.2.52.

b) Configure the PIX to point to the Web Sense server.

3 – Routing Using Interior Gateway Protocols (12 Points)

3.1 – RIP V2 Authentication (2 Points)

a) R1 and BB1 should authenticate to each other using the highest level of Authentication with a password of **ccie**.

3.2 – OSPF Authentication (3 Points)

a) All OSPF routers should exchange packets based on the most secure Authentication method.

b) The password should be set to **ccie**.

c) You cannot use **Area x authentication message-digest** command.

3.3 – EIGRP Authentication (2 Points)

a) All routers in EIGRP should authentication with each other.

b) The password should be set to **ccie** with a key id of 1.

3.4 – GRE thru PIX (3 Points)

a) Configure a GRE Tunnel from R1 F 0/0 to R6 Serial 4/2. Use 172.16.16.0/24 as the Tunnel IP Address.

b) Create the following Loopbacks on R1 and R6:

- ➔ R1 – Loopback 16 – 172.16.1.1/24
- ➔ R6 – Loopback 16 – 172.16.6.1/24

c) Run RIP V2 over the GRE tunnel. Advertise the following networks over the GRE Tunnel:

- ➔ R1 – Loop 16, Tunnel and F 0/0
- ➔ R6 – Loop 16, Tunnel and Serial 4/2

d) Allow the Tunnel thru the PIX Firewall.

e) Make sure that there is no Recursive Routing issue. You can use the static command on the PIX.

3.5 – Redistribution of IGP (2 Points)

a) Redistribute at all appropriate routers. Make sure that all routes are visible and there are no routing loops.

b) R2 should be able to ping 1.1.1.1 or the BB1 routes without having to change anything on the PIX.

4 – BGP Routing (10 Points)

4.1 – Authentication (2 Points)

a) Authenticate all IBGP peerings using MD5 authentication with a password of **ccie**.

4.2 – EBGP thru the PIX (2 Points)

a) Configure EBGP peering between R1 and R2. R1 sees R2 as 2.2.2.2 and R2 sees R1 as 1.1.1.1. You cannot make any configuration changes on the PIX to accomplish this. Statics and static routes are not allowed.

4.3 – BGP Filtering (4 Points)

a) R5 should be receiving the following routes from the BB2:

- → 201.1.4.0/24
- → 201.1.5.0/24
- → 201.1.6.0/24
- → 201.1.7.0/24
- → 201.1.8.0/24
- → 201.1.9.0/24

b) On R5, deny the 201.1.4.0/24 and 201.1.6.0/24 routes from been propagated to R2. Use the Prefix list to accomplish this. Filter based on the Neighbor.

c) On R1, deny all BGP networks with an odd number in the third octet coming into R1. Configure a distribute list to accomplish this. Filtering should be Routing Protocol specific and not neighbor specific. Use the minimum number of lines to accomplish this.

4.4 – Redistribution of BGP (2 Points)

a) Redistribute routes learned through BGP in such a way that the PIX can see all the BGP routes.

5 – Access Management (6 Points)

5.1 – Configuring AAA Authentication on Switch 1 for Telnet Management (4 Points)

a) Configure Switch 1 with AAA access using TACACS+. The secret key is **ccie**. Configure the switch with a default route to communicate to the AAA server. Allow the appropriate entries in the access list of the PIX. You are allowed a static route to make this work.

b) No Authentication should be done on the Console or AUX lines.

c) Setup Authentication based on TACACS+ for the VTY lines.

d) There are 2 users created on the AAA server, User 1 and User2. Both the users have **cisco** as their password.

5.2 –Controlled Telnet Access (2 Points)

a) You want User1 and User2 to have full privilege on the router. When User1 and User2 login, they should be in Privilege Exec mode.

b) You would like to reserve the last telnet line for yourself. Do this by changing the default port to 3099.

c) Disable the telnet client on the switch.

6 – IP Services (5 Points)

6.1 – NAT on R5 (3 Points)

a) Configure NAT such that if F0/0 network wants to go to 1.0.0.0, 4.0.0.0 or 9.0.0.0 networks, it should use the interface IP address of the S0/1/0 interface as the translated address. Configure PAT for this entry.

b) Configure NAT such that if F0/0 network wants to go to 2.0.0.0 or 6.0.0.0 networks, it should use a pool of 192.1.25.151 – 192.1.25.199 as the translated address.

c) There is a Web Server at 10.5.5.80. The Web server should be seen as 192.1.25.80.

6.2 – SNMP Configuration on R2 (2 Points)

a) Configure R2 to allow the management station at 192.1.12.30 to manage R2.

b) Configure the Read-only community as CCIERO and Read-write community as CCIERW.

7 – Virtual Private Networks (20 Points)

7.1 – Basic Concentrator Configuration (4 Points)

a) Configure the IP Address on the Private and Public Interfaces.

b) Do not configure any static routes for the 10.1.1.0 network on the Concentrator.

c) Management of the Concentrator should be done thru the Public interface.

d) Configure the PIX firewall to allow traffic from the Management PC at 10.1.1.100 to communicate to the Concentrator from the Public Interface. You are allowed a static route on R1 to accomplish this.

e) Configure the Concentrator such that it allows management from the Public Interface.

f) Disable RIP on the concentrator and configure a default gateway pointing towards the PIX.

7.2 – Setup a Site-to-Site IPSec VPN between the Concentrator and R5 (5 Points)

a) Encrypt traffic between the 10.2.2.0/24 and 10.5.5.0/24 networks using the following parameters:

- ➔ Authentication is based on Pre-shared key of **ccie**.
- ➔ Use MD5 for the Hashing algorithm. Use defaults for the rest of the ISAKMP parameters.
- ➔ For IPSec, use ESP-DES for encryption and ESP-SHA-HMAC for Data Authentication in Tunnel Mode.

b) You can use static routes on R5 and R1 to accomplish this.

c) The concentrator is seen on the outside as 192.1.12.5. Configure the PIX to translate the concentrator and allow appropriate entries for the IPSec traffic from R5 to the concentrator.

7.3 – Setup a Remote Access VPN between the Concentrator and the Cisco Secure Client using External Authentication (4 Points)

a) Use the following parameters to setup Concentrator with the following options:

- ➔ Assign IP Address in the range of 10.3.3.1 – 10.3.3.254. The pool should be created specific to the group **Remote.**
- ➔ Create a group called Remote with a password of **ccie.**
- ➔ The group should do authentication based on a RADIUS server located at 10.2.2.99. It communicates to the Concentrator using Port 1812 for Authentication and 1813 for Accounting. The secret key is **Ripexpert.**
- ➔ Only allow PPTP and IPSec for the group. Configure it such that only MSCHAP V2 is allowed as the authentication protocol for PPTP.

7.4 – Setup a Site-to-Site IPSec VPN between the PIX and R4 (4 Points)

a) Create the following loopback on R4:

- ➔ **R4** - Int loop 10 : 192.168.104.4/24

b) Encrypt traffic between the 192.168.104.0/24 and 10.2.2.0/24 networks using the following parameters:

- ➔ Authentication is based on Pre-shared key of **ccie**
- ➔ Use MD5 for the Hashing algorithm and Group 2 for the Diffie-Hellman key exchange. Use defaults for the rest of the ISAKMP parameters
- ➔ For IPSec, use ESP-DES for encryption and ESP-MD5-HMAC for Data Authentication in Tunnel Mode

c) Use the PIX outside and R4 S 0/0 as the Tunnel Endpoints.

d) You are allowed a static route on the PIX,R1 and R4.

7.5 – QoS on the VPN Concentrator (3 Points)

a) Create a bandwidth policy for the public interface giving it minimum of 1 Mbps and a maximum of 100 Mbps. Assign a burst of 16000 bytes.

b) You want to limit the amount of bandwidth allocated to the LAN to LAN tunnel between the Concentrator and R5 based on the following:

- ➔ Minimum Bandwidth allocated – 1 Mbps
- ➔ Maximum Bandwidth allowed – 3 Mbps
- ➔ Burst – 16000 bytes

8 – IOS Firewall (5 Points)

8.1 – Cisco IOS Firewall on R4 with non-standard ports (5 Points)

a) Inspect the following traffic from the Ethernet segment going towards the Frame networks:

- ➔ All TCP Based traffic
- ➔ All UDP Based traffic
- ➔ Netmeeting Traffic
- ➔ SMTP traffic should be inspected so that only a limited number of SMTP commands are allowed in

b) FTP should be inspected on the Standard port and also on port 2021.

c) HTTP should also be inspected for a non-standard port of 8000.

d) Only allow Java applets from 2.0.0.0 to be downloaded.

e) Only allow relevant traffic coming in.

f) ACL should be set to inbound on the Serial interface.

9 – Advanced Security and Attacks (12 Points)

9.1 – Ping Block (2 Points)

a) Only R2 F 1/0 should be allowed to ping the outside interface of the PIX.

b) Also allow R4 S0/0.0 and R5 S0/1/0 to ping the PIX outside interface.

9.2 – Preventing the Nimda attack (4 Points)

a) R6 is experiencing the Nimda attack from the Frame Cloud and serial link.

b) Classify the attack on the outside interfaces.

c) Drop the packets using an ACL on the Inside interface.

9.3 – Preventing the W32.Blaster Worm attack (3 Points)

a) R9 is experiencing the W32.Blaster worm attack on the serial link.

b) Use ACL to block this attack.

9.4 – Preventing the Smurf and Fraggle attacks (3 Points)

a) R9 is experiencing the smurf and fraggle attacks from the serial link.

b) Use a Named ACL to block the attack.

c) Allow all other traffic coming in.

10 – IDS (14 Points)

10.1 – Basic Configuration of IDS through IDS, IDM and IEV (3 Points)

a) Configure the IDS Sensor's Command and Control Interface through the CLI to allow access to the Sensor from the IDM PC based on the Network Diagram.

b) Add the Sensor to the IEV Console.

10.2 – Switch Configuration (2 Points)

a) You would like to monitor all traffic received in the outside VLAN of the PIX.

b) Configure the Switch to copy all relevant traffic to the monitoring port.

10.3 – Fine tuning the ICMP Signature (3 Points)

a) Enable the ICMP Echo Request and ICMP Echo Reply Signatures.

b) Set the Alarm Severity to **Medium.**

10.4 – IP Blocking on the Router (6 Points)

a) Configure the IDS Sensor to block the Connection if the ICMP Echo Request or Reply signature is detected

b) The blocking should be done on the R2 S0/1/0.4 and R2 S0/1/0.5 sub-interfaces.

c) Configure the Router to allow the IDS Sensor to Telnet into it.

d) Authenticate the Telnet connection locally. Create a username of **ids** with a password of **ids.**

e) Configure the Sensor with the appropriate information to Telnet into the R2.

f) Set the Block time to 20 Minutes.

g) Sensor should be seen as 192.1.12.77 on the outside. IDS should not use the tunnel to connect to R2. You are allowed a static route to accomplish this step.

h) The sensor should never block itself. Make sure the entry in the access list reflects the correct IP address for the Sensor.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 18: Multiprotocol Challenge E One Day Lab Experience)

This Lab is intended to assess your readiness to attempt the actual CCIE Security lab exam. During this section you will be utilizing the entire topology and all topics listed on the CCIE Security Lab Blueprint are fair game.

Estimated Time to Complete: 8 Hours

MUST DO:

Read the ENTIRE lab prior to beginning.

Diagram 18-A

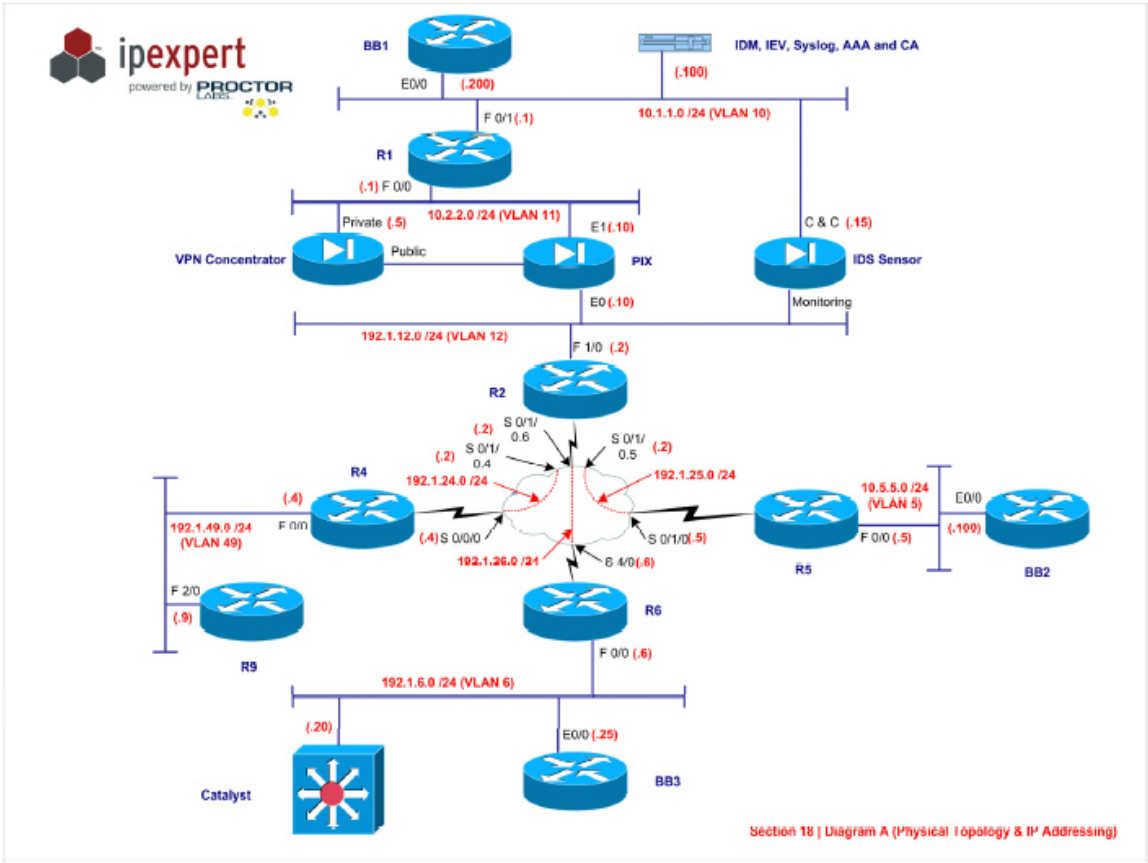
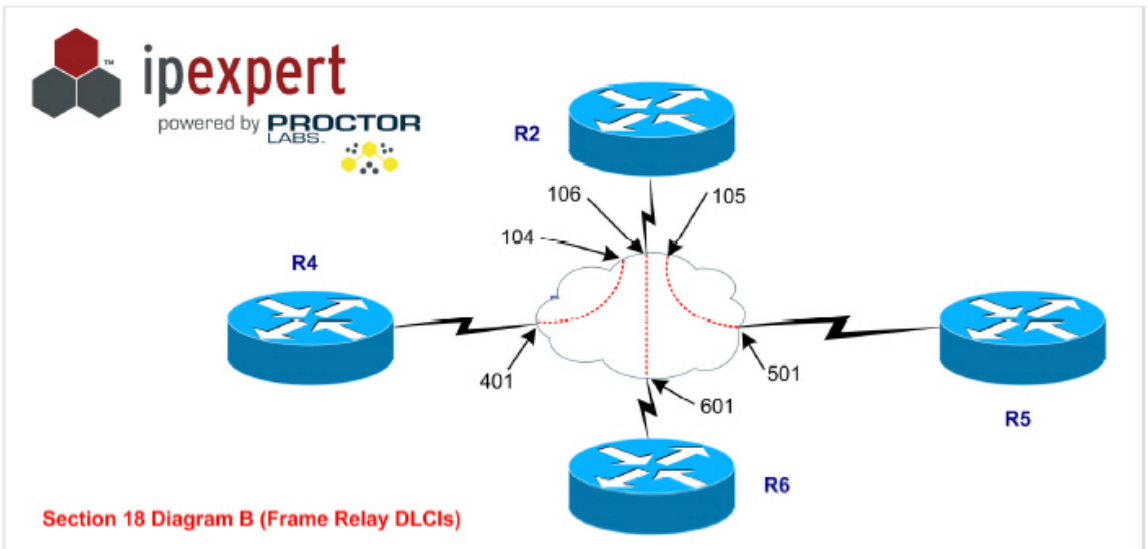


