

## ***Copyright Information***

---

Copyright © 2009 Internetwork Expert, Inc. All rights reserved.

The following publication, CCNP Lab Workbook, was developed by Internetwork Expert, Inc. All rights reserved. No part of this publication may be reproduced or distributed in any form or by any means without the prior written permission of Internetwork Expert, Inc.

Cisco®, Cisco® Systems, CCNP, and Cisco Certified Network Professional, are registered trademarks of Cisco® Systems, Inc. and/or its affiliates in the U.S. and certain countries.

All other products and company names are the trademarks, registered trademarks, and service marks of the respective owners. Throughout this manual, Internetwork Expert, Inc. has used its best efforts to distinguish proprietary trademarks from descriptive names by following the capitalization styles used by the manufacturer.

***Disclaimer***

---

The following publication, CCNP Lab Workbook, is designed to assist candidates in the preparation for Cisco Systems' CCNP certification exams. While every effort has been made to ensure that all material is as complete and accurate as possible, the enclosed material is presented on an "as is" basis. Neither the authors nor Internetwork Expert, Inc. assume any liability or responsibility to any person or entity with respect to loss or damages incurred from the information contained in this workbook.

This workbook was developed by Internetwork Expert, Inc. and is an original work of the aforementioned authors. Any similarities between material presented in this workbook and actual CCNP exam material is completely coincidental.

# Table of Contents

About This Workbook .....	1
How To Use This Workbook.....	2
Hardware Requirements.....	3
Physical Devices Specification.....	3
Physical WAN Cabling .....	4
Physical LAN Cabling.....	5
Software Versions .....	6
Purchasing Equipment .....	7
Online Rack Rentals.....	8
Dynamips, Dynagen, & GNS3 .....	9
Initial Configurations .....	10
Support Resources.....	10
<b>Building Cisco Multilayered Switched Networks (BCMSN) .....</b>	<b>11</b>
Case Study Overview .....	11
DBM Inc. Campus Diagram.....	12
1.1 VLANs .....	13
1.2 Access Ports .....	14
1.3 ISL Trunk Ports .....	15
1.4 802.1Q Trunk Ports .....	15
1.5 Controlling Traffic over Trunk Ports.....	16
1.6 VLAN Trunk Protocol (VTP) .....	16
1.7 VTP Pruning.....	17
1.8 VTP Transparent Mode.....	17
1.9 Spanning-Tree Protocol.....	18
1.10 Rapid PVST+.....	18
1.11 Multiple Spanning-Tree Protocol .....	19
1.12 Spanning-Tree Protocol Features .....	19
1.13 EtherChannel .....	20
1.14 Inter-VLAN Routing .....	21
1.15 Port Security.....	22
1.16 802.1X Authentication .....	22
1.17 VLAN Access Lists .....	23
1.18 DHCP Snooping & DAI.....	23
1.19 Private VLANs .....	23
DBM Inc. Gateway Redundancy Diagram .....	24
1.20 HSRP .....	25
1.21 VRRP .....	26
1.22 GLBP .....	26
<b>BCMSN Solutions.....</b>	<b>27</b>
1.1 VLANs .....	27
1.2 Access Ports .....	29
1.3 ISL Trunk Ports .....	33

1.4	802.1Q Trunk Ports .....	38
1.5	Controlling Traffic over Trunk Ports .....	42
1.6	VLAN Trunk Protocol (VTP) .....	43
1.7	VTP Pruning .....	47
1.8	VTP Transparent Mode .....	51
1.9	Spanning-Tree Protocol.....	53
1.10	Rapid PVST+.....	57
1.11	Multiple Spanning-Tree Protocol .....	61
1.12	Spanning-Tree Protocol Features .....	65
1.13	EtherChannel .....	67
1.14	Inter-VLAN Routing .....	73
1.15	Port Security.....	77
1.16	802.1X Authentication .....	79
1.17	VLAN Access Lists .....	81
1.18	DHCP Snooping & DAI.....	83
1.19	Private VLANs .....	85
1.20	HSRP .....	87
1.21	VRRP .....	91
1.22	GLBP .....	95
<b>Building Scalable Cisco Internetworks (BSCI).....</b>		<b>101</b>
	Case Study Overview .....	101
	DBM Inc. EIGRP Diagram .....	102
2.1	Basic EIGRP .....	103
2.2	EIGRP Security .....	103
2.3	EIGRP Convergence Optimization .....	104
2.4	EIGRP Load Balancing.....	104
2.5	EIGRP Summarization .....	104
2.6	EIGRP Default Routing.....	105
2.7	EIGRP Stub Routing.....	105
	DBM Inc. OSPF Diagram .....	106
3.1	Single Area OSPF .....	107
3.2	Multi-Area OSPF .....	108
3.3	OSPF Optimization.....	109
3.4	OSPF Security.....	109
3.5	OSPF Redundancy.....	109
3.6	OSPF Path Selection.....	110
3.7	OSPF Summarization.....	110
3.8	OSPF Stub Areas.....	110
	DBM Inc. IS-IS Diagram .....	111
4.1	Level-2 IS-IS.....	112
4.2	Level-1 IS-IS.....	113
4.3	IS-IS Optimization.....	113
4.4	IS-IS Security .....	113
4.5	IS-IS Path Selection .....	114
4.6	IS-IS Summarization.....	114

DBM Inc. BGP Diagram.....	115
5.1 iBGP Peerings.....	116
5.2 EBGP Peerings.....	117
5.3 BGP NLRI Advertisements.....	117
5.4 BGP Aggregation.....	117
5.5 Outbound BGP Path Selection.....	118
5.6 Inbound BGP Path Selection.....	118
DBM Inc. Multicast Diagram.....	119
6.1 PIM.....	120
6.2 Multicast Testing.....	120
DBM Inc. IPv6 Diagram.....	121
7.1 IPv6 Addressing.....	122
7.2 IPv6 OSPFv3 Routing.....	122
<b>BSCI Solutions.....</b>	<b>123</b>
2.1 Basic EIGRP.....	123
2.2 EIGRP Security.....	127
2.3 EIGRP Convergence Optimization.....	132
2.4 EIGRP Load Balancing.....	135
2.5 EIGRP Summarization.....	137
2.6 EIGRP Default Routing.....	138
2.7 EIGRP Stub Routing.....	139
3.1 Single Area OSPF.....	142
3.2 Multi-Area OSPF.....	153
3.3 OSPF Optimization.....	166
3.4 OSPF Security.....	174
3.5 OSPF Redundancy.....	178
3.6 OSPF Path Selection.....	182
3.7 OSPF Summarization.....	185
3.8 OSPF Stub Areas.....	187
4.1 Level-2 IS-IS.....	192
4.2 Level-1 IS-IS.....	197
4.3 IS-IS Optimization.....	201
4.4 IS-IS Security.....	204
4.5 IS-IS Path Selection.....	206
4.6 IS-IS Summarization.....	209
5.1 iBGP Peerings.....	211
5.2 EBGP Peerings.....	213
5.3 BGP NLRI Advertisements.....	217
5.4 BGP Aggregation.....	219
5.5 Outbound BGP Path Selection.....	221
5.6 Inbound BGP Path Selection.....	222
6.1 PIM.....	223
6.2 Multicast Testing.....	229
7.1 IPv6 Addressing.....	230
7.2 IPv6 OSPFv3 Routing.....	233

Implementing Secure Converged Wide-Area Networks (ISCW) & Optimizing Converged Cisco Networks (ONT) ..... 237

- Case Study Overview ..... 237
- DBM Inc. VPN Diagram ..... 238
  - 8.1 Site-to-Site VPN ..... 239
  - 8.2 Site-to-Site GRE over IPsec VPN ..... 240
  - 8.3 Easy VPN ..... 240
  - 8.4 One-Step Lockdown ..... 241
  - 8.5 IOS Firewall ..... 241
  - 9.1 Layer 2 AutoQoS ..... 241
  - 9.2 Layer 3 AutoQoS ..... 241
- ISCW & ONT Solutions ..... 242
  - 8.1 Site-to-Site VPN ..... 242
  - 8.2 Site-to-Site GRE over IPsec VPN ..... 253
  - 8.3 Easy VPN ..... 266
  - 8.4 One-Step Lockdown ..... 277
  - 8.5 IOS Firewall ..... 282
  - 9.1 Layer 2 AutoQoS ..... 291
  - 9.2 Layer 3 AutoQoS ..... 292

## About This Workbook

Internetwork Expert's CCNP Lab Workbook is designed to be used as a supplement to INE's CCNP Bootcamp Class-on-Demand, the ultimate all-in-one solution for engineers pursuing the Cisco Certified Network Professional.

Developed from the ground up by Brian Dennis, 5 x CCIE #2210 (Routing & Switching, ISP Dial, Security, Service Provider, Voice) and Brian McGahan, 3 x CCIE #8593 (Routing & Switching, Service Provider, Security), this Class-on-Demand series includes more than 50 hours of instructor-led videos, and uses INE's tried and true hands-on learning approach. This unique method of delivery allows you to not only learn how advanced networking technologies work in real-world design scenarios, but to also see live Cisco IOS command line and SDM GUI examples of how to configure, verify, and troubleshoot them.

Keeping in theme with the Class-on-Demand methodology, the goal of this workbook is to not only prepare you for the hands-on portions of the CCNP BCMSN, BSCI, ISCW, and ONT exams, but to also learn how and why these technologies are implemented in a real world network design.



### **For More Information**

For more information on INE's CCNP Bootcamp Class-on-Demand, along with our other training programs, visit us on the web at <http://www.INE.com> or call toll free 877-224-8987, +1-775-826-4344 outside the US. We are also available via live chat through our website and e-mail at [sales@INE.com](mailto:sales@INE.com)

## How To Use This Workbook

The exercises in this workbook are presented in the form of fictitious case studies in which you have been hired by Dexter Bean Manufacturing Inc. (DBM Inc.) to implement a new network design according to their business needs. Specifically, these exercises are subdivided into two portions, the actual case study questions, followed by the solutions.

The case study questions portion presents various design and implementation problems that must be solved in order to meet the client's requirements. Many of these problems are typical of what you might see in a real-world network design, and attempt to illustrate the "why" behind the chosen solutions.

The solutions portion presents the actual IOS CLI and SDM based configurations needed to solve the client's requirements. This section also includes detailed verification and troubleshooting procedures illustrated through various "show" and "debug" commands supported by the Cisco IOS. This portion attempts to illustrate how a structured approach to implementation, verification, and troubleshooting can be developed, which is vital in a real-world network design to ensure that the network is performing per its design specifications.

In order to complete these hands-on exercises, you must have access to Cisco IOS based routers and switches to perform the configurations. Access to these devices can be acquired through equipment purchased for a home or office based lab, through online rack rentals, or through virtualization software such as Dynamips/Dynagen/GNS3. The following section, *Hardware Requirements*, outlines these needs in detail.

## Hardware Requirements

The hardware topology used for INE's CCNP Lab Workbook is a slightly modified version of INE's CCIE Routing & Switching Lab Workbook (IEWB-RS) Hardware Specification. This specification includes six routers with FastEthernet and Serial interfaces, four Layer 3 IOS based Catalyst switches, a Frame Relay switch, and an optional Terminal Server. Using this specification ensures that all relevant technologies and features tested on in the various CCNP exams can be illustrated live on the equipment.

### Note

For the most updated version of INE's CCIE Routing & Switching Lab Workbook Hardware Specification, visit <http://www.INE.com/topology.htm>.

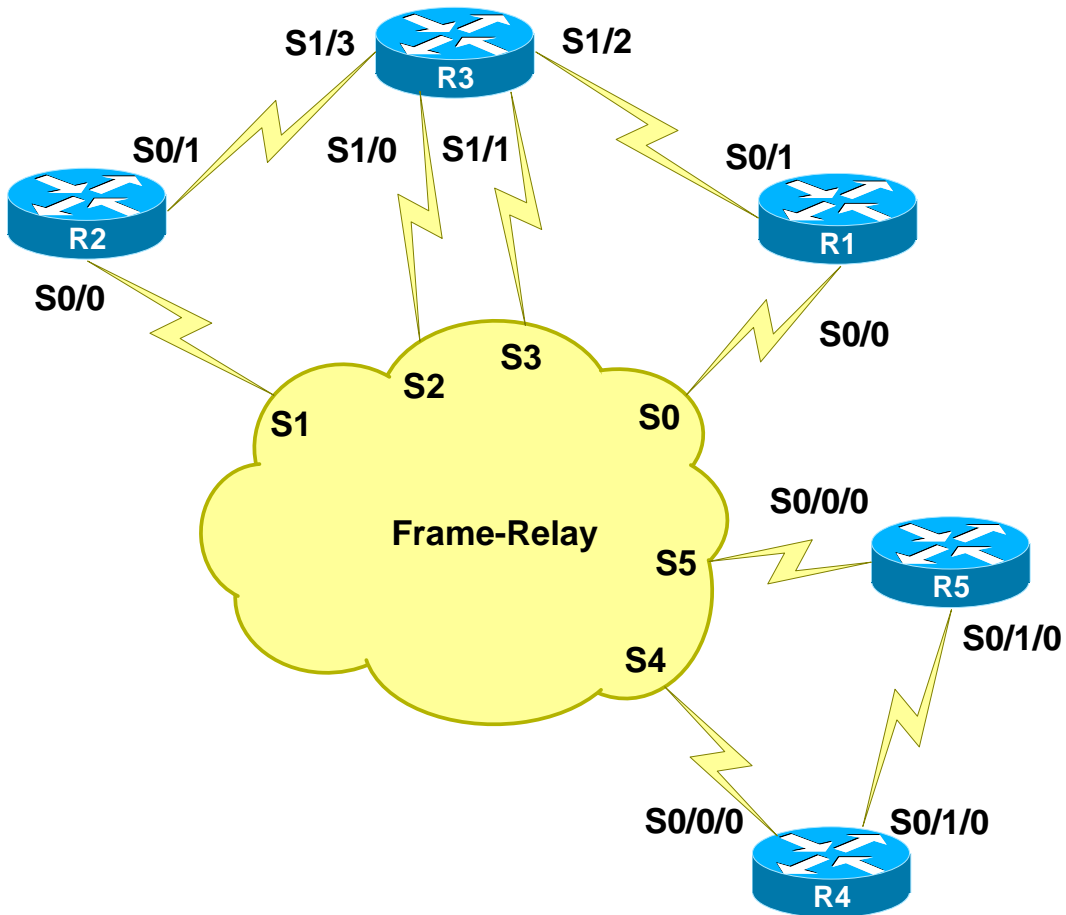
## Physical Devices Specification

The physical platforms, their modules, and memory requirements are as follows.

Device	Platform	DRAM	Flash	Installed WICs / Modules
R1	2610XM	128	32	2 - WIC-1T
R2	2610XM	128	32	2 - WIC-1T
R3	2611XM	128	32	1 - NM-4A/S
R6	1841	256	64	2 - WIC-1T
R6	1841	256	64	2 - WIC-1T
R6	1841	256	64	N/A
SW1	3560-24TS-E	Default	Default	N/A
SW2	3560-24TS-E	Default	Default	N/A
SW3	3550-24-EMI	Default	Default	N/A
SW4	3550-24-EMI	Default	Default	N/A
Frame Relay Switch	2522	16	16	N/A
Terminal Server	2511	16	16	N/A

## Physical WAN Cabling

The physical Serial cabling used is as follows. Note that the Frame Relay Switch will be preconfigured, and requires no user intervention once initially setup. Refer to the *Initial Configurations* section for more information.



## Physical LAN Cabling

The physical Ethernet cabling used is as follows. Note that the Catalyst 3550 series switches do not support the Auto MDIX feature, which means that the Category 5 (or equivalent) cables used should be wired for crossover for all inter-switch links between the 3550's.

Ethernet Connections			
Local Device	Local Interface	Remote Device	Remote Interface
R1	Fa0/0	SW1	Fa0/1
R2	Fa0/0	SW2	Fa0/2
R3	Fa0/0	SW1	Fa0/3
R3	Fa0/1	SW3	Fa0/3
R4	Fa0/0	SW2	Fa0/4
R4	Fa0/1	SW4	Fa0/4
R5	Fa0/0	SW1	Fa0/5
R5	Fa0/1	SW3	Fa0/5
R6	Fa0/0	SW2	Fa0/6
R6	Fa0/1	SW4	Fa0/6
SW1	Fa0/1	R1	Fa0/0
SW1	Fa0/3	R3	Fa0/0
SW1	Fa0/5	R5	Fa0/0
SW2	Fa0/2	R2	Fa0/0
SW2	Fa0/4	R4	Fa0/0
SW2	Fa0/6	R6	Fa0/0
SW3	Fa0/3	R3	Fa0/1
SW3	Fa0/5	R5	Fa0/1
SW4	Fa0/4	R4	Fa0/1
SW4	Fa0/6	R6	Fa0/1

Switch to Switch Connections			
Local Switch	Local Interface	Remote Switch	Remote Interface
SW1	Fa0/13	SW2	Fa0/13
SW1	Fa0/14	SW2	Fa0/14
SW1	Fa0/15	SW2	Fa0/15
SW1	Fa0/16	SW3	Fa0/13
SW1	Fa0/17	SW3	Fa0/14
SW1	Fa0/18	SW3	Fa0/15
SW1	Fa0/19	SW4	Fa0/13
SW1	Fa0/20	SW4	Fa0/14
SW1	Fa0/21	SW4	Fa0/15
Local Switch	Local Interface	Remote Switch	Remote Interface
SW2	Fa0/13	SW1	Fa0/13
SW2	Fa0/14	SW1	Fa0/14
SW2	Fa0/15	SW1	Fa0/15
SW2	Fa0/16	SW3	Fa0/16
SW2	Fa0/17	SW3	Fa0/17
SW2	Fa0/18	SW3	Fa0/18
SW2	Fa0/19	SW4	Fa0/16
SW2	Fa0/20	SW4	Fa0/17
SW2	Fa0/21	SW4	Fa0/18
Local Switch	Local Interface	Remote Switch	Remote Interface
SW3	Fa0/13	SW1	Fa0/16
SW3	Fa0/14	SW1	Fa0/17
SW3	Fa0/15	SW1	Fa0/18
SW3	Fa0/16	SW2	Fa0/16
SW3	Fa0/17	SW2	Fa0/17
SW3	Fa0/18	SW2	Fa0/18
SW3	Fa0/19	SW4	Fa0/19
SW3	Fa0/20	SW4	Fa0/20
SW3	Fa0/21	SW4	Fa0/21
Local Switch	Local Interface	Remote Switch	Remote Interface
SW4	Fa0/13	SW1	Fa0/19
SW4	Fa0/14	SW1	Fa0/20
SW4	Fa0/15	SW1	Fa0/21
SW4	Fa0/16	SW2	Fa0/19
SW4	Fa0/17	SW2	Fa0/20
SW4	Fa0/18	SW2	Fa0/21
SW4	Fa0/19	SW3	Fa0/19
SW4	Fa0/20	SW3	Fa0/20
SW4	Fa0/21	SW3	Fa0/21

## Software Versions

The IOS software versions used are as follows. Note that some of these revisions may be deferred and unavailable if you attempt to download them from [www.cisco.com](http://www.cisco.com). In that case, choose the next or closest revision that is available for download.

Device	Software Version	Software Feature Set	Filename
R1	12.4(10)A	Advanced Enterprise Services	c2600-adventerprisek9-mz.124-10a.bin
R2	12.4(10)A	Advanced Enterprise Services	c2600-adventerprisek9-mz.124-10a.bin
R3	12.4(10)A	Advanced Enterprise Services	c2600-adventerprisek9-mz.124-10a.bin
R4	12.4(24)T1	Advanced Enterprise Services	c1841-adventerprisek9-mz.124-24.T1.bin
R5	12.4(24)T1	Advanced Enterprise Services	c1841-adventerprisek9-mz.124-24.T1.bin
R6	12.4(24)T1	Advanced Enterprise Services	c1841-adventerprisek9-mz.124-24.T1.bin
SW1	12.2(44)SE	EMI	c3560-advipservicesk9-mz.122-44.SE.bin
SW2	12.2(44)SE	EMI	c3560-advipservicesk9-mz.122-44.SE.bin
SW3	12.2(25)SEC2	EMI	c3550-ipservicesk9-mz.122-25.SEC2.bin
SW4	12.2(25)SEC2	EMI	c3550-ipservicesk9-mz.122-25.SEC2.bin
Frame Relay	12.2(15)T17	IP Plus	c2500-is-l.122-15.T17.bin
Terminal Server	12.2(15)T17	IP Plus	c2500-is-l.122-15.T17.bin

## Purchasing Equipment

The most convenient way to have always available access to your practice lab is to simply purchase the equipment to dedicate to your studies. If you were to buy all of the devices listed above, your topology would match ours exactly. However, this option is typically not cost effective for most candidates.

