



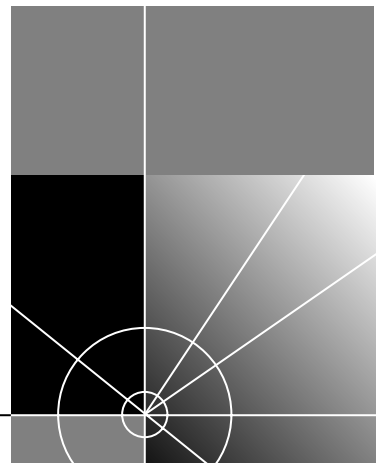
# SuperStack® II Switch Layer 3 Module User Guide

For units in the SuperStack II Switch 1100/3300 family

Switch Agent Software version 2.4 or later and  
SuperStack II Switch Layer 3 Module Management Software  
version 1.0

<http://www.3com.com/>

Part No. DUA1696-8AAA02  
Published October 1999



**3Com Corporation**  
**5400 Bayfront Plaza**  
**Santa Clara, California**  
**95052-8145, U.S.A.**

Copyright © 1999, 3Com Technologies. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Technologies.

3Com Technologies reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Technologies to provide notification of such revision or change. 3Com Technologies provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

#### UNITED STATES GOVERNMENT LEGENDS:

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

**United States Government Legend:** All technical data and computer software is commercial in nature and developed solely at private expense. Software is delivered as Commercial Computer Software as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo, SmartAgent, SuperStack, and Transcend are registered trademarks of 3Com Corporation. PACE is a trademark of 3Com Corporation. 3ComFacts is a service mark of 3Com Corporation.

Adobe, Acrobat and the Acrobat logo are registered trademarks of Adobe Systems Incorporated which may be registered in certain jurisdictions. Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation. Sun is a trademark of Sun Microsystems, Inc.

Other brand and product names may be registered trademarks or trademarks of their respective holders.

#### **Environmental Statement**

It is a 3Com policy to be environmentally friendly in all operations. This manual is printed on paper that comes from sustainable, managed European forests. The production process for making the pulp has a reduced AOX level (absorbable organic halogen) resulting in elemental chlorine-free paper.

The paper is fully biodegradable and recyclable.

Written and illustrated by Laura Fergusson, Katharine Woods and Emma Cuthbert. Edited by Patrina Law. Technical input from Stuart Boutell.

# CONTENTS

---

## ABOUT THIS GUIDE

How to Use This Guide	7
User Guide Conventions	8
Terminology Used in This Guide	9
Related Documentation	9
Feedback about this User Guide	10
Year 2000 Compliance	10
Product Registration	11

---

## 1 INTRODUCING THE LAYER 3 MODULE

About the Layer 3 Module	13
Layer 3 Module Software Features Explained	14

---

## 2 SWITCHING CONCEPTS AND NETWORK CONFIGURATION EXAMPLES

Layer 3 Switching Concepts	15
Benefits of Layer 3 Switches	17
Network Configuration Examples	18
Integrating the Layer 3 Module into the Network	26

---

## 3 INSTALLING AND SETTING UP THE LAYER 3 MODULE

Safety Information	27
Device Support	28
Pre-installation Procedure	28
Physical Installation	29
Essential Configuration	30
Factory Default Values	32
Post-installation Checks	35

---

## **4 MANAGING THE LAYER 3 MODULE**

- Management Methods 37
- Accessing the Web Interface 37
- Accessing the User Interface 39
- Levels of User Access 39

---

## **5 USING THE WEB INTERFACE**

- Web Management Overview 41
- Web Management User Interface 41

---

## **6 SETTING SNMP AND SYSTEM PARAMETERS**

- Available SNMP Context Commands 44
- Setting Up SNMP on Your System 44
- Administering SNMP Trap Reporting 46
- Available System Context Commands 48
- Displaying the System Configuration 48
- Installing System Software using TFTP 49
- Enabling Timeout of Remote Sessions 50
- Setting Passwords 50
- Setting the System Name 51
- Working with Nonvolatile Data 52
- Initializing Data to Factory Defaults 55
- Resetting the Module 56

---

## **7 DISPLAYING VLAN PARAMETERS**

- Displaying VLAN Information 57

---

## **8 SETTING IP PARAMETERS**

- Available IP Commands 60
- Administering IP Interfaces 63
- Administering Routes 66
- Administering the ARP Cache 70
- Administering the Domain Name Server Client 72
- Administering UDP Helper 74
- Administering IP Multicast Routing 76

Administering Multicast Tunnels	80
Enabling and Disabling ICMP Router Discovery	83
Administering OSPF Areas	84
Setting the Default Route Metric	87
Configuring OSPF Interfaces	88
Displaying the Link State Database	96
Administering Neighbors	102
Setting the OSPF Router ID	104
Administering Memory Partitions	105
Administering the Stub Default Metric	107
Administering Virtual Links	107
Displaying OSPF General Statistics	113
Administering RIP	114
Using ping	118
Using traceRoute	123

---

## **9 PROBLEM SOLVING**

Introduction	129
Interpreting LEDs	130
Identifying the Problem	130

---

## **A LAYER 3 MODULE TECHNICAL SPECIFICATIONS**

EMC Statements	138
----------------	-----

---

## **B CONFIGURATION APPLICATION**

About the Configuration Application	139
Accessing the Configuration Application	139
Downloading a Software Update	140
Resetting the Module to the Factory Default Values	143

---

## **C TECHNICAL SUPPORT**

Online Technical Services	145
Support from Your Network Supplier	147
Support from 3Com	147
Returning Products for Repair	149

---

**GLOSSARY**

---

**INDEX**

---

**3COM CORPORATION LIMITED WARRANTY**

# ABOUT THIS GUIDE

This guide describes the SuperStack® II Switch Layer 3 Module for the SuperStack II Switch 1100 and 3300 family. Before reading this guide, make sure that you are familiar with routing concepts and Virtual LANs (VLANs). Make sure you are also familiar with the command line and Web interfaces for the SuperStack II Switch 1100 and 3300 products.



*If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.*

This user guide and its release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) on the 3Com World Wide Web site:

<http://www.3com.com/>

---

## How to Use This Guide

Table 1 shows where to look for specific information in this guide.

**Table 1** Where to find specific information

<b>If you are looking for...</b>	<b>Turn to...</b>
An overview of the module, and an outline of its main features	Chapter 1
Information on where to place the module in your network	Chapter 2
Installation information for the module	Chapter 3
Information on managing the module	Chapter 4
Information about using the Web interface	Chapter 5
Information on configuring system and SNMP parameters	Chapter 6
Information on configuring VLANs	Chapter 7
Information on configuring IP parameters on the module, including RIP and OSPF	Chapter 8
Problem solving information	Chapter 9

(continued)





**Table 1** Where to find specific information (continued)

If you are looking for...	Turn to...
EMC and technical specifications for the module	Appendix A
Information on using the Configuration Application	Appendix B
Technical support information	Appendix C

## User Guide Conventions

Table 2 and Table 3 list conventions that are used throughout this guide.

**Table 2** Notice Icons

Icon	Type	Description
	Information Note	Important features or instructions.
	Caution	Personal safety risk, system damage or loss of data.
	Warning	Risk of severe personal injury.
	Anti-static warning	Risk of electrostatic damage to equipment.

**Table 3** Text Conventions

Convention	Description
"Enter" versus "Type"	The word "enter" means you must type something, then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
Words in <b>bold</b>	<b>Bold</b> is used to emphasize a point.
Words in <i>italics</i>	<i>Italics</i> are used to denote the first occurrence of a new term which is defined in the glossary.
Text represented as screen display	This typeface represents information that appears on your terminal screen.
Text represented as <b>commands</b>	<b>This typeface</b> is used to represent commands that you enter, for example: <b>snmp display</b>
Keys	When specific keys are referred to in the text, they are described by their labels, such as "Return" or "Escape," or they may be shown as [Return] or [Esc].  If two or more keys are to be pressed simultaneously, the keys are linked with a plus sign (+), for example: Press [Ctrl]+[Alt]+[Del].



---

## Terminology Used in This Guide

Unless otherwise specified, the terms *Layer 3 Module* and *module* are used in this user guide to refer to the SuperStack II Switch Layer 3 Module.

The terms *system* and *module* are used interchangeably in the command line and the Web interface.

The terms *Layer 3 switching* and *routing* are used interchangeably throughout this document. The same applies to the terms *Layer 2 switching* and *bridging*.

The device into which the module is fitted is known simply as the *Switch*. An example of a Switch is the SuperStack II Switch 1100.

*Context* is used to describe a particular group of commands. For example, the IP context contains all the commands grouped under IP in the user interface.

---

## Related Documentation

The following documents and Web sites contain useful information.

### Documents

- Documentation accompanying the SuperStack II 1100/3300 family
- SuperStack II Switch Matrix Module user documentation if you are using a Matrix Module in a stack of Switches.
- "OSPF — Anatomy of an Internet Routing Protocol" by John T Moy, Addison Wesley, 1998, ISBN 0-201-63472-4

### Web Sites

3Com Web site:  
<http://www.3com.com>

Internet Engineering Task Force (IETF) information for Request for Comments (RFCs):  
<http://www.ietf.org>

### Request for Comments

The RFCs listed in Table 4 provide additional information on Layer 3 switching. You can access the RFCs from:  
<http://www.ietf.org/rfc.html>

**Table 4** Useful RFC documents

<b>Protocol</b>	<b>RFC Number</b>
Internet Protocol	791
Internet Control Message Protocol (ICMP)	792
Routing Information Protocol	1058
Distance Vector Multicast Routing Protocol	1075
Host extensions for IP multicasting (IGMP)	1112
OSPF Protocol Analysis	1245
Requirements for IP Version 4 routers	1812

---

## Feedback about this User Guide

Your suggestions are very important to us. They will help make our documentation more useful to you. Please e-mail comments about this document to 3Com at:

**[pddtechpubs\\_comments@3com.com](mailto:pddtechpubs_comments@3com.com)**

Please include the following information when commenting:

- Document title
- Document part number (on the title page)
- Page number (if appropriate)

Example:

- SuperStack II Switch Layer 3 Module User Guide
- Part Number DUA1696-8AAA02
- Page 24



*Do not use this E-mail address for technical support questions. For information about contacting Technical Support, see Appendix C.*

---

## Year 2000 Compliance

This product is Year 2000 compliant. For more information on Year 2000 compliance and 3Com products, visit the 3Com Year 2000 Web page:

**<http://www.3com.com/products/yr2000.html>**

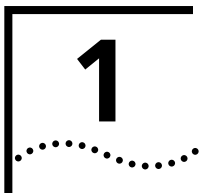
---

## **Product Registration**

You can now register your product online from the 3Com Web site to receive updates and information regarding your product:

<http://www.3com.com/productreg/pdd>





# INTRODUCING THE LAYER 3 MODULE

This chapter provides a brief overview of the SuperStack® II Switch Layer 3 Module, and looks at how it handles routing functionality. It contains the following sections:

- About the Layer 3 Module
- Layer 3 Module Software Features Explained

---

## About the Layer 3 Module

The SuperStack II Switch Layer 3 Module is an expansion module which slots into the SuperStack II Switch 1100 and 3300 family. It provides a Layer 3 switching function between *Virtual LANs (VLANs)*, without resorting to external routers.