Diagram 18-B



Section 18 IP Addressing

Device	Port	IP Address
R1	F 0/0	10.2.2.1/24
	F 0/1	10.1.1.1/24
	Loopback 0	1.1.1.1 / 8
R2	F 1/0	192.1.12.2/24
	S 0/1/0.4	192.1.24.2/24
	S 0/1/0.5	192.1.25.2/24
	S 0/1/0.6	192.1.26.2/24
	Loopback 0	2.2.2.2 / 8
R4	F 0/0	192.1.49.4/24
	S 0/0/0	192.1.24.4/24
	Loopback 0	4.4.4.4/8
R5	F 0/0	10.5.5.5/24
	S 0/1/0	192.1.25.5/24
	Loopback 0	5.5.5.5 / 8
R6	F 0/0	192.1.6.6/24
	S 4/0	192.1.26.6/24
	Loopback 0	6.6.6.6/8
R9	F 0/0	192.1.49.9/24
	Loopback 0	9.9.9.9/8
PIX	E 0 (outside)	192.1.12.10/24
	E 1 (inside)	10.2.2.10/24
Concentrator	Private	10.2.2.5/24
	Public	192.168.5.5/24
IDS Sensor	Command & Control	10.1.1.15/24
BB1	Ethernet	10.1.1.200 /24
BB2	Ethernet	10.5.5.100 /24
BB2	Ethernet	192.1.6.25 /24
PIX	VLAN 55 (DMZ55)	192.168.5.10 /24

Diagram 18-C (RIP)

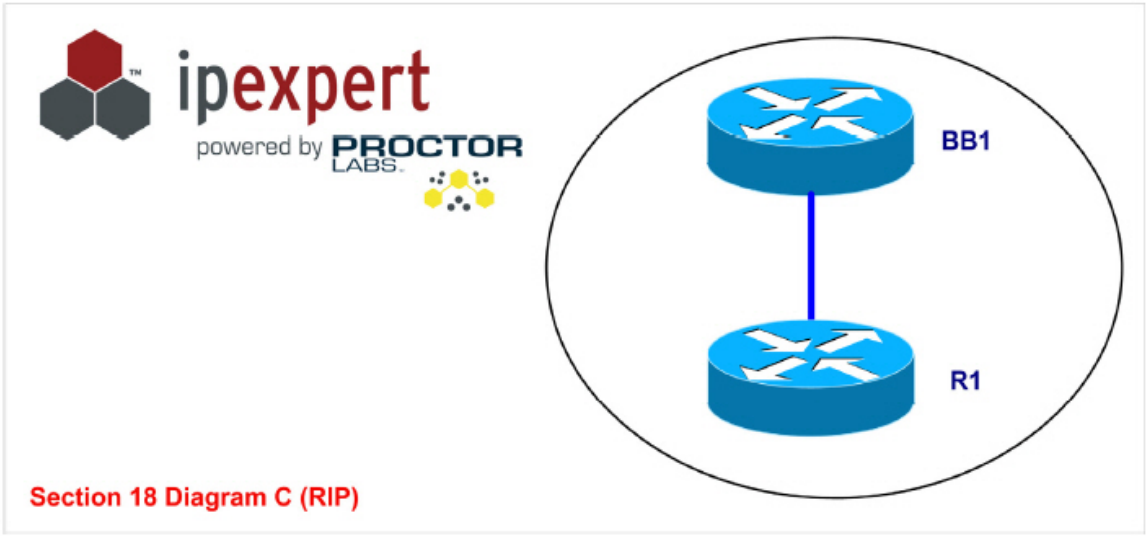


Diagram 18-D (OSPF)

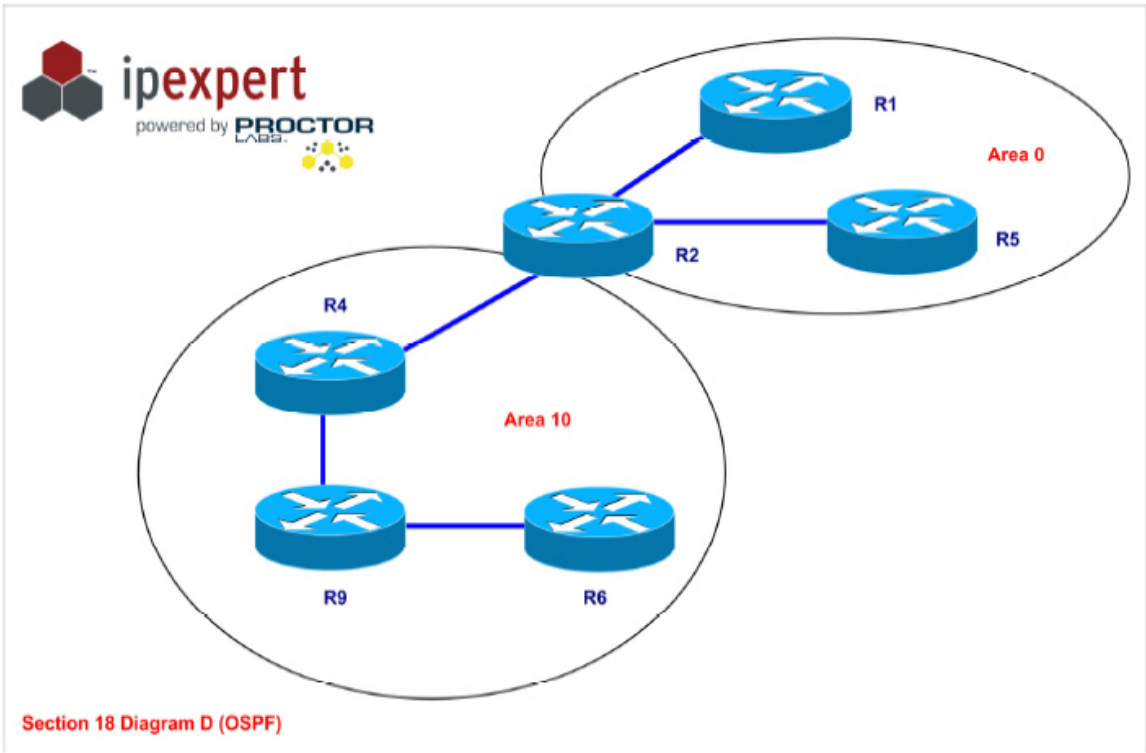


Diagram 18-E (EIGRP)

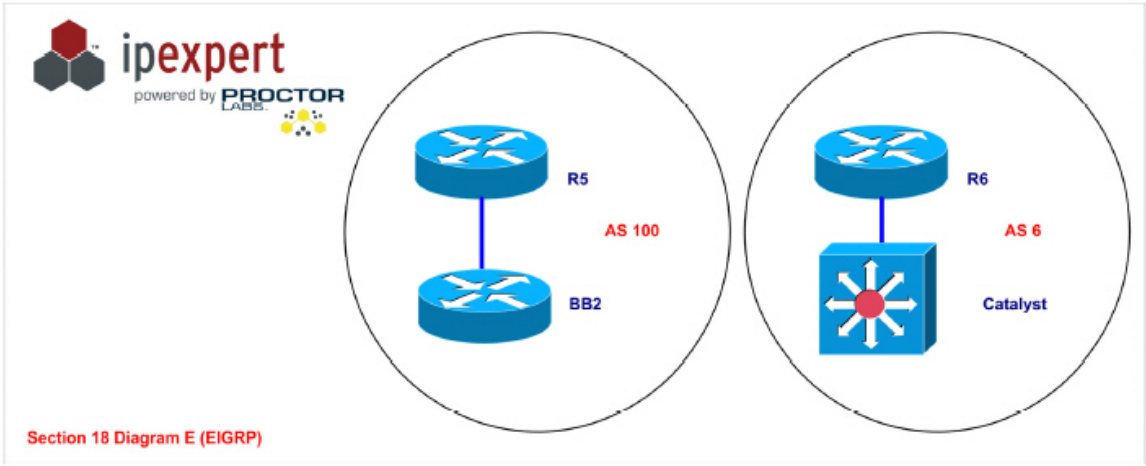
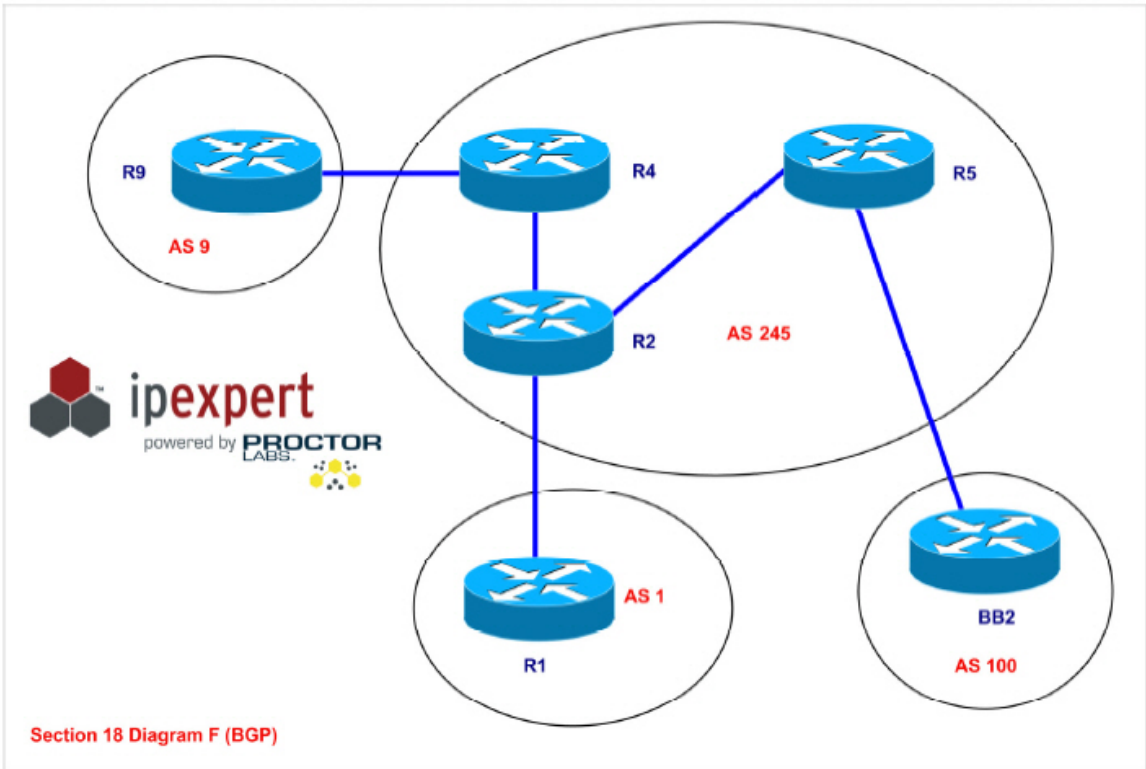


Diagram 18-F (BGP)



Section 18 Pre-Lab Setup

- **Pre-load the Initial Configurations for all the devices.** You will find these configurations in the "Initial Configurations" subfolder within each section *(i.e. IPexpert CCIE Security 3.1 WB Configs → Section 18 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.*

1 – Layer 2 (5 Points)

1.1 – Switch Management (2 Points)

a) Create a Management interface on Switch1 belonging to VLAN 6.

b) Set the IP Address as .20 on that network.

c) Allow management access to this switch from VLAN 6 only.

1.2 – Port Security (3 Points)

a) Configure Port F 0/19 on Switch 1 for Dot1x authentication.

b) Any device that connects to Port F 0/19 should be authenticated by a RADIUS server located at 192.1.6.50.

c) The RADIUS server uses **ipexpert** as the key and 1645 as the Authentication port.

d) The Switch should re-authenticate every 2 hours.

e) This port is connected to a hub. Once a port on that hub authenticates, all devices should be allowed.

2 – Basic PIX Firewall (15 Points)

2.1 – PIX IP Address (4 Points)

a) Create a Logical Interface off of E0 interface on the PIX.

b) The logical interface should belong to VLAN 55.

c) The Physical interface belongs to the outside VLAN. Assign the new VLAN interface a name of DMZ55 and a security level of 50.

d) Configure the switch to allow the PIX to communicate to the rest of the network.

e) Assign IP Addresses to the PIX Interfaces.

2.2 – Routing (2 Points)

a) Configure a default route on the PIX pointing towards R2.

b) Configure a static route for the network behind R1.

2.3 – Static Translation (4 Points)

a) Configure a Loopback 125 on R1. It should be assigned an IP Address of 195.1.1.1/24. This is a network with a public address. Create a static route on R1 for the 192.1.12.0 network towards the PIX.

b) Allow this network to go out without getting translated. You cannot use the static command to accomplish this.

c) R2 should be able to ping this network. You are allowed a static route on R2 and the PIX to accomplish this step.

d) Create a Static entry for the AAA server at 10.1.1.100. Translate it to 192.1.12.100. Allow R4 Loopback 0 to communicate to the TACACS+ server. Also allow R2 F 1/0 interface to communicate to the TACACS+ server.

e) Create a Static entry for R1 E 0/0 at 10.2.2.1. Translate it to 192.1.12.15.

2.4 – Authentication Proxy (5 Points)

a) The AAA server is located at 10.1.1.100. It communicates to the PIX using TACACS+ and a key of **ipexpert**.

b) All outbound Telnet and HTTP Requests have to authenticate against the AAA server. The username to use is **pixuser** with a password of **ipexpert**. Use the same username and password for all authentication passwords.

c) Allow R2 to telnet into R1 through the PIX.

d) All inbound traffic for Telnet should be authenticated against the AAA server.

e) All outbound traffic destined for a custom TCP application should be authenticated against the AAA server. The TCP application uses port 4515. Use virtual telnet and an IP address of 192.1.12.1.

3 – Routing Using Interior Gateway Protocols (15 Points)

3.1 – RIP V2 Authentication (2 Points)

a) R1 and BB1 should authenticate to each other using the highest level of Authentication with a password of **ccie**.

3.2 – OSPF Authentication (2 Points)

a) All OSPF routers should exchange packets based on the most secure Authentication method.

b) The password should be set to **ccie**.

3.3 – EIGRP Authentication (2 Points)

a) All routers in EIGRP should authentication with each other.

b) The password should be set to **ccie** with a key id of 1.

3.4 – GRE thru PIX (4 Points)

a) Configure a GRE Tunnel from R1 F 0/0 to R2 F 1/0. Use 172.16.12.0/24 as the Tunnel IP Address.

b) Run OSPF over the GRE tunnel. Advertise the following networks over the GRE Tunnel:

- ➔ R1 – Loopback 0, Tunnel and F 0/0
- ➔ R2 – Advertise the Tunnel and F 1/0 interface in OSPF. The other interfaces should already have been advertised into OSPF. Use the same process ID.

c) Allow the Tunnel thru the PIX Firewall.

d) Make sure that there is no Recursive Routing issue. You can use the static command on the PIX.

3.5 – Redistribution of IGP (3 Points)

a) Redistribute RIP into OSPF on R1.

b) Redistribute EIGRP into OSPF on R5. OSPF should use a seed cost of 10, and add the cost of the link for metric calculations for the Redistributed routes.

c) Redistribute OSPF into EIGRP on R6. Do not redistribute EIGRP into OSPF.

d) The network 192.1.6.0 should be seen on all OSPF routers. You cannot redistribute EIGRP into OSPF or redistribute connected on R6. You are allowed a single route to the 192.1.6.0 network on only one router.

3.6 – Filtering OSPF (2 Points)

a) Area 10 should not see any External or Inter-Area Routes. It should have connectivity to all the routes.

4 – BGP Routing (11 Points)

4.1 – Authentication (2 Points)

a) Authenticate all IBGP Peerings using MD5 authentication with a password of **ccie**.

4.2 – Controlling BGP Prefixes (2 Points)

a) R5 wants to be notified when it receives 2000 prefixes from BB2. It should be warned when it receives 1000 prefixes and then at 2000.

b) R5 should only send warnings, but should accept the prefixes.

4.3 – EBGP thru the PIX (2 Points)

a) Configure EBGP peering between R1 and R2 thru the PIX. R1 sees R2 as 192.1.12.2 and R2 should see R1 as 192.1.12.15. The Static should have been created in the previous step.

4.4 – BGP Filtering - I (3 Points)

a) R5 should be receiving the following routes from the BB2:

- 200.1.4.0 /24
- 200.1.5.0 /24
- 200.1.6.0 /24
- 200.1.7.0 /24

b) Summarize these routes and send the summary route to R2. Use bit-based summarization.

c) The more specific routes should not be sent to R2, except for 201.1.5.0/24. 201.1.5.0 should be sent along with the summary route.

4.5 – BGP Filtering - II (2 Points)

a) AS 245 should only advertise its local AS routes to the directly connected ASs (AS 1, AS 9, AS 100).

b) Use the AS-PATH Filter list to accomplish this task.

5 – Access Management (4 Points)

5.1 – Configuring SSH on R4 (4 Points)

a) Configure SSH on R4.

b) SSH authentication should be done locally.

c) Create a user **admin** with a password of **ipexpert**.

6 – IP Services (5 Points)

6.1 – DHCP Server and Relay Agent (5 Points)

a) Enable R2 as a DHCP Server with the following information:

- IP ADDRESS : 192.1.49.0/24
- WINS ADDRESS : 192.1.49.135
- DNS ADDRESS : 192.1.49.53
- DEFAULT GATEWAY : 192.1.49.4
- LEASE TIME : 6 Days

b) Enable R4 to forward DHCP requests to R2.