If you are purchasing your own equipment, the devices do not need to be an exact match to our specification. For example, 2800s and 3800s will support all features that 1800s do, but they are generally more expensive. What is most important however, is what software versions the platform supports.

Before choosing a platform to buy visit the Cisco IOS Feature Navigator at <http://www.cisco.com/go/fn/> to compare which features and IOS versions a particular platform supports, along with what the memory requirements in order to run it are.

For pricing on new equipment contact your local Cisco reseller. Used equipment pricing can be found on [www.ebay.com](http://www.ebay.com). Affordable pricing for memory and cables can be found at sites such as [www.monoprice.com](http://www.monoprice.com), [www.crucial.com](http://www.crucial.com), and [www.anthonypanda.com](http://www.anthonypanda.com). As usual, buyer beware whenever purchasing equipment on the used market.

Lastly, an important part of buying equipment that many people overlook is the space, power, and cooling requirements, along with the noise generated by ten or more routers sitting on your desk. Be sure to budget all of these into your overall equipment investment decision.

## Online Rack Rentals

An affordable alternative to purchasing equipment that many engineers turn to is using online rack rental providers. Using rack rental providers allows you the same access to real live equipment as if you had it sitting physically in your office, but you don't need to worry about issues such as a large upfront cost, auction sites, cabling problems, memory, obtaining software, space, power, cooling, etc.

Most rack rental providers offer pricing per hour or block of hours, as well as bulk pricing per week, month, etc. Typically the only requirement to access online racks is an internet connection, and a terminal emulation software such as HyperTerminal or SecureCRT for initiating a Telnet connection.

Note that any rack rental provider that supports INE's CCIE Routing & Switching Lab Workbook (IEWB-RS) topology will be able to support the topology needed for this CCNP Lab Workbook.

### Note

INE's preferred rack rental provider is <http://www.GradedLabs.com>. GradedLabs not only provides the highest value at the lowest cost, they also provide top-notch support and a suite of sophisticated tools to enhance your learning experience, such as automated configuration archiving, automated scheduling, and the ability to immediately schedule sessions already in progress at a discounted price.

More information about these services can be found at <http://www.INE.com/rackrentals.htm> and <http://www.GradedLabs.com>.

## Dynamips, Dynagen, & GNS3

Another alternative to using real equipment is an IOS virtualization program known as Dynamips. Unlike IOS simulation programs, such as Cisco's Packet Tracer, Dynamips allows you to run real IOS code on your Windows, MacOS, or Linux based desktop or laptop, and have the different IOS instances interact with each other as if they were real physical routers. While simulation programs may be good for entry level training such as CCENT, they lack the full IOS feature set support that is required for advanced applications such as CCNP or CCIE preparation.

The two main disadvantages of using Dynamips are the learning curve of getting a functional and stable topology, and the physical hardware requirements of your laptop or desktop. However, with the advent of the CLI based Dynagen application, and the GUI based GNS3 application, both which are simplified launchers for Dynamips, many engineers are turning to this as an alternative to buying equipment.

There are many resources available for how to use Dynamips, Dynagen, and GNS3, all of which are outside the scope of this workbook. INE does however officially support these programs for its products, and also has multiple Class-on-Demand video tutorials on how to use them.



### **For More Information**

For more information on using Dynamips for CCNP preparation, along with Class-on-Demand video tutorials, visit <http://www.INE.com/dynamips.htm>.

## Initial Configurations

In order to streamline the configuration for some sections and devices, INE's CCNP Lab Workbook requires that the initial configuration scripts be loaded prior to starting some individual lab exercises. For example, the Frame Relay Switch configuration is static, and once loaded with the initial configuration script, requires no interaction from the candidate's perspective.

If an initial configuration is required for a section, it will be clearly outlined in that actual lab task. For the most recent copy of these configuration scripts see the CCNP Bootcamp Class-on-Demand section of Internetnetwork Expert's members site where you downloaded this workbook at <http://members.INE.com>.

## Support Resources

Achieving the CCNP certification is just one continuing step in advancing your career as a network engineer. Like many other industries, the computer networking field is not only about networking with computers, it is about networking with people. Internetnetwork Expert's Online Community – <http://www.IEOC.com> – offers you the chance to interact with thousands of other engineers involved in the networking field, and specifically with Cisco certification.

IEOC allows you to create new posts and reply to other posts like a normal web forum, but you can also read and submit posts via email. For example if you email [ccnp@ieoc.com](mailto:ccnp@ieoc.com) your message will be sent out to all users subscribed to the CCNP email feed, plus posted on the web forum as viewable and searchable content.

An additional free resource offered by INE is our blog. The INE blog contains hundreds of articles on technical topics from A to Z, or AAA to Zone Based Firewall to be more specific. To read previous posts or submit topic requests visit <http://blog.INE.com>.

# Building Cisco Multilayered Switched Networks (BCMSN)

## Case Study Overview

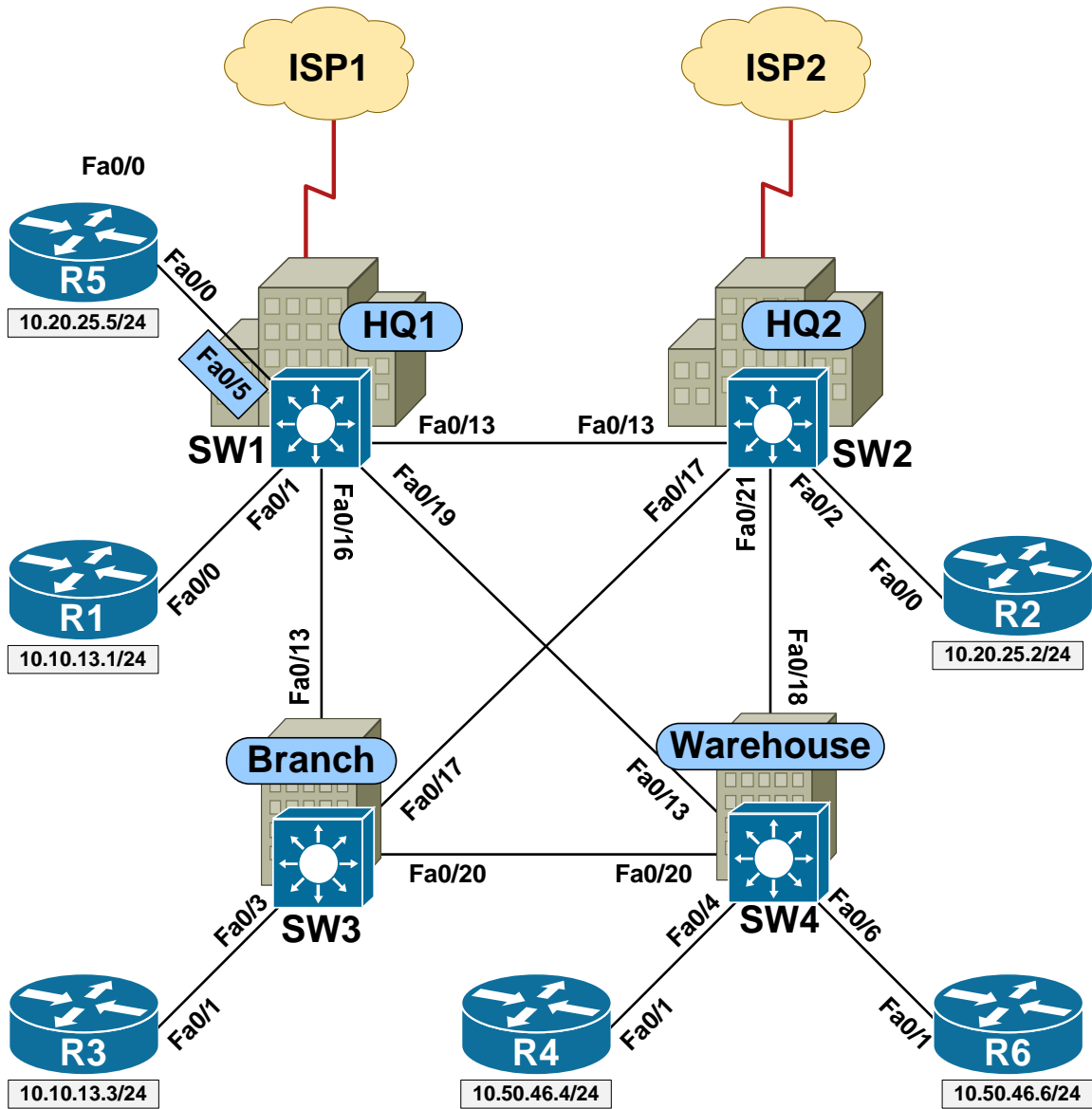
Dexter Bean Manufacturing was founded five years ago by partners Dexter and Bean in order to provide their customers with high quality widgets and exceptional customer service at a reasonable price. Since its humble beginnings with the two partners, DBM Inc. has expanded their market share exponentially each year, and currently employs 300 workers spread between four offices.

As DBM Inc.'s business needs have far outgrown the original capacity of their part-time IT department, you have been hired along with a network architecture team in order to implement a new network infrastructure that will support their growth for the foreseeable future.

The first major infrastructure change at DBM Inc. is the migration from a flat shared layer 2 network consisting of hubs and unmanaged switches, to a hierarchical layer 2 and layer 3 switched network employing VLANs and routing for traffic separation and security.

Using the included physical wiring table, configure the layer 2 switched network per the following architecture team's requirements.

## DBM Inc. Campus Diagram



 **Note**

Prior to starting this section load the *BCMSN Basic Initial Configs* for all devices. Refer to the *DBM Inc. Campus Diagram* for device and port information.

## 1.1 VLANs

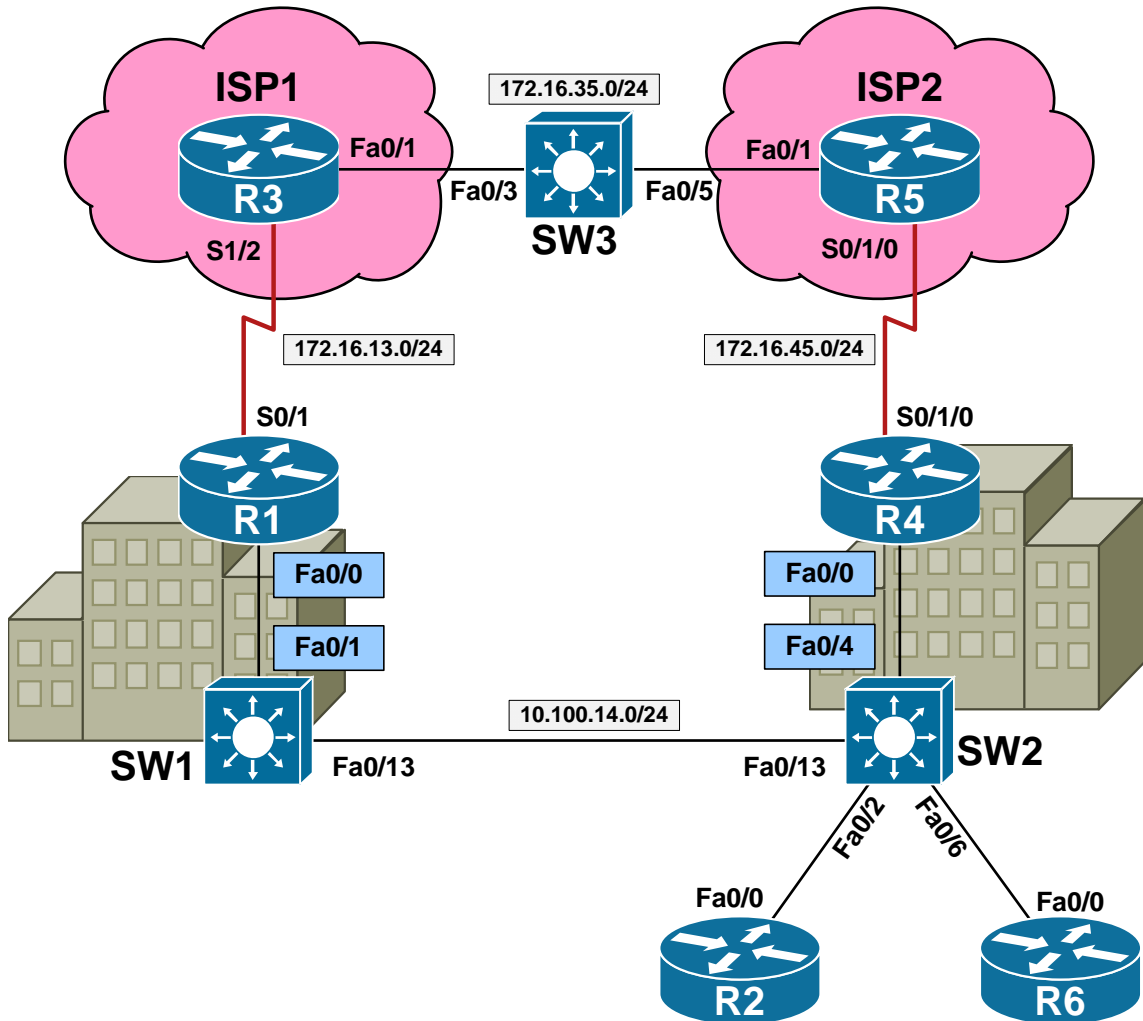
- The design team has mandated that traffic be logically separated in the network based on the organizational chart that was supplied to them by management. Specifically, VLANs have been mapped to different functional departments as follows:
  - SALES – VLAN 10
  - ACCOUNTING – VLAN 20
  - MANAGEMENT – VLAN 30
  - CUSTOMER\_SERVICE – VLAN 40
  - WAREHOUSE – VLAN 50
  - GUEST\_ACCESS – VLAN 60
- Using the VLAN database mode on SW1 and SW2, configure the VLANs as listed above, including their names.
- Using global configuration mode on SW3 and SW4, configure the VLANs as listed above, including their names.

## 1.2 Access Ports

- Now that VLANs have been created in order to separate traffic logically at layer 2 in the network, the design team has provided you a list of port assignments for the VLANs. Additionally, they have requested that these ports be configured in access mode to prevent any negotiation errors related to Dynamic Trunking Protocol (DTP).
- Configure the access mode and VLAN assignments per the list:

Device	Port	VLAN
SW1	Fa0/1	10
SW1	Fa0/2	60
SW1	Fa0/4	20
SW1	Fa0/5	20
SW1	Fa0/7	60
SW1	Fa0/8	10
SW2	Fa0/1	40
SW2	Fa0/2	20
SW2	Fa0/3	40
SW2	Fa0/5	30
SW2	Fa0/8	30
SW2	Fa0/9	30
SW3	Fa0/2	10
SW3	Fa0/3	10
SW3	Fa0/4	50
SW3	Fa0/9	50
SW3	Fa0/10	60
SW3	Fa0/11	60
SW4	Fa0/1	50
SW4	Fa0/2	50
SW4	Fa0/3	60
SW4	Fa0/4	50
SW4	Fa0/5	60
SW4	Fa0/6	50

## DBM Inc. Gateway Redundancy Diagram



 **Note**

Prior to starting this section erase all previous configuration and load the *BCMSN Gateway Redundancy Initial Configs* for all devices. Refer to the *DBM Inc. Gateway Redundancy Diagram* for device and port information.

Internet Access from DBM Inc.'s campus network is via redundant point-to-point T1 links at the HQ1 and HQ2 sites. Edge router R1 at HQ1 connects to ISP1 via the link to R3, while edge router R4 at HQ2 connects to ISP2 via the link to R5. In order to allow for fast and transparent convergence in the event that a link or router failure occurs, the design team has requested a gateway redundancy protocol to be configured on the inside subnet that connects R1 and R4 across the layer 2 network. Configure gateway redundancy per the below requirements in order to accomplish this.

## 1.20 HSRP

- The design team has mandated that the primary link to the Internet should be via R1's link to ISP1, and that HSRP be used for redundancy for this connection. Configure HSRP on the inside interfaces of R1 and R4 per the following specification:
  - Use the virtual gateway address 10.100.14.254/24
  - R1 should be the primary gateway
  - If R1 is unreachable, or its link to ISP1 goes down, R4 should take over as the primary gateway
  - If R1 goes down and then comes back up at a later time it should resume its role as the primary gateway after being stable for 30 seconds
  - Authenticate the HSRP communication between R1 and R4 using the MD5 based password DBM\_HSRP
  - For fast convergence HSRP keepalives should be sent every 333ms, and a neighbor should be declared down if a keepalive isn't heard within one second
- To test this configuration ping from R2 and R6 to the Internet addresses 3.3.3.3/32 and 5.5.5.5/32, and verify that reconvergence occurs if R1 is unreachable or its link to R3 is down.