*If your Switch does not already have version 2.4 or later of the Switch software installed, you must upgrade the Switch software before installing the Layer 3 Module. See “Upgrading Software” on page 28 for more information about upgrading the Switch software.*

## Summary of Hardware Features

The Layer 3 Module has the following hardware features:

- Layer 3 switch capability within the stack
- Hardware support for Layer 3 switching

## Summary of Software Features

The Layer 3 Module has the following software features:

- IPv4 unicast routing
- IPv4 multicast routing
- Static routes
- Support for the following protocols:
  - Routing Information Protocol (RIP)
  - Open Shortest Path First Protocol (OSPF)

- Internet Group Management Protocol (IGMP)
- Distance Vector Multicast Routing Protocol (DVMRP)
- User Datagram Protocol (UDP) helper (BOOTP/DHCP Relay)
- Several management options:
  - Web-based management
  - Command line interface management
  - SNMP management

---

## Layer 3 Module Software Features Explained

The following sections explain in more detail the software features listed in “Summary of Software Features” on page 13.

### IP v4 Unicast Routing

The Layer 3 Module supports IP v4 unicast routing and its associated features. This allows packets to be routed between individual hosts on different VLANs.

### IP v4 Multicast Routing

The Layer 3 Module supports IP v4 multicast routing and its associated protocols. These protocols allow packets to be efficiently routed from a single host to many other hosts:

- Distance Vector Multicast Routing Protocol (DVMRP). This supports IP multicast routing by broadcasting data to each router in an internetwork when users join or leave multicast groups.
- Internet Group Management Protocol (IGMP). This is used by IP hosts to report their multicast group memberships to any adjacent multicast routers.

### Static Routes

Both dynamic and static routes are explained in detail in “Dynamic and Static Routes” on page 16.

### UDP Helper

UDP Helper permits the routing of UDP broadcast frames between VLANs when these broadcasts are not normally routed between VLANs. With UDP Helper, protocols such as the Bootstrap Protocol (BOOTP) and the Dynamic Host Configuration Protocol (DHCP) are available so that you can boot hosts through this router.

# 2

## SWITCHING CONCEPTS AND NETWORK CONFIGURATION EXAMPLES

This chapter contains basic switching concepts for users that are new to Layer 3 switching. It also sets out some network configuration examples for the SuperStack® II Switch Layer 3 Module, showing where it can be placed in the network for maximum benefit. This chapter contains the following sections:

- Layer 3 Switching Concepts
- Benefits of Layer 3 Switches
- Network Configuration Examples
- Integrating the Layer 3 Module into the Network



*Throughout this section, the term Layer 3 switch applies to all routers.*

---

### Layer 3 Switching Concepts

This section introduces basic Layer 3 switching concepts for new users.

#### What is a Layer 3 Switch?

A Layer 3 switch routes data at high speed between VLANs. Layer 3 switches share information with each other, allowing them to determine the best route through a network that links many LANs. In this way they build up a logical picture of the network, known as a *routing table*.

#### Layer 3 Switching and the OSI Reference Model

Conceptually, Layer 3 switching occurs at the network layer of the OSI reference model. It involves two basic activities:

- Determining the best path
- Forwarding frames to the correct network

Layer 3 switches can connect any two networks, provided that the hosts on the network are using the same network layer protocols supported by the Layer 3 switch.

## Routing Protocols

Routers communicate with each other through protocols that operate at the network layer level. These routing protocols determine whether routing tables are static or dynamic and whether *link-state* (OSPF) or *distance-vector routing* (RIP) is used. In link-state routing, each device maintains a part of a replicated, distributed database of routing information and collects the local link-state information from all other devices. In distance-vector routing, each device calculates the best path to all destinations and then shares that information with neighboring routers.

There are a large number of standards-based routing protocols. The Layer 3 Switch offers the Routing Information Protocol (RIP) and the Open Shortest Path First Protocol (OSPF).

## Routing Tables

A routing table contains routing information including destination/next hop associations and path desirability. Next hop associations tell a router that a particular destination can best be reached by sending the packet to a specific router which represents the 'next hop' on the way to the final destination. When a router receives a packet, it examines the destination address and determines the most appropriate next hop.

Path desirability concerns the most efficient path a packet can take. The source and destination devices compare routing metrics to determine the most desirable path between them. A routing metric is a standard of measurement used by routing algorithms to determine the most efficient path to a particular destination. Routing algorithms store route information in routing tables. This information varies with the routing algorithm used.

### Dynamic and Static Routes

Routing tables usually consist of a mixture of dynamic and static routes.

- Dynamic routes allow routers to continually learn the network topology on a regular basis and update their own routing tables accordingly. They are learned using a routing information protocol. Routers using the Routing Information Protocol (RIP) send out RIP advertisements at regular intervals to advertise their network status to other routers. Dynamic routes age out automatically if an update is not received for a device for a set period of time.



- Static routes are entered manually into the routing table, and are used to reach networks not advertised by routers, for example, if a particular routing policy needs to be enforced. Static routes force traffic to follow a specific path through the network.

The network administrator can set up a special static route, called the default route or default gateway. Any frames containing a destination address which the routing table does not recognize are sent to this destination by default.

The advantage of static routes is that they cannot easily be disrupted by routing protocol instability and can be used to provide a backup routing infrastructure in such cases. The disadvantage of static routes is that if the network links in the route definition are down, traffic cannot be routed. The implementation of a static route usually prohibits the router from offering an alternative data path.

---

## Benefits of Layer 3 Switches

Layer 3 switches offer the following benefits:

- Layer 3 switches can reduce traffic on a network because they do not forward broadcast packets from one VLAN to another.
- They can provide a simple firewall between subnetworks. This prevents incidents that occur within one subnet from affecting others.
- They make large Layer 3 switched networks easier to maintain than their Layer 2 switch-based equivalents.
- Router-based networks support any topology, and can more easily accommodate greater network size and complexity than similar Layer 2 switched networks.
- Layer 3 switches can be used to off-load IP traffic from older legacy routers that may have become overloaded.

## Network Configuration Examples

The following sections look at different network examples in which the Layer 3 Module can be used. They show where the module can be placed in flat networks to maximize its effectiveness.

### Example 1: Simple Flat Network

Figure 1 shows a flat network in which all hosts and servers are attached to the same LAN. All broadcast traffic on the LAN is seen by all devices.

**Figure 1** Example of a Pre-VLAN Flat Network

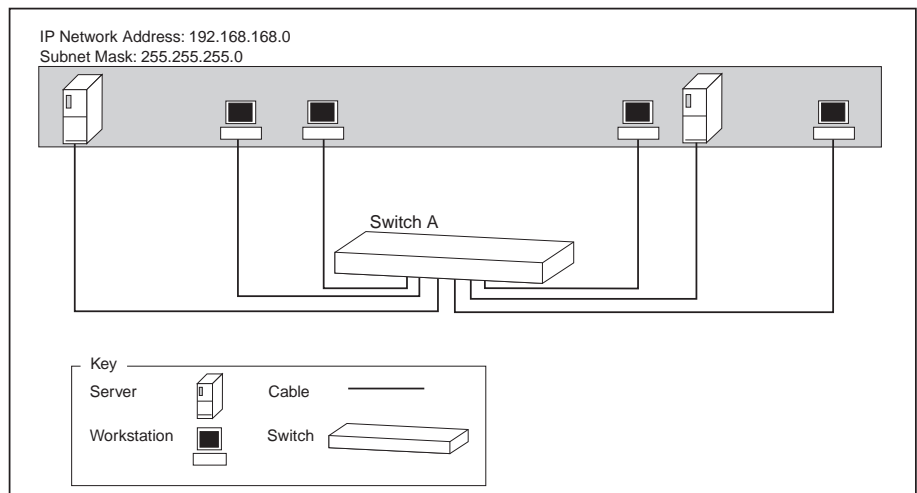
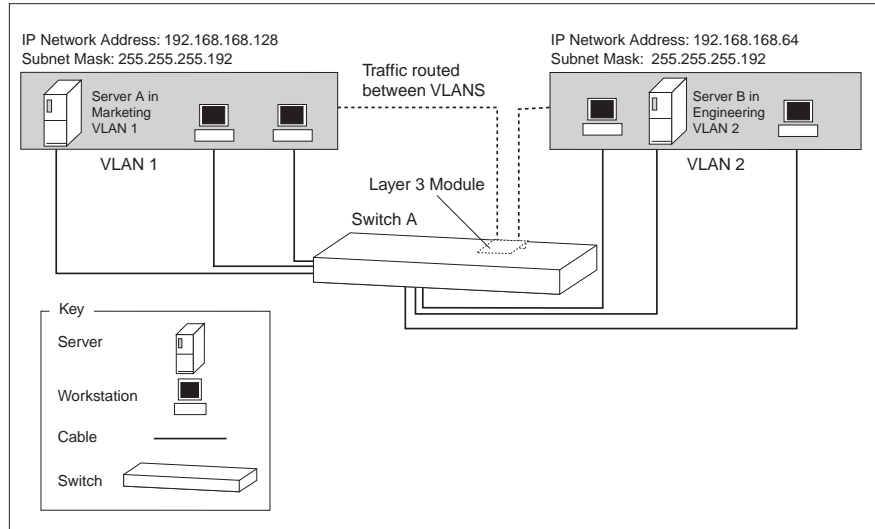


Figure 2 and Figure 3 are variations on the network in Figure 1.

## Suggested Deployment of VLANs

In Figure 2, the same LAN is divided into two VLANs.

**Figure 2** Example of VLANs Used in the Simple Network



The addition of VLANs means that:

- Traffic between devices on VLAN 1 is not seen on VLAN 2.
- Broadcast traffic from hosts on VLAN 1 is not seen on VLAN 2.

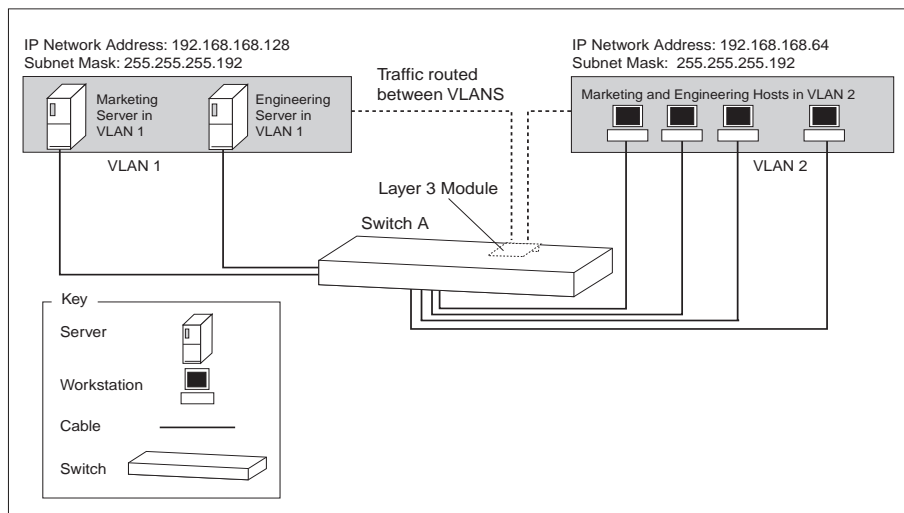
However, devices on VLAN 1 and VLAN 2 cannot communicate at Layer 2.

The addition of the Layer 3 Module in Switch A allows packets to be routed between VLANs.

## Dividing VLANs According to Traffic Requirements

For greatest efficiency, make sure that the VLANs are split according to traffic requirements, as shown in Figure 3, which may not necessarily be along functional lines. For example, the heaviest use of your network may be between your servers, with only a small amount of traffic between each of the desktop hosts and the servers. In this case, it is sensible to place your servers on one VLAN, and your users on another.