7 –Virtual Private Networks (20 Points)

7.1 – Basic Concentrator Configuration (3 Points)

a) Configure the IP Address of the Private Interface thru the CLI.

b) The Public interface should be configured from the Graphical interface.

c) Make sure the PC can access the Concentrator. You are allowed a static route on the Concentrator to accomplish this.

d) Configure a Default Route on the Concentrator pointing towards the DMZ55 interface on the PIX. You are allowed a static route on R1 to accomplish this.

7.2 – Configure a Remote Access Easy VPN using PIX as a Server and Cisco Secure VPN Client (5 Points)

a) Configure the PIX as the Easy VPN Server using the following parameters:

- Group name and password: Name: **EZGroup**, Password: **abcd1234**
- DNS and WINS Address: 10.2.2.175
- Domain Name: ipexpert.net
- Address Pool (local): 10.3.3.1 – 10.3.3.253
- The address should be assigned to the client from the pool above.
- The authentication should be done locally.
- Hashing for the ISAKMP policy should be done based on MD5.
- Authentication for ISAKMP policy should be done based on a pre-shared key.
- Use ESP-DS and ESP-MD5-HMAC for your transform set.

7.3 – Setup a Site-to-Site IPSec VPN between the Concentrator and R5 (4 Points)

a) The concentrator should be seen as 192.1.12.5 on the outside network. Configure the PIX to accomplish this.

b) Encrypt traffic between the 10.2.2.0/24 and 10.5.5.0/24 networks using the following parameters:

- Authentication is based on Pre-shared key of **ccie**.
- Use MD5 for the Hashing algorithm. Use defaults for the rest of the ISAKMP parameters.
- For IPSec, use ESP-DES for encryption and ESP-SHA-HMAC for Data Authentication in Tunnel Mode.

c) You can use static routes on R5 and R1 to accomplish this.

d) Create the appropriate entries in the PIX firewall to accomplish this.

7.4 – Event Management on the Concentrator (3 Points)

a) Configure the Concentrator to send e-mail messages to concadmin@ipexepert.com.

b) The SMTP Server to be used for sending messages is located at 10.2.2.25.

c) Disable the ability of users to Telnet into the Concentrator.

7.5 – Web VPN on the Concentrator (5 Points)

a) Enable HTTP Services on R1.

b) Create a Group called **WebVPN** with a password of **abcd**.

c) Enable WebVPN for the public interface.

d) Create a Pool of IP Address 192.168.2.1-192.168.2.254. This pool should be specific to this group.

e) Allow the Inside PC to connect to the Public interface of the Concentrator thru the PIX Firewall. Use the Static command to accomplish this on the PIX.

f) Create a static route for the 192.168.2.0 network on R1 pointing towards the Concentrator. Also create a static route on R1 for the 192.168.5.0 /24 network thru the PIX. The user at 10.1.1.100 should be able to Web VPN into the concentrator from the public interfaces thru the PIX.

g) Enable the Concentrator to redirect HTTP requests to HTTPS.

h) Disable the ability of the users to enter a URL.

i) Create a URL Link for the HTTP Server on R1 such that when a user part of this group logs in, he has the ability to click on a Link to connect to the HTTP server on R1.

j) Also allow the Client to use a Custom application that allows the user to connect into R1 using a port 3001.

k) Create a user **webvpnuser** with a password of **webvpn12.** Assign the user to the **WebVPN** group.

l) Verify the config by logging on and verifying the configuration from the Inside PC. Delete the static route for the 10.1.10 network for testing the WebVPN setup.

m) You should be able to telnet into R1 thru the WebVPN connection.

8 – IOS Firewall (4 Points)

8.1 – Cisco IOS Firewall on R4 (4 Points)

a) Inspect all tcp, udp and icmp traffic from the Ethernet segment going towards the Frame networks.

b) Only allow relevant traffic coming in.

c) ACL should be set to inbound on the Serial interface.

9 – Advanced Security and Attacks (8 Points)

9.1 – IP TCP Intercept (4 Points)

a) The 192.1.6.0 network is experiencing SYN attacks from the Frame cloud to your web servers.

b) R6 should watch the traffic and if it does not complete the TCP handshake in 20 seconds, it should drop the packets.

c) Limit IP TCP intercept to only watch packets coming from 192.1.26.0, 192.1.24.0 or the 192.1.25.0 networks for Web traffic towards R6.

d) Configure IP TCP intercept such that the router drops embryonic connections if they reach 1050. It should stop dropping the embryonic connections once the number reaches 850.

9.2 – Preventing IP Spoofing (4 Points)

a) R5 is seeing a lot of spoofed packets from the BB2.

b) You want to make sure that RFC 1918 addresses are not received from the backbone. Create an ACL to block all RFC 1918 addresses coming in as source packets. Allow 10.5.5.0 to come in.

c) You also would like to make sure that the internal networks are not seen as source packets on the E 0/0 interface of R5. Don't use an ACL for this step.

10 – IDS (13 Points)

10.1 – Basic Configuration of IDS through IDS, IDM and IEV (3 Points)

a) Configure the IDS Sensor's Command and Control Interface through the CLI to allow access to the Sensor from the IDM PC based on the Network Diagram.

b) Add the Sensor to the IEV Console.

10.2 – Switch Configuration (2 Points)

a) You would like to monitor all traffic received in the outside VLAN of the PIX.

b) Configure the Switch to copy all relevant traffic to the monitoring port.

10.3 – Creating a Custom Signature (4 Points)

a) Create a custom string signature that detects the word "cmd.exe" anywhere in a HTTP url.

b) Set the Alarm Severity to **High**.

10.4 – PIX IDS (4 Points)

a) Configure a Syslog Server at 10.1.1.100. Configure the PIX to send message to the Syslog server.

b) Configure Console Logging to level 4. Configure Trap logging level to debugging.

c) Configure the PIX IDS with the following parameters:

- ➔ Send an alarm for Info signatures
- ➔ Send an alarm and drop packets for Attack signatures

d) Enable the IDS sensing on the outside interface of the PIX.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Appendix A: CCIE Lab Test Taking Strategy, Tips and Hints

- Technical Preparation
- Technical Content on the Lab
- Travel
- Day One Focus
- Test Taking Strategy
- The Lab Proctor

Two things stand out in preparation for the lab; **time and desire**. Time will be your enemy leading up to the lab and it will be your biggest enemy in the actual lab. Assuming that you have passed the CCIE written exam and have significant experience in multi-protocol support, you now have to narrow your focus down to one thing – the lab.

Technical Preparation

It is not uncommon for people to devote 200+ hours to practice during the 4 – 8 weeks leading up to their lab attempt. The more you practice, the better prepared you will be. Finding equipment to practice on can present another obstacle. Hopefully your employer has a lab that you can use. If you decide to use production networks to practice scenarios, make sure your resume is up to date. Some people purchase used equipment to work with at home, use it until they pass (or give up the chase), and resell the equipment to other candidates. There are also a number of online sites that sell lab time. Proctor Labs, Inc. provides an excellent and inexpensive on-line rack consisting of the latest and great Cisco hardware including 2800's, 3800's, 7200's, and the latest IOS (12.2T +). Be sure to investigate their incredible GUI interface management system and online capabilities located at www.ProctorLabs.com.

You need to be very serious when blocking out practice time. Becoming a CCIE requires not only expert level knowledge; you have to really want it. Many have studied, attempted, failed (possibly multiple times), and given up. They may have had the knowledge but lacked the will. It takes an incredible amount of self-determination to succeed.

Familiarize yourself with the Cisco Documentation CD. This is the only reference material available to you in the lab. You can be assured that you will be tested on topics that you may not know. If you know where to look on the CD, this can save you valuable time. It's also very important to join 2 of the industries online study communities located at www.certificationtalk.com and www.onlinestudylist.com.

Technical Content on the Lab

You can be virtually certain that some items will appear on the lab. Check Cisco's Website for current information. You must become very comfortable with the core competencies. This would include all of the IGPs and BGP. For IP routing it is not enough to merely know how to configure the different protocols. You must understand all of the rules for route-redistribution between the protocols. You should be aware of multiple ways to accomplish a task, such as the use of prefix-lists in lieu of access-lists. There are five ways to implement OSPF over Frame Relay; it would be a good idea to know them all. Through repeated experimentation, force yourself to become familiar with all of the command options related to IP routing. The less you have to research during the lab, the greater your chances of success will be.

Travel

On the travel day prior to your lab do not take the last flight of the day. You want to get in earlier in the day, get to your hotel, and get a good night's rest. Rest can never be overlooked. Last minute cramming is not the way to go, since you are probably not going to learn anything new in the last few hours before the exam. You want to stay focused. On the morning of your lab, eat a good breakfast and get to the test site early. If you are late it will only add to your stress level. The lab is stressful enough on its own.

Day One Focus

There will probably be a handful of candidates there for the lab. Do not bring anything with you. No paper, no CDs, anything. Cisco will provide all the materials you need. The proctor will give you a quick tour and then seat you at a terminal. Each candidate will have his or her own rack of equipment. You will be provided a document that details what you are to configure. Read the entire document carefully. You should be able to spot issues related to IP addressing, classfull/classless route interaction, split-horizon, etc. Diagram your network and document your layer two parameters on the paper provided. When you have finished with layer two, document all of your layer three addressing. When you have finished layer three, document your routing protocols.

Once your documentation is complete then begin the actual configuration. At this point you should be able to reference your diagram to configure each device. For your configuration take the same approach as you did when diagramming your network. You should go through each router and configure all layer two information first. Ensure that your interfaces are "up and up", then configure all layer three information. Ensure that you can ping across all directly connected interfaces prior to adding the complexity of routing protocols. If you configure routing protocols prior to verifying that you have IP connectivity, you could be easily misled when routing adjacencies are not formed.

It is quite possible there will be items on the test that you are not familiar with. Focus on the items that you do know and get them out of the way. Remember, time is your biggest enemy. You could lose valuable time trying various ways to complete an unfamiliar task, leaving more familiar tasks unfinished. If you need to start a search on the CD there should not be any "downtime", start the search and go back to your configuration. Check the search results when it has finished.

Test Taking Strategy

If there are multiple items that you are not familiar with, focus on the items that are worth more points. Would you rather spend 30 minutes working for one point or invest the same time for three points?

Save your configuration often. On rare occasion (less rare in some cases) the router may reload of its own accord. Or you may need to reload the router. In either case, if you have made numerous configuration changes without saving, you will have lost valuable time. Not only will you have to remember the changes you have lost, mentally this can be crushing.

At some point you will need to verify connectivity. If you make changes after your verification, make sure that you have not broken your network in some unforeseen fashion.

The Lab Proctor

This may sound hard to believe but the proctor is there to help you. They will not explain things to you that you do not understand but they will clarify things for you. If you present your question in a manner that demonstrates that you understand the issues, you are far more likely to have your question answered. If you pose a vague question you will get a vague answer.

Conclusion

Remain calm at all times. Your first thought upon reading a scenario may be that it is not possible. It would not be on the test if it were not possible. Keep a positive attitude throughout the test. A few thousand people have passed the lab - thousands more have failed. Desire is what separates those who get a number from those who do not. The test may not present "real world" scenarios and may ask you to do things that you normally would not, but that is the point of the test. The CCIE lab exam will test the way that you perform under constant pressure while being asked something that you may not have ever done before, and with limited resources. After you finish your exam and take the trip home you get to endure one of the hardest parts of the exam…waiting for the email with your score report. Hopefully it will bring you great joy, but if not, don't give up. It is well worth the effort. – Good Luck!

IPexpert is pleased to be a part of your success strategy. Please be sure to let us know when you have earned your CCIE number! Send us an email to success@ipexpert.com.

- Good Luck!

Appendix B: IPexpert's IPv6 e-Book and Advanced IPv6 Lab Scenario

- IPv6 Addressing
- General Addressing format
- Addressing convention
- IPv6 address types
- Global Address
- Link Local vs. Site Local
- IPv4 in IPv6 addresses
- Anycast
- Multicast Addresses
- IPv6 Packet Header Format
- ICMP
- DNS
- DHCP
- Ethernet
- Frame Relay
- RIP
- OSPF
- BGP
- Mobile IPv6
- DSCP
- Tunneling
- IP6to4
- Security

Introduction

IPv6 was proposed when it became clear that the 32 bit addressing scheme of IP version 4 (IPv4) was inadequate to meet the demands of Internet growth. IPv6 has a larger address space. The architecture of IPv6 was designed to allow existing IPv4 users to transition easily to IPv6, while providing services such as end-to-end security, Quality of Service (QoS), and globally unique addresses. The larger IPv6 address space allows networks to scale and provide global reachability. The simplified IPv6 packet header format handles packets more efficiently. IPv6 supports widely deployed routing protocols such as RIP, IS-IS, OSPF, and Multiprotocol BGP.

IPv6 Addressing

IPv6 addresses are 128-bit identifiers for interfaces and sets of interfaces. These are represented as a series of 16-bit hexadecimal fields and each 16-bit block is converted to a 4-digit hexadecimal number separated by colons (:) in the format: x:x:x:x:x:x:x:x. The resulting representation is called colon-hexadecimal. The IPv6 addressing architecture is described in RFC 3513.

There are three types of addresses:

- **Unicast**: An identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address.
- **Anycast**: An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the "nearest" one, according to the routing protocols' measure of distance). Anycast addresses are taken from the unicast address spaces (of any scope) and are not syntactically distinguishable from unicast addresses.
- **Multicast**: An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to a multicast address is delivered to all interfaces identified by that address. There are no broadcast addresses in IPv6, their function being superseded by multicast addresses.

IPv6 addresses of all types are assigned to interfaces, not nodes. An IPv6 unicast address refers to a single interface. Since each interface belongs to a single node, any of that node's interface unicast addresses may be used as an identifier for the node.

General Addressing format

The general format for IPv6 global unicast addresses is as follows:

n bits	*m bits*	*128-n-m bits*
Global routing prefix	**Subnet ID**	**Interface ID**

- **Global routing prefix -** value assigned to a site
- **Subnet ID -** an identifier of a link within the site

It is also required that all unicast addresses, except those that start with binary value 000, have Interface IDs that are 64 bits long and must be constructed in Modified EUI-64 format. The format of global unicast address in this case is:

n bits	*64-n bits*	*64 bits*
Global routing prefix	**Subnet ID**	**Interface ID**

Addressing convention

There are some conventions for representing IPv6 addresses as text strings:

- It is common for IPv6 addresses to contain successive hexadecimal fields of zeros. To make IPv6 addresses less cumbersome, two colons (::) may be used to compress successive hexadecimal fields of zeros at the beginning, middle, or end of an IPv6 address (the colons represent successive hexadecimal fields of zeros).
- The preferred form is x:x:x:x:x:x:x:x, where the 'x's are the hexadecimal values of the eight 16-bit pieces of the address. Note that it is not necessary to write the leading zeros in an individual field, but there must be at least one numeral in every field.
- Due to some methods of allocating certain styles of IPv6 addresses, it will be common for addresses to contain long strings of zero bits. In order to make writing addresses containing zero bits easier, a special syntax is available to compress the zeros. The use of "::" indicates one or more groups of 16 bits of zeros. The "::" can only appear once in an address. The "::" can also be used to compress leading or trailing zeros in an address. For example, the following addresses:

Type	Full Address	Simplified Address
Unicast address	1234:0:0:0:8:888:200C:4444	1234::8:888:200C:4444
Multicast address	FF01:0:0:0:0:0:0:123	FF01::123
Loopback address	0:0:0:0:0:0:0:1	::1
Unspecified address	0:0:0:0:0:0:0:0	::

  - The loopback address may be used by a node to send an IPv6 packet to itself. The loopback address in IPv6 functions the same as the loopback address in IPv4 (127.0.0.1).
  - The unspecified address indicates the absence of an IPv6 address. For example, a newly initialized node on an IPv6 network may use the unspecified address as the source address in its packets until it receives its IPv6 address.

- An alternative form that is sometimes more convenient when dealing with a mixed environment of IPv4 and IPv6 nodes is x:x:x:x:x:x:d.d.d.d, where the 'x's are the hexadecimal values of the six high-order 16-bit pieces of the address, and the 'd's are the decimal values of the four low-order 8-bit pieces of the address (standard IPv4 representation). Examples:

  0:0:0:0:0:0:13.1.68.3
  0:0:0:0:0:FFFF:129.144.52.38

The text representation of IPv6 address prefixes is similar to the way IPv4 address prefixes are written in Classless Inter-Domain Routing (CIDR) notation. An IPv6 address prefix is represented by the notation: ipv6-address/prefix-length

IPv6 address types

The type of an IPv6 address is identified by the high-order bits of the address, as follows:

Address Type	Binary Prefix	Ipv6 notation
Unspecified	000…000 (128 bits)	::/128
Loopback	000…001 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Link-local unicast	1111111010	FE80::/10
Site-local unicast	1111111011	FEC0::/10
Global unicast	Everything else	

Interface identifiers in IPv6 unicast addresses are used to identify interfaces on a link. They are required to be unique within a subnet prefix. It is recommended that the same interface identifier not be assigned to different nodes on a link. They may also be unique over a broader scope.