# BCMSN Solutions

## 1.1 VLANs

### *Configuration*

---

```
SW1#vlan database
% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.

SW1(vlan)#vlan 10 name SALES
VLAN 10 added:
  Name: SALES
SW1(vlan)#vlan 20 name ACCOUNTING
VLAN 20 added:
  Name: ACCOUNTING
SW1(vlan)#vlan 30 name MANAGEMENT
VLAN 30 added:
  Name: MANAGEMENT
SW1(vlan)#vlan 40 name CUSTOMER_SERVICE
VLAN 40 added:
  Name: CUSTOMER_SERVICE
SW1(vlan)#vlan 50 name WAREHOUSE
VLAN 50 added:
  Name: WAREHOUSE
SW1(vlan)#vlan 60 name GUEST_ACCESS
VLAN 60 added:
  Name: GUEST_ACCESS
SW1(vlan)#exit
APPLY completed.
Exiting....
SW1#
```

```
SW2#vlan database
% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.

SW2(vlan)#vlan 10 name SALES
VLAN 10 added:
  Name: SALES
SW2(vlan)#vlan 20 name ACCOUNTING
VLAN 20 added:
  Name: ACCOUNTING
SW2(vlan)#vlan 30 name MANAGEMENT
VLAN 30 added:
  Name: MANAGEMENT
SW2(vlan)#vlan 40 name CUSTOMER_SERVICE
VLAN 40 added:
  Name: CUSTOMER_SERVICE
SW2(vlan)#vlan 50 name WAREHOUSE
VLAN 50 added:
  Name: WAREHOUSE
```

```
SW2(vlan)#vlan 60 name GUEST_ACCESS
VLAN 60 added:
  Name: GUEST_ACCESS
SW2(vlan)#exit
APPLY completed.
Exiting....
SW2#
```

```
SW3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW3(config)#vlan 10
SW3(config-vlan)#name SALES
SW3(config-vlan)#vlan 20
SW3(config-vlan)#name ACCOUNTING
SW3(config-vlan)#vlan 30
SW3(config-vlan)#name MANAGEMENT
SW3(config-vlan)#vlan 40
SW3(config-vlan)#name CUSTOMER_SERVICE
SW3(config-vlan)#vlan 50
SW3(config-vlan)#name WAREHOUSE
SW3(config-vlan)#vlan 60
SW3(config-vlan)#name GUEST_ACCESS
SW3(config-vlan)#end
SW3#
```

```
SW4#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW4(config)#vlan 10
SW4(config-vlan)#name SALES
SW4(config-vlan)#vlan 20
SW4(config-vlan)#name ACCOUNTING
SW4(config-vlan)#vlan 30
SW4(config-vlan)#name MANAGEMENT
SW4(config-vlan)#vlan 40
SW4(config-vlan)#name CUSTOMER_SERVICE
SW4(config-vlan)#vlan 50
SW4(config-vlan)#name WAREHOUSE
SW4(config-vlan)#vlan 60
SW4(config-vlan)#name GUEST_ACCESS
SW4(config-vlan)#end
SW4#
```

## 1.2 Access Ports

### *Configuration*

---

```
SW1#
interface FastEthernet0/1
  switchport mode access
  switchport access vlan 10
!
interface FastEthernet0/2
  switchport mode access
  switchport access vlan 60
!
interface FastEthernet0/4
  switchport mode access
  switchport access vlan 20
!
interface FastEthernet0/5
  switchport mode access
  switchport access vlan 20
!
interface FastEthernet0/7
  switchport mode access
  switchport access vlan 60
!
interface FastEthernet0/8
  switchport mode access
  switchport access vlan 10

SW2#
interface FastEthernet0/1
  switchport mode access
  switchport access vlan 40
!
interface FastEthernet0/2
  switchport mode access
  switchport access vlan 20
!
interface FastEthernet0/3
  switchport mode access
  switchport access vlan 40
!
interface FastEthernet0/5
  switchport mode access
  switchport access vlan 30
!
interface FastEthernet0/8
  switchport mode access
  switchport access vlan 30
!
interface FastEthernet0/9
  switchport mode access
  switchport access vlan 30
```

```
SW3#
interface FastEthernet0/2
  switchport mode access
  switchport access vlan 10
!
interface FastEthernet0/3
  switchport mode access
  switchport access vlan 10
!
interface FastEthernet0/4
  switchport mode access
  switchport access vlan 50
!
interface FastEthernet0/9
  switchport mode access
  switchport access vlan 50
!
interface FastEthernet0/10
  switchport mode access
  switchport access vlan 60
!
interface FastEthernet0/11
  switchport mode access
  switchport access vlan 60
```

```
SW4#
interface FastEthernet0/1
  switchport mode access
  switchport access vlan 50
!
interface FastEthernet0/2
  switchport mode access
  switchport access vlan 50
!
interface FastEthernet0/3
  switchport mode access
  switchport access vlan 60
!
interface FastEthernet0/4
  switchport mode access
  switchport access vlan 50
!
interface FastEthernet0/5
  switchport mode access
  switchport access vlan 60
!
interface FastEthernet0/6
  switchport mode access
  switchport access vlan 50
```

## Verification

---

SW1#show vlan brief

VLAN Name	Status	Ports
1 default	active	Fa0/3, Fa0/6, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
10 SALES	active	Fa0/1, Fa0/8
20 ACCOUNTING	active	Fa0/4, Fa0/5
30 MANAGEMENT	active	
40 CUSTOMER_SERVICE	active	
50 WAREHOUSE	active	
60 GUEST_ACCESS	active	Fa0/2, Fa0/7
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

SW2#show vlan brief

VLAN Name	Status	Ports
1 default	active	Fa0/4, Fa0/6, Fa0/7, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
10 SALES	active	
20 ACCOUNTING	active	Fa0/2
30 MANAGEMENT	active	Fa0/5, Fa0/8, Fa0/9
40 CUSTOMER_SERVICE	active	Fa0/1, Fa0/3
50 WAREHOUSE	active	
60 GUEST_ACCESS	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

**SW3#show vlan brief**

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/12, Fa0/22, Fa0/23 Fa0/24, Gi0/1, Gi0/2
10 SALES	active	Fa0/2, Fa0/3
20 ACCOUNTING	active	
30 MANAGEMENT	active	
40 CUSTOMER_SERVICE	active	
50 WAREHOUSE	active	Fa0/4, Fa0/9
60 GUEST_ACCESS	active	Fa0/10, Fa0/11
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

**SW4#show vlan brief**

VLAN Name	Status	Ports
1 default	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/22 Fa0/23, Fa0/24, Gi0/1, Gi0/2
10 SALES	active	
20 ACCOUNTING	active	
30 MANAGEMENT	active	
40 CUSTOMER_SERVICE	active	
50 WAREHOUSE	active	Fa0/1, Fa0/2, Fa0/4
60 GUEST_ACCESS	active	Fa0/3, Fa0/5
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

## 1.20 HSRP

### Configuration

---

```
R1:
interface FastEthernet0/0
 standby 1 ip 10.100.14.254
 standby 1 timers msec 333 1
 standby 1 priority 255
 standby 1 preempt delay minimum 30
 standby 1 authentication md5 key-string DBM_HSRP
 standby 1 track Serial0/1 255
```

```
R4:
interface FastEthernet0/0
 standby 1 ip 10.100.14.254
 standby 1 timers msec 333 1
 standby 1 preempt
 standby 1 authentication md5 key-string DBM_HSRP
```

### Verification

---

**R1#show standby**

```
FastEthernet0/0 - Group 1
  State is Active
    11 state changes, last state change 00:00:09
  Virtual IP address is 10.100.14.254
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 333 msec, hold time 1 sec
    Next hello sent in 0.261 secs
  Authentication MD5, key-string "DBM_HSRP"
  Preemption enabled, delay min 30 secs
  Active router is local
  Standby router is 10.100.14.4, priority 100 (expires in 0.703 sec)
  Priority 255 (configured 255)
    Track interface Serial0/1 state Up decrement 255
  IP redundancy name is "hsrp-Fa0/0-1" (default)
```

**R4#show standby**

```
FastEthernet0/0 - Group 1
  State is Standby
    10 state changes, last state change 00:01:03
  Virtual IP address is 10.100.14.254
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 333 msec, hold time 1 sec
    Next hello sent in 0.096 secs
  Authentication MD5, key-string "DBM_HSRP"
  Preemption enabled
  Active router is 10.100.14.1, priority 255 (expires in 0.992 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Fa0/0-1" (default)
```

 **Note**

The below output illustrates how the reconvergence process of HSRP can be verified. To start, R2 sees the virtual IP & MAC address for 10.100.14.254 in its ARP table. A PING is initiated from R2 out to the Internet (3.3.3.3), and then R1's link to the ISP is disabled. Based on the low OSPF & HSRP hello timers, reconvergence occurs in about 4 seconds.

```
R2#show arp
Protocol  Address          Age (min)  Hardware Addr  Type   Interface
Internet  10.100.14.2      -          0011.2058.0fe0 ARPA   FastEthernet0/0
Internet  10.100.14.254    0          0000.0c07.ac01 ARPA   FastEthernet0/0
```

```
R2#ping 3.3.3.3 repeat 1000
```

```
Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
```

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface Serial0/1
R1(config-if)#shutdown
R1(config-if)#
R1(config-if)#
*Mar  1 00:21:13.231: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on
Serial0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
*Mar  1 00:21:13.403: %HSRP-5-STATECHANGE: FastEthernet0/0 Grp 1 state
Active -> Speak
*Mar  1 00:21:14.405: %HSRP-5-STATECHANGE: FastEthernet0/0 Grp 1 state
Speak -> Standby
*Mar  1 00:21:15.230: %LINK-5-CHANGED: Interface Serial0/1, changed
state to administratively down
*Mar  1 00:21:16.232: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/1, changed state to down
```

```
R2#
!!! ..!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
Success rate is 99 percent (998/1000), round-trip min/avg/max = 28/30/101 ms
```

**R1#show standby**

FastEthernet0/0 - Group 1

**State is Standby**

7 state changes, last state change 00:00:48  
Virtual IP address is 10.100.14.254  
Active virtual MAC address is 0000.0c07.ac01  
Local virtual MAC address is 0000.0c07.ac01 (v1 default)  
Hello time 333 msec, hold time 1 sec  
Next hello sent in 0.193 secs  
Authentication MD5, key-string "DBM\_HSRP"  
Preemption enabled  
**Active router is 10.100.14.4**, priority 100 (expires in 0.700 sec)  
Standby router is local  
**Priority 0 (configured 255)**  
**Track interface Serial0/1 state Down decrement 255**  
IP redundancy name is "hsrp-Fa0/0-1" (default)

**R4#show standby**

FastEthernet0/0 - Group 1

**State is Active**

5 state changes, last state change 00:00:54  
Virtual IP address is 10.100.14.254  
Active virtual MAC address is 0000.0c07.ac01  
Local virtual MAC address is 0000.0c07.ac01 (v1 default)  
Hello time 333 msec, hold time 1 sec  
Next hello sent in 0.096 secs  
Authentication MD5, key-string  
Preemption enabled  
**Active router is local**  
**Standby router is 10.100.14.1, priority 0 (expires in 0.864 sec)**  
Priority 100 (default 100)  
Group name is "hsrp-Fa0/0-1" (default)

**R2#traceroute 3.3.3.3**

Type escape sequence to abort.

Tracing the route to 3.3.3.3

```
1 10.100.14.4 0 msec 0 msec 4 msec
2 172.16.45.5 12 msec 12 msec 16 msec
3 172.16.35.3 17 msec * 12 msec
```

Traffic now exits via R4's link to ISP2, as R4 is the active HSRP router.

When R1's link to ISP1 comes back, the preempt delay of 30 seconds allows for the IGP network to fully reconverge before R1 regains its active status. This can be seen from the timestamps of the log messages on R1.

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface Serial0/1
R1(config-if)#no shutdown
R1(config-if)#end
R1#
*Mar  1 00:23:53.553: %SYS-5-CONFIG_I: Configured from console by console
*Mar  1 00:23:54.788: %LINK-3-UPDOWN: Interface Serial0/1, changed state to up
*Mar  1 00:23:55.216: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/1 from
LOADING to FULL, Loading Done
*Mar  1 00:23:55.789: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/1, changed state to up
*Mar  1 00:24:24.845: %HSRP-5-STATECHANGE: FastEthernet0/0 Grp 1 state Standby
-> Active

R1#show standby
FastEthernet0/0 - Group 1
  State is Active
    11 state changes, last state change 00:00:09
  Virtual IP address is 10.100.14.254
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 333 msec, hold time 1 sec
    Next hello sent in 0.261 secs
  Authentication MD5, key-string "DBM_HSRP"
  Preemption enabled, delay min 30 secs
  Active router is local
  Standby router is 10.100.14.4, priority 100 (expires in 0.703 sec)
  Priority 255 (configured 255)
    Track interface Serial0/1 state Up decrement 255
  IP redundancy name is "hsrp-Fa0/0-1" (default)
```

# Building Scalable Cisco Internetworks (BSCI)

## Case Study Overview

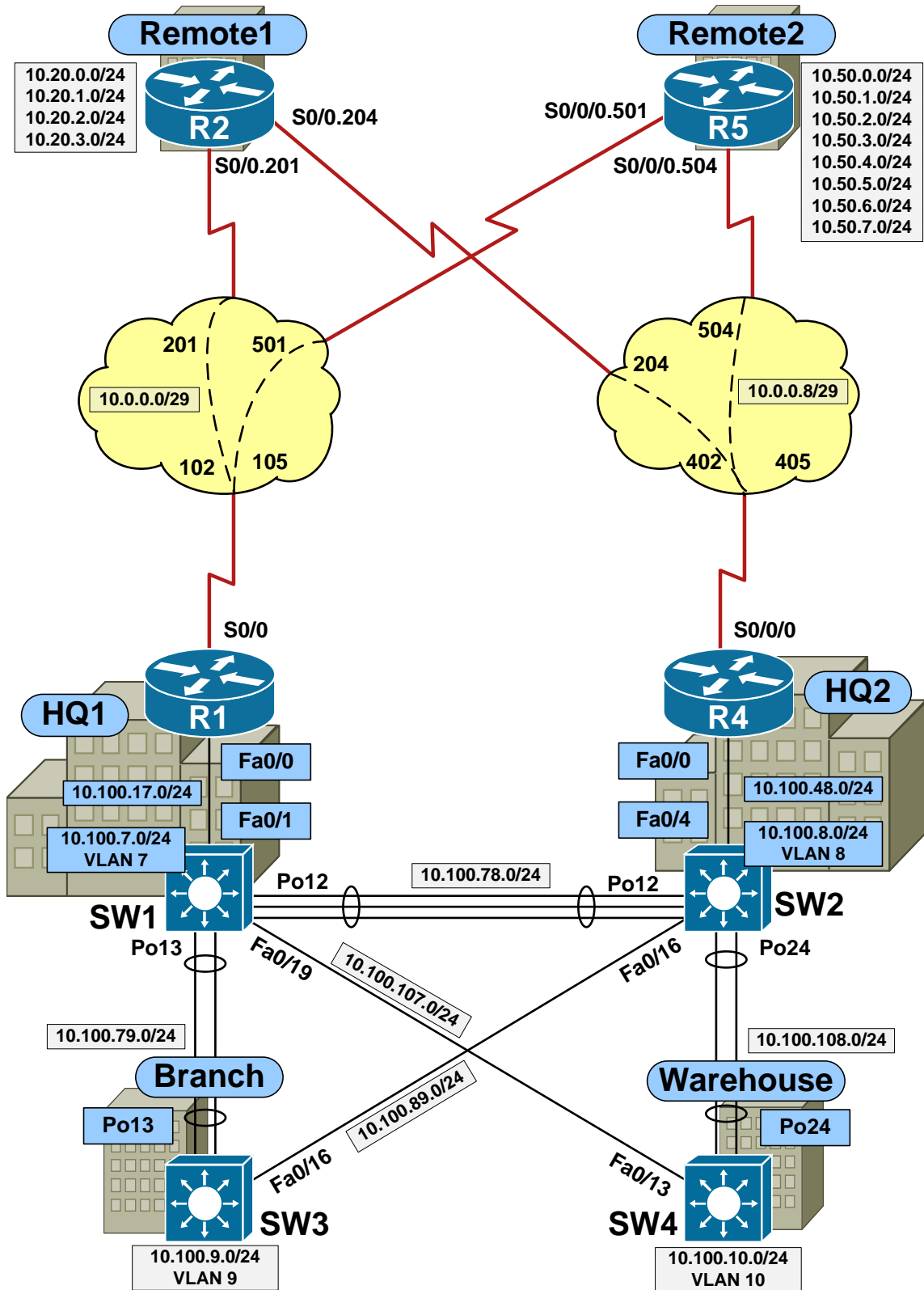
The next phase of network migration for Dexter Bean Manufacturing involves implementing a scalable Interior Gateway Protocol (IGP) for dynamic layer 3 IP routing between the various sites of DBM Inc, BGP for routing to the Internet, and various services such as Multicast, IPv6, DHCP, etc.

The scope of this implementation includes the four buildings in the main campus network of DBM Inc., HQ1, HQ2, the Branch, and the Warehouse, along with the two remote offices Remote1 and Remote2. The layer 2 trunks previously used as interconnections between the campus buildings have been replaced with layer 3 routed links, in order to eliminate the additional convergence time needed for STP. The two remote offices are connected to HQ1 and HQ2 through dual hub-and-spoke Frame Relay WAN links for redundancy. Internet connectivity occurs through redundant WAN links to ISP1 and ISP2 at the HQ1 and HQ2 offices respectively.

This case study is subdivided into various technology sections such as EIGRP, OSPF, IS-IS, BGP, Multicast, IPv6, and Services. Each section's configuration is unrelated to the others, and separate sets of initial configurations should be loaded per the included instructions before starting an individual section.

Use the enclosed logical layer 3 diagrams in order to configure the network per the architecture team's requirements. Note that there are minor differences between some diagrams, such as the EIGRP and OSPF network diagrams vs. the IS-IS network diagrams, due to the design limitations of running IS-IS over hub-and-spoke NBMA links.

## DBM Inc. EIGRP Diagram



 **Note**

Prior to starting this section load the *BSCI EIGRP Initial Configs* for all devices. Refer to the *DBM Inc. EIGRP Diagram* for device, port, and addressing information.

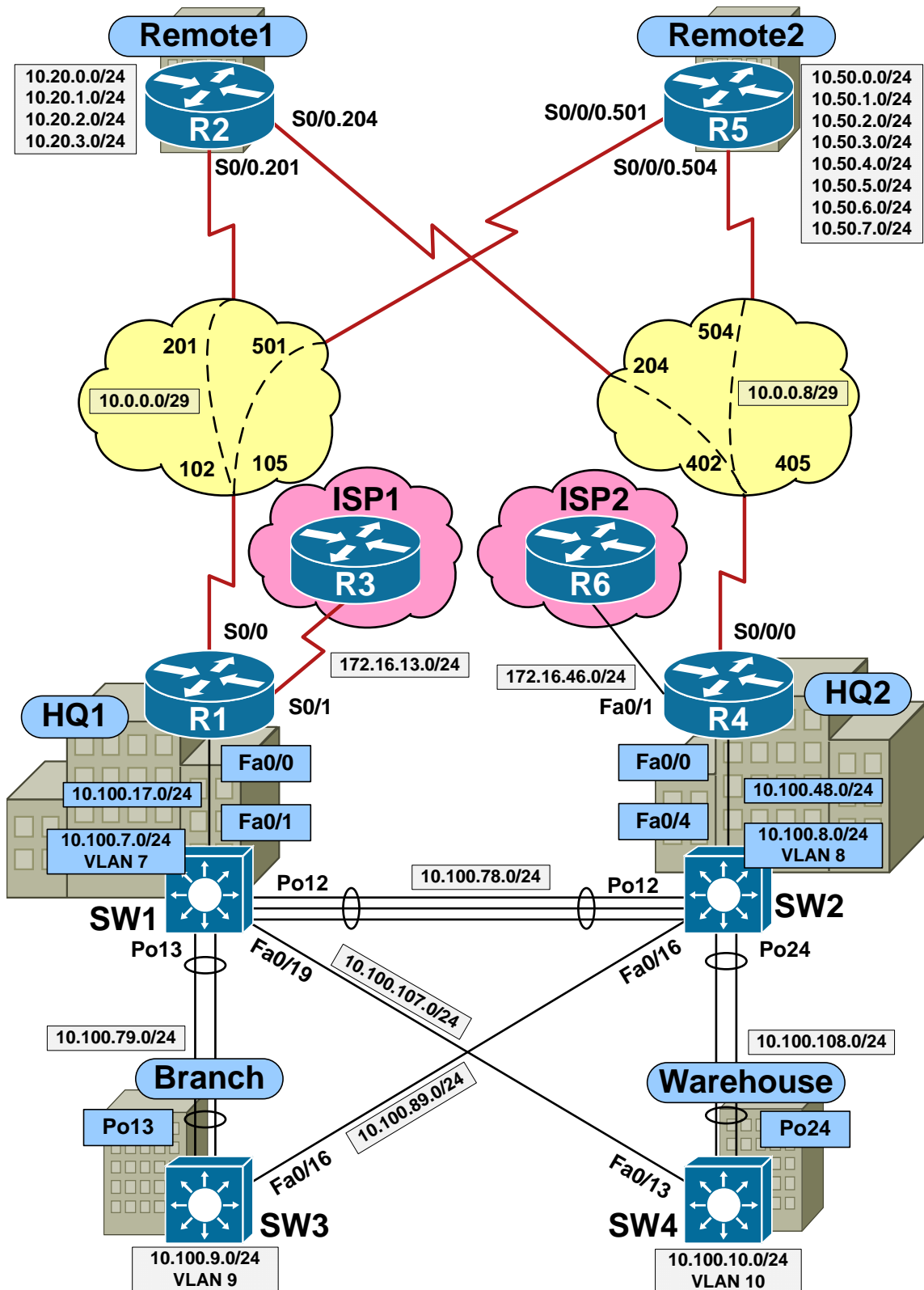
## 2.1 Basic EIGRP

- Based on the fact that all routers in the DBM network are Cisco routers, and due to its fast convergence and VLSM support, the design team has decided that EIGRP will be used as the primary IGP.
- Per their request, implement EIGRP in the network using AS number 100 so that it runs on all IP enabled links.
- Once complete, ensure that all devices have IP reachability to all segments in the network, and that offices Remote1 and Remote2 maintain connectivity to all sites in the event that either R1 or R4 goes down.