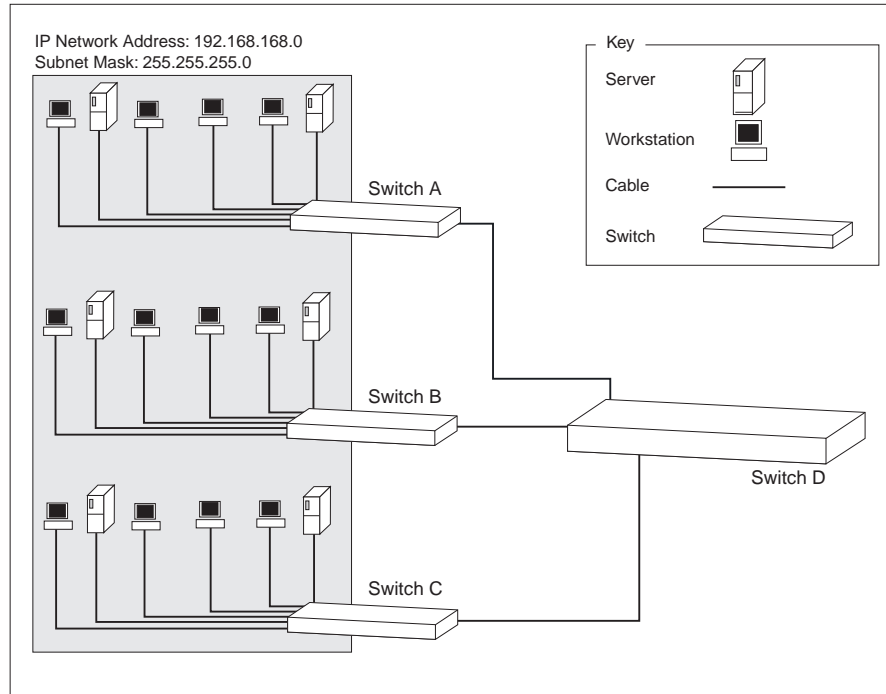
**Figure 3** VLANs Divided according to Traffic Requirements



## Example 2: Large Flat Network

Figure 4 shows a large flat network consisting of a single LAN and no VLANs.

**Figure 4** Flat Network without VLANs



In Figure 4, all devices on the LAN can communicate with all other devices. However, this can lead to network overloading and, if there is a large number of hosts, you may use up all the IP addresses within a given subnet. To accommodate more hosts, you need to add another subnet.

The addition of VLANs to this network:

- Contains broadcasts within each VLAN.
- Enables the deployment of IP subnets.

You can then use the Layer 3 Module to route traffic between VLANs and allow them to communicate. The following examples show how VLANs and the module can work together.

The following figures are variations on the network in Figure 4.

## Deployment of VLANs in a More Complex Network

In Figure 5, the Layer 3 Module in Switch D routes packets between VLANs.

**Figure 5** Complex Network with VLANs

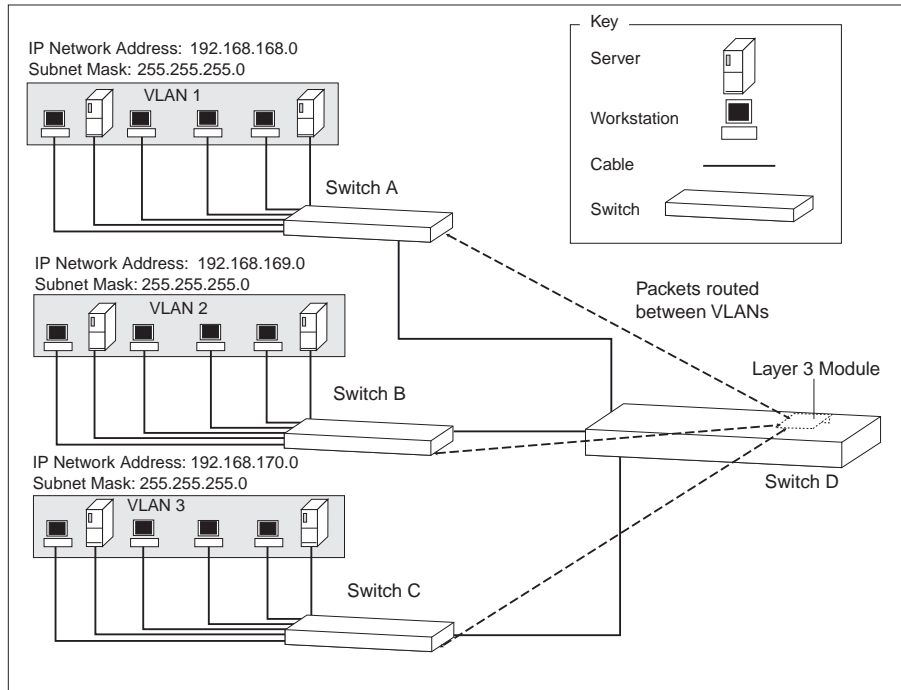


Figure 5 shows the same network as Figure 4, but here the LAN has been divided into VLANs.

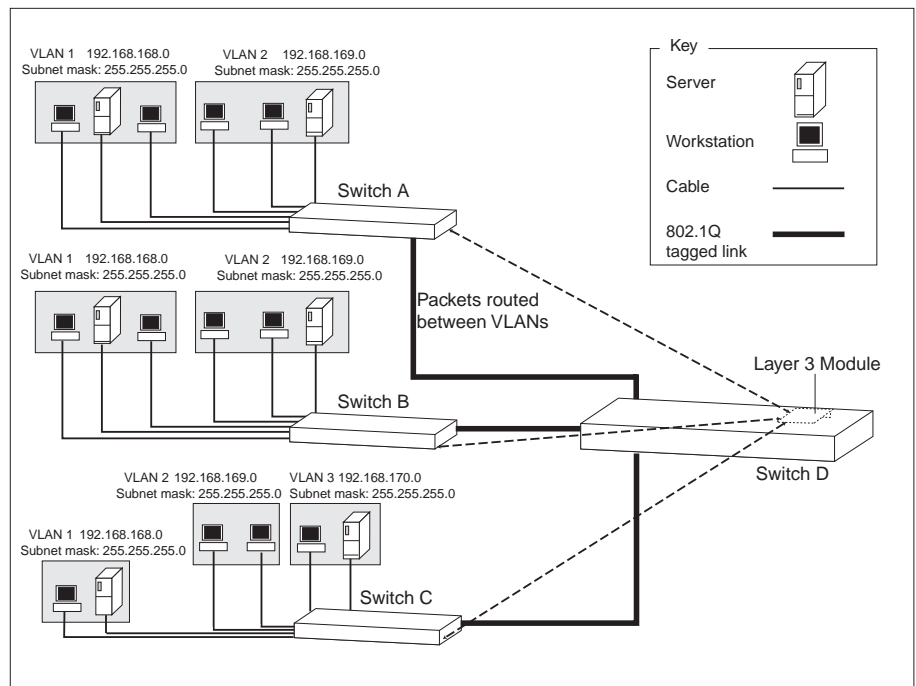
Small groups of ports on Switch D have each been assigned to particular VLANs.

This scenario reduces the load on Switch D, because broadcast and multicast traffic between devices on each VLAN is not seen by the rest of the network.

## Addition of Multiple VLANs per Switch

In Figure 6, the Switches are connected by 802.1Q tagged links. 802.1Q tagged links are links that use the tagging system defined in the IEEE 802.1Q standard to carry traffic for multiple VLANs. Using the 802.1Q tagged links, the Layer 3 Module can tell Switches A, B and C which VLAN the packets are destined for. All Switches at the end of the links receive traffic for all VLANs.

**Figure 6** Network Using Multiple VLANs



*The Switches could also be connected in a stack using a SuperStack II Switch Matrix Module. For further information, see the user guide for the SuperStack II Switch Matrix Module.*

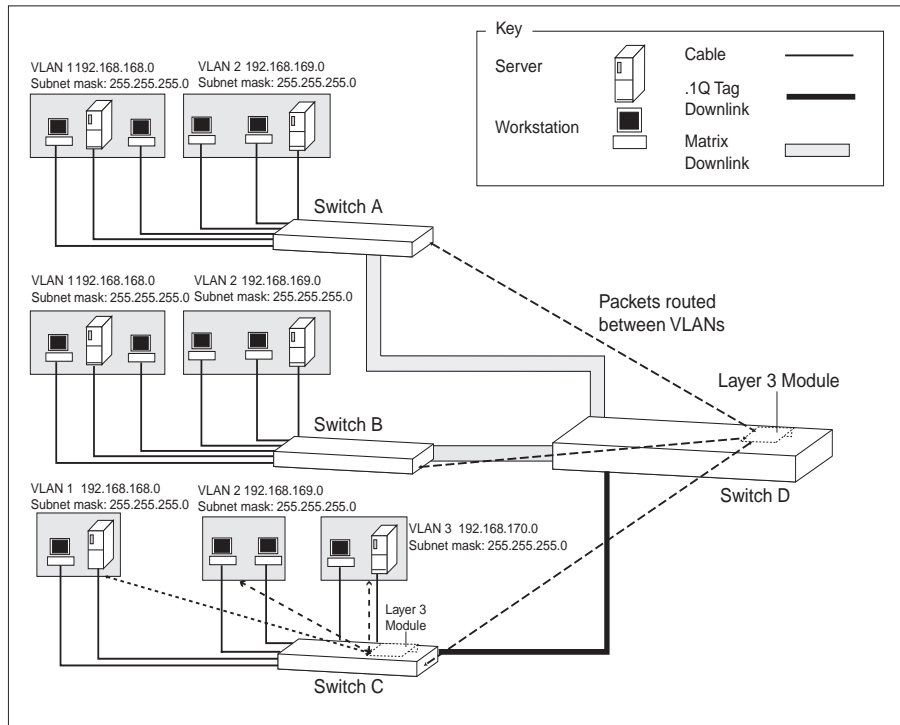
Traffic on each VLAN is switched at Layer 2 via Switch D, and routed at Layer 3 to other VLANs via the Layer 3 Module. For example, traffic from VLAN 1 on Switch A is switched to VLAN 1 on Switch B via Switch D.

Traffic from VLAN 1 on Switch C to VLAN 2 on Switch C is routed at Layer 3 through the Layer 3 Module on Switch D.

## Heavy inter-VLAN Traffic

If a particular Switch has a lot of inter-VLAN traffic, you can use a Layer 3 Module in the Switch to route packets between VLANs in one part of the network, as shown in Figure 7.

**Figure 7** Network Using Multiple Layer 3 Modules



Here there is heavy traffic between the VLANs on Switch C. The addition of a Layer 3 Module in Switch C allows traffic to be routed to the correct VLANs, without having to cross the downlink to the Layer 3 Module in Switch D to be routed. Traffic from a host on VLAN 1 on Switch C, destined for a host on VLAN 2 of Switch B, is routed in Switch C onto VLAN 2 and switched at Layer 2 through Switch D to Switch B.