For all unicast addresses, except those that start with binary value 000, Interface IDs are required to be 64 bits long and to be constructed in Modified EUI-64 format. In addition:

- The address 0:0:0:0:0:0:0:0 is called the unspecified address. It must never be assigned to any node. It indicates the absence of an address.
- The unicast address 0:0:0:0:0:0:0:1 is called the loopback address. It may be used by a node to send an IPv6 packet to itself.

Global Address

Aggregate-able global addresses are used on links that are aggregated upward through organizations,

3 bits	*45 bits*	*16 bits*	*64 bits*
001	**Routing Prefix**	**SLA**	**Interface ID**

- **001** - identifies the address as being an aggregate-able global address.
- **Routing Prefix -** included two other hierarchically structured fields named Top-Level Aggregator (TLA) and Next-Level Aggregator (NLA).
- **SLA** – subnet ID, used by individual organizations to create their own local addressing hierarchy and to identify subnets.
- **Interface ID** - must be unique to the link.

Link Local vs. Site Local

There are two types of local-use unicast addresses defined:

- **Link-Local** - for use on a single link. Routers must not forward any packets with link-local source or destination addresses to other links. Link-Local addresses are designed to be used for addressing on a single link for purposes such as automatic address configuration, neighbor discovery, or when no routers are present.

10 bits	*54 bits*	*64 bits*
1111111010	000…000	**Interface ID**

- **Site-Local** - for addressing inside a site without the need for a global prefix. Routers must not forward any packets with site-local source or destination addresses outside of the site.

10 bits	*54 bits*	*64 bits*
1111111011	**Subnet ID**	**Interface ID**

IPv4 in IPv6 addresses

The IPv6 transition mechanisms include a technique for hosts and routers to tunnel dynamically IPv6 packets over IPv4 routing infrastructure. IPv6 nodes that use this technique are assigned special IPv6 unicast addresses that carry a global IPv4 address in the low-order 32 bits. This type of address is termed an "IPv4-compatible IPv6 address" and has the format:

80 bits	*16 bits*	*32 bits*
000…000	0000	IPv4 address

A second type of IPv6 address that holds an embedded IPv4 address is also defined. This address type is used to represent the addresses of IPv4 nodes as IPv6 addresses. This type of address is termed an "IPv4-mapped IPv6 address" and has the format:

80 bits	*16 bits*	*32 bits*
000…000	FFFF	IPv4 address

Anycast

An IPv6 anycast address is an address that is assigned to more than one interface (typically belonging to different nodes), with the property that a packet sent to an anycast address is routed to the "nearest" interface having that address, according to the routing protocols' calculation. Anycast addresses are allocated from the unicast address space, using any of the defined unicast address formats. Thus, anycast addresses are syntactically indistinguishable from unicast addresses. When a unicast address is assigned to more than one interface, thus turning it into an anycast address, the nodes to which the address is assigned must be explicitly configured to know that it is an anycast address. Its format is as follows:

n bits	*128-n bits*
Subnet prefix	000…000

- **Subnet prefix -** identifies a specific link

Here is the limitation for anycast:

- An anycast address must not be used as the source address of an IPv6 packet.
- An anycast address must not be assigned to an IPv6 host, that is, it may be assigned to an IPv6 router only.

Multicast Addresses

An IPv6 multicast address is an identifier for a group of interfaces (typically on different nodes). An interface may belong to any number of multicast groups. Multicast addresses have the following format:

8 bits	*4 bits*	*4 bits*	*112 bits*
11111111	**Flgs** = 000T	**Scope**	**Group ID**

- **11111111** - identifies the address as being a multicast address.
- **flgs = 000T**

  T = 0 indicates a permanently-assigned ("well-known") multicast address.
  T = 1 indicates a non-permanently-assigned ("transient") multicast address.

- **scope** - limit the scope of the multicast group. The values are:

1	interface-local scope
2	link-local scope
4	admin-local scope
5	site-local scope
8	organization-local scope
E	global scope
0, 3, F	reserved
6, 7, 9 – D	(unassigned)

- **group ID** - identifies the multicast group, either permanent or transient, within the given scope.

IPv6 Packet Header Format

<table>
<tr><td colspan="4">0 1 2 3</td><td colspan="8">4 5 6 7 8 9 0 1</td><td colspan="16">2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</td></tr>
<tr><td colspan="4">Version</td><td colspan="8">Traffic Class</td><td colspan="16">Flow Label</td></tr>
<tr><td colspan="16">Payload Length</td><td colspan="8">Next Header</td><td colspan="8">Hop Limit</td></tr>
<tr><td colspan="32">Source Address</td></tr>
<tr><td colspan="32">Destination Address</td></tr>
<tr><td colspan="8">Next Header</td><td colspan="24">Extension Header Information</td></tr>
<tr><td colspan="8"></td><td colspan="24"></td></tr>
<tr><td colspan="32">Data</td></tr>
</table>

- **Version** – IPv6.
- **Traffic Class** - Similar to the Type of Service field in the IPv4 packet header.
- **Flow Label** - Tags packets with a specific flow that differentiates the packets at the network layer.
- **Payload Length** - Indicates the total length of the data portion of the packet.
- **Next Header** - Determines the type of information following the basic IPv6 header.
- **Hop Limit** - Specifies the maximum number of routers that an IPv6 packet can pass through before the packet is considered invalid.
- **Source Address** - 128-bit source address for IPv6.
- **Destination Address** - 128-bit destination address for IPv6.

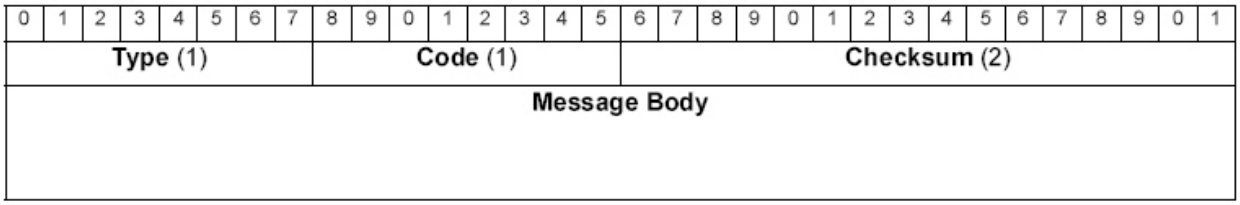
ICMP

ICMPv6 is used by IPv6 nodes to report errors encountered in processing packets and to perform other internet-layer functions. ICMPv6 is an integral part of IPv6 and must be fully implemented by every IPv6 node.

ICMPv6 messages are grouped into two classes: error messages and informational messages. Error messages are identified as such by having a zero in the high-order bit of their message Type field values. Thus, error messages have message Types from 0 to 127; informational messages have message Types from 128 to 255.

- **ICMPv6 error messages**: Destination Unreachable, Packet Too Big, Time Exceeded, and Parameter Problem.
- **ICMPv6 informational messages**: Echo Request and Echo Reply.

Every ICMPv6 message is preceded by an IPv6 header and zero or more IPv6 extension headers. The ICMPv6 header is identified by a Next Header value of 58 in the immediately preceding header. The ICMPv6 messages have the following general format:



- **Type** - The type of the message.
- **Code** - Create an additional level of message granularity.
- **Checksum** - Detect data corruption in the ICMPv6 message and parts of the IPv6 header.

DNS

IPv6 introduces new DNS record types that are supported in the DNS name-to-address and address-to-name lookup processes. The new DNS record types support IPv6 addresses. The DNS Recursive Name Server option provides a list of one or more IPv6 addresses of DNS recursive name servers to which a client's DNS resolver MAY send DNS queries. The DNS servers are listed in the order of preference for use by the client resolver. The Domain Search List option specifies the domain search list the client is to use when resolving hostnames with DNS. This option does not apply to other name resolution mechanisms.

The DNS Recursive Name Server option may be used by an intruder DHCP server to cause DHCP clients to send DNS queries to an intruder DNS recursive name server. The results of these misdirected DNS queries may be used to spoof DNS names. To avoid attacks through the DNS Recursive Name Server option, the DHCP client SHOULD require DHCP authentication before installing a list of DNS recursive name servers obtained through authenticated DHCP.

Support for IPv6.arpa reverse lookups is not in the current release of the Cisco IOS software.

DHCP

A delegating router is provided IPv6 prefixes to be delegated to requesting routers. The delegating router chooses prefix(es) for delegation, and responds with prefix(es) to the requesting router. The requesting router is then responsible for the delegated prefix(es). For example, the requesting router might assign a subnet from a delegated prefix to one of its interfaces, and begin sending router advertisements for the prefix on that link.

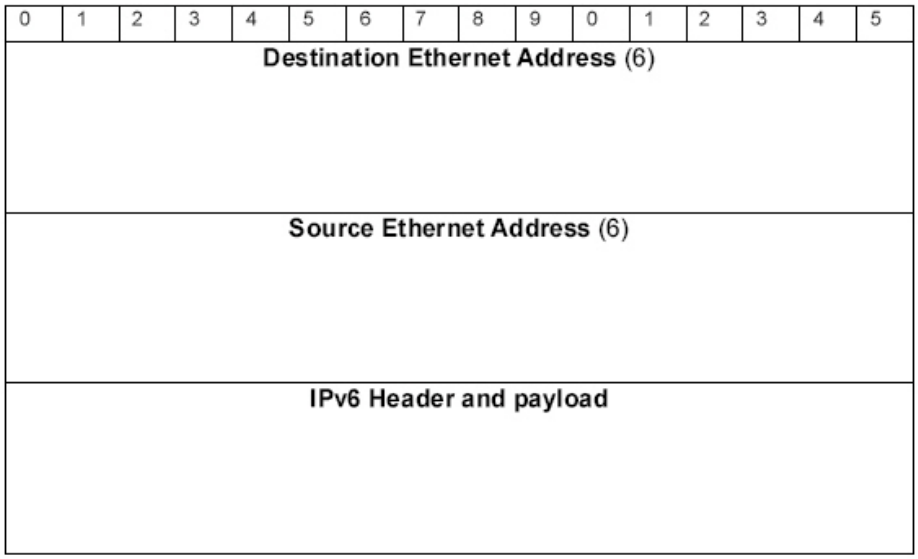
Each prefix has an associated valid and preferred lifetime, which constitutes an agreement about the length of time over which the requesting router is allowed to use the prefix. A requesting router can request an extension of the lifetimes on a delegated prefix and is required to terminate the use of a delegated prefix if the valid lifetime of the prefix expires. This prefix delegation mechanism would be appropriate for use by an ISP to delegate a prefix to a subscriber, where the delegated prefix would possibly be subnetted and assigned to the links within the subscriber's network.

Prefix delegation with DHCP is independent of address assignment with DHCP. A requesting router can use DHCP for just prefix delegation or for prefix delegation along with address assignment and other configuration information.

The DHCP for IPv6 implementation in the Cisco IOS Release 12.3(4)T supports only stateless address assignment, in this case, configuration parameters that do not require a server to maintain any dynamic state for individual clients, such as DNS server addresses and domain search list options. The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed: "Interface is in DHCP client mode," "Interface is in DHCP server mode," or "Interface is in DHCP relay mode."

Ethernet

The default MTU size for IPv6 packets on an Ethernet is 1500 octets. IPv6 packets are transmitted in standard Ethernet frames. The Ethernet header contains the Destination and Source Ethernet addresses and the Ethernet type code, which must contain the value 86DD hexadecimal. The data field contains the IPv6 header followed immediately by the payload, and possibly padding octets to meet the minimum frame size for the Ethernet link.



The Interface Identifier for an Ethernet interface is based on the EUI-64 identifier derived from the interface's built-in 48-bit IEEE 802 address. The OUI of the Ethernet address (the first three octets) becomes the company_id of the EUI-64 (the first three octets). The fourth and fifth octets of the EUI are set to the fixed value FFFE hexadecimal. The last three octets of the Ethernet address become the last three octets of the EUI-64.

The Interface Identifier is then formed from the EUI-64 by complementing the "Universal/Local" (U/L) bit, which is the next-to- lowest order bit of the first octet of the EUI-64. Complementing this bit will generally change a 0 value to a 1, since an interface's built-in address is expected to be from a universally administered address space and hence have a globally unique value. A universally administered IEEE 802 address or an EUI-64 is signified by a 0 in the U/L bit position, while a globally unique IPv6 Interface Identifier is signified by a 1 in the corresponding position. For example, the Interface Identifier for an Ethernet interface whose built-in address is, in hexadecimal, 34-56-78-9A-BC-DE would be 36-56-78-FF-FE-9A-BC-DE.

The IPv6 link-local address for an Ethernet interface is formed by appending the Interface Identifier to the prefix FE80::/64.

10 bits	*54 bits*	*64 bits*
1111111010	**All zero**	**Interface ID**

Frame Relay

In general, Frame Relay devices are configured to have a maximum frame size of at least 1600 octets. Therefore, the default IPv6 MTU size for a Frame Relay interface is considered to be 1592. A smaller than default frame size can be configured, but not smaller than the minimum IPv6 MTU. Although a Frame Relay circuit allows the definition of distinct maximum frame sizes for input and output, for simplification purposes, this specification assumes symmetry, i.e., the same MTU for both input and output.

The encapsulation of data or control messages exchanged by various protocols that use SNAP encapsulation (with their own PIDs) is not affected. The encoding of the IPv6 protocol identifier in such messages MUST be done according to the specifications of those protocols.

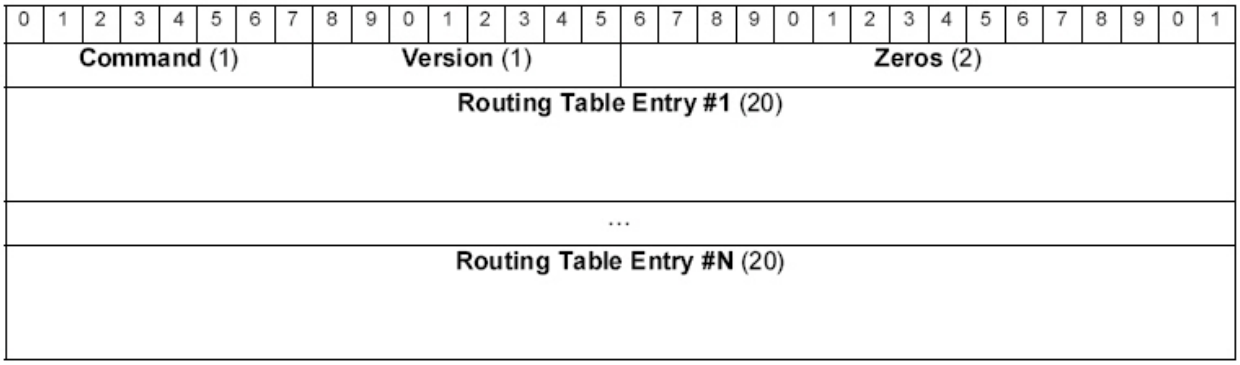
An interface identifier for an IPv6 Frame Relay interface must be unique on a Frame Relay link, and must be unique on each of the virtual links represented by the VCs terminated on the interface. The interface identifier for the Frame Relay interface is locally generated by the IPv6 module.

Given that IPv6 supports multiple address types, and depending on which applications or protocols are configured on a point-to-multipoint interface, you may need to configure multiple explicit mappings between the IPv6 addresses of the interface and the PVC used to reach the addresses. For example, explicitly mapping both the link-local and global IPv6 address of a point-to-multipoint interface to the PVC that the interface terminates ensures that the Interior Gateway Protocol configured on the interface forwards traffic to and from the PVC correctly.

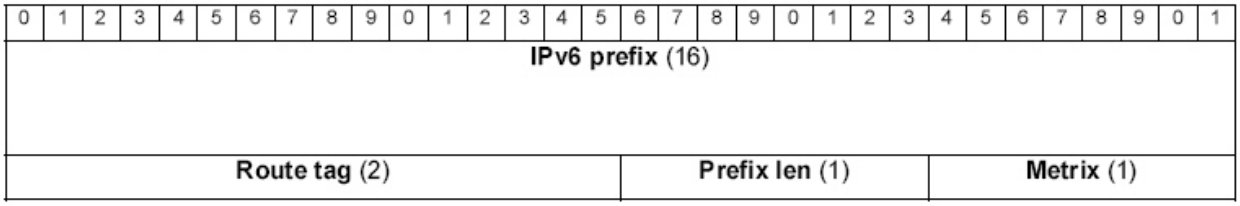
RIP

RIP has been used for routing computations in computer networks since the early days of the ARPANET. RIPng (Routing Information Protocol next generation) uses a class of algorithms known as Distance Vector algorithms. It is intended to allow routers to exchange information for computing routes through an IPv6-based network. RIPng is a distance vector routing protocol and should be implemented only in routers. The RIPng metric of a network is an integer between 1 and 15, inclusive. In addition to the metric, each network will have an IPv6 destination address prefix and prefix length associated with it. These are to be set by the system administrator in a manner not specified in this protocol.