## 2.2 EIGRP Security

- To protect the network control plane, the design team has given you the following additional requirements to implement related to EIGRP:
  - EIGRP hello packets should not be sent out host facing interfaces (e.g. non-transit links).
  - All EIGRP adjacencies should be MD5 authenticated with the password DBMI\_EIGRP.
  - EIGRP hello packets should be sent as unicast between R1 & SW1 and R4 & SW2 to protect against reconnaissance attacks.

## DBM Inc. BGP Diagram



 **Note**

Prior to starting this section load the *BSCI BGP Initial Configs* for all devices. Refer to the *DBM Inc. BGP Diagram* for device, port, and addressing information.

The new DBMI network design includes access to Internet via redundant links to multiple ISPs. Specifically, R1 connects to ISP1 (R3) via a Serial link at the HQ1 office, while R4 connects to ISP2 (R6) via a FastEthernet link at the HQ2 office. Since the connection to ISP2 is via a higher speed link, the network design requires the majority of traffic to transit through HQ2, while the HQ1 office be primarily used as a backup. To ensure proper routing of the traffic, DBMI has been assigned the public ASN 100, and the peering agreements with ISP1 and ISP2 dictate that BGP should be used for network advertisements.

To limit the resource impact of running BGP, only R1 & SW1 at the HQ1 office, and R4 & SW2 at the HQ2 office will be running BGP, while the rest of the network will gain access to the Internet primarily by using default routing to the HQ offices. Configure the network per the design teams below specifications in order to gain reachability to the Internet, and provide redundancy for the network. Note that ISP1 (R3) and ISP2 (R6) are preconfigured for these tasks, and require no modification to accomplish the network design goals. For reachability (PING) testing to the networks learned from ISP1 or ISP2, use the first host address of the subnet.

## 5.1 iBGP Peerings

- The first step the design team has requested for you to configure in the BGP implementation is the establishment of iBGP peerings between the devices in the HQ1 and HQ2 offices. Specifically they have requested that the following occurs:
  - R1, R4, SW1, and SW2 should form a full mesh of BGP peerings
  - The Loopback0 interfaces should be used as the source and destinations of the peerings to provide for additional redundancy
  - To protect the network control plane, the password DBMIBGP should be used to perform MD5 authentication of the sessions.

## 5.2 EBGP Peerings

- Next, they have requested that the EBGP peerings to ISP1 and ISP2 be established per the negotiated peering agreements. Specifically the peering agreements are as follows:
  - ISP1 uses the BGP ASN 300, is expecting the peering to use the directly connected link between R1 & R3, and requires authentication using the password ISP1BGP
  - ISP2 uses the BGP ASN 600, is expecting the peering to use the directly connected link between R4 & R6, requires authentication using the password ISP2BGP, and uses high speed hello timers of 1 second and a hold time of 3 seconds
- Since the transit links to ISP1 and ISP2 are not part of your IGP domain, the design team has requested that any required next-hop modification be performed on the border routers R1 & R4 in order to access networks on the Internet.

## 5.3 BGP NLRI Advertisements

- Internet access is required for hosts on the VLAN 7, 8, 9, & 10 segments, along with hosts on the LAN segments of R2 (10.20.x.x) and R5 (10.50.x.x) at the Remote1 and Remote2 offices respectively. Since the design team has specified that Internet traffic should not be sent to the transit links of the network, e.g. the Frame Relay WAN links, these networks will not be part of the AS 100 advertisements.
- Per their request, configure the border routers R1 and R4 to advertise the required networks into BGP.

## 5.4 BGP Aggregation

- Both ISP1 and ISP2's BGP routing policies require that the maximum possible aggregation be performed on any networks their customers are advertising to them. To comply with this, the design team has requested for you to perform optimal summarization on R1 and R4 in such a way that they advertise the minimum networks necessary to the ISPs, but at the same time do not advertise reachability for any subnets that are not actually allocated to the DBMI network.

# BSCI Solutions

## 2.1 Basic EIGRP

### *Configuration*

---

```
R1#  
interface Serial0/0  
  no ip split-horizon eigrp 100  
!  
router eigrp 100  
  network 10.0.0.0
```

```
R2#  
router eigrp 100  
  network 10.0.0.0
```

```
R4#  
interface Serial0/0/0  
  no ip split-horizon eigrp 100  
!  
router eigrp 100  
  network 10.0.0.0
```

```
R5#  
router eigrp 100  
  network 10.0.0.0
```

```
SW1#  
ip routing  
!  
router eigrp 100  
  network 10.0.0.0
```

```
SW2#  
ip routing  
!  
router eigrp 100  
  network 10.0.0.0
```

```
SW3#  
ip routing  
!  
router eigrp 100  
  network 10.0.0.0
```

```
SW4#  
ip routing  
!  
router eigrp 100  
  network 10.0.0.0
```

## Verification

### R1#show ip eigrp neighbors

IP-EIGRP neighbors for process 100

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
2	10.100.17.7	Fa0/0	13	00:08:46	57	342	0	66
1	10.0.0.2	Se0/0	12	00:08:46	83	498	0	51
0	10.0.0.3	Se0/0	12	00:08:46	48	288	0	46

### R1#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

```

10.0.0.0/8 is variably subnetted, 33 subnets, 3 masks
D    10.255.255.10/32
      [90/161280] via 10.100.17.7, 00:07:32, FastEthernet0/0
D    10.255.255.8/32 [90/158720] via 10.100.17.7, 00:07:37, FastEthernet0/0
D    10.100.108.0/24 [90/33280] via 10.100.17.7, 00:07:37, FastEthernet0/0
D    10.0.0.8/29 [90/2177536] via 10.100.17.7, 00:05:06, FastEthernet0/0
D    10.255.255.9/32 [90/158720] via 10.100.17.7, 00:07:35, FastEthernet0/0
D    10.100.107.0/24 [90/30720] via 10.100.17.7, 00:07:42, FastEthernet0/0
D    10.255.255.2/32 [90/2297856] via 10.0.0.2, 00:08:54, Serial0/0
C    10.0.0.0/29 is directly connected, Serial0/0
C    10.255.255.1/32 is directly connected, Loopback0
D    10.255.255.7/32 [90/156160] via 10.100.17.7, 00:07:42, FastEthernet0/0
D    10.255.255.4/32 [90/161280] via 10.100.17.7, 00:08:53, FastEthernet0/0
D    10.255.255.5/32 [90/2297856] via 10.0.0.3, 00:08:51, Serial0/0
D    10.20.2.0/24 [90/2172416] via 10.0.0.2, 00:08:54, Serial0/0
D    10.20.3.0/24 [90/2172416] via 10.0.0.2, 00:08:54, Serial0/0
D    10.20.0.0/24 [90/2172416] via 10.0.0.2, 00:08:54, Serial0/0
D    10.20.1.0/24 [90/2172416] via 10.0.0.2, 00:08:54, Serial0/0
D    10.100.78.0/24 [90/30720] via 10.100.17.7, 00:07:42, FastEthernet0/0
D    10.100.79.0/24 [90/30720] via 10.100.17.7, 00:07:42, FastEthernet0/0
D    10.100.89.0/24 [90/33280] via 10.100.17.7, 00:07:38, FastEthernet0/0
D    10.50.0.0/24 [90/2172416] via 10.0.0.3, 00:08:52, Serial0/0
D    10.50.1.0/24 [90/2172416] via 10.0.0.3, 00:08:52, Serial0/0
D    10.50.2.0/24 [90/2172416] via 10.0.0.3, 00:08:52, Serial0/0
D    10.50.3.0/24 [90/2172416] via 10.0.0.3, 00:08:52, Serial0/0
D    10.50.4.0/24 [90/2172416] via 10.0.0.3, 00:08:52, Serial0/0
D    10.50.5.0/24 [90/2172416] via 10.0.0.3, 00:08:52, Serial0/0
D    10.50.6.0/24 [90/2172416] via 10.0.0.3, 00:08:52, Serial0/0
D    10.50.7.0/24 [90/2172416] via 10.0.0.3, 00:08:52, Serial0/0
D    10.100.48.0/24 [90/33280] via 10.100.17.7, 00:07:40, FastEthernet0/0
D    10.100.10.0/24 [90/33536] via 10.100.17.7, 00:07:34, FastEthernet0/0
D    10.100.8.0/24 [90/30976] via 10.100.17.7, 00:07:40, FastEthernet0/0
D    10.100.9.0/24 [90/30976] via 10.100.17.7, 00:07:37, FastEthernet0/0
D    10.100.7.0/24 [90/28416] via 10.100.17.7, 00:07:43, FastEthernet0/0
C    10.100.17.0/24 is directly connected, FastEthernet0/0

```

### R1#show ip eigrp topology

IP-EIGRP Topology Table for AS(100)/ID(10.255.255.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,  
r - reply Status, s - sia Status

```
P 10.255.255.10/32, 1 successors, FD is 158720
  via 10.100.17.7 (161280/145920), FastEthernet0/0
P 10.0.0.8/29, 1 successors, FD is 2177536
  via 10.100.17.7 (2177536/2174976), FastEthernet0/0
  via 10.0.0.3 (2681856/2169856), Serial0/0
  via 10.0.0.2 (2681856/2169856), Serial0/0
P 10.255.255.8/32, 1 successors, FD is 158720
  via 10.100.17.7 (158720/139008), FastEthernet0/0
P 10.100.108.0/24, 1 successors, FD is 33280
  via 10.100.17.7 (33280/17920), FastEthernet0/0
P 10.255.255.9/32, 1 successors, FD is 158720
  via 10.100.17.7 (158720/143360), FastEthernet0/0
P 10.100.107.0/24, 1 successors, FD is 30720
  via 10.100.17.7 (30720/28160), FastEthernet0/0
P 10.255.255.2/32, 1 successors, FD is 2297856
  via 10.0.0.2 (2297856/128256), Serial0/0
P 10.0.0.0/29, 1 successors, FD is 2169856
  via Connected, Serial0/0
P 10.255.255.1/32, 1 successors, FD is 128256
  via Connected, Loopback0
P 10.255.255.7/32, 1 successors, FD is 156160
  via 10.100.17.7 (156160/128256), FastEthernet0/0
P 10.255.255.4/32, 1 successors, FD is 161280
  via 10.100.17.7 (161280/158720), FastEthernet0/0
P 10.255.255.5/32, 1 successors, FD is 2297856
  via 10.0.0.3 (2297856/128256), Serial0/0
P 10.20.2.0/24, 1 successors, FD is 2172416
  via 10.0.0.2 (2172416/28160), Serial0/0
P 10.20.3.0/24, 1 successors, FD is 2172416
  via 10.0.0.2 (2172416/28160), Serial0/0
P 10.20.0.0/24, 1 successors, FD is 2172416
  via 10.0.0.2 (2172416/28160), Serial0/0
P 10.20.1.0/24, 1 successors, FD is 2172416
  via 10.0.0.2 (2172416/28160), Serial0/0
P 10.100.78.0/24, 1 successors, FD is 30720
  via 10.100.17.7 (30720/11008), FastEthernet0/0
P 10.100.79.0/24, 1 successors, FD is 30720
  via 10.100.17.7 (30720/15360), FastEthernet0/0
P 10.100.89.0/24, 1 successors, FD is 33280
  via 10.100.17.7 (33280/30720), FastEthernet0/0
P 10.50.0.0/24, 1 successors, FD is 2172416
  via 10.0.0.3 (2172416/28160), Serial0/0
P 10.50.1.0/24, 1 successors, FD is 2172416
  via 10.0.0.3 (2172416/28160), Serial0/0
P 10.50.2.0/24, 1 successors, FD is 2172416
  via 10.0.0.3 (2172416/28160), Serial0/0
P 10.50.3.0/24, 1 successors, FD is 2172416
  via 10.0.0.3 (2172416/28160), Serial0/0
P 10.50.4.0/24, 1 successors, FD is 2172416
  via 10.0.0.3 (2172416/28160), Serial0/0
P 10.50.5.0/24, 1 successors, FD is 2172416
  via 10.0.0.3 (2172416/28160), Serial0/0
P 10.50.6.0/24, 1 successors, FD is 2172416
  via 10.0.0.3 (2172416/28160), Serial0/0
P 10.50.7.0/24, 1 successors, FD is 2172416
  via 10.0.0.3 (2172416/28160), Serial0/0
P 10.100.48.0/24, 1 successors, FD is 33280
```

```
    via 10.100.17.7 (33280/30720), FastEthernet0/0
P 10.100.10.0/24, 1 successors, FD is 30976
    via 10.100.17.7 (33536/18176), FastEthernet0/0
P 10.100.8.0/24, 1 successors, FD is 30976
    via 10.100.17.7 (30976/11264), FastEthernet0/0
P 10.100.9.0/24, 1 successors, FD is 30976
    via 10.100.17.7 (30976/15616), FastEthernet0/0
P 10.100.7.0/24, 1 successors, FD is 28416
    via 10.100.17.7 (28416/2816), FastEthernet0/0
P 10.100.17.0/24, 1 successors, FD is 28160
    via Connected, FastEthernet0/0
```

## 2.2 EIGRP Security

### Configuration

---

```
R1#
key chain EIGRP
  key 1
    key-string DBMI_EIGRP
!
interface FastEthernet0/0
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
!
interface Serial0/0
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
!
router eigrp 100
  neighbor 10.100.17.7 FastEthernet0/0

R2#
key chain EIGRP
  key 1
    key-string DBMI_EIGRP
!
interface Serial0/0.201 point-to-point
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
!
interface Serial0/0.204 point-to-point
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
!
router eigrp 100
  passive-interface default
  no passive-interface Serial0/0.201
  no passive-interface Serial0/0.204

R4#
key chain EIGRP
  key 1
    key-string DBMI_EIGRP
!
interface FastEthernet0/0
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
!
interface Serial0/0/0
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
!
router eigrp 100
  neighbor 10.100.48.8 FastEthernet0/0
```

```
R5#
key chain EIGRP
  key 1
    key-string DBMI_EIGRP
!
interface Serial0/0/0.501 point-to-point
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
!
interface Serial0/0/0.504 point-to-point
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
!
router eigrp 100
  passive-interface default
  no passive-interface Serial0/0/0.501
  no passive-interface Serial0/0/0.504
```

```
SW1#
key chain EIGRP
  key 1
    key-string DBMI_EIGRP
!
interface Port-channel12
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
!
interface Port-channel13
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
!
interface FastEthernet0/1
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
!
interface FastEthernet0/19
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
!
router eigrp 100
  passive-interface Vlan7
  neighbor 10.100.17.1 FastEthernet0/1
```

```
SW2#
key chain EIGRP
  key 1
    key-string DBMI_EIGRP
  !
interface Port-channel12
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
  !
interface Port-channel24
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
  !
interface FastEthernet0/4
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
  !
interface FastEthernet0/16
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
  !
router eigrp 100
  passive-interface Vlan8
  neighbor 10.100.48.4 FastEthernet0/4
```

```
SW3#
key chain EIGRP
  key 1
    key-string DBMI_EIGRP
  !
interface Port-channel13
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
  !
interface FastEthernet0/16
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
  !
router eigrp 100
  passive-interface Vlan9
```

```
SW4#
key chain EIGRP
  key 1
    key-string DBMI_EIGRP
  !
interface Port-channel24
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
  !
interface FastEthernet0/13
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
  !
router eigrp 100
  passive-interface Vlan10
```

**Verification**

---

**R2#show ip protocols**

```
Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
  Passive Interface(s):
    FastEthernet0/0
    FastEthernet0/0.200
    FastEthernet0/0.201
    FastEthernet0/0.202
    FastEthernet0/0.203
    Serial0/0
    Serial0/1
    Loopback0
    VoIP-Null0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.0.0.9         90           00:05:05
    10.0.0.1         90           00:05:05
  Distance: internal 90 external 170
```

 **Note**

The below debug output indicates that only unicast hellos are exchanged between R1 and SW1.

```
R1#debug ip packet
IP packet debugging is on
IP: s=10.100.17.1 (local), d=10.100.17.7 (FastEthernet0/0), len 100,
sending
IP: s=10.0.0.3 (Serial0/0), d=224.0.0.10, len 100, rcvd 2
IP: s=10.255.255.1 (local), d=224.0.0.10 (Loopback0), len 60, sending
broad/multicast
IP: s=10.255.255.1 (Loopback0), d=224.0.0.10, len 60, rcvd 2
IP: s=10.0.0.2 (Serial0/0), d=224.0.0.10, len 100, rcvd 2
IP: tableid=0, s=10.100.17.7 (FastEthernet0/0), d=10.100.17.1
(FastEthernet0/0), routed via RIB
IP: s=10.100.17.7 (FastEthernet0/0), d=10.100.17.1 (FastEthernet0/0),
len 100, rcvd 3
IP: s=10.100.17.1 (local), d=10.100.17.7 (FastEthernet0/0), len 100,
sending
IP: s=10.0.0.3 (Serial0/0), d=224.0.0.10, len 100, rcvd 2
IP: s=10.255.255.1 (local), d=224.0.0.10 (Loopback0), len 60, sending
broad/multicast
IP: s=10.255.255.1 (Loopback0), d=224.0.0.10, len 60, rcvd 2
IP: s=10.0.0.2 (Serial0/0), d=224.0.0.10, len 100, rcvd 2
IP: tableid=0, s=10.100.17.7 (FastEthernet0/0), d=10.100.17.1
(FastEthernet0/0), routed via RIB
IP: s=10.100.17.7 (FastEthernet0/0), d=10.100.17.1 (FastEthernet0/0),
len 100, rcvd 3
```

 **Note**

If EIGRP authentication failed, neighbor adjacency would not have occurred.