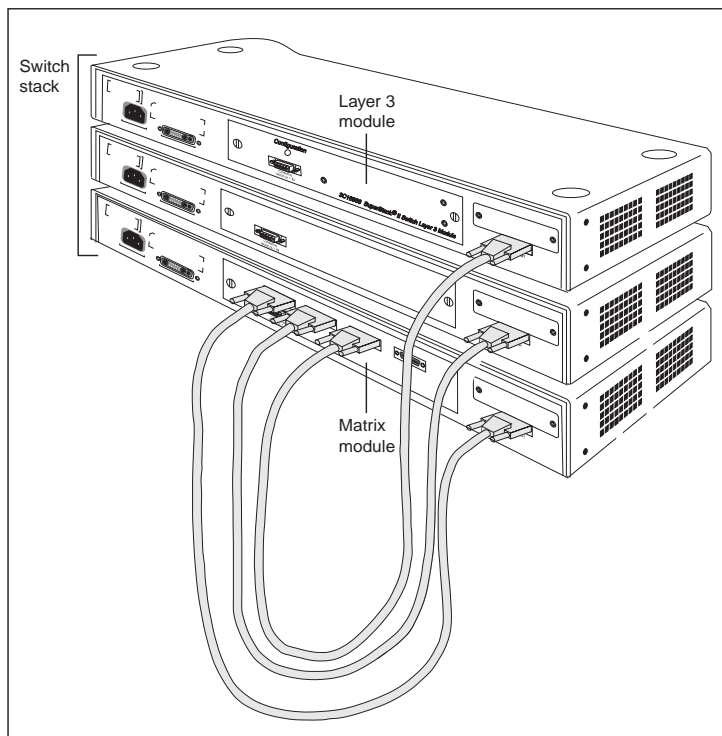
*If you have stacked your Switches, install only one Layer 3 Module in the stack. In Figure 7, Switch A, Switch B and Switch D form a stack, using a Matrix Module, with Switch C connected via an 802.1Q tagged link. See "Using the Layer 3 Module in a Switch Stack" on page 25 for more information about Matrix modules and the Layer 3 Module.*



## Using the Layer 3 Module in a Switch Stack

Figure 8 shows how to connect several switches using the Layer 3 Module and Matrix modules in a stack. There is only one Layer 3 Module in the stack because only one Layer 3 Module is supported per stack.

**Figure 8** Layer 3 Module Used with the SuperStack II Switch Matrix Module



*3Com does not support more than one Layer 3 Module per stack. Do not install more than one Layer 3 Module in a stack.*

---

## Integrating the Layer 3 Module into the Network

This section outlines the steps you need to take to integrate your Layer 3 Module into a network containing hosts, Layer 2 switches and other routers.

Hosts include any PCs and servers on your network. Follow the steps in the order indicated.

- 1 Decide how to divide your hosts into IP subnets.
- 2 Allocate a VLAN identifier (the 802.1Q VLAN identifier) to each of these IP subnets.
- 3 Create these VLANs on each of your Layer 2 switches.
- 4 Select the IP addresses, from your IP subnet allocation, to use on the VLAN interfaces on the Layer 3 Module.

To make it easier to remember which IP address belongs to the Layer 3 Module, reserve the .1 host address in each subnet for the router. For example, in the network 192.168.168.0, the IP address 192.168.168.1 is the router address and becomes the address assigned to the corresponding Layer 3 Module.

# 3

## INSTALLING AND SETTING UP THE LAYER 3 MODULE

This chapter describes how to install the SuperStack® II Switch Layer 3 Module into your Switch. It contains the following sections:

- Safety Information
- Device Support
- Pre-installation Procedure
- Physical Installation
- Essential Configuration
- Factory Default Values
- Post-installation Checks

---

### Safety Information

Read the following information before installing the Layer 3 Module.



**WARNING:** Installation and removal of the module must be carried out by qualified personnel only. Before installing the module into a unit, you must first disconnect the unit from the main power supply. For full safety instructions, see the user guide that accompanies the unit.



**AVERTISSEMENT:** Confiez l'installation et la dépose de ce module à un personnel qualifié. Avant d'installer ce module dans un groupe, vous devez au préalable débrancher ce groupe de l'alimentation secteur. Pour prendre connaissance des consignes complètes de sécurité, consultez le guide utilisateur qui accompagne ce groupe.



**WARNHINWEIS:** Die Installation und der Ausbau des Moduls darf nur durch Fachpersonal erfolgen. Vor dem Installieren des Moduls in einem Gerät muß zuerst der Netzstecker des Geräts abgezogen werden. Vollständige Sicherheitsanweisungen sind dem Benutzerhandbuch des Geräts zu entnehmen.

### Handling the Layer 3 Module



The Layer 3 Module contains parts that are susceptible to electrostatic discharge damage. To prevent damage, please observe the following:

- *Always wear an anti-static wristband connected to a suitable earth point.*
- *Always transport or store the module in appropriate anti-static packaging.*
- *Do not remove the module from its packaging until you are ready to install it.*
- *Handle the module only by its edges and front panel and avoid touching any of the connectors or components on the module.*

---

### Device Support

The SuperStack II Switch 1100/3300 family supports the Layer 3 Module.

3Com recommends that you check the Release Notes that accompany the module for information on any additional device support.

---

### Pre-installation Procedure

This section describes the procedures you need to follow before installing the Layer 3 Module.

#### Upgrading Software

To determine the version of software installed on the Switch, do one of the following:

- Use the Unit Status page on the Switch's Web interface.
- Use the Switch **system display** command. The number shown in the Operational Version field is also the version number for the software.

For further information, see your Switch management guide.



*If your Switch does not already have version 2.4 or later of the Switch software installed, you must upgrade the Switch software before installing the Layer 3 Module.*

If you need to upgrade the software:

- 1 Use the Switch software CD if one has been included with your Layer 3 Module. Otherwise, download the latest version of the software from 3Com's information delivery systems, as described in "Online Technical Services" on page 145.
- 2 Follow the instructions for upgrading software that are provided in the Switch management guide.

## Physical Installation

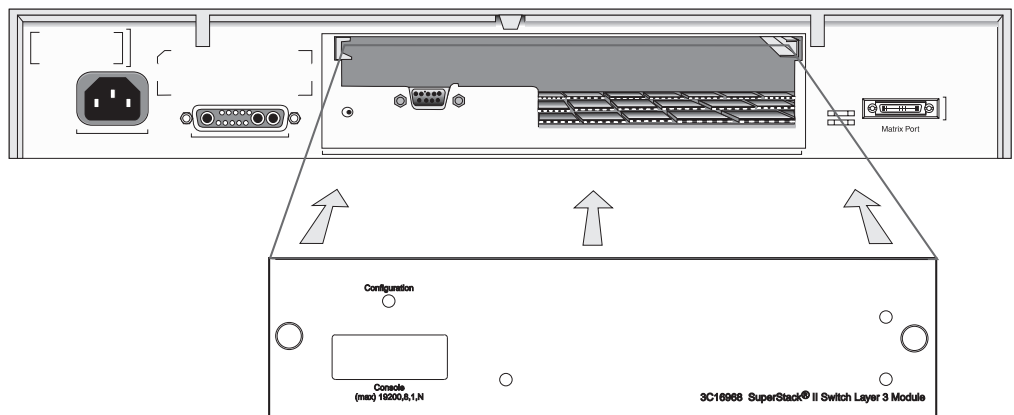
This section describes how to install the Layer 3 Module using the example of a SuperStack II Switch 3300.



*If you have connected several switches in a stack using the SuperStack II Switch Matrix Module, install only one Layer 3 Module in the stack.*

- 1 Turn off the power to the Switch and disconnect the Switch from the main power supply.
- 2 Locate and remove the blanking plate which covers the module slot. Retain the blanking plate and the screws for future use.  
See your Switch management guide to locate the slot for the module.
- 3 Use the guide rails within the Switch slot to align the Layer 3 Module. The location of the guide rails and the correct positioning of the module is shown in Figure 9.

**Figure 9** Fitting the Layer 3 Module



*The configuration switch is used to access the Configuration Application, as described in Appendix B.*

- 4 Slide the module into the slot without touching the top or bottom of the circuit board. Make sure that the module is pushed fully into the unit.
- 5 Use the thumb screws attached to the module to fix it firmly into place.
- 6 Power up the Switch as described in "Powering Up the Switch".  
If you have taken the Layer 3 Module from another Switch, follow the procedure in "Resetting the Module to the Factory Default Values" in Appendix B to return to the factory default values.
- 7 Follow the post-installation checks, as described in "Post-installation Checks" on page 35.
- 8 Follow the procedure in "Essential Configuration" on page 30 to make sure that the Layer 3 Module is ready for you to manage.

### Powering Up the Switch

The Switch does not have an On/Off button, so you must power it up by connecting it to the main power supply using a power cable.



*It can take up to 90 seconds before the Layer 3 Module is accessible.*

You can find further information on connecting a power supply and safety information in your Switch Management Guide.

### Power On Self Test

Each time the Switch and Layer 3 Module power up, they run a *Power On Self Test (POST)*.

The POST for the Layer 3 Module consists of basic checks on the hardware. These checks take approximately five seconds and run simultaneously with the self-tests for the Switch.

---

### Essential Configuration

When first installed, the Layer 3 Module has no effect on the Switch into which it is plugged. The module is notionally "present" on all 16 Virtual Local Area Networks (VLANs) supported by the Switch. However, it does not have any IP addresses, and does not route between VLANs.



*You must allocate an IP address to the Layer 3 Module before you can manage it. The IP address that you assign to the Layer 3 Module must be on the same IP network and subnet as the Switch.*

You must use the Switch command line or Web management interface to set the first IP address for the Layer 3 Module. This is because the Layer 3 Module does not support a local management port. The module uses this

IP address on VLAN 1 (the default VLAN). Once the first IP address has been set on the Layer 3 Module, you can manage the module using its own management interfaces.



*You cannot manage the Layer 3 Module directly from the Switch; you must use Telnet or the Web interface to manage the module.*

To get your Layer 3 Module up and running, you *must* follow this configuration process:

- 1** Upgrade the Switch software, if necessary, as described in “Upgrading Software” on page 28.
- 2** Insert the Layer 3 Module, as described in “Physical Installation” on page 29.
- 3** Use the Switch Web management interface or the Switch command line interface to add the IP address of the Layer 3 Module.

To add the IP address using the Web management interface:

- a** Launch the Web management interface for the Switch.
- b** Click the *Unit* icon on the side-bar. If there are several units in the icon, click the unit containing the Layer 3 Module. The Switch Graphic page is displayed, containing a graphic of the Switch.
- c** Click the Layer 3 Module area on the graphic. The Module Setup page is displayed.
- d** In the IP Address field, enter the IP address for the module.
- e** In the Subnet Mask field, enter a subnet mask for the module.
- f** In the Default Router field, enter the IP address of the Default Gateway, if your network has one.

Enter **0.0.0.0** to indicate that you do not have a Default Router, or to remove an existing Default Router.

- g** Click *Apply*.



*You must reboot the Switch for the Layer 3 Module IP address to take effect.*

To add the IP address of the Layer 3 Module using the Switch command line interface:

- a** Use Telnet to access the command line interface for the Switch.



*If your Layer 3 Module is in a stack, type **unit** to access the command line of the Switch containing the module.*

**b** Enter the following:

```
system module define
```

The following prompt is displayed:

```
Enter IP address [0.0.0.0]
```

**c** Enter the IP address of the Layer 3 Module.

```
Enter Subnet Mask [255.0.0.0]
```

**d** Enter the Subnet Mask.

```
Enter Default Router [0.0.0.0]
```

**e** Enter the Default Router.



*The Switch must have a management address. The IP address that you assign to the Layer 3 Module must be on the same IP network and subnet as the Switch. You can configure the Switch management IP address using the **ip interface define** command on the Switch.*

**4** Connect to the Layer 3 Module using the Web interface or command line interface:

**a** Add an IP address for each VLAN that you want to route between.

For information on using the Web interface, see Chapter 5.

For information on using the command line interface, see “Defining an IP Interface” on page 64 and see Chapter 7, “Displaying VLAN Parameters” for specific information about VLANs.



*The Layer 3 Module learns its VLANs from the Switch. Use the Switch Web management interface or command line to add new VLANs.*

**b** If required, configure OSPF and RIP for each interface. See Chapter 8, “Setting IP Parameters” for further information.



*You must also make changes to the appropriate hosts on your network to define the Layer 3 Module as their default router. See “Integrating the Layer 3 Module into the Network” on page 26.*

---

## Factory Default Values

When you have installed the Layer 3 Module, there are factory default values for SNMP, system, management, passwords and IP configuration. Table 5 to Table 10 list these values.