RIPng is a UDP-based protocol. Each router that uses RIPng has a routing process that sends and receives datagrams on UDP port number 521, the RIPng port. All communications intended for another router's RIPng process are sent to the RIPng port. All routing update messages are sent from the RIPng port. The RIPng packet format is:



In addition, each Route Table Entry (RTE) has the following format:



- **Command field** - to specify the purpose of this message, either request or response.
- **RTE** - contains destination prefix, the number of significant bits in the prefix, and the cost to reach that destination (metric).
- **Destination prefix** - the usual 128-bit, IPv6 address prefix stored as 16 octets in network byte order.
- **Route tag field** - an attribute assigned to a route that must be preserved and re-advertised with a route.
- **Prefix length fie**ld - the length in bits of the significant part of the prefix (a value between 0 and 128 inclusive) starting from the left of the prefix.
- **Metric field** - contains a value between 1 and 15 inclusive, or the value 16 (infinity), which indicates that the destination is not reachable.

The distinction between network, subnet, and host routes does not need to be made for RIPng because an IPv6 address prefix is unambiguous. Every 30 seconds, the RIPng process is awakened to send an unsolicited Response message, containing the complete routing table to every neighboring router (subject to the split-horizon rule).

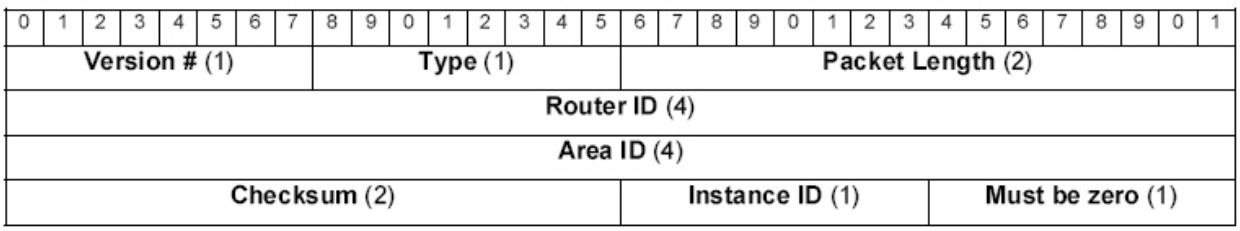
OSPF

Most of the algorithms from OSPF (Open Shortest Path First) for IPv4 have been preserved in OSPF for IPv6. However, some changes have been necessary. Here are some of the key points:

- In OSPF for IPv6, neighboring routers on a given link are always identified by their OSPF Router ID.
- Flooding scope for LSAs has been generalized and is now explicitly coded in the LSA's LS type field. There are now three separate flooding scopes for LSAs: Link-local scope, Area scope, and AS scope.

- IPv6 link-local addresses are for use on a single link, for purposes of neighbor discovery, auto-configuration, etc. IPv6 routers do not forward IPv6 datagrams having link-local source addresses.
- In OSPF for IPv6, authentication has been removed from OSPF itself. All authentication-related fields have been removed from the OSPF area and interface structures. When running over IPv6, OSPF relies on the IP Authentication Header and the IP Encapsulating Security Payload to ensure integrity and authentication/confidentiality of routing exchanges.
- All addressing semantics have been removed from the OSPF packet headers, making it essentially "network-protocol-independent."
- Handling of unknown LSA types has been made more flexible so that, based on LS type, unknown LSA types are either treated as having link-local flooding scope, or are stored and flooded as if they were understood.
- OSPF now supports the ability to run multiple OSPF protocol instances on a single link.
- In OSPF for IPv6, addressing semantics have been removed from the OSPF protocol packets and the main LSA types, leaving a network-protocol-independent core.
- IPv6 uses the term "link" to indicate "a communication facility or medium over which nodes can communicate at the link layer." OSPF for IPv6 runs per-link instead of the IPv4 behavior of per-IP-subnet.

There are five distinct OSPF packet types. All OSPF packet types begin with a standard 16-byte header. The OSPF header contains all the information necessary to determine whether the packet should be accepted for further processing.



- **Version #** - v3.
- **Type** - OSPF packet types (Hello=1; Database Description=2; Link State Request=3; Link State Update=4; Link State Acknowledgment =5).
- **Packet length** - The length of the OSPF protocol packet in bytes.
- **Router ID** - The Router ID of the packet's source.
- **Area ID** - A 32-bit number identifying the area that this packet belongs to.
- **Checksum** - the standard checksum calculation for IPv6 applications.
- **Instance ID** - Enables multiple instances of OSPF to be run over a single link.

BGP

The BGP-4 (Border Gateway Protocol version 4) protocol is mostly independent of the particular Address Family for which the protocol is being used. IPv6 falls under the generic category of protocols for which BGP-4 is suitable and the BGP-4 procedures to apply when using BGP-4 to carry IPv6 reachability information are those defined in BGP-4 and in subsequent documents that extend or update the BGP-4 specification. The most significant difference between IPv6 and IPv4 is the fact that IPv6 introduces scoped unicast addresses and defines particular situations when a particular address scope must be used.

When BGP-4 is used to convey IPv6 reachability information it is necessary to announce a next hop attribute that consists of a global address and a link-local address.

A BGP speaker shall advertise to its peer in the Network Address of Next Hop field the global IPv6 address of the next hop.

A BGP speaker that advertises a route to an internal peer may modify the Network Address of Next Hop field by removing the link-local IPv6 address of the next hop. TCP connections, on top of which BGP-4 messages are exchanged, can be established either over IPv4 or over IPv6. While BGP-4 itself is independent of the particular transport used, it derives implicit configuration information from the address used to establish the peering session. Thus, when using TCP over IPv4 as a transport for IPv6 reachability information, additional explicit configuration of the peer's network address is required. The use of TCP over IPv6 as transport protocol for IPv6 reachability information has the advantage of providing explicit confirmation of IPv6 network reachability between two peers.

The only three pieces of information carried by BGP-4 that are IPv4 specific are: (a) the NEXT_HOP attribute (expressed as an IPv4 address); (b) AGGREGATOR (contains an IPv4 address); and (c) NLRI (expressed as IPv4 address prefixes). Therefore, to enable BGP-4 to support routing for multiple Network Layer protocols the only two things that have to be added to BGP-4 are (a) the ability to associate a particular Network Layer protocol with the next hop information, and (b) the ability to associate a particular Network Layer protocol with NLRI.
A BGP speaker must never advertise an address of a peer to that peer as a next hop, for a route that the speaker is originating. A BGP speaker must never install a route with itself as the next hop. When a BGP speaker advertises the route to an internal peer, the advertising speaker should not modify the next hop information associated with the route. When a BGP speaker receives the route via an internal link, it may forward packets to the next hop address if the address contained in the attribute is on a common subnet with the local and remote BGP speakers.

Mobile IPv6

Mobile IP is implemented by provisioning a home agent on the home subnet on which the mobile node's home address resides. This agent has a security association with the mobile node and accepts updates from the mobile node informing the agent to where the mobile node has roamed. The agent then acts as a proxy for the mobile node, intercepting traffic to the mobile node's home address and tunneling it to the mobile node's current location. Because of the common usage of ingress filtering, the mobile node will reverse tunnel return traffic to the home agent, so that the mobile node source address is always topographically correct. Direct routing is built into Mobile IPv6, and direct routing uses the IPv6 routing header and the IPv6 destination options header. Support for Mobile IPv6 is not in the current release of the Cisco IOS software.

DSCP

Differentiated services are intended to provide a framework and building blocks to enable deployment of scalable service discrimination in the Internet. The differentiated services approach aims to speed deployment by separating the architecture into two major components.

- Packet forwarding is the relatively simple task that needs to be performed on a per-packet basis as quickly as possible. In the packet-forwarding path, differentiated services are realized by mapping the codepoint contained in a field in the IP packet header to a particular forwarding treatment, or per-hop behavior (PHB), at each network node along its path.
- Per-hop behaviors and mechanisms to select them on a per-packet basis can be deployed in network nodes today and it is this aspect of the differentiated services architecture that is being addressed first.

A replacement header field, called the DS field, is defined, which is intended to supersede the existing definitions of the IPv4 TOS octet. Six bits of the DS field are used as a codepoint (DSCP) to select the PHB a packet experiences at each node. A two-bit currently unused (CU) field is reserved. The value of the CU bits is ignored by differentiated services-compliant nodes, when determining the per-hop behavior to apply to a received packet.

Tunneling

Tunneling is a method and generic mechanism by which a packet is encapsulated and carried as payload within an IPv6 packet. The resulting packet is called an IPv6 tunnel packet. The forwarding path between the source and destination of the tunnel packet is called an IPv6 tunnel. The technique is called IPv6 tunneling. This would establish a "virtual link" between two IPv6 nodes for transmitting data packets as payloads of IPv6 packets. From the point of view of the two nodes, this "virtual link," called an IPv6 tunnel, appears as a point-to-point link on which IPv6 acts like a link-layer protocol. The two IPv6 nodes play specific roles. One node encapsulates original packets received from other nodes or from itself and forwards the resulting tunnel packets through the tunnel. The other node decapsulates the received tunnel packets and forwards the resulting original packets towards their destinations, possibly itself. The encapsulator node is called the tunnel entry-point node, and it is the source of the tunnel packets. The decapsulator node is called the tunnel exit-point, and it is the destination of the tunnel packets.

The encapsulation takes place in an IPv6 tunnel entry-point node, as the result of an original packet being forwarded onto the virtual link represented by the tunnel. The original packet is processed during forwarding according to the forwarding rules of the protocol of that packet. The intermediate nodes in the tunnel process the IPv6 tunnel packets according to the IPv6 protocol. Upon receiving an IPv6 packet destined to an IPv6 address of a tunnel exit-point node, its IPv6 protocol layer processes the tunnel headers.

The key to a successful IPv6 transition is compatibility with the large installed base of IPv4 hosts and routers. Maintaining compatibility with IPv4, while deploying IPv6, will streamline the task of transitioning the Internet to IPv6. The mechanisms are designed to be employed by IPv6 hosts and routers that need to interoperate with IPv4 hosts and utilize IPv4 routing infrastructures. We expect that most nodes in the Internet will need such compatibility for a long time to come, and perhaps even indefinitely. Because they support both protocols, IPv6/IPv4 nodes may be configured with both IPv4 and IPv6 addresses. IPv6/IPv4 nodes use IPv4 mechanisms (e.g., DHCP) to acquire their IPv4 addresses, and IPv6 protocol mechanisms (e.g., stateless address autoconfiguration) to acquire their IPv6-native addresses.

In most deployment scenarios, the IPv6 routing infrastructure will be built up over time. While the IPv6 infrastructure is being deployed, the existing IPv4 routing infrastructure can remain functional and can be used to carry IPv6 traffic. Tunneling provides a way to utilize an existing IPv4 routing infrastructure to carry IPv6 traffic. IPv6/IPv4 hosts and routers can tunnel IPv6 datagrams over regions of IPv4 routing topology by encapsulating them within IPv4 packets. Tunneling can be used in a variety of ways:

- **Router-to-Router**. IPv6/IPv4 routers interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans one segment of the end-to-end path that the IPv6 packet takes.
- **Host-to-Router**. IPv6/IPv4 hosts can tunnel IPv6 packets to an intermediary IPv6/IPv4 router that is reachable via an IPv4 infrastructure. This type of tunnel spans the first segment of the packet's end-to-end path.

- **Host-to-Host**. IPv6/IPv4 hosts that are interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans the entire end-to-end path that the packet takes.
- **Router-to-Host**. IPv6/IPv4 routers can tunnel IPv6 packets to their final destination IPv6/IPv4 host. This tunnel spans only the last segment of the end-to-end path.

In the first two tunneling methods listed above – router-to-router and host-to-router – the IPv6 packet is being tunneled to a router. The endpoint of this type of tunnel is an intermediary router, which must decapsulate the IPv6 packet and forward it on to its final destination. When tunneling to a router, the endpoint of the tunnel is different from the destination of the packet being tunneled. So the addresses in the IPv6 packet being tunneled can not provide the IPv4 address of the tunnel endpoint. Instead, the tunnel endpoint address must be determined from configuration information on the node performing the tunneling. We use the term "configured tunneling" to describe the type of tunneling where the endpoint is explicitly configured.

In the last two tunneling methods – host-to-host and router-to-host – the IPv6 packet is tunneled all the way to its final destination. In this case, the destination address of both the IPv6 packet and the encapsulating IPv4 header identify the same node! This fact can be exploited by encoding information in the IPv6 destination address that will allow the encapsulating node to determine tunnel endpoint IPv4 address automatically. Automatic tunneling employs this technique, using a special IPv6 address format with an embedded IPv4 address to allow tunneling nodes to derive automatically the tunnel endpoint IPv4 address. This eliminates the need to explicitly configure the tunnel endpoint address, greatly simplifying configuration.

IPv6-over-IPv4 tunnels are modeled as "single-hop." That is, the IPv6 hop limit is decremented by 1 when an IPv6 packet traverses the tunnel. The single-hop model serves to hide the existence of a tunnel. The tunnel is opaque to users of the network, and is not detectable by network diagnostic tools such as traceroute. The single-hop model is implemented by having the encapsulating and decapsulating nodes process the IPv6 hop limit field as they would if they were forwarding a packet on to any other datalink. That is, they decrement the hop limit by 1 when forwarding an IPv6 packet.

When decapsulating the packet, the IPv6 header is not modified. As part of the decapsulation the node SHOULD silently discard a packet with an invalid IPv4 source address such as a multicast address, a broadcast address, 0.0.0.0, and 127.0.0.1.

IP6to4

Effectively, it treats the wide area IPv4 network as a unicast point-to-point link layer. The mechanism is intended as a start-up transition tool used during the period of co-existence of IPv4 and IPv6. It is not intended as a permanent solution.

This is considered to be an interim solution and requires that sites should migrate when possible to native IPv6 prefixes and native IPv6 connectivity. This will be possible as soon as the site's ISP offers native IPv6 connectivity.

The motivation for this method is to allow isolated IPv6 sites or hosts, attached to a wide area network which has no native IPv6 support, to communicate with other such IPv6 domains or hosts with minimal manual configuration. IPv6 sites or hosts connected using this method do not require IPv4- compatible IPv6 addresses or configured tunnels. In this way, IPv6 gains considerable independence of the underlying wide area network and can step over many hops of IPv4 subnets. The abbreviated name of this mechanism is 6to4.

The 6to4 mechanism is typically implemented almost entirely in border routers, without specific host modifications except a suggested address selection default. Only a modest amount of router configuration is required.

IPv6 packets from a 6to4 site are encapsulated in IPv4 packets when they leave the site via its external IPv4 connection.

IPv6 packets are transmitted in IPv4 packets with an IPv4 protocol type of 41, the same as has been assigned for IPv6 packets that are tunneled inside of IPv4 frames. The IPv4 header contains the Destination and Source IPv4 addresses.

The IPv4 packet body contains the IPv6 header and payload.

Security

IPSec functionality is essentially identical in both IPv6 and IPv4; however, IPSec in IPv6 can be deployed from end-to-end; data may be encrypted along the entire path between a source node and destination node. In IPv6, IPSec is implemented using the authentication extension header and the ESP extension header. The authentication header provides integrity and authentication of the source. It also provides optional protection against replayed packets. The authentication header protects the integrity of most of the IP header fields and authenticates the source through a signature-based algorithm. The ESP header provides confidentiality, authentication of the source, connectionless integrity of the inner packet, anti-replay, and limited traffic flow confidentiality.

Cisco IOS Firewall coexists with Cisco IOS Firewall for IPv4 networks and is supported on all dual-stack routers. In additional to the IPv4 functionality, it will perform IPv6 DoS attack mitigation. These mitigation mechanisms have been implemented in the same fashion as for the current IPv4 implementation, including SYN half-open connections. It also performs the tunneled packet inspection. Tunneled IPv6 packets terminated at a Cisco IOS firewall router can be inspected by the Cisco IOS Firewall for IPv6.

IPv6 Lab Introduction

The following lab has been designed to prepare you for the CCIE™ practical exam. While each of the IPexpert-developed lab scenarios present different challenges, all labs strive to go beyond the normal environments that you may have encountered. It is IPexpert's policy that, to prepare CCIE™ level material, the author must have passed the CCIE™ R&S practical exam. Therefore, all CCIE™ labs offered through IPexpert, Inc. were written, performed, and reviewed by a team of CCIEs.

Each IPexpert lab scenario has been designed around a standard topology. This topology can be rented (online access) at http://www.proctorlabs.com.

You can also discuss these scenarios on the CCIE R&S mailing list located at http://www.online-studylist.com and at the IPexpert online support community: www.certificationtalk.com.