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                Interface      Hold Uptime    SRTT   RTO   Q   Seq
                               (sec)          (ms)          Cnt   Num
2   10.100.17.7              Fa0/0         13 00:07:06    3    200   0   291
1   10.0.0.3                  Se0/0         11 00:07:49    65   390   0   152
0   10.0.0.2                  Se0/0         11 00:08:01    71   426   0   146
```

## 5.1 iBGP Peerings

### *Configuration*

---

R1#

```
router bgp 100
 neighbor 10.255.255.4 remote-as 100
 neighbor 10.255.255.4 update-source Loopback0
 neighbor 10.255.255.4 password DBMIBGP
 neighbor 10.255.255.7 remote-as 100
 neighbor 10.255.255.7 update-source Loopback0
 neighbor 10.255.255.7 password DBMIBGP
 neighbor 10.255.255.8 remote-as 100
 neighbor 10.255.255.8 update-source Loopback0
 neighbor 10.255.255.8 password DBMIBGP
```

R4#

```
router bgp 100
 neighbor 10.255.255.1 remote-as 100
 neighbor 10.255.255.1 update-source Loopback0
 neighbor 10.255.255.1 password DBMIBGP
 neighbor 10.255.255.7 remote-as 100
 neighbor 10.255.255.7 update-source Loopback0
 neighbor 10.255.255.7 password DBMIBGP
 neighbor 10.255.255.8 remote-as 100
 neighbor 10.255.255.8 update-source Loopback0
 neighbor 10.255.255.8 password DBMIBGP
```

SW1#

```
router bgp 100
 neighbor 10.255.255.1 remote-as 100
 neighbor 10.255.255.1 update-source Loopback0
 neighbor 10.255.255.1 password DBMIBGP
 neighbor 10.255.255.4 remote-as 100
 neighbor 10.255.255.4 update-source Loopback0
 neighbor 10.255.255.4 password DBMIBGP
 neighbor 10.255.255.8 remote-as 100
 neighbor 10.255.255.8 update-source Loopback0
 neighbor 10.255.255.8 password DBMIBGP
```

SW2#

```
router bgp 100
 neighbor 10.255.255.1 remote-as 100
 neighbor 10.255.255.1 update-source Loopback0
 neighbor 10.255.255.1 password DBMIBGP
 neighbor 10.255.255.4 remote-as 100
 neighbor 10.255.255.4 update-source Loopback0
 neighbor 10.255.255.4 password DBMIBGP
 neighbor 10.255.255.7 remote-as 100
 neighbor 10.255.255.7 update-source Loopback0
 neighbor 10.255.255.7 password DBMIBGP
```

**Verification**

---

**R1#show ip bgp summary**

BGP router identifier 10.255.255.1, local AS number 100  
 BGP table version is 1, main routing table version 1

Neighbor State/PfxRcd	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	
10.255.255.4	4	100	2	2	0	0	0	00:00:27	0
10.255.255.7	4	100	2	2	0	0	0	00:00:18	0
10.255.255.8	4	100	2	2	0	0	0	00:00:03	0

**R4#show ip bgp summary**

BGP router identifier 10.255.255.4, local AS number 100  
 BGP table version is 1, main routing table version 1

Neighbor State/PfxRcd	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	
10.255.255.1	4	100	3	2	0	0	0	00:00:39	0
10.255.255.7	4	100	2	2	0	0	0	00:00:33	0
10.255.255.8	4	100	2	2	0	0	0	00:00:24	0

**SW1#show ip bgp summary**

BGP router identifier 10.255.255.7, local AS number 100  
 BGP table version is 1, main routing table version 1

Neighbor State/PfxRcd	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	
10.255.255.1	4	100	3	2	0	0	0	00:00:34	0
10.255.255.4	4	100	2	2	0	0	0	00:00:36	0
10.255.255.8	4	100	2	2	0	0	0	00:00:28	0

**SW2#show ip bgp summary**

BGP router identifier 10.255.255.8, local AS number 100  
 BGP table version is 1, main routing table version 1

Neighbor State/PfxRcd	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	
10.255.255.1	4	100	2	2	0	0	0	00:00:21	0
10.255.255.4	4	100	2	2	0	0	0	00:00:29	0
10.255.255.7	4	100	2	2	0	0	0	00:00:30	0

## 5.2 EBGP Peerings

### Configuration

---

```
R1#
router bgp 100
 neighbor 172.16.13.3 remote-as 300
 neighbor 172.16.13.3 password ISP1BGP
 neighbor 10.255.255.4 next-hop-self
 neighbor 10.255.255.7 next-hop-self
 neighbor 10.255.255.8 next-hop-self
```

```
R4#
router bgp 100
 neighbor 172.16.46.6 remote-as 600
 neighbor 172.16.46.6 password ISP2BGP
 neighbor 172.16.46.6 timers 1 3
 neighbor 10.255.255.1 next-hop-self
 neighbor 10.255.255.7 next-hop-self
 neighbor 10.255.255.8 next-hop-self
```

### Verification

---

#### R1#show ip bgp summary

```
BGP router identifier 10.255.255.1, local AS number 100
BGP table version is 37, main routing table version 37
24 network entries using 2808 bytes of memory
36 path entries using 1872 bytes of memory
13/6 BGP path/bestpath attribute entries using 1612 bytes of memory
12 BGP AS-PATH entries using 336 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 6628 total bytes of memory
BGP activity 24/0 prefixes, 48/12 paths, scan interval 60 secs
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	
State/PfxRcd									
10.255.255.4	4	100	10	8	37	0	0	00:02:24	12
10.255.255.7	4	100	4	8	37	0	0	00:02:15	0
10.255.255.8	4	100	4	7	37	0	0	00:02:00	0
172.16.13.3	4	300	10	11	37	0	0	00:00:02	24

**R4#show ip bgp summary**

```
BGP router identifier 10.255.255.4, local AS number 100
BGP table version is 37, main routing table version 37
24 network entries using 3168 bytes of memory
36 path entries using 1872 bytes of memory
10/6 BGP path/bestpath attribute entries using 1680 bytes of memory
9 BGP AS-PATH entries using 312 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 2 (at peak 2) using 64 bytes of memory
BGP using 7096 total bytes of memory
BGP activity 24/0 prefixes, 36/0 paths, scan interval 60 secs
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.255.255.1	4	100	8	10	37	0	0	00:02:41	12
10.255.255.7	4	100	4	10	37	0	0	00:02:35	0
10.255.255.8	4	100	4	10	37	0	0	00:02:25	0
172.16.46.6	4	600	52	48	37	0	0	00:00:43	24

 **Note**

Without next-hop modification on R1 and R4, SW1 and SW2 use default routes to reach the next-hop values of the BGP routes. Since they both default to their closest neighbor, either R1 or R4 respectively, traffic could be blackholed, as seen below. This is solved by using the next-hop-self command on R1 and R4 so that SW1 and SW2 choose the correct exit point out of the network.

**SW1#show ip route 182.17.0.1**

```
Routing entry for 182.17.0.0/16
  Known via "bgp 100", distance 200, metric 0
  Tag 600, type internal
  Last update from 172.16.46.6 00:03:37 ago
  Routing Descriptor Blocks:
  * 172.16.46.6, from 10.255.255.4, 00:03:37 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
    Route tag 600
```

**SW1#show ip route 172.16.46.6**

```
% Network not in table
```

**SW1#show ip route 0.0.0.0**

```
Routing entry for 0.0.0.0/0, supernet
  Known via "eigrp 100", distance 170, metric 284160, candidate default path,
  type external
  Redistributing via eigrp 100
  Last update from 10.100.17.1 on FastEthernet0/1, 00:04:23 ago
  Routing Descriptor Blocks:
  * 10.100.17.1, from 10.100.17.1, 00:04:23 ago, via FastEthernet0/1
    Route metric is 284160, traffic share count is 1
    Total delay is 10100 microseconds, minimum bandwidth is 100000 Kbit
    Reliability 255/255, minimum MTU 1500 bytes
    Loading 1/255, Hops 1
```

**R1#show ip route 182.17.0.1**

```
Routing entry for 182.17.0.0/16
  Known via "bgp 100", distance 200, metric 0
  Tag 600, type internal
  Last update from 172.16.46.6 00:17:42 ago
  Routing Descriptor Blocks:
  * 172.16.46.6, from 10.255.255.4, 00:17:42 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
    Route tag 600
```

**R1#show ip route 172.16.46.6**

% Subnet not in table

**R1#show ip route 0.0.0.0**

```
Routing entry for 0.0.0.0/0, supernet
  Known via "static", distance 1, metric 0 (connected), candidate
  default path
  Redistributing via eigrp 100
  Advertised by eigrp 100 metric 100000 1000 255 1 1500
  Routing Descriptor Blocks:
  * directly connected, via Null0
    Route metric is 0, traffic share count is 1
```

**SW1#traceroute**

```
Protocol [ip]:
Target IP address: 182.17.0.1
Source address: 10.100.7.7
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 182.17.0.1
```