## SNMP Default Values

After installation, the default SNMP values are as follows:



**Table 5** SNMP Default Values

SNMP Community	Default value
read-only	public
read-write	private

By default, no SNMP trap destinations are configured.

## System Default Values

After installation, the default system values are as follows:

**Table 6** System Default Values

Parameter	Default Value
System Name	L3Module-XXXXXX where the last six digits are the product-unique portion of the MAC address.
Timeout	Disabled

## Management Default Values

You cannot manage the Layer 3 Module until it has a default IP address. You must assign an IP address to the Layer 3 Module before you can manage it. To do this, see “Essential Configuration” on page 30.

This IP address is assigned to VLAN 1 when the Switch and Layer 3 Module are restarted. The IP address is passed from the Switch to the Layer 3 Module.



*The IP address is assigned to VLAN 1 because it is the only VLAN on which the Switch management software can be used.*

Once this IP address has been configured, you can use Telnet, the Web interface or SNMP to manage the Layer 3 Module.

## Default Passwords

After installation, the default passwords, which specify the level of access to the system for a user, are as follows:

**Table 7** Default Telnet and Web Passwords

Access Level	Password	Privileges
admin	No default password	read and write, change passwords, reset
write	No default password	read and write
read	No default password	read

**Table 8** Default SNMP Community Passwords

Access Level	Password
read and write	private
read-only	public

## IP Configuration Default Values

The following default IP configuration values apply to each module.

**Table 9** IP Default Values for Each Module

Parameter	Default Value
arp	<ul style="list-style-type: none"> <li>■ arp entries age out after 15 minutes</li> </ul>
multicast	<ul style="list-style-type: none"> <li>■ DVMRP disabled</li> <li>■ IGMP query enabled</li> <li>■ No tunnels defined</li> </ul>
domain name service	<ul style="list-style-type: none"> <li>■ Domain name undefined</li> <li>■ No name servers defined</li> </ul>
udp helper	<ul style="list-style-type: none"> <li>■ No udp helpers defined</li> <li>■ Default hop count = 4</li> <li>■ Default relay threshold = 0</li> </ul>
ICMP router discovery	<ul style="list-style-type: none"> <li>■ Disabled</li> </ul>
OSPF	<ul style="list-style-type: none"> <li>■ No areas defined (except the implicit definition of the backbone, 0.0.0.0)</li> <li>■ No neighbors defined</li> <li>■ Router ID pre-defined based upon the system ID of the Layer 3 Module</li> <li>■ No virtual links defined</li> </ul>
static routes	<ul style="list-style-type: none"> <li>■ No static routes defined</li> </ul>

The following default values apply to each interface.



**CAUTION:** Do not change the values marked with a \* in the following table unless you are an experienced network operator and are aware of the consequences.

**Table 10** IP Default Values for Each Interface

Parameter	Default Value
OSPF	<ul style="list-style-type: none"> <li>■ OSPF disabled on each new IP interface</li> <li>■ Hello timer = 10 seconds*</li> <li>■ Retransmit = 5 seconds*</li> <li>■ Dead interval = 40 seconds*</li> <li>■ Area ID = 0.0.0.0 for each interface</li> <li>■ No password</li> <li>■ Interface cost = 1</li> <li>■ Priority = 1</li> </ul>
RIP	<ul style="list-style-type: none"> <li>■ RIP is enabled and will learn, but not advertise routes</li> <li>■ Interface cost = 1</li> <li>■ Poison reverse = enabled</li> <li>■ No additional advertisement addresses are defined</li> </ul>

## Post-installation Checks

This section describes the LEDs and basic checks that you can use to verify your installation, and to ensure that the Switch and module are operating correctly.

### LED Summary

This section describes the Switch LEDs that provide status and troubleshooting information.

**Table 11** Switch Module Status LEDs

LED Name	Color/State	Indicates
Packet	Yellow	Packets are being routed.
	Off	No packets are being routed.
Status	Yellow	The Layer 3 Module is functioning.
	Yellow flashing	An unrecognized or faulty module is installed in the Switch.
	Off	There is no module installed in the Switch.

For information on solving problems after installation, see Chapter 9.



# 4

## MANAGING THE LAYER 3 MODULE

This chapter contains the following information:

- Management Methods
- Accessing the Web Interface
- Accessing the User Interface
- Levels of User Access



*The terms system and module are used interchangeably in the command line and the Web interface.*

---

### Management Methods

You can manage the Layer 3 Module in the following ways:

- Using the Web interface.
- Using the command line interface (Telnet).
- Using the 3Com® Transcend® Network Control Services software. See your network management documentation for details.

Depending on the tasks you need to carry out, there are different levels of access, described in “Levels of User Access” on page 39.

---

### Accessing the Web Interface

To access the Web interface over the network:

- 1 Make sure that your network is correctly set up for management using the Web interface. You must have configured at least one IP address on your Layer 3 Module (see “Essential Configuration” on page 30).
- 2 Open your Web browser. The Web management suite of applications requires one of the following:
  - Internet Explorer 4.0 or later

- Netscape Navigator 4.03 or later
- 3 In the Location field of the browser, enter the URL of the Layer 3 Module in the following format:

**http://nnn.nnn.nnn.nnn/**

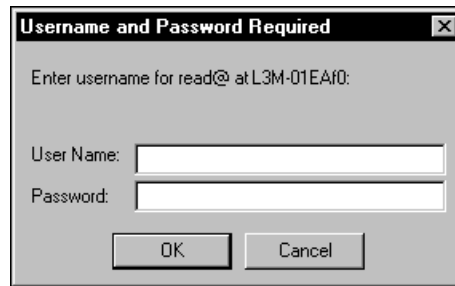
where **nnn.nnn.nnn.nnn** is the IP address of the module.



*If you have added the configuration name and IP address of the Layer 3 Module to your Domain Name Server, you can enter the name of the module in the URL instead of the IP address.*

You are prompted to enter the required access level and password, as shown in Figure 10:

**Figure 10** Access Level and Password dialog box



When the browser has located the module, the Web interface opens. See Chapter 5, “Using the Web Interface” for more information about the Web interface.

Enter the user name *admin* when you log on initially because there is no default password for this user. See “Default Passwords” on page 33 for a list of the default passwords for different access levels.

To prevent unauthorized configuration of the module, change the default passwords as soon as possible. To do this using the Web interface, you must log on as each default user and then follow the steps described in “Setting Passwords” on page 50.

### Exiting the Web Interface

You can exit the Web interface at any time; to do this, close your Web browser. For security reasons, always close your Web browser after a management session.

## Accessing the User Interface

You can access the user interface in the following ways:

- From a PC or workstation, to a Layer 3 Module IP address, using Telnet.
- Through an SNMP-based network management application such as the 3Com Transcend Network Control Services suite of network management tools.

### Using an IP Management Interface

An IP management interface allows you to manage the system through an Ethernet port. After you configure an IP management interface with a unique IP address, you can also use Telnet to connect remotely to the user interface using the TCP/IP protocol from a host computer, or you can reach the SNMP agent from a network management application.

When you enter the user interface, the system prompts you for an access level and password:

```
Select access level (read, write, administer):
Password:
```

The passwords are stored in nonvolatile memory. You must enter the password correctly before you can continue.

## Levels of User Access

The Layer 3 Module supports three password levels so that the network administrator can provide different levels of access for different users. Table 12 describes these access levels.

**Table 12** Password Access Levels

Access Level	For users who need to:	Allows users to:
Administer	Perform system setup and management tasks (usually a single network administrator)	Perform system-level administration tasks (such as setting passwords, loading new software, and so on)
Write	Perform active network management	Configure network parameters (such as configuring IP VLAN addresses)
Read	Only view parameters	View "display-only" menu items (such as display, summary, detail)



*The access available at each level is also available by default at higher levels. For example, Read and Write access is available when in Administer mode.*



# 5

## USING THE WEB INTERFACE

This chapter contains the following sections:

- Web Management Overview
- Web Management User Interface



*The terms system and module are used interchangeably in the command line and the Web interface.*

---

### Web Management Overview

You use the Web management application to manage a Layer 3 Module from a Web browser. The Web management application for the Layer 3 Module is the WebConsole which is an HTML-based application.

From this application you can manage a single Layer 3 Module. Alternatively, you can manage several modules at the same time if you are using multiple windows.

### WebConsole

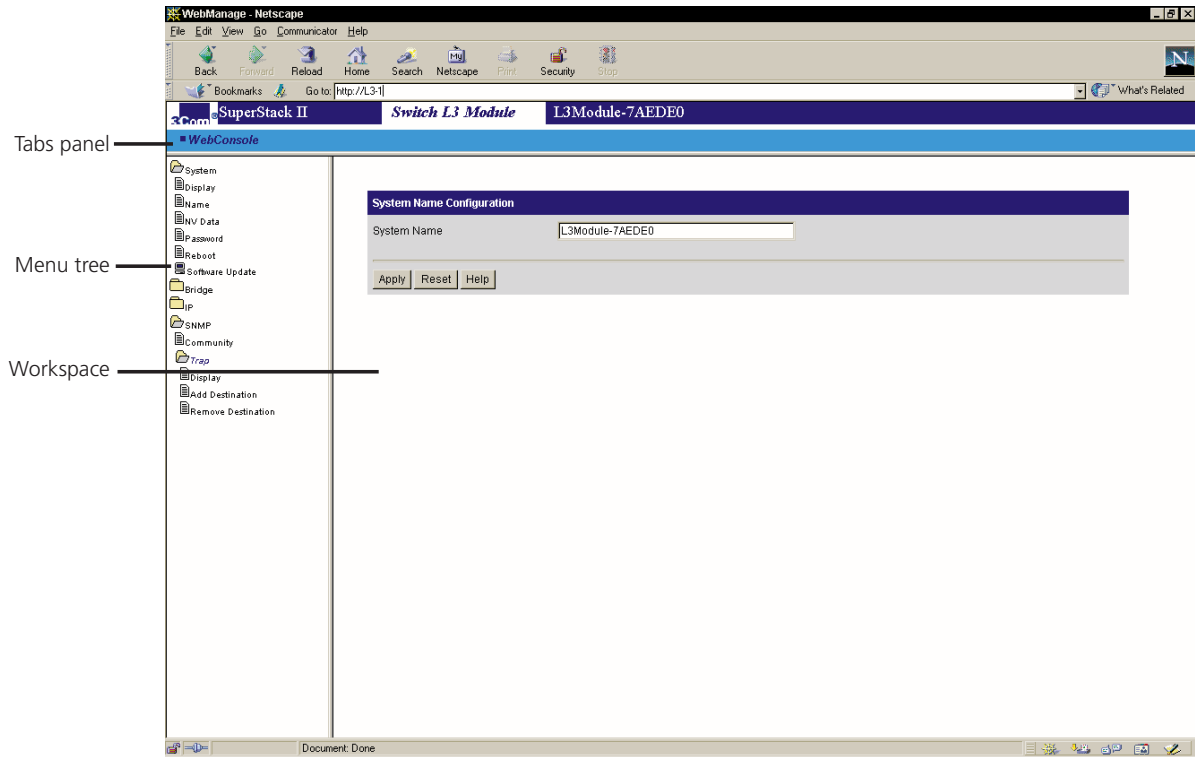
The WebConsole application displays a tree of options for managing your devices. Each option calls up one or more forms in which you can set parameters and view statistics.