Topics Covered

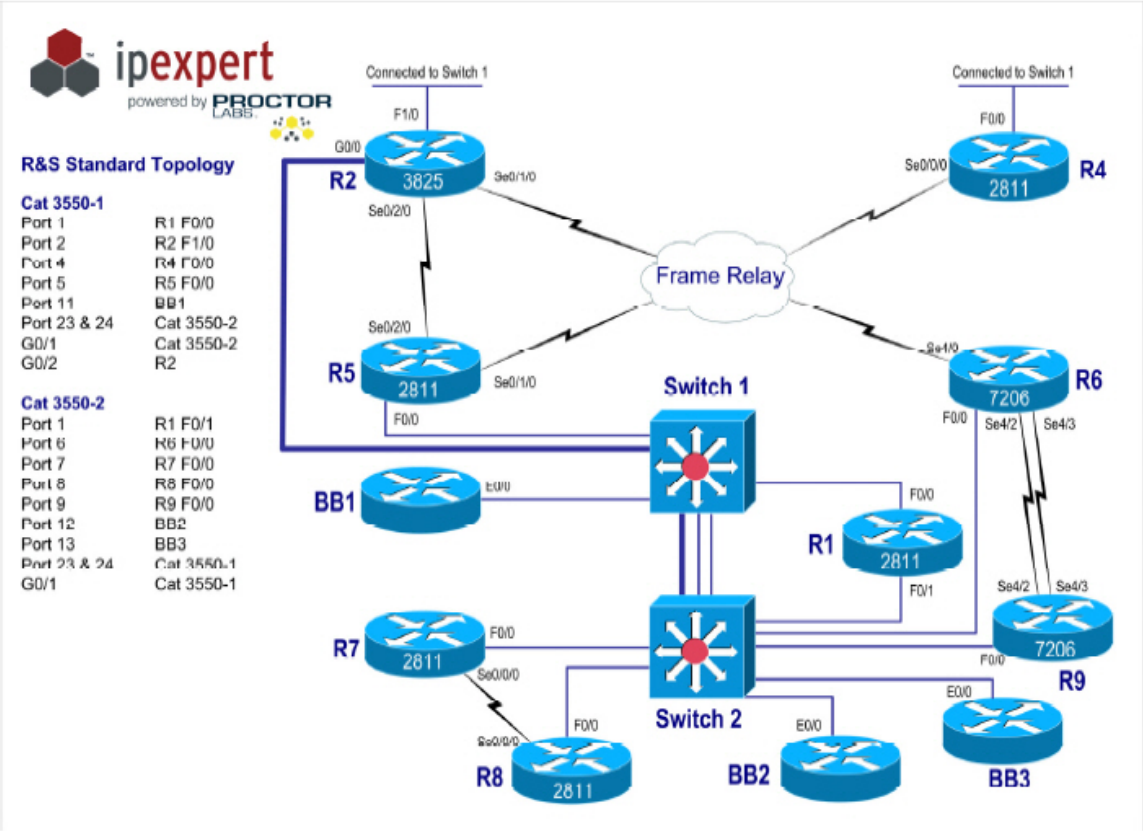
- IPv6 EUI-64 address
- Frame Relay IPv6 mapping
- Static Route
- IPv6 OSPF
- IPv6 RIP
- Redistribution

Average Completion Time: 4 Hours

Technical Support

IPexpert is proud to lead the industry with multiple support options at your disposal free of charge. Our online forums (www.CertificationTalk.com) have attracted a membership of nearly 20,000 of your peers from around the world! At www.OnlineStudyList.com, you may subscribe to multiple "SPAM-free" email lists. Also, if you are an IPexpert Elite Member and need support for your IPexpert products, simply open a support ticket at www.IPexpert.com and it will be addressed promptly. In fact, IPexpert guarantees a response within one business day.

Standard Physical Topology



Addressing Scheme

Router	Interface	IP Address
R2	Loopback0	2001:2222:2222::/64
	Serial0/1/0.24	2001:24:24:0::/64
	Serial0/1/0.256	2001:256:256::/64
R4	Serial0/0/0.24	2001:24:24::/64
	Loopback0	2001:4444:4444::/64
	Loopback1	2001:4411:4411::/64
R5	Loopback0	2001:5555:5555::/64
	Serial0/1/0	2001:256:256::/64
R6	Loopback0	2001:6666:6666::/64
	Serial4/0	2001:256:256::/64

Frame Relay DLCI Assignments

Router	DLCI
R2 to R4	104
R2 to R5	105
R2 to R6	106
R4 to R2	401
R5 to R2	501
R6 to R2	601

IPv6 Lab Configuration Tasks

A. Using an EUI-64 interface ID, configure Loopback address on R2, R4, R5, R6, as indicated in table above.

B. R2's s0/1/0, R5's s0/1/0 and R6's s4/0 are the main FR cloud. Configure multipoint sub-interface on R2's s0/1/0 and use physical interfaces for R5 and R6.

C. Configure a point-to-point sub-interface for the FR connection between R2's s0/1/0 and R4's s0/0/0.

D. Configure a host table on every router with the IPv6 address.

E. Configure a static route for R4 pointing to R5's loopback. Change the administrative distance to 2.

F. Configure OSPF Area 0 for R2's loopback, s0/1/0.256, R5's loopback, s0/1/0, R6's loopback and s4/0. Use x.x.x.x as the router-ID, where x is the router number. For example, R2 should have router-ID as 2.2.2.2.

G. Configure OSPF Area 24 for R2's s0/1/0.24, R4's s0/0/0.24 and loopback 0.

H. Configure RIP for R2's s0/1/0.24, R4's s0/0/0.24 and loopback 1.

I. Redistribute OSPF and RIP into each other. The RIP metric after redistribution should be 7 and the OSPF Type 1 metric should be 1000.

J. Verify connectivity by telneting and pinging different places.

IPv6 Lab Instructor's Comments and Technical Tips

A. To configure an IPv6 address for an interface and enable IPv6 processing on the interface using an EUI-64 interface ID in the low order 64 bits of the address, use the IPv6 address EUI-64 command.

B. The Frame Relay map IPv6 command is similar to the Frame Relay map command, except that it is IPv6-specific. The Frame Relay map defines the logical connection between a specific protocol and address pair and the correct DLCI.

C. None.

D. To define a static host name-to-address mapping in the host name cache, use the IPv6 host command.

E. Use the IPv6 route command to implement static multicast routes in IPv6. The administrative-multicast-distance argument determines the distance that will be used.

F. You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique. The router ID is chosen automatically from among the set of IPv4 addresses configured on the router.

G. None.

H. In IPv4, the network-number router configuration command is used to implicitly specify the interfaces on which to run IPv4 RIP. The IPv6 rip enable command is used to enable IPv6 RIP explicitly on required interfaces. Use the IPv6 router rip command to enable an IPv6 RIP routing process. Configuring this command places the router in router configuration mode for the IPv6 RIP routing process.

I. None.

J. None.

IPv6 Lab Technical Verification

Technical Verification for Task A

Router 2

```
r2#show ipv6 interface brief
GigabitEthernet0/0        [administratively down/down]
    unassigned
GigabitEthernet0/1        [administratively down/down]
    unassigned
BRI0/0/0                  [administratively down/down]
    unassigned
BRI0/0/0:1                [administratively down/down]
    unassigned
BRI0/0/0:2                [administratively down/down]
    unassigned
Serial0/1/0               [up/up]
    unassigned
Serial0/1/0.24            [up/up]
    FE80::211:93FF:FE68:B360
    2001:24:24:0:211:93FF:FE68:B360
Serial0/1/0.256           [up/up]
    FE80::211:93FF:FE68:B360
    2001:256:256:0:211:93FF:FE68:B360
FastEthernet1/0           [administratively down/down]
    unassigned
FastEthernet1/1           [administratively down/down]
    unassigned
FastEthernet1/2           [administratively down/down]
    unassigned
FastEthernet1/3           [administratively down/down]
    unassigned
FastEthernet1/4           [administratively down/down]
    unassigned
FastEthernet1/5           [administratively down/down]
    unassigned
FastEthernet1/6           [administratively down/down]
    unassigned
FastEthernet1/7           [administratively down/down]
    unassigned
FastEthernet1/8           [administratively down/down]
    unassigned
FastEthernet1/9           [administratively down/down]
    unassigned
FastEthernet1/10          [administratively down/down]
    unassigned
FastEthernet1/11          [administratively down/down]
    unassigned
FastEthernet1/12          [administratively down/down]
    unassigned
FastEthernet1/13          [administratively down/down]
    unassigned
FastEthernet1/14          [administratively down/down]
    unassigned
FastEthernet1/15          [administratively down/down]
    unassigned
Vlan1                     [up/down]
    unassigned
Loopback0                 [up/up]
    FE80::211:93FF:FE68:B360
    2001:2222:2222:0:211:93FF:FE68:B360
```

```
r2#show ipv6 interface s0/1/0.24
Serial0/1/0.24 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::211:93FF:FE68:B360
  Global unicast address(es):
    2001:24:24:0:211:93FF:FE68:B360, subnet is 2001:24:24::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::9
    FF02::1:FF68:B360
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  Hosts use stateless autoconfig for addresses.

r2#show ipv6 interface s0/1/0.256
Serial0/1/0.256 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::211:93FF:FE68:B360
  Global unicast address(es):
    2001:256:256:0:211:93FF:FE68:B360, subnet is 2001:256:256::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::1:FF68:B360
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is not supported
  ND reachable time is 30000 milliseconds
  Hosts use stateless autoconfig for addresses.

r2#show ipv6 traffic
IPv6 statistics:
  Rcvd:  16324 total, 16307 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  10527 generated, 10 forwarded
         0 fragmented into 0 fragments, 0 failed
         6 encapsulation failed, 0 no route, 0 too big
  Mcast: 16092 received, 10178 sent

ICMP statistics:
  Rcvd: 12 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 5 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 0 neighbor advert
  Sent: 9 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        5 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        2 neighbor solicit, 2 neighbor advert
```

```
UDP statistics:
  Rcvd: 2145 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 2147 output

TCP statistics:
  Rcvd: 22 input, 0 checksum errors
  Sent: 27 output, 0 retransmitted
```

Router 4

```
r4#show ipv6 interface brief
FastEthernet0/0          [administratively down/down]
    unassigned
FastEthernet0/1          [administratively down/down]
    unassigned
Serial0/0/0              [up/up]
    unassigned
Serial0/0/0.24           [up/up]
    FE80::20F:35FF:FE2D:8409
    2001:24:24:0:20F:35FF:FE2D:8409
Loopback0                [up/up]
    FE80::20F:35FF:FE2D:8409
    2001:4444:4444:0:20F:35FF:FE2D:8409
Loopback1                [up/up]
    FE80::20F:35FF:FE2D:8409
    2001:4411:4411:0:20F:35FF:FE2D:8409

r4#show ipv6 interface s0/0/0.24
Serial0/0/0.24 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20F:35FF:FE2D:8409
  Global unicast address(es):
    2001:24:24:0:20F:35FF:FE2D:8409, subnet is 2001:24:24::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::9
    FF02::1:FF2D:8409
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  Hosts use stateless autoconfig for addresses.

r4#show ipv6 traffic
IPv6 statistics:
  Rcvd:  10391 total, 10378 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  10405 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         3 encapsulation failed, 0 no route, 0 too big
  Mcast: 10386 received, 10400 sent
```

```
ICMP statistics:
  Rcvd: 18 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 5 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 0 neighbor advert
  Sent: 9 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        5 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        2 neighbor solicit, 2 neighbor advert

UDP statistics:
  Rcvd: 4318 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 4317 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

Router 5

```
r5#show ipv6 interface brief
FastEthernet0/0          [administratively down/down]
    unassigned
FastEthernet0/1          [administratively down/down]
    unassigned
BRI0/0/0                 [administratively down/down]
    unassigned
BRI0/0/0:1               [administratively down/down]
    unassigned
BRI0/0/0:2               [administratively down/down]
    unassigned
Serial0/1/0              [up/up]
    FE80::20F:35FF:FE2D:5B21
    2001:256:256:0:20F:35FF:FE2D:5B21
Loopback0                [up/up]
    FE80::20F:35FF:FE2D:5B21
    2001:5555:5555:0:20F:35FF:FE2D:5B21

r5#show ipv6 interface s0/1/0
Serial0/1/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20F:35FF:FE2D:5B21
  Global unicast address(es):
    2001:256:256:0:20F:35FF:FE2D:5B21, subnet is 2001:256:256::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::1:FF2D:5B21
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is not supported
  ND reachable time is 30000 milliseconds
  Hosts use stateless autoconfig for addresses.
```

```
r5#show ipv6 traffic
IPv6 statistics:
  Rcvd:  4206 total, 4199 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  2143 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         2 encapsulation failed, 0 no route, 0 too big
  Mcast: 4009 received, 2013 sent

ICMP statistics:
  Rcvd: 17 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout, 0 too big
        10 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 0 neighbor advert
  Sent: 10 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout, 0 too big
        0 echo request, 10 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 0 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output

TCP statistics:
  Rcvd: 27 input, 0 checksum errors
  Sent: 22 output, 0 retransmitted
```

Router 6

```
r6#show ipv6 interface brief
FastEthernet0/0          [administratively down/down]
    unassigned
ATM1/0                   [administratively down/down]
    unassigned
FastEthernet2/0          [administratively down/down]
    unassigned
Serial4/0                [up/up]
    FE80::250:73FF:FED0:DD00
    2001:256:256:0:250:73FF:FED0:DD00
Serial4/1                [administratively down/down]
    unassigned
Serial4/2                [administratively down/down]
    unassigned
Serial4/3                [administratively down/down]
    unassigned
Virtual-Access1          [up/up]
    unassigned
Loopback0                [up/up]
    FE80::250:73FF:FED0:DD00
    2001:6666:6666:0:250:73FF:FED0:DD00
```

```
r6#show ipv6 interface s4/0
Serial4/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::250:73FF:FED0:DD00
  Global unicast address(es):
    2001:256:256:0:250:73FF:FED0:DD00, subnet is 2001:256:256::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::6
    FF02::1:FFD0:DD00
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is not supported
  ND reachable time is 30000 milliseconds
  Hosts use stateless autoconfig for addresses.

r6#show ipv6 traffic
IPv6 statistics:
  Rcvd:  4164 total, 4164 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  2102 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         2 encapsulation failed, 0 no route, 0 too big
  Mcast: 4006 received, 2004 sent

ICMP statistics:
  Rcvd: 2 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout, 0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 2 neighbor advert
  Sent: 2 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout, 0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 4 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

Technical Verification for Task G

Router 2

```
r2#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
6.6.6.6           1   FULL/  -        00:01:36    6               Serial0/1/0.256
5.5.5.5           1   FULL/  -        00:01:50    9               Serial0/1/0.256
4.4.4.4           1   FULL/  -        00:00:39    12              Serial0/1/0.24

r2#show ipv6 ospf interface
Serial0/1/0.256 is up, line protocol is up
  Link Local Address FE80::211:93FF:FE68:B360, Interface ID 33
  Area 0, Process ID 7, Instance ID 0, Router ID 2.2.2.2
  Network Type POINT_TO_MULTIPOINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    Hello due in 00:00:08
  Index 1/2/3, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 6
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 6.6.6.6
    Adjacent with neighbor 5.5.5.5
  Suppress hello for 0 neighbor(s)
Loopback0 is up, line protocol is up
  Link Local Address FE80::211:93FF:FE68:B360, Interface ID 31
  Area 0, Process ID 7, Instance ID 0, Router ID 2.2.2.2
  Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
Serial0/1/0.24 is up, line protocol is up
  Link Local Address FE80::211:93FF:FE68:B360, Interface ID 32
  Area 24, Process ID 7, Instance ID 0, Router ID 2.2.2.2
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 1/1/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 10, maximum is 10
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 4.4.4.4
  Suppress hello for 0 neighbor(s)

r2#show ipv6 ospf database

        OSPFv3 Router with ID (2.2.2.2) (Process ID 7)

            Router Link States (Area 0)

ADV Router      Age         Seq#       Fragment ID  Link count  Bits
2.2.2.2         1451        0x80000020 0            2           EB
5.5.5.5         1221        0x8000001F 0            1           None
6.6.6.6         1231        0x8000001F 0            1           None

            Inter Area Prefix Link States (Area 0)

ADV Router      Age         Seq#       Prefix
2.2.2.2         1451        0x8000001E 2001:24:24::/64
2.2.2.2         1451        0x8000001E 2001:4444:4444:0:20F:35FF:FE2D:8409/128

            Link (Type-8) Link States (Area 0)
```

```
ADV Router      Age       Seq#       Link ID   Interface
2.2.2.2         1451      0x8000001E 33        Se0/1/0.256
5.5.5.5         1221      0x8000001E 9         Se0/1/0.256
6.6.6.6         1231      0x8000001E 6         Se0/1/0.256
2.2.2.2         1451      0x8000001E 31        Lo0

            Intra Area Prefix Link States (Area 0)

ADV Router      Age       Seq#       Link ID   Ref-lstype  Ref-LSID
2.2.2.2         1451      0x8000001E 0         0x2001      0
5.5.5.5         1222      0x8000001E 0         0x2001      0
6.6.6.6         1232      0x8000001E 0         0x2001      0

            Router Link States (Area 24)

ADV Router      Age       Seq#       Fragment ID  Link count  Bits
2.2.2.2         1452      0x8000001F 0            1           EB
4.4.4.4         1391      0x8000001F 0            1           None

            Inter Area Prefix Link States (Area 24)

ADV Router      Age       Seq#       Prefix
2.2.2.2         1454      0x8000001E 2001:256:256:0:211:93FF:FE68:B360/128
2.2.2.2         1454      0x8000001E 2001:2222:2222:0:211:93FF:FE68:B360/128
2.2.2.2         1454      0x8000001E 2001:256:256:0:20F:35FF:FE2D:5B21/128
2.2.2.2         1454      0x8000001E 2001:5555:5555:0:20F:35FF:FE2D:5B21/128
2.2.2.2         1454      0x8000001E 2001:256:256:0:250:73FF:FED0:DD00/128
2.2.2.2         1454      0x8000001E 2001:6666:6666:0:250:73FF:FED0:DD00/128

            Link (Type-8) Link States (Area 24)

ADV Router      Age       Seq#       Link ID   Interface
2.2.2.2         1454      0x8000001F 32        Se0/1/0.24
4.4.4.4         1391      0x8000001F 12        Se0/1/0.24

            Intra Area Prefix Link States (Area 24)

ADV Router      Age       Seq#       Link ID   Ref-lstype  Ref-LSID
2.2.2.2         1454      0x8000001E 0         0x2001      0
4.4.4.4         1392      0x8000001F 0         0x2001      0

            Type-5 AS External Link States

ADV Router      Age       Seq#       Prefix
2.2.2.2         1455      0x8000001E 2001:4411:4411::/64
```