```
 1 10.100.17.1 0 msec 8 msec 0 msec
 2 10.100.17.1 !H * !H
```

After next-hop modification

SW1#show ip bgp

BGP table version is 49, local router ID is 10.255.255.7  
 Status codes: s suppressed, d damped, h history, \* valid, > best, i - internal,  
 r RIB-failure, S Stale  
 Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*>i1.0.0.0/10	10.255.255.1	0	100	0	300 ?
*>i1.64.0.0/10	10.255.255.1	0	100	0	300 ?
*>i1.128.0.0/10	10.255.255.1	0	100	0	300 ?
*>i1.192.0.0/10	10.255.255.1	0	100	0	300 ?
*>i2.0.0.0/24	10.255.255.4	0	100	0	600 600 600 600 8543 i
*>i2.0.18.0/24	10.255.255.4	0	100	0	600 600 600 600 8543 i
*>i2.0.35.0/24	10.255.255.4	0	100	0	600 600 600 600 8543 i
*>i2.0.87.0/24	10.255.255.4	0	100	0	600 600 600 600 8543 i
*>i4.0.0.0/9	10.255.255.4	0	100	0	600 1221 4637 335 ?
*>i4.128.0.0/9	10.255.255.4	0	100	0	600 1221 4637 335 ?
*>i182.12.0.0	10.255.255.4	0	100	0	600 i
*>i182.13.0.0	10.255.255.4	0	100	0	600 i
*>i182.14.0.0	10.255.255.4	0	100	0	600 i
*>i182.15.0.0	10.255.255.4	0	100	0	600 i
*>i182.16.0.0	10.255.255.4	0	100	0	600 i
*>i182.17.0.0	10.255.255.4	0	100	0	600 i
*>i192.10.0.0/20	10.255.255.1	0	100	0	300 18 243 93 813 i
*>i192.10.16.0/20	10.255.255.1	0	100	0	300 18 243 93 813 i
*>i192.10.32.0/20	10.255.255.1	0	100	0	300 18 243 93 813 i
*>i192.10.48.0/20	10.255.255.1	0	100	0	300 18 243 93 813 i
*>i192.168.0.0	10.255.255.1	0	100	0	300 7018 7018 7018 1200 i
*>i192.168.1.0	10.255.255.1	0	100	0	300 7018 7018 7018 1200 i
*>i192.168.2.0	10.255.255.1	0	100	0	300 7018 7018 7018 1200 i
*>i192.168.3.0	10.255.255.1	0	100	0	300 7018 7018 7018 1200 i

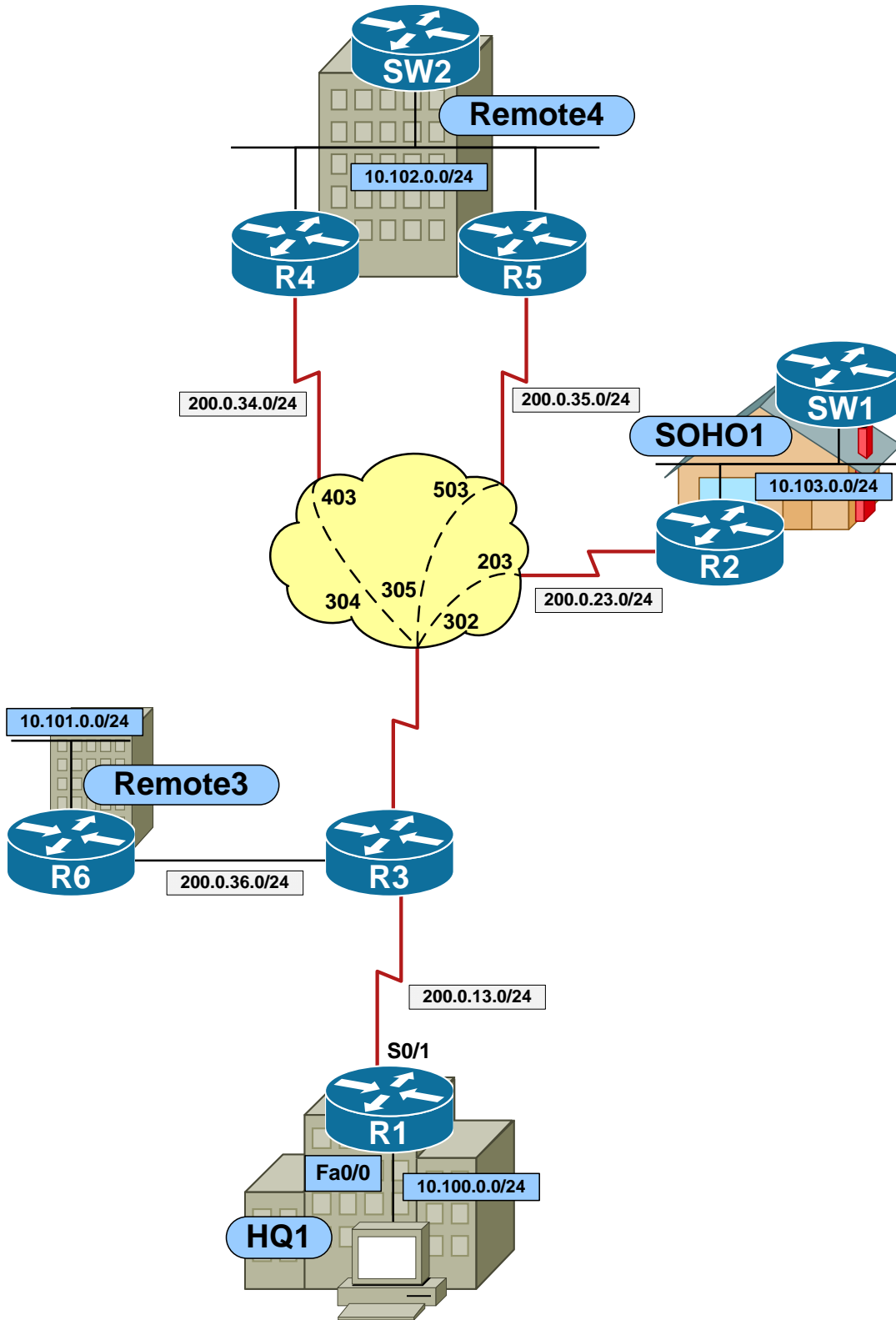
# Implementing Secure Converged Wide-Area Networks (ISCW) & Optimizing Converged Cisco Networks (ONT)

## Case Study Overview

The next phase of network migration for Dexter Bean Manufacturing involves implementing secure remote access for additional business units that connect back to the HQ office via the Internet, securing the network from unauthorized access, and optimizing application response times through QoS.

Note that since these configurations requires access to the Security Device Manager (SDM) GUI, a PC with access into the rack topology is required. The physical topology in the solutions uses INE's CCIE Security hardware specification, since that topology includes Virtual Machines that can be used to access the SDM of the devices. Like the CCIE R&S topology, the CCIE Security topology is available for rent via GradedLabs, however other methods discussed before such as Dynamips/GNS3 would also suffice.

## DBM Inc. VPN Diagram



 **Note**

Prior to starting this section load the *ISCW VPN Initial Configs* for all devices. Refer to the *DBM Inc. VPN Diagram* for device, port, and addressing information.

The final phase of the new DBMI network design allows for secure remote access into the network via IPsec based VPNs terminating at the HQ1 office. The scope of this implementation includes two additional remote offices that will be connected by static Site-to-Site IPsec VPNs, and support for additional home office users via Remote Access IPsec VPNs.

The design team has informed you that all remote devices have been preconfigured in order to connect to the HQ1 office, but that you will need to configure the VPN server (R1) in order to allow access to the remote users. R1 is preconfigured with the username "sdm" and the password "cisco" for SDM GUI access.

## 8.1 Site-to-Site VPN

- The newly opened Remote3 office requires access to the DBMI network, but due to cost limitations a private circuit was not provisioned between the sites. Instead, the Remote3 office uses the public Internet to reach the HQ1 office. To accommodate this, the design team has requested that R1 be configured to support a Site-to-Site IPsec based VPN using the following parameters:
  - ISAKMP Pre-Shared Key: S2SKEY
  - ISAKMP Encryption: 3DES
  - ISAKMP Hash: MD5
  - ISAKMP DH Group: 5
  - IPsec Integrity Checking: ESP MD5 HMAC
  - IPsec Encryption: ESP AES 128-bit
  - Traffic between the 10.100.0.0/24 and 10.101.0.0/24 subnets should be encrypted.

## 8.2 Site-to-Site GRE over IPsec VPN

- Like the Remote3 office, the Remote4 office uses the public Internet to reach HQ1. The design team has informed you, however, that the Remote4 office has multiple Internet connections for redundancy. To accommodate this, the design team has requested that R1 create two VPN tunnels to the Remote4 office as follows:
  - The tunnel to R4 should use the IP address 10.104.0.1, be sourced from R1's link to R3, and destined to 200.0.34.4.
  - The tunnel to R5 should use the IP address 10.105.0.1, be sourced from R1's link to R3, and destined to 200.0.35.5.
  - Use the following IPsec parameters:
    - ISAKMP Pre-Shared Key: GREKEY
    - ISAKMP Encryption: 3DES
    - ISAKMP Hash: MD5
    - ISAKMP DH Group: 5
    - IPsec Integrity Checking: ESP MD5 HMAC
    - IPsec Encryption: ESP 3DES
  - EIGRP AS 100 should be used for dynamic routing of the 10.100.0.0/24 network.
  - Traffic between the 10.100.0.0/24 and 10.102.0.0/24 networks should route through R4; if R4's link to the Internet is down traffic should be rerouted through R5.

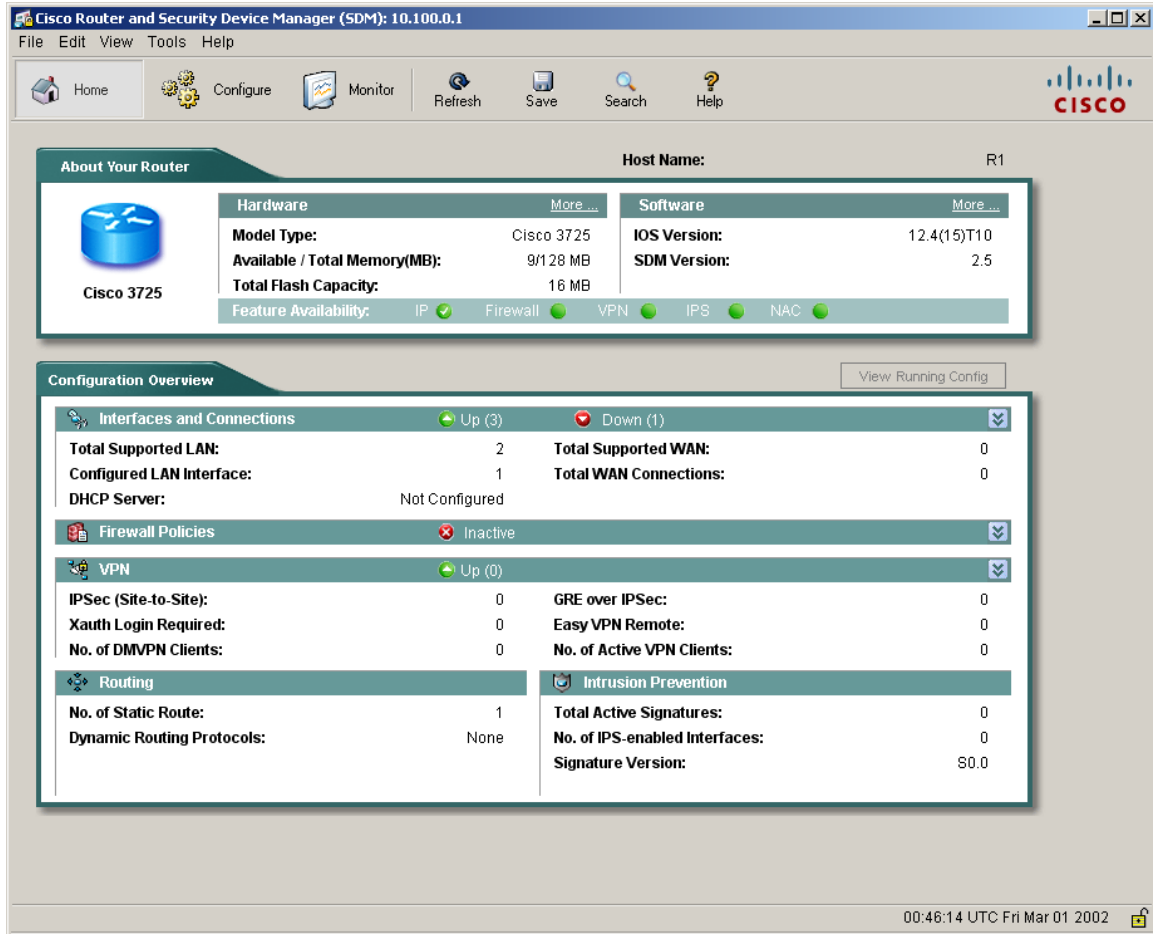
## 8.3 Easy VPN

- Home office users will be accessing the HQ1 office's resources by using the Cisco VPN client over the Internet. To facilitate this, the design team has requested you to configure R1 as an EasyVPN server using the following parameters:
  - ISAKMP Authentication: Pre-Shared Key
  - ISAKMP Encryption: 3DES
  - ISAKMP Hash: SHA
  - ISAKMP DH Group: 2
  - IPsec Integrity Checking: ESP MD5 SHA
  - IPsec Encryption: ESP 3DES
  - VPN group name: DBMIGROUP
  - VPN group Pre-Shared Key: DBMIPASS
  - XAuth username: vpnuser
  - XAuth password: vpnpass
  - IP address pool: 10.255.0.0/24

# ISCW & ONT Solutions

## 8.1 Site-to-Site VPN

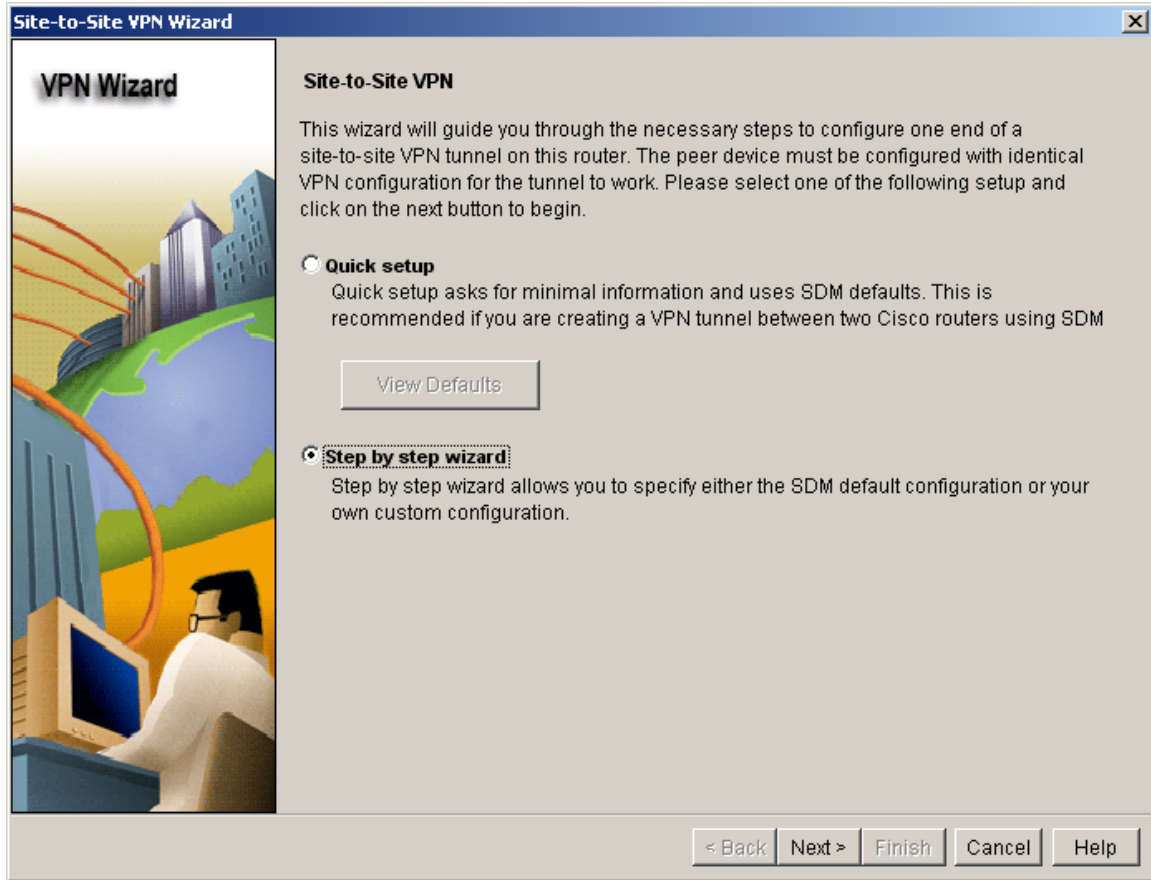
From the main SDM home screen, click the Configure tab.



Select the VPN task, then launch the Site-to-Site VPN wizard.

The screenshot shows the Cisco SDM (Security Device Manager) interface for a Cisco Router and Security Device Manager (SDM) at 10.100.0.1. The interface is titled "SDM:33168 - Remote Desktop" and "Cisco Router and Security Device Manager (SDM): 10.100.0.1". The main menu includes "File", "Edit", "View", "Tools", and "Help". The "Tasks" pane on the left shows a tree view under "VPN" with the following items: "Site-to-Site VPN", "Easy VPN Remote", "Easy VPN Server", "Dynamic Multipoint VPN", "SSL VPN", and "VPN Components". The "Site-to-Site VPN" item is selected. The main content area displays the "Create Site to Site VPN" wizard. It includes a "Use Case Scenario" diagram showing a "Local" site connected to an "Internet" cloud, which is then connected to a "Remote" site. Below the diagram, there are two radio button options: "Create a Site to Site VPN" (which is selected) and "Create a secure GRE tunnel (GRE over IPsec)". The "Create a Site to Site VPN" option has a description: "Use this option to configure a VPN tunnel from this router to another VPN device using either a pre-shared key or using digital certificates. To complete this configuration, you must know the remote device's IP address. If a pre-shared key is used for authentication, it must match the pre-shared key configured on the remote device." Below this description is a "Launch the selected task" button. At the bottom of the wizard, there is a "How do I:" dropdown menu with the text "How Do I Configure a Backup for an Easy VPN Remote connection?" and a "Go" button. The status bar at the bottom of the window shows "VPN" and the time "12:25:25 UTC Mon Nov 16 2009".

Select the step by step wizard.

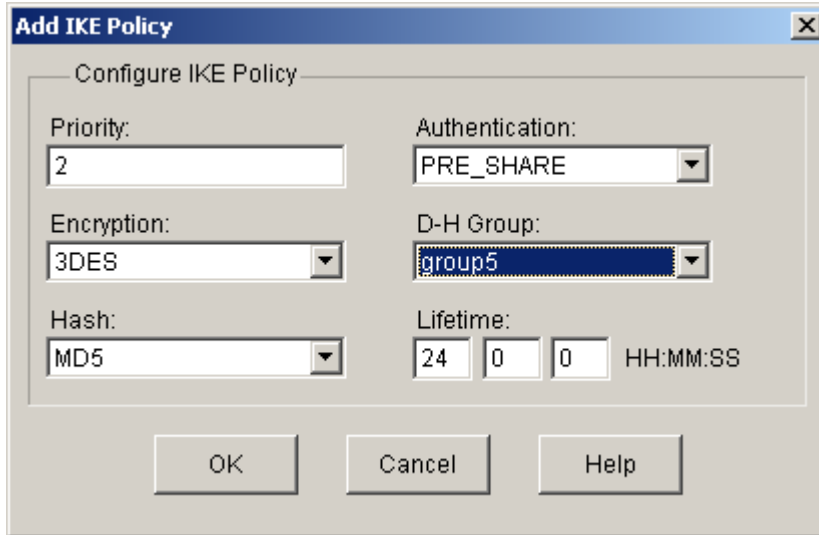


The outgoing interface for the tunnel should be S0/1 towards peer 200.0.36.6 with key S2SKEY.

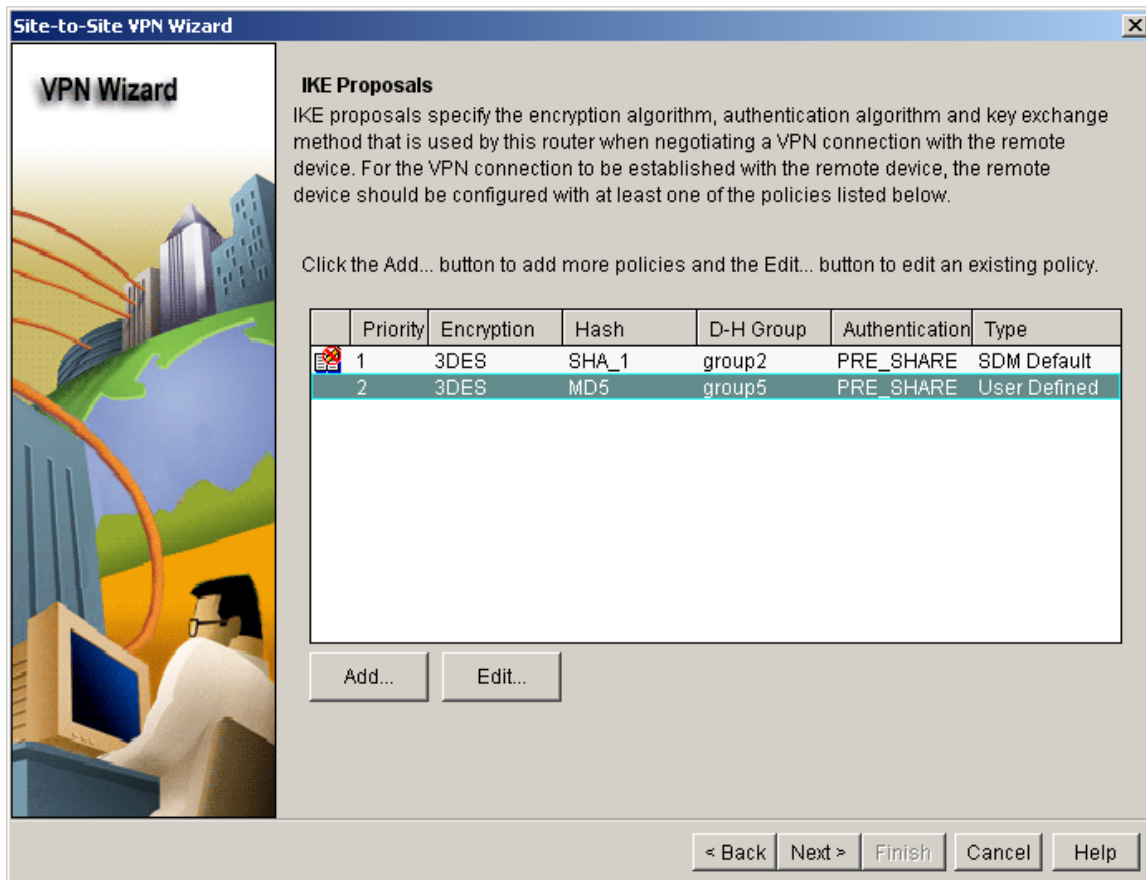
The screenshot shows the 'Site-to-Site VPN Wizard' configuration window. On the left is a graphic with the text 'VPN Wizard' and an illustration of a person at a computer. The main area is divided into three sections: 'VPN Connection Information', 'Peer Identity', and 'Authentication'. In the 'VPN Connection Information' section, the interface is set to 'Serial0/1'. The 'Peer Identity' section shows the peer type as 'Peer with static IP address' and the remote IP as '200.0.36.6'. The 'Authentication' section has 'Pre-shared Keys' selected, with two input fields for the key, both containing '\*\*\*\*\*'. Navigation buttons at the bottom include '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Section	Field	Value
VPN Connection Information	Select the interface for this VPN connection:	Serial0/1
	Peer Identity	Peer with static IP address
Peer Identity	Enter the IP address of the remote peer:	200.0.36.6
	Authentication	Pre-shared Keys (selected)
Authentication	Re-enter Key:	*****

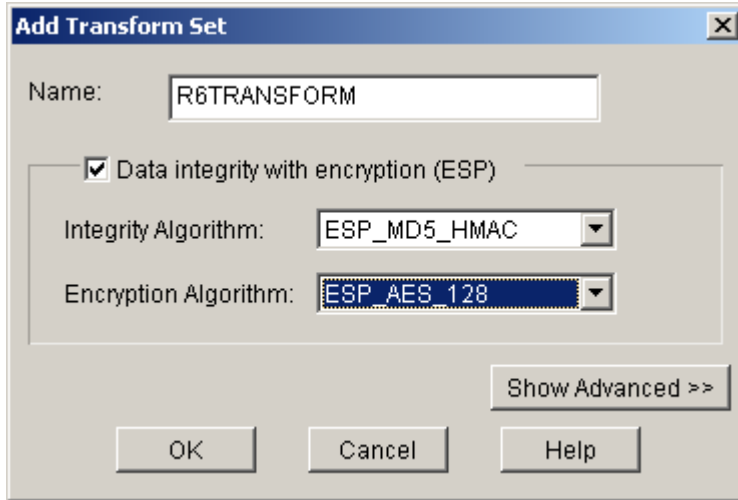
Add a new ISAKMP policy with the required parameters.



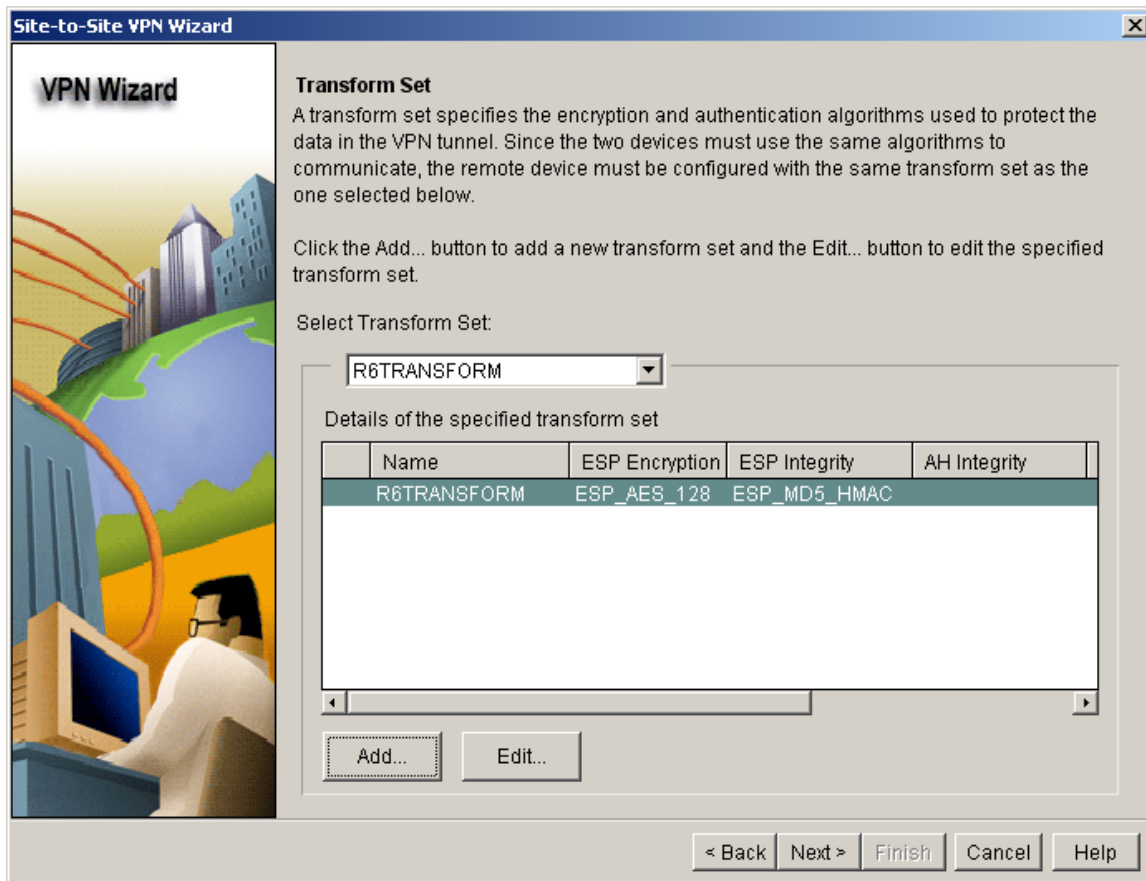
The final result is shown here.



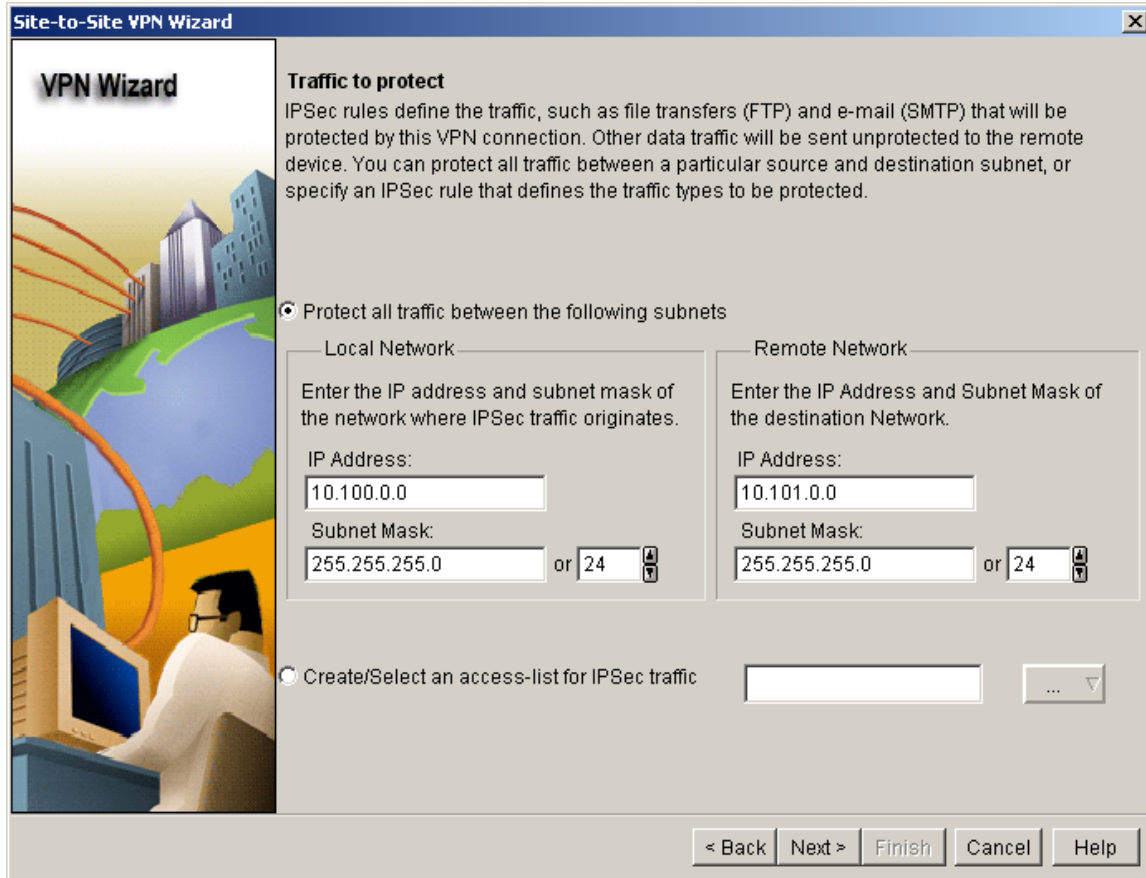
Create a new transform set with the following parameters.



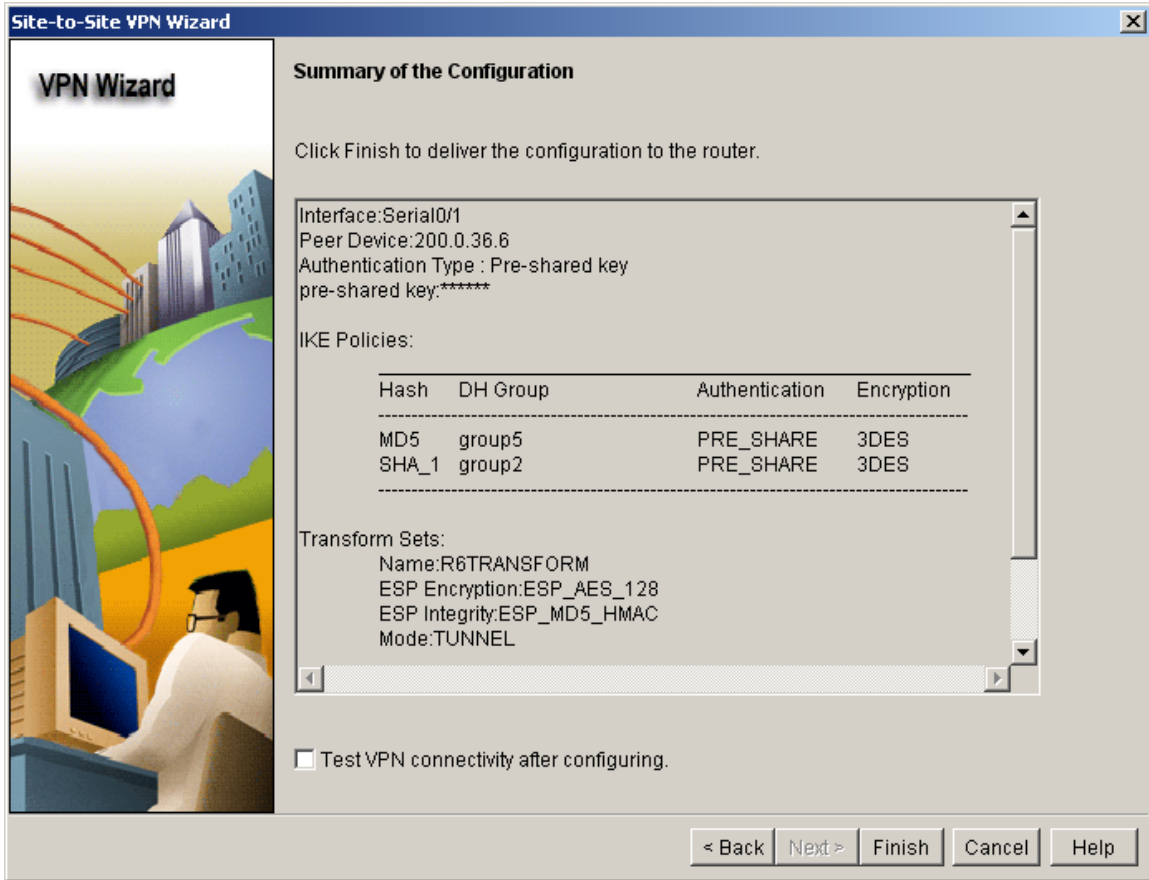
The final result is seen here.



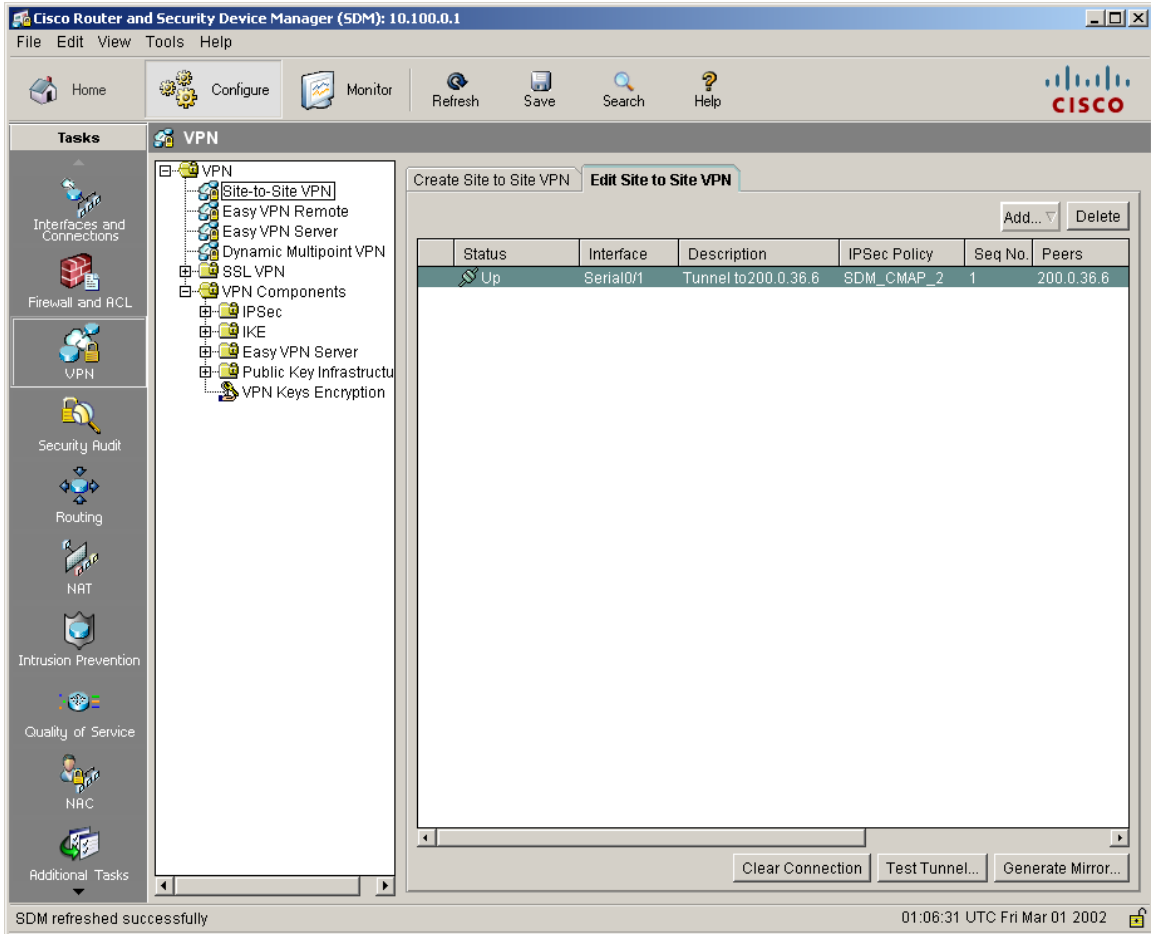
The proxy ACL defines what traffic goes over the tunnel.



Finally, apply the configuration.



The tunnel to R6 should show its status as up.



## Verification

R1#ping 10.101.0.6 source 10.100.0.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.101.0.6, timeout is 2 seconds:  
Packet sent with a source address of 10.100.0.1

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 8/11/24 ms

R1#show crypto isakmp sa