---

### Web Management User Interface

The user interface for the Web management applications is divided into three areas, as shown in Figure 11:

Figure 11 Web Management Interface



- **Tabs panel** — Located at the top of your browser window and contains the WebConsole tab. The WebConsole tab displays a menu tree that lists the parameters that you can configure for the selected device.
- **Menu tree** — Lists system menu options, much like the user interface. Click a menu item to view the associated form in the workspace.
- **Workspace** — Displays forms for the selected menu option.



*When a Telnet icon appears besides a device name in the menu tree, you can click the icon to launch a Telnet session to configure system parameters which are not supported through the WebConsole.*

# 6

## SETTING SNMP AND SYSTEM PARAMETERS

This chapter contains the following information:

- Available SNMP Context Commands
- Setting Up SNMP on Your System
- Administering SNMP Trap Reporting
- Available System Context Commands
- Displaying the System Configuration
- Installing System Software using TFTP
- Enabling Timeout of Remote Sessions
- Setting Passwords
- Setting the System Name
- Working with Nonvolatile Data
- Initializing Data to Factory Defaults
- Resetting the Module



*See "Accessing the User Interface" on page 39, for information on launching the user interface.*

## Available SNMP Context Commands

Table 13 lists the commands available in the SNMP context.

**Table 13** SNMP Context Commands

Command	Options	Syntax
<code>display</code>		Display current SNMP settings
<code>community</code>		Set an SNMP community string
<code>trap</code>	<code>display</code>	Display trap reporting information
	<code>addModify</code>	Add a new trap reporting destination configuration or modify a current one
	<code>remove</code>	Remove a trap destination
	<code>flush</code>	Flush all SNMP trap reporting destinations

## Setting Up SNMP on Your System

To manage the Layer 3 Module from an external management application, you must configure SNMP community strings and set up trap reporting. The SNMP-based external management application (called the SNMP manager) sends requests to the system, where they are processed by the Layer 3 Module SNMP software. In addition, the Layer 3 Module SNMP software can send traps to an SNMP manager to report significant events.

The SNMP software provides access to information about the module. The displays of Management Information Base (MIB) information differ depending on the module SNMP management method that you choose.

Access to system information through SNMP is controlled by community strings.

## Configuring SNMP for System Management

SNMP requests can be sent to any configured IP address on the Layer 3 Module.

To manage the module you need to assign at least one IP address to an IP Virtual LAN (VLAN). See “Essential Configuration” on page 30, for information on defining the first IP address. For information on defining subsequent IP addresses, use the `ip interface define` command, described in “Defining an IP Interface” on page 64.

## Displaying SNMP Settings

To display the current module SNMP configurations for community strings, enter the following at the top-level menu:

```
snmp display
```

The following example shows an SNMP settings display:

```
Read-only community is public
Read-write community is private
```

## Configuring Community Strings

A community string is an octet string, included in each SNMP message, that controls access to system information. The SNMP software for the module internally maintains two community strings that you can configure:

- *Read-only* community strings with the default “public”
- *Read-write* community strings with the default “private”

When the SNMP software receives an SNMP request, the module compares the community string in the request with the community strings that are configured for the module.

- SNMP *get*, *get-next*, and *set* requests are valid if the community string in the request matches the module’s *read-write* community.
- Only the SNMP *get* and *get-next* requests are valid if the community string in the request matches the module’s *read-only* community string.

When you set a community string, you can specify any value up to 48 characters long.

To configure the community strings:

- 1 Enter the following at the top-level menu:

```
snmp community
```

The system prompts you for the new community strings.

```
Enter new read-only community {?} [public]:
```

- 2 At the read-only prompt, enter the new community string.

```
Enter new read-write community {?} [private]:
```

- 3 At the read-write prompt, enter the new community string.

The following example retains the read-only community string as public and sets a secret read-write community string:

```
Enter new read-only community [public]:
Enter new read-write community [private]: secret
```



*You can only change the community strings if you are logged into the user interface as administrator.*

## Administering SNMP Trap Reporting

For network management applications, you can manually administer the trap reporting address information.

### Displaying Trap Reporting Information

To display trap reporting information, including the various SNMP traps and their current configured destinations, enter the following at the top-level menu:

```
snmp trap display
```

The following example shows a trap settings display:

Trap Descriptions:		
Trap #	Description	
1	MIB II: Coldstart	
Trap Destinations Configured:		
Address	Trap Numbers Enabled	
40.220.22.20	1	

### Configuring Trap Reporting

You can define up to 10 destination addresses and modify the set of traps that are sent to each destination address.

To configure trap reporting:

- 1 Enter the following at the top-level menu:

```
snmp trap addModify
```

The following prompt is displayed:

```
Enter the trap destination address:
```

- 2 Enter the IP address of the SNMP manager (destination address).  
Enter the trap numbers to enable (1-4|all) [all]:
- 3 Enter one or more trap numbers or **a11** for that destination.

Separate a series of more than two trap numbers with a hyphen (-) and nonsequential trap numbers by commas.



*The trap numbers that you enter allow the trap specified by that number to be sent to the destination address when the corresponding event occurs. No unlisted traps are transmitted.*

If the following message appears:

```
Trap address invalid or unreachable  
make sure that:
```

- The destination address that you entered is a valid end station.
- The end station is online.
- A valid IP interface is defined on the module.
- The module has a route to the destination.

### Removing Trap Destinations

When you remove a trap destination, no SNMP traps are reported to that destination.

To remove a trap destination:

- 1 Enter the following at the top-level menu:

```
snmp trap remove
```

The following prompt is displayed:

```
Enter the trap destination address:
```

- 2 Enter the SNMP trap reporting destination address that you want to remove.

The system removes the destination address and displays the previous menu.

### Flushing All SNMP Trap Destinations

When you flush the SNMP trap reporting destinations, you remove all trap destination address information for the SNMP module.

To flush the trap reporting destinations:

- 1 Enter the following at the top-level menu:

```
snmp trap flush
```

The following prompt is displayed:

```
Are you sure? (n/y) [y]:
```

- 2 Enter **y** (yes) or **n** (no) as required. If you enter **y**, the addresses are immediately flushed. If you enter **n**, the previous menu appears on the screen.

## Available System Context Commands

The following commands are available in the system context:

**Table 14** System Context Commands

Command	Options	Syntax
<code>display</code>		Display the configuration of the Layer 3 Module
<code>softwareUpgrade</code>		Initiate a TFTP download of new system software
<code>initialize</code>		Reset nonvolatile data to factory defaults
<code>consoleTimeout</code>	<code>timeout</code>	Enable/disable the console inactivity time-out
	<code>interval</code>	Set the console inactivity time-out (in minutes)
<code>password</code>		Change password for browsing or viewing, configuring network parameters, or for full system administration
<code>name</code>		Assign an easily recognizable and unique name to the Layer 3 Module
<code>nvData</code>	<code>save</code>	Save nonvolatile data
	<code>restore</code>	Restore nonvolatile data
<code>reset</code>		Reboot the system

## Displaying the System Configuration

The system configuration display provides software and hardware revisions, module status information, and warning messages for certain system conditions.

To display the system configuration, enter the following at the top-level menu:

```
system display
```

The display contains the following general system information:

- The system name
- The system ID
- The software version, build date, and time



## Installing System Software using TFTP

To download the Layer 3 Module software using TFTP, follow the procedures in this section.



*You can load the system software into flash memory while the Layer 3 Module is operating. You do not need to shut down the system.*

*Before you begin this procedure, make sure that the TFTP server software is running on the device from which you will be installing the software.*

Loading software into flash memory takes approximately 5 minutes to complete, depending on your network load.

To install the system software using TFTP:

- 1 Enter the following at the top-level menu:

```
system softwareUpgrade
```

The following prompt is displayed:

```
Host IP address [172.16.200.14]:
```

Enter the IP address of the host machine (such as a Sun workstation or PC) from which you are installing the software.

```
Install file name {?}:
```

- 2 To display the filename conventions that you can use, enter ?
- 3 Enter the complete path and filename.



*Some TFTP servers do not accept the full path. If that is the case for your server, enter only the filename of the image. See your server documentation for more information.*



**CAUTION:** *If the flash installation stops (that is, if you see no activity for more than 2 minutes), wait for the TFTP session to time out. Do not reboot the system. When the session has timed out, follow the installation procedure again.*

After the software has been loaded successfully, the following message appears:

```
Software upgrade completed
```

The Layer 3 Module restarts, running the new software after a few seconds delay.

---

## Enabling Timeout of Remote Sessions

You can configure the Layer 3 Module to disconnect remote sessions after a specified time interval of inactivity.

The default Telnet timeout value is *disabled*.

To enable or disable the timeout interval:

- 1 Enter the following at the top-level menu:

```
system consoleTimeout timeOut
```

The following prompt is displayed:

```
Enter new value (disabled, enabled) [disabled]:
```

- 2 Enable or disable the Telnet timeout state as required.

The default time interval is 30 minutes. Follow the instructions in “Setting Timeout Interval for Remote Sessions” if you want to change the default timeout interval.

## Setting Timeout Interval for Remote Sessions

You can set the timeout interval for remote sessions to any value from 1 minute to 60 minutes. The default timeout interval is 30 minutes.

To change the timeout interval:

- 1 Enter the following at the top-level menu:

```
system consoleTimeout interval
```

The following prompt is displayed:

```
Enter new value (1-60) [30]:
```

- 2 Enter the Telnet timeout interval.

---

## Setting Passwords

The user interface supports three levels of access: one for only browsing or viewing (*Read*), one for configuring network parameters (*Write*), and one for full system administration (*Administer*).

Because the initial passwords stored in the nonvolatile memory of the module are null for all access levels, press [Enter] at the password prompt when you log on for the first time.

You can change passwords only if you enter the user interface at the Administer access level.

To change the password:

- 1 Enter the following at the top-level menu:

```
system password
```

The following prompt is displayed:

```
Password access level (read,write,administer):
```

- 2 Enter the required access level.

```
Old password:
```

- 3 Enter the old password.

```
New password:
```

- 4 Enter the new password.

The password can have up to 31 characters and is case-sensitive. To enter a null password, press [Enter].

- 5 Retype the new password for verification. The system does not display the password in any of the fields as you type.
- 6 Repeat steps 1 to 5 for each level of password that you want to configure.

---

## Setting the System Name

Assign an easily recognizable and unique name to the Layer 3 Module to help you manage the module. For example, name the system according to its physical location (for example, *ENGLAB*).

To set the system name:

- 1 Enter the following at the top-level menu:

```
system name
```

The following prompt is displayed:

```
Enter new string {?} [L3Module-000000]:
```

- 2 Enter a name that is both unique on the network and meaningful to you. The new system name appears the next time that you display the system configuration.

---

## Working with Nonvolatile Data

Nonvolatile data is information stored by the Layer 3 Module which is retained even when the module is not powered on.

You can do the following tasks with nonvolatile data:

- Create a backup copy of the module's nonvolatile configuration.
- Retrieve the backed-up file.
- Reset system data to its factory-configured values, if necessary.

### Nonvolatile Parameters

During a save, the contents of nonvolatile memory are written to a disk file. All configurable parameters are saved in nonvolatile memory, including:

- Module name
- Passwords
- IP interface configurations
- RIP mode setting
- SNMP community string settings
- SNMP trap destination configurations

The file also contains the following information, which is used to resolve any inconsistencies when nonvolatile data is restored:

- Software version number
- System ID
- Date and time of creation
- Type of configuration
- Data checksums

### Creating a Backup of Nonvolatile Data

When the module saves nonvolatile data, it writes it to a disk file on a host computer (that is, a server) using the Trivial File Transfer Protocol (TFTP). You can then retrieve the information from the disk file by using the `system nvData restore` command.