Router 4

```
r4#show ipv6 ospf  neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
2.2.2.2           1   FULL/  -        00:00:34    32              Serial0/0/0.24
```

```
r4#show ipv6 ospf interface
Serial0/0/0.24 is up, line protocol is up
  Link Local Address FE80::20F:35FF:FE2D:8409, Interface ID 12
  Area 24, Process ID 7, Instance ID 0, Router ID 4.4.4.4
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 3, maximum is 3
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
Loopback0 is up, line protocol is up
  Link Local Address FE80::20F:35FF:FE2D:8409, Interface ID 10
  Area 24, Process ID 7, Instance ID 0, Router ID 4.4.4.4
  Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host

r4#show ipv6 ospf database

            OSPFv3 Router with ID (4.4.4.4) (Process ID 7)

                Router Link States (Area 24)

ADV Router      Age         Seq#       Fragment ID  Link count  Bits
2.2.2.2         1762        0x8000001F  0           1           EB
4.4.4.4         1698        0x8000001F  0           1           None

                Inter Area Prefix Link States (Area 24)

ADV Router      Age         Seq#       Prefix
2.2.2.2         1762        0x8000001E  2001:256:256:0:211:93FF:FE68:B360/128
2.2.2.2         1762        0x8000001E  2001:2222:2222:0:211:93FF:FE68:B360/128
2.2.2.2         1762        0x8000001E  2001:256:256:0:20F:35FF:FE2D:5B21/128
2.2.2.2         1762        0x8000001E  2001:5555:5555:0:20F:35FF:FE2D:5B21/128
2.2.2.2         1762        0x8000001E  2001:256:256:0:250:73FF:FED0:DD00/128
2.2.2.2         1762        0x8000001E  2001:6666:6666:0:250:73FF:FED0:DD00/128

                Link (Type-8) Link States (Area 24)

ADV Router      Age         Seq#       Link ID    Interface
2.2.2.2         1762        0x8000001F  32        Se0/0/0.24
4.4.4.4         1699        0x8000001F  12        Se0/0/0.24
4.4.4.4         1699        0x8000001E  10        Lo0

                Intra Area Prefix Link States (Area 24)

ADV Router      Age         Seq#       Link ID    Ref-lstype  Ref-LSID
2.2.2.2         1763        0x8000001E  0         0x2001      0
4.4.4.4         1699        0x8000001F  0         0x2001      0

                Type-5 AS External Link States

ADV Router      Age         Seq#       Prefix
2.2.2.2         1763        0x8000001E  2001:4411:4411::/64
```

Router 5

```
r5#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
2.2.2.2           1   FULL/  -        00:01:55    33              Serial0/1/0

r5#show ipv6 ospf interface
Serial0/1/0 is up, line protocol is up
  Link Local Address FE80::20F:35FF:FE2D:5B21, Interface ID 9
  Area 0, Process ID 7, Instance ID 0, Router ID 5.5.5.5
  Network Type POINT_TO_MULTIPOINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    Hello due in 00:00:23
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 3, maximum is 3
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
Loopback0 is up, line protocol is up
  Link Local Address FE80::20F:35FF:FE2D:5B21, Interface ID 13
  Area 0, Process ID 7, Instance ID 0, Router ID 5.5.5.5
  Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host

r5#show ipv6 ospf database

            OSPFv3 Router with ID (5.5.5.5) (Process ID 7)

                Router Link States (Area 0)

ADV Router      Age         Seq#       Fragment ID  Link count  Bits
2.2.2.2         1947        0x80000020 0            2           EB
5.5.5.5         1716        0x8000001F 0            1           None
6.6.6.6         1727        0x8000001F 0            1           None

                Inter Area Prefix Link States (Area 0)

ADV Router      Age         Seq#       Prefix
2.2.2.2         1947        0x8000001E 2001:24:24::/64
2.2.2.2         1947        0x8000001E 2001:4444:4444:0:20F:35FF:FE2D:8409/128

                Link (Type-8) Link States (Area 0)

ADV Router      Age         Seq#       Link ID    Interface
2.2.2.2         1947        0x8000001E 33         Se0/1/0
5.5.5.5         1716        0x8000001E 9          Se0/1/0
6.6.6.6         1727        0x8000001E 6          Se0/1/0
5.5.5.5         1716        0x8000001E 13         Lo0

                Intra Area Prefix Link States (Area 0)

ADV Router      Age         Seq#       Link ID    Ref-lstype  Ref-LSID
2.2.2.2         1947        0x8000001E 0          0x2001      0
5.5.5.5         1717        0x8000001E 0          0x2001      0
6.6.6.6         1728        0x8000001E 0          0x2001      0

                Type-5 AS External Link States

ADV Router      Age         Seq#       Prefix
2.2.2.2         1948        0x8000001E 2001:4411:4411::/64
```

Router 6

```
r6#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
2.2.2.2           1   FULL/  -        00:01:36    33              Serial4/0

r6#show ipv6 ospf interface
Serial4/0 is up, line protocol is up
  Link Local Address FE80::250:73FF:FED0:DD00, Interface ID 6
  Area 0, Process ID 7, Instance ID 0, Router ID 6.6.6.6
  Network Type POINT_TO_MULTIPOINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    Hello due in 00:00:24
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 3, maximum is 3
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
Loopback0 is up, line protocol is up
  Link Local Address FE80::250:73FF:FED0:DD00, Interface ID 13
  Area 0, Process ID 7, Instance ID 0, Router ID 6.6.6.6
  Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host

r6#show ipv6 ospf database

            OSPFv3 Router with ID (6.6.6.6) (Process ID 7)

                Router Link States (Area 0)

ADV Router      Age         Seq#       Fragment ID  Link count  Bits
2.2.2.2         35          0x80000021 0            2           EB
5.5.5.5         1825        0x8000001F 0            1           None
6.6.6.6         1832        0x8000001F 0            1           None

                Inter Area Prefix Link States (Area 0)

ADV Router      Age         Seq#       Prefix
2.2.2.2         35          0x8000001F 2001:24:24::/64
2.2.2.2         35          0x8000001F 2001:4444:4444:0:20F:35FF:FE2D:8409/128

                Link (Type-8) Link States (Area 0)

ADV Router      Age         Seq#       Link ID    Interface
2.2.2.2         35          0x8000001F 33         Se4/0
6.6.6.6         1832        0x8000001E 6          Se4/0
6.6.6.6         1832        0x8000001E 13         Lo0

                Intra Area Prefix Link States (Area 0)

ADV Router      Age         Seq#       Link ID    Ref-lstype  Ref-LSID
2.2.2.2         35          0x8000001F 0          0x2001      0
5.5.5.5         1826        0x8000001E 0          0x2001      0
6.6.6.6         1833        0x8000001E 0          0x2001      0

                Type-5 AS External Link States

ADV Router      Age         Seq#       Prefix
2.2.2.2         36          0x8000001F 2001:4411:4411::/64
```

Technical Verification for Task H

Router 2

```
r2#show ipv6 rip
RIP process "abcd", port 521, multicast-group FF02::9, pid 231
    Administrative distance is 120. Maximum paths is 16
    Updates every 30 seconds, expire after 180
    Holddown lasts 0 seconds, garbage collect after 120
    Split horizon is on; poison reverse is off
    Default routes are not generated
    Periodic updates 2147, trigger updates 5
  Interfaces:
    Serial0/1/0.24
  Redistribution:
    Redistributing protocol ospf 7 with metric 7

r2#show ipv6 rip database
RIP process "abcd", local RIB
 2001:24:24::/64, metric 2
     Serial0/1/0.24/FE80::20F:35FF:FE2D:8409, expires in 174 secs
 2001:4411:4411::/64, metric 2, installed
     Serial0/1/0.24/FE80::20F:35FF:FE2D:8409, expires in 174 secs

r2#show ipv6 rip next-hops
 RIP process "abcd", Next Hops
  FE80::20F:35FF:FE2D:8409/Serial0/1/0.24 [2 paths]
```

Router 4

```
r4#show ipv6 rip
RIP process "abcd", port 521, multicast-group FF02::9, pid 209
    Administrative distance is 120. Maximum paths is 16
    Updates every 30 seconds, expire after 180
    Holddown lasts 0 seconds, garbage collect after 120
    Split horizon is on; poison reverse is off
    Default routes are not generated
    Periodic updates 2159, trigger updates 1
  Interfaces:
    Serial0/0/0.24
    Loopback1
  Redistribution:
    None

r4#show ipv6 rip  database
RIP process "abcd", local RIB
 2001:24:24::/64, metric 2
     Serial0/0/0.24/FE80::211:93FF:FE68:B360, expires in 179 secs
 2001:256:256:0:20F:35FF:FE2D:5B21/128, metric 8
     Serial0/0/0.24/FE80::211:93FF:FE68:B360, expires in 179 secs
 2001:256:256:0:250:73FF:FED0:DD00/128, metric 8
     Serial0/0/0.24/FE80::211:93FF:FE68:B360, expires in 179 secs
 2001:4444:4444:0:20F:35FF:FE2D:8409/128, metric 8
     Serial0/0/0.24/FE80::211:93FF:FE68:B360, expires in 179 secs
 2001:5555:5555:0:20F:35FF:FE2D:5B21/128, metric 8
     Serial0/0/0.24/FE80::211:93FF:FE68:B360, expires in 179 secs
 2001:6666:6666:0:250:73FF:FED0:DD00/128, metric 8
     Serial0/0/0.24/FE80::211:93FF:FE68:B360, expires in 179 secs

r4#show ipv6 rip next-hops
 RIP process "abcd", Next Hops
  FE80::211:93FF:FE68:B360/Serial0/0/0.24 [6 paths]
```

Technical Verification for Task I

Router 2

```
r2#show ipv6 route
IPv6 Routing Table - 14 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2001:24:24::/64 [0/0]
     via ::, Serial0/1/0.24
L   2001:24:24:0:211:93FF:FE68:B360/128 [0/0]
     via ::, Serial0/1/0.24
C   2001:256:256::/64 [0/0]
     via ::, Serial0/1/0.256
O   2001:256:256:0:20F:35FF:FE2D:5B21/128 [110/64]
     via FE80::20F:35FF:FE2D:5B21, Serial0/1/0.256
L   2001:256:256:0:211:93FF:FE68:B360/128 [0/0]
     via ::, Serial0/1/0.256
O   2001:256:256:0:250:73FF:FED0:DD00/128 [110/64]
     via FE80::250:73FF:FED0:DD00, Serial0/1/0.256
C   2001:2222:2222::/64 [0/0]
     via ::, Loopback0
L   2001:2222:2222:0:211:93FF:FE68:B360/128 [0/0]
     via ::, Loopback0
R   2001:4411:4411::/64 [120/2]
     via FE80::20F:35FF:FE2D:8409, Serial0/1/0.24
O   2001:4444:4444:0:20F:35FF:FE2D:8409/128 [110/64]
     via FE80::20F:35FF:FE2D:8409, Serial0/1/0.24
O   2001:5555:5555:0:20F:35FF:FE2D:5B21/128 [110/64]
     via FE80::20F:35FF:FE2D:5B21, Serial0/1/0.256
O   2001:6666:6666:0:250:73FF:FED0:DD00/128 [110/64]
     via FE80::250:73FF:FED0:DD00, Serial0/1/0.256
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

Router 4

```
r4# show ipv6 route
IPv6 Routing Table - 14 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2001:24:24::/64 [0/0]
     via ::, Serial0/0/0.24
L   2001:24:24:0:20F:35FF:FE2D:8409/128 [0/0]
     via ::, Serial0/0/0.24
OI  2001:256:256:0:20F:35FF:FE2D:5B21/128 [110/128]
     via FE80::211:93FF:FE68:B360, Serial0/0/0.24
OI  2001:256:256:0:211:93FF:FE68:B360/128 [110/64]
     via FE80::211:93FF:FE68:B360, Serial0/0/0.24
OI  2001:256:256:0:250:73FF:FED0:DD00/128 [110/128]
     via FE80::211:93FF:FE68:B360, Serial0/0/0.24
OI  2001:2222:2222:0:211:93FF:FE68:B360/128 [110/64]
     via FE80::211:93FF:FE68:B360, Serial0/0/0.24
C   2001:4411:4411::/64 [0/0]
     via ::, Loopback1
L   2001:4411:4411:0:20F:35FF:FE2D:8409/128 [0/0]
     via ::, Loopback1
C   2001:4444:4444::/64 [0/0]
     via ::, Loopback0
L   2001:4444:4444:0:20F:35FF:FE2D:8409/128 [0/0]
     via ::, Loopback0
```

```
S   2001:5555:5555:0:20F:35FF:FE2D:5B21/128 [2/0]
     via ::, Serial0/0/0.24
OI  2001:6666:6666:0:250:73FF:FED0:DD00/128 [110/128]
     via FE80::211:93FF:FE68:B360, Serial0/0/0.24
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

Router 5

```
r5#show ipv6 route
IPv6 Routing Table - 13 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OI  2001:24:24::/64 [110/128]
     via FE80::211:93FF:FE68:B360, Serial0/1/0
C   2001:256:256::/64 [0/0]
     via ::, Serial0/1/0
L   2001:256:256:0:20F:35FF:FE2D:5B21/128 [0/0]
     via ::, Serial0/1/0
O   2001:256:256:0:211:93FF:FE68:B360/128 [110/64]
     via FE80::211:93FF:FE68:B360, Serial0/1/0
O   2001:256:256:0:250:73FF:FED0:DD00/128 [110/128]
     via FE80::211:93FF:FE68:B360, Serial0/1/0
O   2001:2222:2222:0:211:93FF:FE68:B360/128 [110/64]
     via FE80::211:93FF:FE68:B360, Serial0/1/0
OE1  2001:4411:4411::/64 [110/1064]
     via FE80::211:93FF:FE68:B360, Serial0/1/0
OI  2001:4444:4444:0:20F:35FF:FE2D:8409/128 [110/128]
     via FE80::211:93FF:FE68:B360, Serial0/1/0
C   2001:5555:5555::/64 [0/0]
     via ::, Loopback0
L   2001:5555:5555:0:20F:35FF:FE2D:5B21/128 [0/0]
     via ::, Loopback0
O   2001:6666:6666:0:250:73FF:FED0:DD00/128 [110/128]
     via FE80::211:93FF:FE68:B360, Serial0/1/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

Router 6

```
r6#show ipv6 route
IPv6 Routing Table - 13 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
OI  2001:24:24::/64 [110/128]
     via FE80::211:93FF:FE68:B360, Serial4/0
C   2001:256:256::/64 [0/0]
     via ::, Serial4/0
O   2001:256:256:0:20F:35FF:FE2D:5B21/128 [110/128]
     via FE80::211:93FF:FE68:B360, Serial4/0
O   2001:256:256:0:211:93FF:FE68:B360/128 [110/64]
     via FE80::211:93FF:FE68:B360, Serial4/0
L   2001:256:256:0:250:73FF:FED0:DD00/128 [0/0]
     via ::, Serial4/0
O   2001:2222:2222:0:211:93FF:FE68:B360/128 [110/64]
     via FE80::211:93FF:FE68:B360, Serial4/0
OE1  2001:4411:4411::/64 [110/1064]
     via FE80::211:93FF:FE68:B360, Serial4/0
OI  2001:4444:4444:0:20F:35FF:FE2D:8409/128 [110/128]
     via FE80::211:93FF:FE68:B360, Serial4/0
```

```
O   2001:5555:5555:0:20F:35FF:FE2D:5B21/128 [110/128]
     via FE80::211:93FF:FE68:B360, Serial4/0
C   2001:6666:6666::/64 [0/0]
     via ::, Loopback0
L   2001:6666:6666:0:250:73FF:FED0:DD00/128 [0/0]
     via ::, Loopback0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

IPv6 Lab Configuration Verification

NOTE: Only relevant portions of the configuration have been included.