```
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
200.0.13.1  200.0.36.6  QM_IDLE       1001     0 ACTIVE
```

R1#show crypto ipsec sa

interface: Serial0/1

Crypto map tag: SDM\_CMAP\_2, local addr 200.0.13.1

protected vrf: (none)

local ident (addr/mask/prot/port): (10.100.0.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (10.101.0.0/255.255.255.0/0/0)

current\_peer 200.0.36.6 port 500

PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9

#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 8, #recv errors 0

local crypto endpt.: 200.0.13.1, remote crypto endpt.: 200.0.36.6

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1

current outbound spi: 0xAE7FEA10(2927618576)

inbound esp sas:

spi: 0x45DEA640(1172219456)

transform: esp-aes esp-md5-hmac ,

in use settings ={Tunnel, }

conn id: 1, flow\_id: SW:1, crypto map: SDM\_CMAP\_2

sa timing: remaining key lifetime (k/sec): (4378303/3460)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:

spi: 0xAE7FEA10(2927618576)

transform: esp-aes esp-md5-hmac ,

in use settings ={Tunnel, }

conn id: 2, flow\_id: SW:2, crypto map: SDM\_CMAP\_2

sa timing: remaining key lifetime (k/sec): (4378303/3460)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE

outbound ah sas:

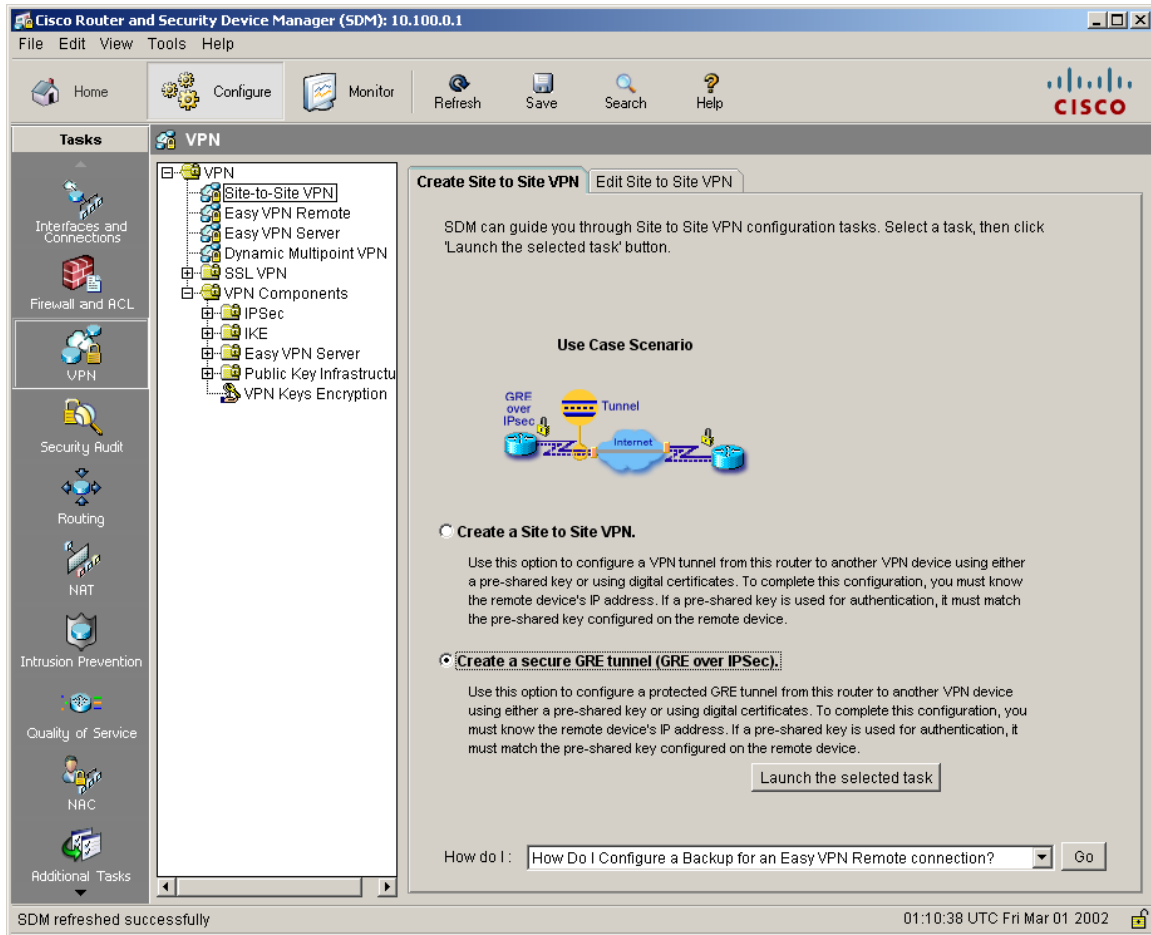
outbound pcg sas:

R1's final SDM configuration can be seen below:

```
R1#
crypto isakmp policy 2
  encr 3des
  hash md5
  authentication pre-share
  group 5
!
crypto isakmp key S2SKEY address 200.0.36.6
!
crypto ipsec transform-set R6TRANSFORM esp-aes esp-md5-hmac
!
crypto map SDM_CMAP_2 1 ipsec-isakmp
  description Tunnel to200.0.36.6
  set peer 200.0.36.6
  set transform-set R6TRANSFORM
  match address 101
!
interface Serial0/1
  crypto map SDM_CMAP_2
!
access-list 101 remark SDM_ACL Category=4
access-list 101 remark IPSec Rule
access-list 101 permit ip 10.100.0.0 0.0.0.255 10.101.0.0 0.0.0.255
```

## 8.2 Site-to-Site GRE over IPsec VPN

Under the VPN task, select the GRE over IPsec wizard.



Create the tunnel to R4.

**Secure GRE Wizard**

**VPN Wizard**

**GRE Tunnel Information**

Tunnel Source

Interface:  
 Serial0/1 Details...

IP Address:

Tunnel Destination

IP address of the Tunnel Destination:  
200.0.34.4

IP address of the GRE tunnel

GRE tunnel IP address is required to establish a tunnel with the peer.  
This entry can be a private address.

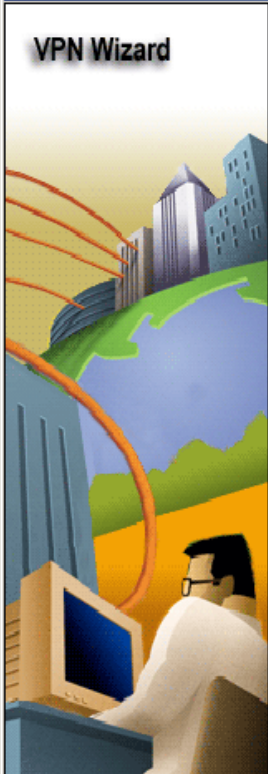
IP Address: 10.104.0.1 Subnet Mask: 255.255.255.0 or 24

Enable path MTU discovery

< Back Next > Finish Cancel Help

The tunnel to R5 is used as a backup.

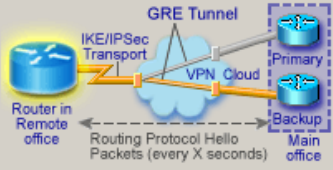
Secure GRE Wizard
✕



VPN Wizard

### Backup GRE Tunnel Information

Backup GRE tunnel can be configured for VPN resilience. If the primary GRE tunnel is down, the router will detect this loss of connectivity and will provide stateless failover by choosing the backup GRE tunnel.



Create a backup secure GRE tunnel for resilience

IP address of the backup GRE tunnel's destination:  
(Backup VPN Peer)

TunnelIP Address

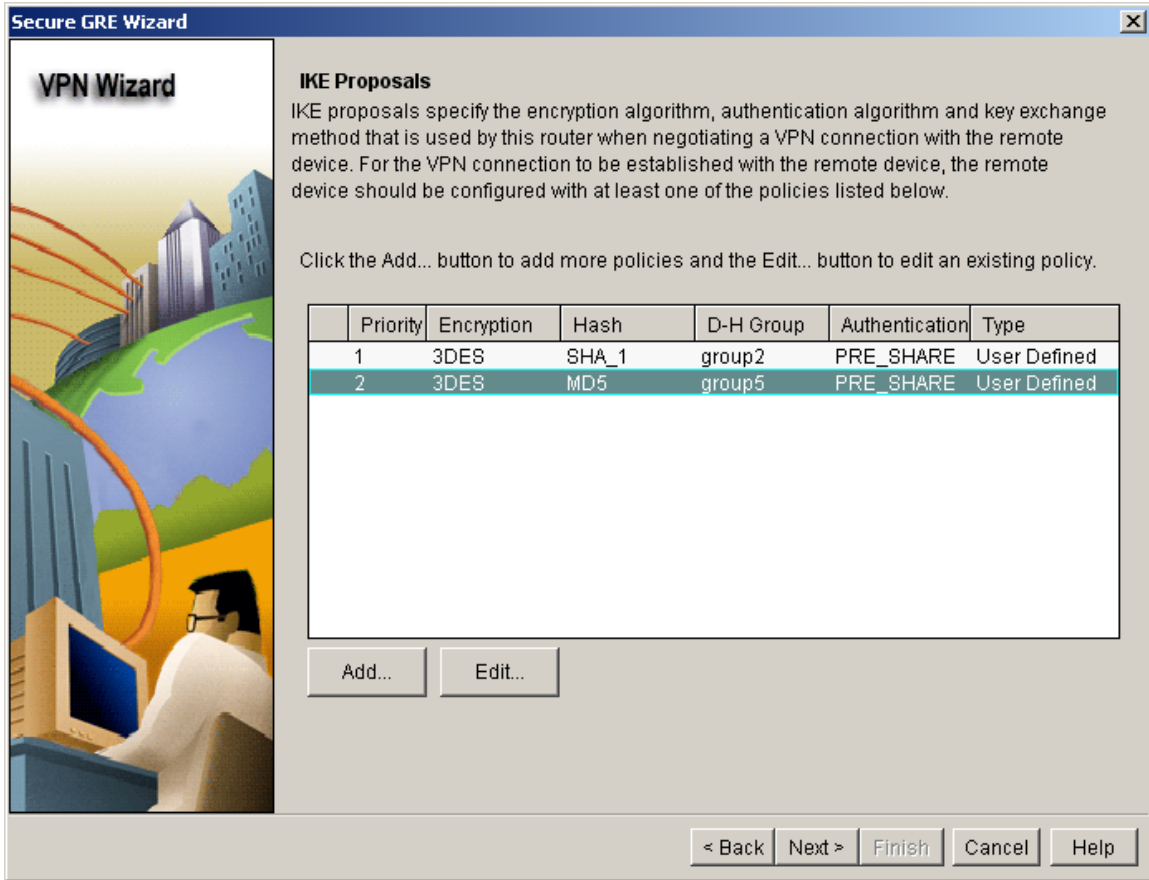
IP Address: <input style="width: 90%;" type="text" value="10.105.0.1"/>	Network Mask: <input style="width: 90%;" type="text" value="255.255.255.0"/> or <input style="width: 30px;" type="text" value="24"/>
--	---

< Back
Next >
Finish
Cancel
Help

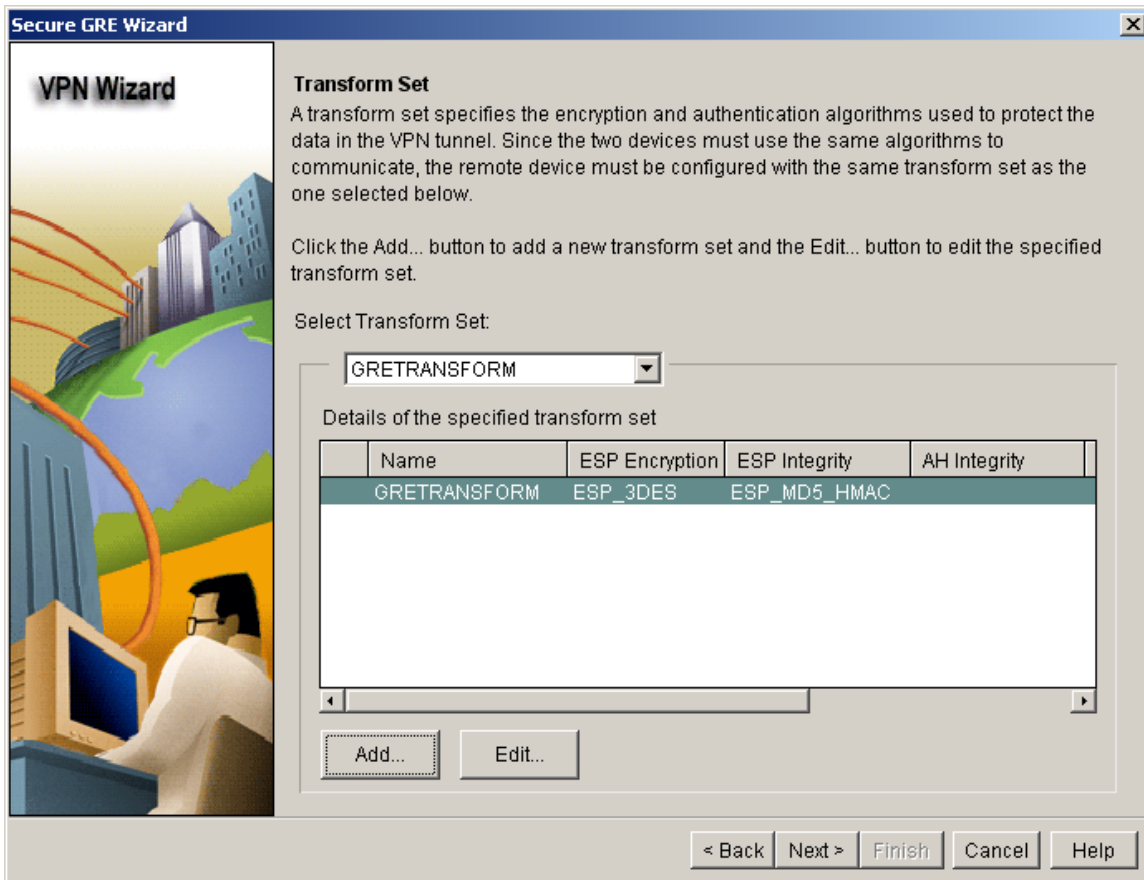
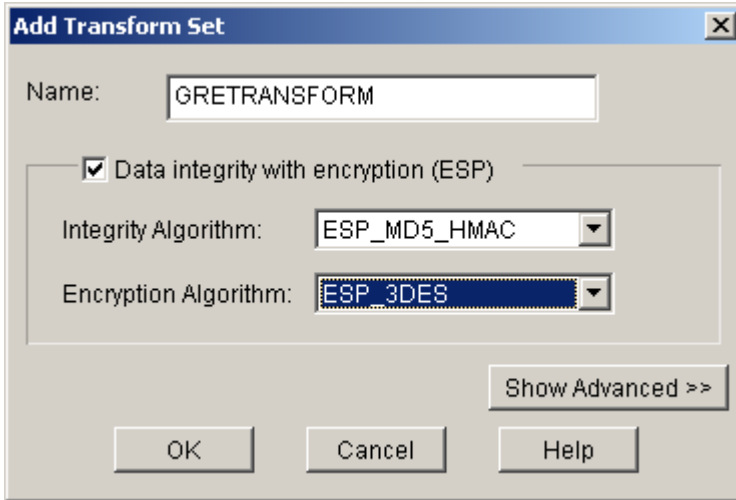
Define the ISAKMP Pre-Shared Key.

The screenshot shows a window titled "Secure GRE Wizard" with a close button in the top right corner. On the left side, there is a vertical panel with the text "VPN Wizard" and an illustration of a person at a computer with a globe and city buildings in the background. The main area of the window is titled "VPN Authentication Information". Underneath this title is a section labeled "Authentication" with the text "Authentication ensures that each end of the VPN connection uses the same secret key." Below this text are two radio button options: "Pre-shared Keys" (which is selected) and "Digital Certificates". Under the "Pre-shared Keys" option, there are two text input fields. The first is labeled "pre-shared key:" and contains seven asterisks. The second is labeled "Re-enter Key:" and also contains seven asterisks. At the bottom right of the window, there are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

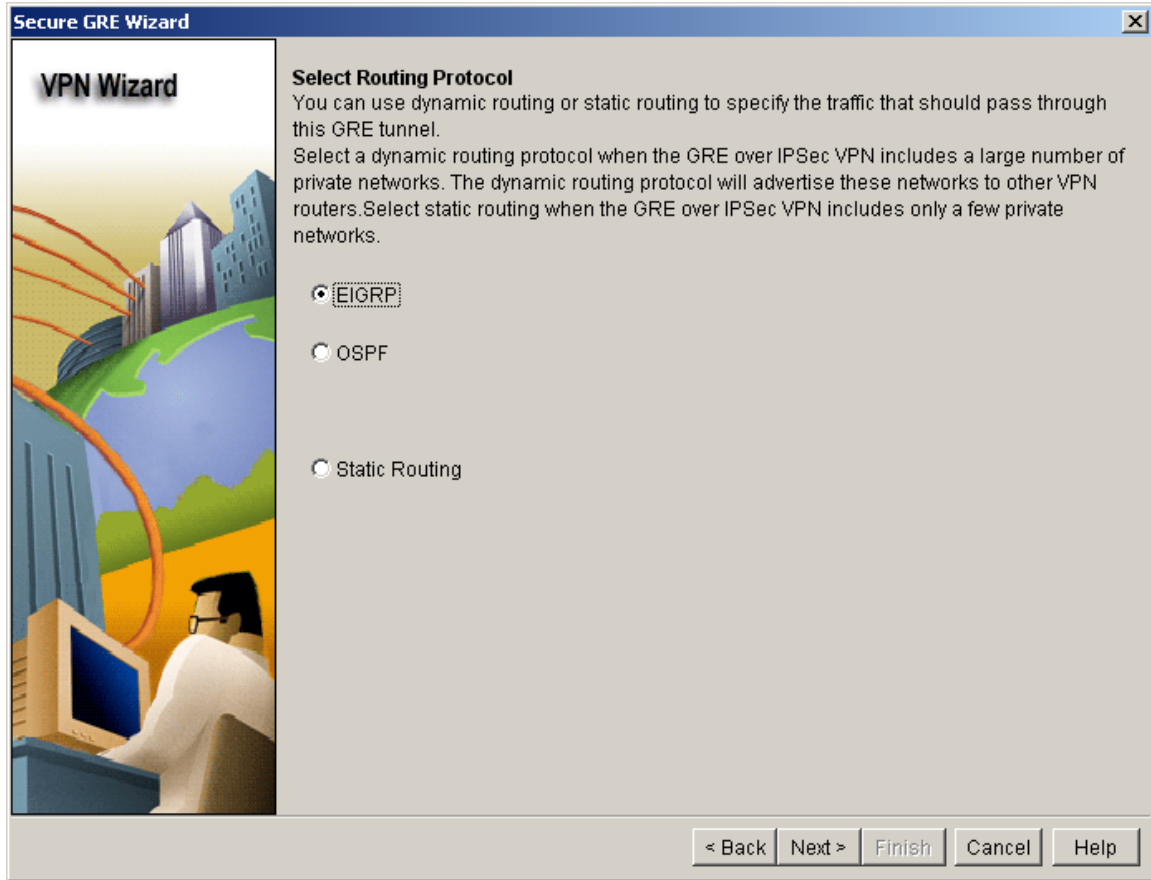
The same ISAKMP policy from before can be reused.



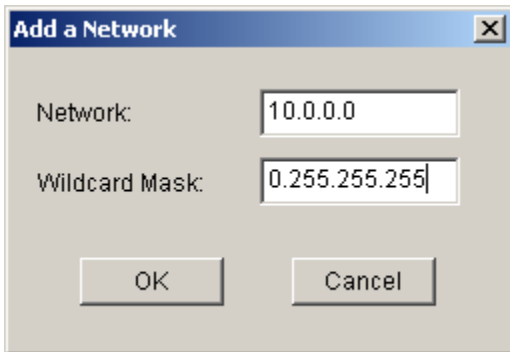
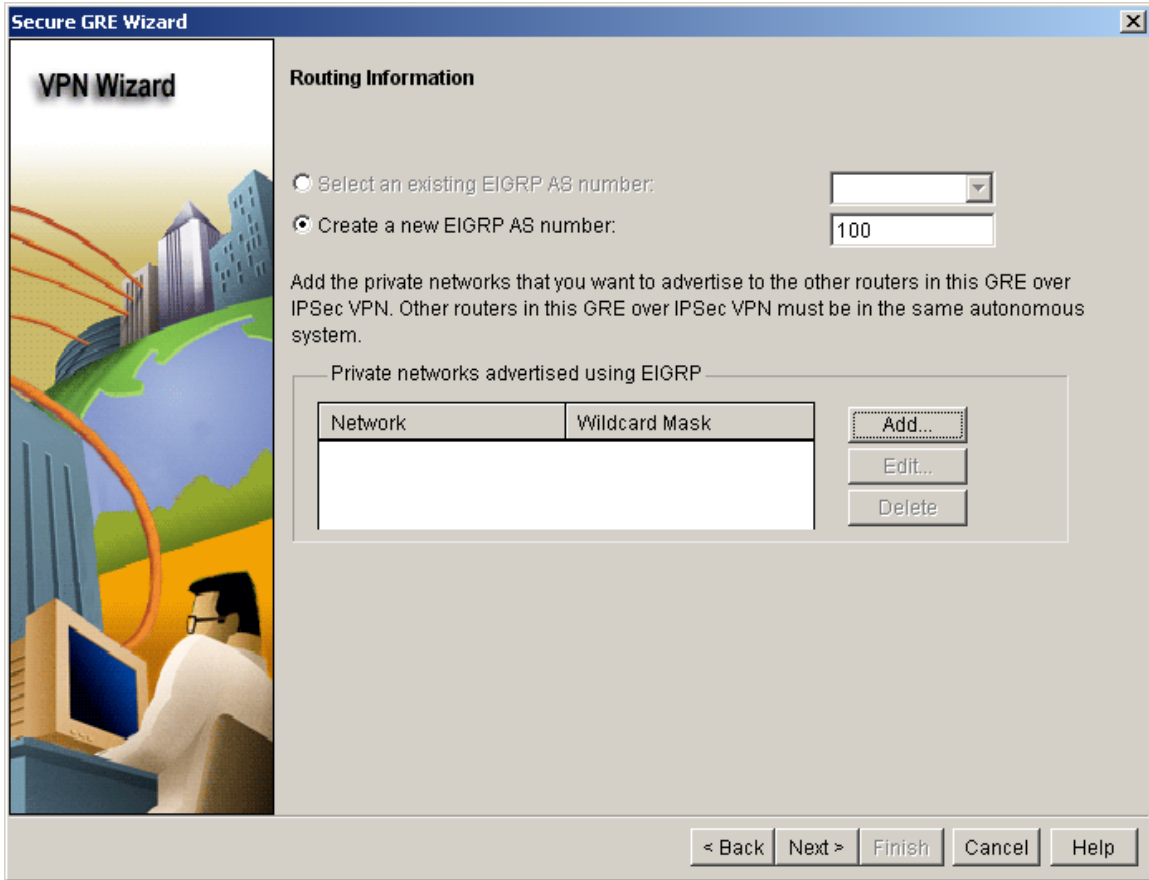
The Transform Set should be defined as follows.



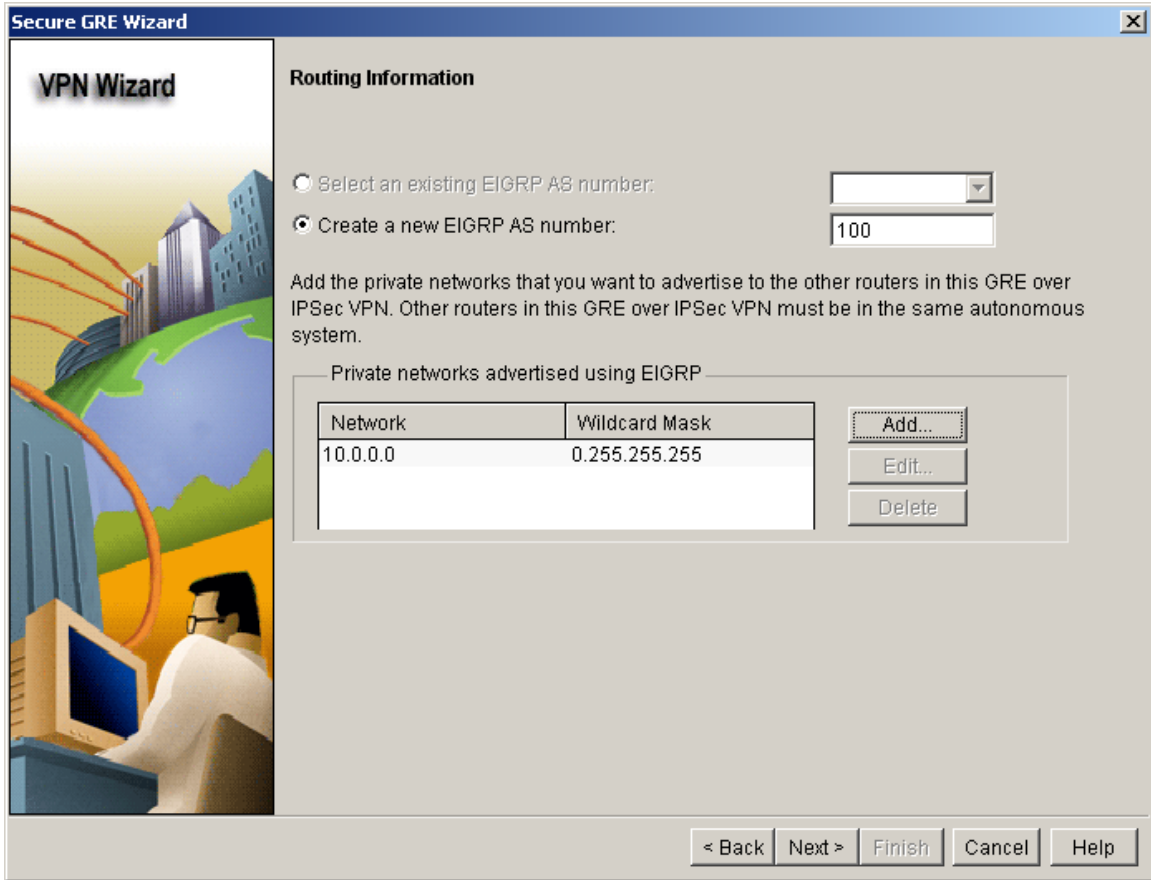
Select EIGRP for dynamic routing.



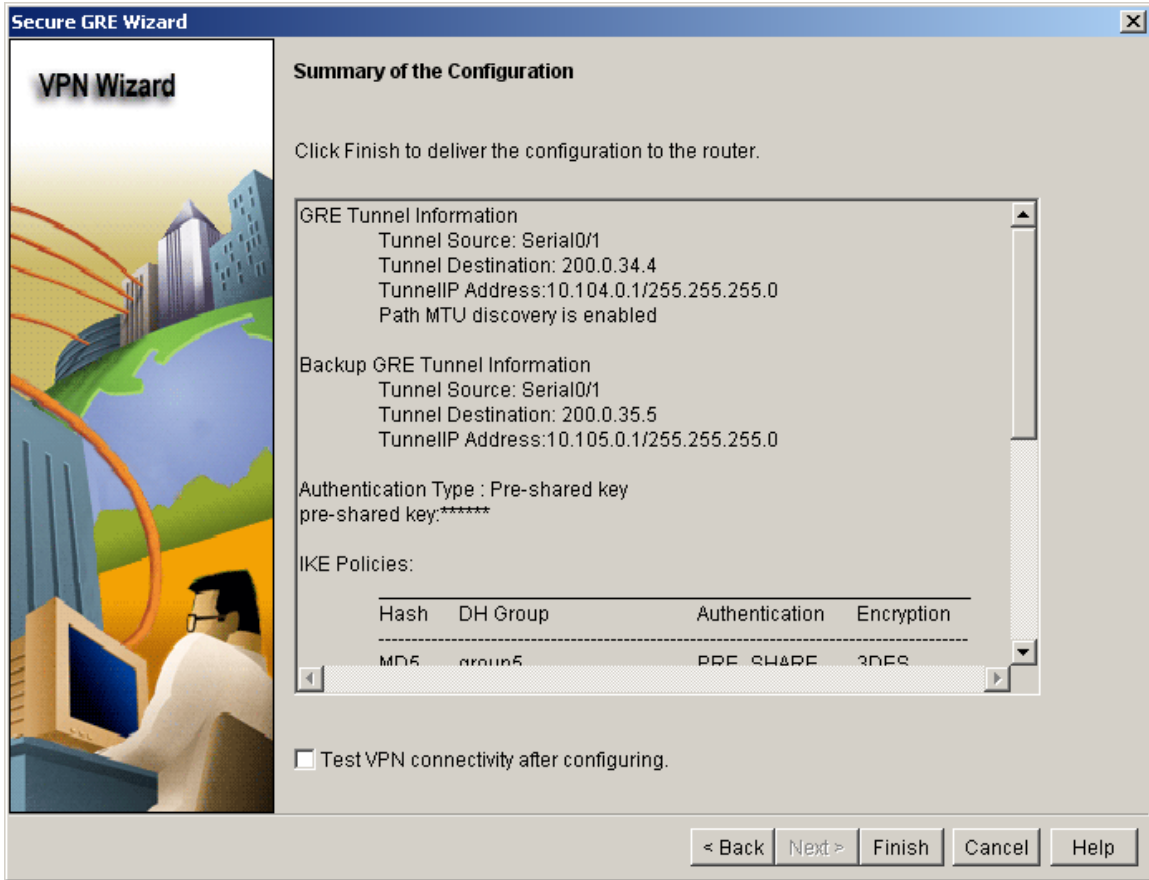
Define the EIGRP AS 100, then add the network.



The result:



Finally, apply the config.



If successful, all tunnels should have a status of Up.

The screenshot shows the Cisco Router and Security Device Manager (SDM) interface. The main window is titled "Cisco Router and Security Device Manager (SDM): 10.100.0.1". The interface includes a menu bar (File, Edit, View, Tools, Help) and a toolbar with icons for Home, Configure, Monitor, Refresh, Save, Search, and Help. The left sidebar contains various task categories: Interfaces and Connections, Firewall and ACL, VPN, Security Audit, Routing, NAT, Intrusion Prevention, Quality of Service, NAC, and Additional Tasks. The central pane shows the "VPN" configuration tree, with "Site-to-Site VPN" selected. The right pane displays the "Edit Site to Site VPN" configuration, which includes a table of active tunnels.

Status	Interface	Description	IPSec Policy	Seq No.	Peers
Up	Tunnel0 / Ser	Tunnel to200.0.35.5	SDM_CMAP_2	3	200.0.35.5
Up	Tunnel0 / Ser	Tunnel to200.0.34.4	SDM_CMAP_2	2	200.0.34.4
Up	Tunnel0 / Ser	Tunnel to200.0.36.6	SDM_CMAP_2	1	200.0.36.6
Up	Tunnel1 / Ser	Tunnel to200.0.35.5	SDM_CMAP_2	3	200.0.35.5
Up	Tunnel1 / Ser	Tunnel to200.0.34.4	SDM_CMAP_2	2	200.0.34.4
Up	Tunnel1 / Ser	Tunnel to200.0.36.6	SDM_CMAP_2	1	200.0.36.6

At the bottom of the interface, a status bar indicates "SDM refreshed successfully" on the left and "01:22:48 UTC Fri Mar 01 2002" on the right.

## Verification

### R1#show crypto isakmp sa

```
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
200.0.13.1  200.0.35.5  QM_IDLE       1003      0 ACTIVE
200.0.13.1  200.0.36.6  QM_IDLE       1001      0 ACTIVE
200.0.13.1  200.0.34.4  QM_IDLE       1002      0 ACTIVE
200.0.35.5  200.0.13.1  QM_IDLE       1004      0 ACTIVE
```

IPv6 Crypto ISAKMP SA

### R1#show ip eigrp neighbor

```
IP-EIGRP neighbors for process 100
H   Address          Interface      Hold Uptime    SRTT   RTO  Q  Seq
                               (sec)          (ms)          Cnt  Num
1   10.104.0.4        Tu0           12 00:01:17    117   702  0   3
0   10.105.0.5        Tu1           13 00:01:57     63   378  0   3
```

### R1#show ip route eigrp

```
10.0.0.0/24 is subnetted, 4 subnets
D    10.102.0.0 [90/16090880] via 10.104.0.4, 00:01:19, Tunnel0
```

### R1#show ip eigrp topology 10.102.0.0 255.255.255.0

```
IP-EIGRP (AS 100): Topology entry for 10.102.0.0/24
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 16090880
Routing Descriptor Blocks:
 10.104.0.4 (Tunnel0), from 10.104.0.4, Send flag is 0x0
   Composite metric is (16090880/281600), Route is Internal
   Vector metric:
     Minimum bandwidth is 784 Kbit
     Total delay is 501000 microseconds
     Reliability is 255/255
     Load is 1/255
     Minimum MTU is 1420
     Hop count is 1
 10.105.0.5 (Tunnell1), from 10.105.0.5, Send flag is 0x0
   Composite metric is (16193792/281600), Route is Internal
   Vector metric:
     Minimum bandwidth is 760 Kbit
     Total delay is 501000 microseconds
     Reliability is 255/255
     Load is 1/255
     Minimum MTU is 1420
     Hop count is 1
```

### R1#ping 10.102.0.8 source 10.100.0.1

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.102.0.8, timeout is 2 seconds:
Packet sent with a source address of 10.100.0.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/16 ms
```

### R1#traceroute 10.102.0.8 source 10.100.0.1

```
Type escape sequence to abort.
Tracing the route to 10.102.0.8

 1 10.104.0.4 12 msec 12 msec 8 msec
 2 10.102.0.8 12 msec * 8 msec
```

R4 loses its connection to the WAN:

```
R4#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#interface Serial0/0
R4(config-if)#shutdown
R4(config-if)#end
R4#
*Mar  1 01:48:09.351: %SYS-5-CONFIG_I: Configured from console by console
*Mar  1 01:48:10.763: %LINK-5-CHANGED: Interface Serial0/0, changed state to
administratively down
*Mar  1 01:48:11.763: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0, changed state to down
```

R1 reroutes via R5's tunnel:

```
R1#traceroute 10.102.0.8 source 10.100.0.1
```

```
Type escape sequence to abort.
Tracing the route to 10.102.0.8
```

```
 1  *
   10.105.0.5 8 msec 8 msec
 2 10.102.0.8 12 msec * 12 msec
```