To back up nonvolatile data, you must first create two files on the TFTP server *before* you send the data:

- **Control file** — Use any filename that is meaningful to you. Example: `ctrlfile`
- **Nonvolatile data file** — Use the control filename plus the `.nvd` extension. Example: `ctrlfile.nvd`

These files must reside in the directory in which the TFTP daemon is running.

Because TFTP provides no user authentication, make sure that the control file and the nonvolatile data file on the remote host are publicly readable and writable. Otherwise, the TFTP server cannot grant requests for file access.

To make a backup of nonvolatile data:

- 1 Enter the following at the top-level menu:

```
system nvData save
```

The following prompt is displayed:

```
Host IP Address [172.16.100.1]:
```

- 2 Enter the IP address of the TFTP server.

```
NV Control file (full pathname):
```

- 3 Enter the full pathname of the control file *without* the `.nvd` extension.



*Some TFTP implementations may allow or require you to supply the filename with the directory path. The file is then saved in the default TFTP directory.*

```
Enter an optional file label[<none>]:
```

- 4 Optionally, enter a label for the file.

If a session is successfully opened, a message notifies you of the success or failure of your save.

If the save succeeds, a message appears that is similar to the following example:

```
System NV data successfully stored on host 158.101.100.1.
```

If the save fails, a message appears that is similar to the following example:

```
Saving system...transfer timed out.  
Error - I/O error while writing nonvolatile data. Do you wish  
to retry the save using the same parameters? (n,y) [y].
```

If you enter **y**, the system attempts to save the data as proposed.

If you enter **n**, the nonvolatile data is not saved and the previous menu appears on the screen.

The exact text of the failure message depends on the problem that the system encountered while saving the nonvolatile data.

At the end of the save, the system display returns to the previous menu.

### Retrieving Saved Nonvolatile Data

You can retrieve nonvolatile data that you have backed up, regardless of the system configuration.

To retrieve nonvolatile data:

- 1 Enter the following at the top-level menu:

```
system nvData restore
```

The following prompt is displayed:

```
Host IP address [0.0.0.0]:
```

- 2 Enter the IP address of the host on which the nonvolatile data file resides.

```
NV Control file (full pathname):
```

- 3 Enter the nonvolatile data filename.



*Some TFTP implementations may allow or require you to supply the filename with the directory path. The system will save the file in the default TFTP directory. Consult your network administrator for details.*

If a saved system ID is different from the current system ID, the module prompts you with a message that is similar to this one:

```
Warning - mismatch between saved system ID (27DA00) and  
current system (28DA900)  
Do you want to disregard this and continue the restore (n, y)  
[y]:
```

If the saved system ID is the same as the current system ID, the system prompts you with a message that is similar to this one:

```
CAUTION - Restoring nonvolatile data may leave the system
in an inconsistent state and therefore a reboot is
necessary after each restore.
```

```
Do you wish to continue? (y/n):
```

- 4 Enter **y** (yes) or **n** (no) as required. If you enter **y**, the module's nonvolatile data is restored as proposed. If you enter **n**, the restoration fails and the previous menu appears on the screen.

The module automatically reboots after restoring nonvolatile data.

---

## Initializing Data to Factory Defaults

At times you may not want to *restore* the module's nonvolatile data. Instead, you may want to *reset* the values to the factory defaults (see "Factory Default Values" on page 32) so that you can start configuring the module from the original settings.



**CAUTION:** *Resetting the nonvolatile data means that all nonvolatile memory is set back to the factory defaults. Before proceeding, be sure that you want to reset your nonvolatile data. Consider saving the nonvolatile data to a file first.*

To set the module to the factory defaults:

- 1 Enter the following at the top-level menu:

```
system initialize
```

The following prompt is displayed:

```
Resetting nonvolatile data may leave the system in an
inconsistent state and therefore a reboot is necessary
after each reset. If you continue the system will be rebooted
after the nonvolatile data is reset.
```

```
Do you wish to continue (n,y) [y]:
```

- 2 Enter **y** (yes) or **n** (no) as required.

---

## Resetting the Module

If you reboot the module while you are connected through an rlogin or Telnet session, rebooting disconnects your session.

To reboot the module:

- 1 Enter the following at the top-level menu:

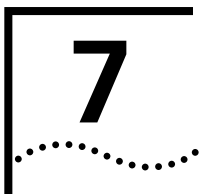
```
system reset
```

The following prompt is displayed:

```
Are you sure you want to reboot the system? (n,y) [y]:
```

- 2 Enter **y** (yes) or **n** (no) as required. If you enter **y**, the system reboots. If you enter **n**, the previous menu appears on the screen.





# DISPLAYING VLAN PARAMETERS

This chapter describes how to display information about VLANs to find what VLAN indexes the Layer 3 Module has created for the 802.1Q VLANs on which it is present.

---

## Displaying VLAN Information

The Layer 3 Module learns on which 802.1Q VLANs it is present from the host switch. These VLANs are either statically configured, or learnt through *GVRP (GARP VLAN Registration Protocol)*. The module creates corresponding VLAN indexes for all these VLANs automatically. The module uses these VLAN indexes to assign IP addresses to VLANs.

You can display the VLANs that the module has learnt from the Switch using the `bridge vlan summary` command.

The summary includes the following fields:

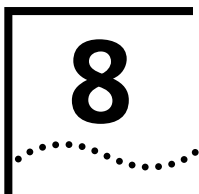
- **Index** — The system-assigned index number that identifies a VLAN.
- **VID** — The VLAN ID, which is a unique, user-defined (12-bit) integer that identifies this VLAN and is used by the global management operations.
- **Name** — The user-assigned name of the VLAN on the Switch.

To display a summary of VLAN information, enter the following at the top-level menu:

```
bridge vlan summary
```

The following example shows a VLAN summary display:

```
VLAN summary
Index  VID  Name
  1     1  Default VLAN
  3  1025  test net
  4  2048  10 net
```



# SETTING IP PARAMETERS

This chapter describes how to configure the IP parameters on your SuperStack® II Switch Layer 3 Module to allow it to work with your Switch. It contains the following sections:

- Available IP Commands
- Administering IP Interfaces
- Administering Routes
- Administering the ARP Cache
- Administering the Domain Name Server Client
- Administering UDP Helper
- Administering IP Multicast Routing
- Administering Multicast Tunnels
- Enabling and Disabling ICMP Router Discovery
- Administering OSPF Areas
- Setting the Default Route Metric
- Configuring OSPF Interfaces
- Displaying the Link State Database
- Administering Neighbors
- Setting the OSPF Router ID
- Administering Memory Partitions
- Administering the Stub Default Metric
- Administering Virtual Links
- Displaying OSPF General Statistics

- Administering RIP
- Using ping
- Using traceRoute



See “Accessing the User Interface” on page 39 for information about launching the user interface.

## Available IP Commands

The following commands are available in the IP context:

**Table 15** IP Context Commands

Command	Options	Sub-options	Syntax	
<b>interface</b>	<b>summary</b>		Display IP interface information	
	<b>define</b>		Define an IP address	
	<b>modify</b>		Modify an IP address	
	<b>remove</b>		Remove an existing IP address definition	
	<b>statistics</b>		Display IP interface statistics	
<b>route</b>	<b>display</b>		Display the contents of the routing table	
	<b>static</b>		Define a static route	
	<b>remove</b>		Remove a static route	
	<b>flush</b>		Flush all learned routes	
<b>arp</b>	<b>display</b>		Display the contents of the ARP cache	
	<b>static</b>		Define a static ARP cache entry	
	<b>remove</b>		Remove an ARP cache entry	
	<b>flush</b>		Remove all entries from the ARP cache	
	<b>age</b>		Set the age time for dynamic ARP cache entries	
<b>multicast</b>	<b>dvmrp</b>		Enable/disable DVMRP	
	<b>igmp</b>		Enable/disable IGMP features	
	<b>interface</b>		<b>display</b>	Display multicast settings on each interface
			<b>enable</b>	Enable multicast routing on a given IP interface
			<b>disable</b>	Disable multicast routing on a given IP interface
	<b>tunnel</b>		<b>display</b>	Display the configured multicast tunnels
			<b>define</b>	Define a multicast tunnel
			<b>remove</b>	Remove a multicast tunnel
		<b>routeDisplay</b>		Display the summary of the multicast routing table

(continued)

**Table 15** IP Context Commands (continued)

Command	Options	Sub-options	Syntax
<b>dns</b>	<b>cacheDisplay</b>		Display multicast cache entries
	<b>display</b>		Display the current domain name and the name servers associated with it
	<b>domainName</b>		Modify a currently defined domain name
	<b>define</b>		Define a new name server IP address
	<b>modify</b>		Modify a name server IP address
	<b>remove</b>		Remove a name server IP address
<b>udpHelper</b>	<b>nslookup</b>		Query a name server
	<b>display</b>		Display UPD Helper information
	<b>define</b>		Define port numbers and IP forwarding addresses
	<b>remove</b>		Remove a port number or IP forwarding address
<b>icmpRouterDiscovery</b>	<b>hopCountLimit</b>		Set the BOOTP hop count limit
	<b>threshold</b>		Set the BOOTP relay threshold
<b>ospf</b>	<b>areas</b>	<b>display</b>	View areas and range definitions for each area
		<b>defineArea</b>	Define a new area
		<b>modifyArea</b>	Modify an existing area
		<b>removeArea</b>	Remove an area definition and its associated ranges
		<b>addRange</b>	Add a range to an area
		<b>modifyRange</b>	Modify a range in an area
		<b>removeRange</b>	Remove a range from an area
	<b>defaultRouteMetric</b>	<b>display</b>	Display the default route metric
		<b>define</b>	Define the default route metric
		<b>remove</b>	Remove the default route metric
	<b>interface</b>	<b>summary</b>	Display a summary of the OSPF configuration on each IP interface
		<b>detail</b>	Display details of the OSPF configuration on each IP interface
		<b>statistics</b>	Display the OSPF statistics for each specified IP interface
		<b>mode</b>	Enable/disable OSPF on each of the specified interfaces
<b>priority</b>		Specify the OSPF priority of each interface	
<b>areaID</b>		Assign an area to an interface	
<b>cost</b>		Specify an OSPF interface cost	

(continued)

**Table 15** IP Context Commands (continued)

Command	Options	Sub-options	Syntax
		<b>delay</b>	Specify a transit delay
		<b>hello</b>	Specify the hello packet interval on a given interface
		<b>retransmit</b>	Specify the link state advertisement retransmit time on a given interface
		<b>dead</b>	Specify the interface dead interval
		<b>password</b>	Specify the authentication password for OSPF state messages
	<b>linkStateData</b>	<b>databaseSummary</b>	Generate a report of the specified area ID
		<b>router</b>	Display the OSPF router link state advertisements
		<b>network</b>	Display the OSPF network link state advertisements
		<b>summary</b>	Display the OSPF summary link state advertisements
		<b>external</b>	Display the OSPF external link state advertisements
	<b>neighbors</b>	<b>display</b>	Display the neighbors table
		<b>add</b>	Define a static neighbor
		<b>remove</b>	Remove a static neighbor
	<b>routerID</b>		Define router IDs
	<b>partition</b>	<b>display</b>	Display the current memory allocated to OSPF
		<b>modify</b>	Allocate less or more memory resource to OSPF
	<b>stubDefaultMetric</b>	<b>display</b>	Display the stub default metric
		<b>define</b>	Define the stub default metric
		<b>remove</b>	Remove the stub default metric
	<b>virtualLinks</b>	<b>summary</b>	Display a summary of configured virtual links
		<b>detail</b>	Display detailed information for the configured virtual links
		<b>statistics</b>	Display statistics on OSPF virtual links
		<b>define</b>	Specify a virtual link
		<b>remove</b>	Remove a virtual link
		<b>areaID</b>	Change the target area of a virtual link
		<b>delay</b>	Specify the transmit delay for each virtual link
		<b>hello</b>	Specify the frequency of hello messages
		<b>retransmit</b>	Specify the retransmit time for link state advertisements for virtual links
		<b>dead</b>	Specify the dead interval

(continued)

**Table 15** IP Context Commands (continued)

Command	Options	Sub-options	Syntax
		<code>password</code>	Specify the password to be used to generate the OSPF authentication checksum on virtual link frames
<code>rip</code>	<code>statistics</code>		Display general OSPF statistics
	<code>display</code>		Display the current IP routing configuration
	<code>mode</code>		Set the RIP Mode on an interface
	<code>cost</code>		Set the RIP cost on an interface
	<code>poisonReverse</code>		Enable/disable RIP Poisoned Reverse mode on an interface
	<code>addAdvertisement</code>		Define RIP advertisement addresses
	<code>removeAdvertisement</code>		Remove RIP advertisement addresses
	<code>statistics</code>		Display internal statistics about RIP engine
<code>ping</code>			Ping a host using default settings
<code>advancedPing</code>			Ping a host specifying the settings to use
<code>traceRoute</code>			Trace a route using default settings
<code>advancedTraceRoute</code>			Trace a route specifying the settings to use
<code>statistics</code>			Display IP, UDP and ICMP statistics

## Administering IP Interfaces

An IP interface defines the relationship between a Virtual Local Area Network (VLAN) and the subnets in the IP network. Every IP interface has one VLAN associated with it. You must first define a VLAN, as described in your Switch management guide, before you can define an associated IP interface.