Router 2

```
R2#sh run

ipv6 unicast-routing
ipv6 host r2s 2001:256:256:0:211:93FF:FE68:B360
ipv6 host r2s2 2001:24:24:0:211:93FF:FE68:B360
ipv6 host r2l 2001:2222:2222:0:211:93FF:FE68:B360
ipv6 host r4s2 2001:24:24:0:20F:35FF:FE2D:8409
ipv6 host r4l 2001:4444:4444:0:20F:35FF:FE2D:8409
ipv6 host r5s 2001:256:256:0:20F:35FF:FE2D:5B21
ipv6 host r5l 2001:5555:5555:0:20F:35FF:FE2D:5B21
ipv6 host r6s 2001:256:256:0:250:73FF:FED0:DD00
ipv6 host r6l 2001:6666:6666:0:250:73FF:FED0:DD00
ipv6 host r4l2 2001:4411:4411:0:20F:35FF:FE2D:8409

interface Loopback0
 no ip address
 ipv6 address 2001:2222:2222::/64 eui-64
 ipv6 ospf 7 area 0

interface Serial0/1/0
 no ip address
 encapsulation Frame Relay

interface Serial0/1/0.24 point-to-point
 ipv6 address 2001:24:24::/64 eui-64
 ipv6 rip abcd enable
 ipv6 ospf network point-to-point
 ipv6 ospf 7 area 24
 Frame Relay interface-dlci 104

interface Serial0/1/0.256 multipoint
 ipv6 address 2001:256:256::/64 eui-64
 ipv6 ospf network point-to-multipoint
 ipv6 ospf 7 area 0
 Frame Relay map ipv6 2001:256:256:0:250:73FF:FED0:DD00 206 broadcast
 Frame Relay map ipv6 FE80::20F:35FF:FE2D:5B21 105 broadcast
 Frame Relay map ipv6 FE80::250:73FF:FED0:DD00 206 broadcast
 Frame Relay map ipv6 2001:256:256:0:20F:35FF:FE2D:5B21 105 broadcast
 Frame Relay interface-dlci 105
 Frame Relay interface-dlci 106

ipv6 router ospf 7
 router-id 2.2.2.2
 log-adjacency-changes
 redistribute rip abcd metric 1000 metric-type 1

ipv6 router rip abcd
 redistribute ospf 7 metric 7
```

Router 4

```
R4#sh run

ipv6 unicast-routing
ipv6 host r2s 2001:256:256:0:211:93FF:FE68:B360
ipv6 host r2s2 2001:24:24:0:211:93FF:FE68:B360
ipv6 host r2l 2001:2222:2222:0:211:93FF:FE68:B360
ipv6 host r4s2 2001:24:24:0:20F:35FF:FE2D:8409
ipv6 host r4l 2001:4444:4444:0:20F:35FF:FE2D:8409
ipv6 host r5s 2001:256:256:0:20F:35FF:FE2D:5B21
ipv6 host r5l 2001:5555:5555:0:20F:35FF:FE2D:5B21
ipv6 host r6s 2001:256:256:0:250:73FF:FED0:DD00
ipv6 host r6l 2001:6666:6666:0:250:73FF:FED0:DD00
ipv6 host r4l2 2001:4411:4411:0:20F:35FF:FE2D:8409

interface Loopback0
 no ip address
 ipv6 address 2001:4444:4444::/64 eui-64
 ipv6 ospf 7 area 24

interface Loopback1
 no ip address
 ipv6 address 2001:4411:4411::/64 eui-64
 ipv6 rip abcd enable

interface Serial0/0/0
 no ip address
 encapsulation Frame Relay IETF

interface Serial0/0/0.24 point-to-point
 ipv6 address 2001:24:24::/64 eui-64
 ipv6 rip abcd enable
 ipv6 ospf network point-to-point
 ipv6 ospf 7 area 24
 Frame Relay interface-dlci 401

ipv6 route 2001:5555:5555:0:20F:35FF:FE2D:5B21/128 Serial0/0/0.24 2
ipv6 router ospf 7
 router-id 4.4.4.4
 log-adjacency-changes

ipv6 router rip abcd
```

Router 5

```
R5#sh run

ipv6 unicast-routing
ipv6 host r2s 2001:256:256:0:211:93FF:FE68:B360
ipv6 host r2s2 2001:24:24:0:211:93FF:FE68:B360
ipv6 host r2l 2001:2222:2222:0:211:93FF:FE68:B360
ipv6 host r4s2 2001:24:24:0:20F:35FF:FE2D:8409
ipv6 host r4l 2001:4444:4444:0:20F:35FF:FE2D:8409
ipv6 host r5s 2001:256:256:0:20F:35FF:FE2D:5B21
ipv6 host r5l 2001:5555:5555:0:20F:35FF:FE2D:5B21
ipv6 host r6s 2001:256:256:0:250:73FF:FED0:DD00
ipv6 host r6l 2001:6666:6666:0:250:73FF:FED0:DD00
ipv6 host r4l2 2001:4411:4411:0:20F:35FF:FE2D:8409

interface Loopback0
 no ip address
 ipv6 address 2001:5555:5555::/64 eui-64
 ipv6 ospf 7 area 0
```

```
interface Serial0/1/0
 no ip address
 encapsulation Frame Relay
 ipv6 address 2001:256:256::/64 eui-64
 ipv6 ospf network point-to-multipoint
 ipv6 ospf 7 area 0
 Frame Relay map ipv6 FE80::211:93FF:FE68:B360 501 broadcast
 Frame Relay map ipv6 2001:256:256:0:211:93FF:FE68:B360 501 broadcast

ipv6 router ospf 7
 router-id 5.5.5.5
 log-adjacency-changes
```

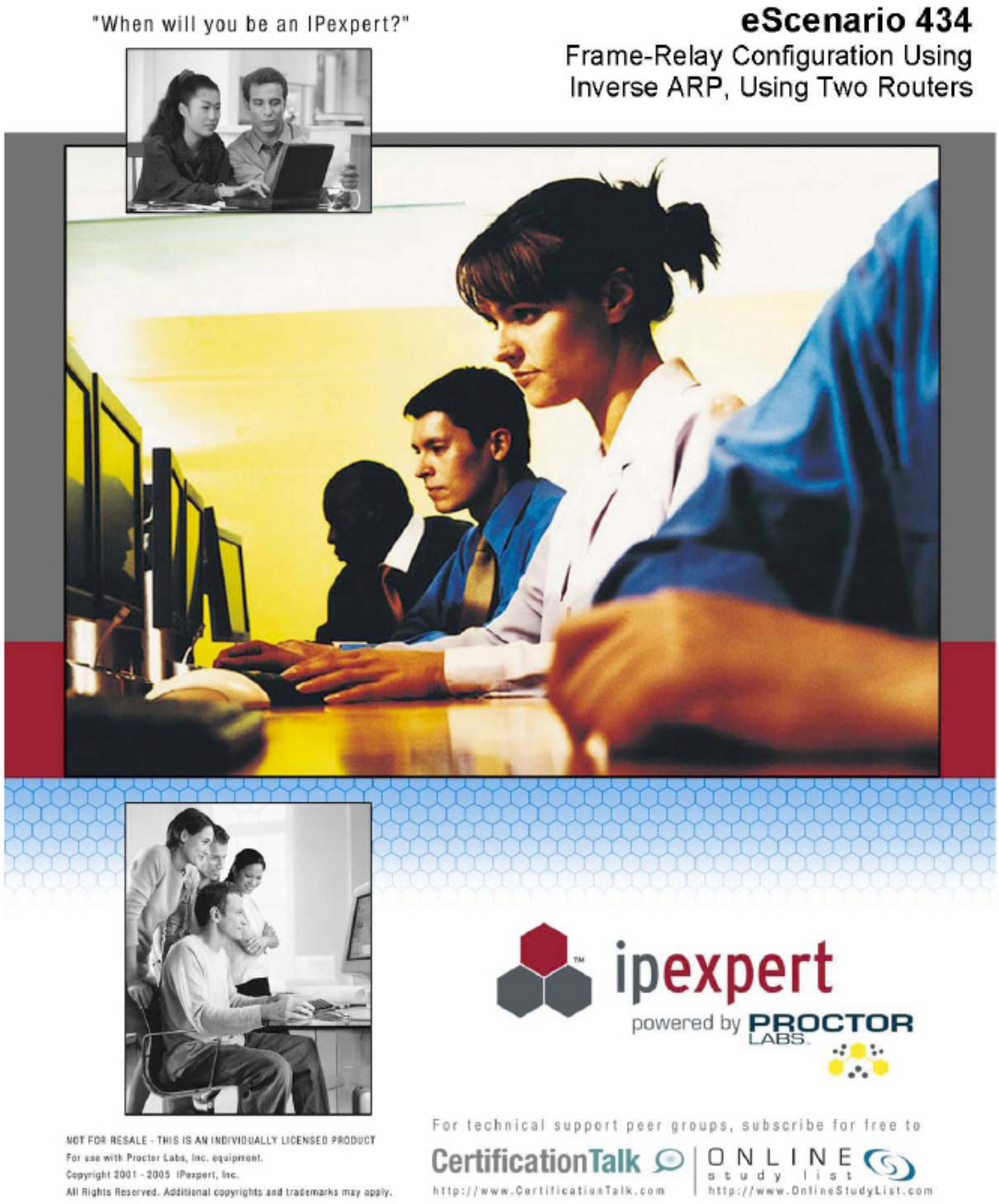
Router 6

```
R6#sh run

ipv6 unicast-routing
ipv6 host r2s 2001:256:256:0:211:93FF:FE68:B360
ipv6 host r2s2 2001:24:24:0:211:93FF:FE68:B360
ipv6 host r2l 2001:2222:2222:0:211:93FF:FE68:B360
ipv6 host r4s2 2001:24:24:0:20F:35FF:FE2D:8409
ipv6 host r4l 2001:4444:4444:0:20F:35FF:FE2D:8409
ipv6 host r5s 2001:256:256:0:20F:35FF:FE2D:5B21
ipv6 host r5l 2001:5555:5555:0:20F:35FF:FE2D:5B21
ipv6 host r6s 2001:256:256:0:250:73FF:FED0:DD00
ipv6 host r6l 2001:6666:6666:0:250:73FF:FED0:DD00
ipv6 host r4l2 2001:4411:4411:0:20F:35FF:FE2D:8409

interface Loopback0
 ipv6 address 2001:6666:6666::/64 eui-64
 ipv6 ospf 7 area 0

interface Serial4/0
 no ip address
 encapsulation Frame Relay
 ipv6 address 2001:256:256::/64 eui-64
 ipv6 ospf network point-to-multipoint
 ipv6 ospf 7 area 0
 Frame Relay map ipv6 FE80::211:93FF:FE68:B360 601 broadcast
 Frame Relay map ipv6 2001:256:256:0:211:93FF:FE68:B360 601 broadcast

ipv6 router ospf 7
 router-id 6.6.6.6
 log-adjacency-changes
```

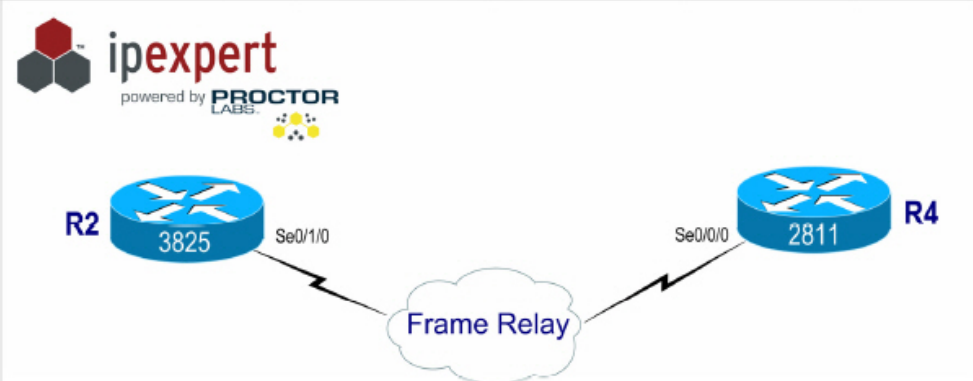
Appendix C: Bonus Lab | Sample V3 IPexpert eScenario

As an IPexpert Gold, Platinum, or Elite Member, you will be given access to over 80 completely updated / new (meeting the January 1, 2006 CCIE lab blue print) virtual lab e-Scenarios (LEARNING LABS) for the CCIE Routing & Switching, Voice, Security and Service Provider Lab Exams. Each virtual lab e-Scenario has been developed around a standard topology consisting of 2800 and 3800 series routers running 12.3 / 12.4 mainline, providing you with an in-depth look into various technical topics (protocol / technology-focused). Our developers, all whom are CCIE and / or CCSI certified, have purposely written these e-Scenarios to be utilized as a self-paced teaching tool. These e-Scenarios are not easy, however they are the starting point for all of our CCIE candidates (per our recommendation / self-paced product path). Each lab will take an average completion time of 1 to 4 hours and provide an unlimited amount of technical challenges that will assist you in mastering all of the necessary topics outlined on the CCIE lab exam blueprint(s). All e-Scenarios are written utilizing the same format providing our customers with a standard look and feel within each electronic document. Within each document you will have to complete various technical tasks, these tasks will be outlined within the eScenario document AND you will also have access to a flash-based walk-through for each eScenario – essentially you will have a CCIE-level instructor walking you through the completion of the scenario! The flash-based walk-through will eliminate any doubts you may have – and ensure that you fully understand how to accomplish the lab scenario. An average of 10 new eScenarios will be added monthly with CCIE Voice and Service Provider eScenarios to be added within the next 30 to 60 days.

For more information regarding IPexpert's eScenario Membership Programs, please visit www.IPexpert.com.



eScenario 434 – Frame-Relay Configuration Using Inverse ARP, Using Two Routers



eScenario 434 Diagram

Scenario Overview

Configure the two routers connected to the frame-relay using inverse-arp; this configuration is known to be a multipoint configuration which is an important issue to remember when configuring routing protocols.

Frame-Switch Configuration

➔ **NOTE: You do NOT need to configure the Frame-Relay Switch, this device is already configured in a full mesh manner, and therefore every lab will work.**

DLCI Assignment

From	To	DLCI
R2	R4	104
R2	R5	105
R2	R6	106
R4	R2	401
R4	R5	405
R4	R6	406
R5	R2	501
R5	R4	504
R5	R6	506
R6	R2	601
R6	R4	604
R6	R5	605

Configuring the Routers

R2

```
en
conf t
host r2

int s0/1/0
 ip address 150.50.24.2 255.255.255.0
 encap frame-relay
```

R4

```
en
conf t
host r4

int s0/0/0
 ip address 150.50.24.4 255.255.255.0
 encap frame-relay
```

Enable the Frame-Relay Interface on Both Routers

R2

```
int s0/1/0
 no shut
```

R4

```
int s0/0/0
 no shut
```

➔ **NOTE: It is a good idea to do the "no shutdown" commands after the configuration for the serial interface is completed, so when inverse-arp goes out to get the IP address, one is defined.**

Ping Your Partner's IP Address

➔ You should be successful, if you are not successful, there are a couple of options that can be performed, one option is to reset the frame-relay inverse-arp by entering "clear frame-relay inarp" command in privilege mode, but if this does not help then the only other choice to get inverse-arp to work is to reboot one or both routers.

➔ **NOTE: inverse-arp is not the best solution.**

Ping Your Own Frame-Relay Interface

➔ **NOTE: This does not work because there is no frame-relay mapping for this address, in order for ping or any communication to work, there must be a frame-relay mapping for the destination IP address even if it's local to the router. In order for the routers to ping their own IP address, enter the following command on both routers:**

R2

```
interface s0/1/0
 frame-relay map ip 150.50.24.2 104
```

R4

```
interface s0/0/0
 frame-relay map ip 150.50.24.4 401
```

➔ Now you should be able to ping your own Frame-Relay's IP address.

➔ Enter the following commands to check Layer 1 connectivity to the Frame-relay cloud:

```
sh frame-relay lmi
```

➔ **NOTE: The Status Enq. Sent and Status Msgs Rcvd numbers are the only ones that are changing. The LMIs are sent every 10 seconds. These are also known as Keepalives.**

➔ Enter the following commands to check Layer 2 connectivity to the Frame-relay cloud:

```
sh frame-relay pvc
```

➔ Note your Local DLCI number and its status.

➔ Enter the following commands to check Layer 2 to Layer 3 mapping for the Frame-relay connection:

```
sh frame-relay map
```

➔ **Note: It automatically maps your local DLCI number to the remote router's IP address with the broadcast option; this option is useful for routing protocols.**

IMPORTANT:

You should never have a combination of dynamic and static Frame-Relay mappings in the Frame-Relay mapping table, even though the configuration will work—if the routers are reloaded, only the Frame-Relay static mapping/s will remain in the table. The reason for this behavior is because when a static frame-relay mapping is configured, inverse-arp is disabled for that specific protocol for the given interface.

If you are in a situation like this, you should shutdown the interface and then create a static frame-relay mapping for every dynamic frame-relay mapping, you can also create the static mappings for all the dynamic frame-relay maps in the notepad, and then copy and paste after entering "clear frame-relay inarp" command.