### Interface Characteristics

Each IP interface has the following characteristics:

- **IP Address** — Choose this address from the range of addresses assigned to your organization by the central agency. This address is specific to your network.
- **Subnet mask** — Subnet masks differentiate the network ID part of an IP address from the host ID part. They assign the number one (1) to bits that correspond to the network ID and zeros to bits that correspond to the host ID. A subnet mask is a 32-bit number expressed as four decimal numbers from 0 to 255 separated by periods, for example, 255.255.0.0. The first two octets represent the network ID, and the final two represent the host part of the address.

- **Advertisement Address** — The Layer 3 Module uses this IP address when it advertises routes to other stations on the same subnet. In particular, the Layer 3 Module uses this address for sending RIP updates. By default, the Layer 3 Module uses a directed advertisement (all number ones in the host field). The default advertisement address that the Layer 3 Module provides is appropriate for most networks.
- **Cost** — The Layer 3 Module uses this number, between 1 and 15, to calculate route metrics. Unless your network has special requirements, assign a cost of 1 to all interfaces.
- **State** — This status of the IP interface indicates whether the interface is available for communication. Because the Layer 3 Module is an internal module, the interface is always up, regardless of the state of the front panel ports.
- **VLAN Index** — VLAN ID. The VLAN index indicates which 802.1Q VLAN is associated with that IP interface. When the menu prompts you for this option, it displays a list of available VLANs.

To display the mappings between the VLAN indexes and the 802.1Q VLANs, use the **bridge vlan summary** command.

See Chapter 7, “Displaying VLAN Parameters” for more information about this command.

## Displaying Interfaces

You can display summary information about all IP interfaces configured on the Layer 3 Module. The detail display contains summary information and information about the advertisement address.

Enter the following at the top-level menu:

```
ip interface summary
```

The following example shows an IP interface summary display:

Index	Type	IP address	Subnet mask	State	VLAN index
1	VLAN	10.0.0.2	255.0.0.0	Up	1

## Defining an IP Interface

When you define an IP interface, you specify several characteristics associated with that interface, as well as the VLAN associated with it.

The default values that the Layer 3 Module provides for some interface characteristics are appropriate for most networks.





*Make sure that you define a VLAN, as described in your Switch management guide, before you define an associated IP VLAN interface.*

To define an IP interface:

- 1 Enter the following at the top-level menu:

```
ip interface define
```

The following prompt is displayed:

```
Enter IP address:
```

- 2 Enter the IP address of the interface.

```
Enter subnet mask [255.255.0.0]:
```

- 3 Enter the subnet mask of the interface.

```
Enter VLAN interface index [2]:
```

- 4 Enter the VLAN index that is associated with the 802.1Q VLAN ID for this VLAN.

### **Modifying an IP Interface**

You can change the configuration of an interface you have already defined.

To modify an IP interface:

- 1 Enter the following at the top-level menu:

```
ip interface modify
```

The following prompts are displayed:

```
Select IP interface {1-4}:
```

```
Enter IP address [12.0.0.2]:
```

```
Enter subnet mask [255.0.0.0]:
```

```
Enter VLAN interface index {3|?} [3]:
```

- 2 Modify the existing interface parameters by entering a new value at the required prompt(s).

### **Removing an Interface**

You can remove an interface if you are no longer using it to route on the ports associated with the interface.

To remove an IP interface:

- 1 Enter the following at the top-level menu:

```
ip interface remove
```

The following prompt is displayed:

Select IP interfaces (2-4|all):

- 2 Enter the index number of the interface you want to remove.

## Administering Routes

The Layer 3 Module maintains a table of routes to other IP networks, subnets, and hosts. You can make static entries in this table using the command line interface or configure the Layer 3 Module to use a routing information protocol to exchange routing information automatically.

Each routing table entry contains the following information:

- **Destination IP Address and Subnet Mask** — Defines the address of the destination network, subnet, or host.
- **Next Hop** — Defines the next switch or router to which packets destined for this network must be forwarded.
- **Routing Metric** — Specifies the number of networks or subnets through which a packet must pass to reach its destination. The Layer 3 Module includes the metric in its RIP updates to allow other routers to compare routing information received from different sources.
- **Gateway IP Address** — Tells the module how to forward packets whose destination addresses match the route's IP address and subnet mask. The module forwards such packets to the indicated gateway.
- **Status** — For each interface, the route provides the status information in Table 16.

**Table 16** Interface Status Information

Field	Description
Direct	Route goes to a directly connected network
Static	Route was statically configured
Learned	Route was learned using indicated protocol
Timing out	Route was learned but has partially timed out
Timed out	Route has timed out and is no longer valid
Local	The address for the module

In addition to the routes to specific destinations, the routing table can contain an additional entry called the *default route*. The Layer 3 Module uses the default route to forward packets that do not match any other routing table entry. You may want to use the default route in place of

routes to numerous destinations that all have the same gateway IP address.

### How Routes are Used by the Layer 3 Module

The following example shows how the Layer 3 Module uses routes in the routing table to forward packets.

A route in the routing table may contain the following details:

- Network address of 89.1.0.0
- Subnet mask of 255.255.0.0
- Next hop of 90.5.5.4

A packet is received by the Layer 3 Module with a destination address of 89.1.9.99. When the Layer 3 Module receives the packet, the module follows this process:

- 1 The Layer 3 Module applies the route's subnet mask to this destination address.

In this case, the subnet mask of 255.255.0.0 applied to the destination address of 89.1.9.99 yields 89.1.0.0.

- 2 The Layer 3 Module compares the masked destination address to the network address of the route.

In this case, the masked destination address of 89.1.0.0 matches the network address of 89.1.0.0. The Layer 3 Module now uses the next hop contained within that route (90.5.5.4) to forward the packet nearer to its final destination.



*If the Layer 3 Module finds more than one routing table entry matching an address, it uses the most specific route, which is the route with the most bits set in its subnet mask. For example, the route to a subnet within a destination network is more specific than the route to the destination network.*

### Displaying the Routing Table

You can display the Layer 3 Module's routing table to determine which routes are configured and whether the routes are operational.

Enter the following at the top-level menu:

```
ip route display
```

The following example shows a Layer 3 Module's routing table display:

```
Select menu option: ip route display
IP routing is enabled, ICMP router discovery is disabled
There are 5 Routing Table entries
```

Destination	Subnet mask	Metric	Gateway	Status
Default Route	--	--	172.16.20.20	Static
172.16.20.0	255.255.254.0	--	--	Direct
172.16.21.184	255.255.255.255	--	--	Local
172.16.231.96	255.255.255.224	--	--	Direct
172.16.231.97	255.255.255.255	--	--	Local

### Defining a Static Route

Before you can enter a static route, you must define at least one IP interface (see "Defining an IP Interface" on page 64). Static routes remain in the table until you remove them or the corresponding interface. They take precedence over dynamically learned routes to the same destination.



*Static routes are not included in periodic RIP updates sent by the Layer 3 Module.*

To define a static route:

- 1 Enter the following at the top-level menu:

```
ip route static
```

The following prompt is displayed:

```
Enter destination IP address:
```

- 2 Enter the destination IP address of the route.

```
Enter subnet mask [255.255.0.0]:
```

- 3 Enter the subnet mask of the route.

```
Enter gateway IP address:
```

- 4 Enter the gateway IP address of the route.

### Removing a Static Route

To remove an existing route:

- 1 Enter the following at the top-level menu:

```
ip route remove
```

The following prompt is displayed:

```
Select destination IP address:
```

- 2 Enter the destination IP address of the route.  
`Select subnet mask [255.255.0.0]:`
- 3 Enter the subnet mask of the route. The Layer 3 Module deletes the route from the routing table immediately.

### Flushing All Learned Routes

Flushing deletes all learned routes from the routing table. To flush all learned routes, enter the following at the top-level menu:

```
ip route flush
```

The Layer 3 Module deletes all learned routes from the routing table immediately.

### Setting the Default Route

If you define a default route, the Layer 3 Module uses it to forward packets that do not match any other routing table entry. The Layer 3 Module can learn a default route using RIP, or you can configure a default route statically.

If the routing table does not contain a default route, then the Layer 3 Module cannot forward a packet that does not match any other routing table entry. If this occurs, then the Layer 3 Module drops the packet and sends an ICMP "destination unreachable" message to the host that sent the packet.



*You cannot configure the default route using the command line interface; you must use the Web management interface for the Switch.*

To set the default route, follow the procedure described in step 3 on page 31.

### Removing the Default Route

To remove a default route from the routing table, follow the procedure described in step 3 on page 31.

## Administering the ARP Cache

The Layer 3 Module uses the Address Resolution Protocol (ARP) to find the MAC addresses corresponding to the IP addresses of hosts and other routers on the same subnets. Each device participating in routing maintains an ARP cache — a table of known IP addresses and their corresponding MAC addresses.



*ARP usually learns the MAC and IP addresses of devices. Static entries are useful to make sure that key hosts, for example, other routers, can be contacted immediately after a restart.*

## Displaying the ARP Cache

Enter the following at the top-level menu:

```
ip arp display
```

The following example shows an IP ARP cache display:

```
IP routing is enabled, ICMP router discovery is disabled
There is 1 ARP cache entry
IP address      Type      I/F      Hardware address
10.0.0.19      static    1        44-13-16-24-80-82
```

## Defining a Static ARP Cache Entry

ARP usually learns the MAC to IP address mapping of devices dynamically. Static entries are useful to ensure that key hosts, for example, other routers, can be contacted immediately after the Layer 3 Module is restarted.

To define a static ARP cache entry:

- 1 Enter the following at the top-level menu:

```
ip arp static
```

The following prompt is displayed:

```
Select interface index {1-2}:
```

- 2 Select the IP interface index.

```
Enter IP address:
```

- 3 Enter the IP address of the ARP cache entry.

```
Enter MAC address:
```

- 4 Enter the MAC address of the ARP cache entry.

### Removing an ARP Cache Entry

To remove an entry from the ARP cache:

- 1 Enter the following at the top-level menu:

```
ip arp remove
```

The following prompt is displayed:

```
Select IP address:
```

- 2 Enter the IP address of the entry you want to remove.

The Layer 3 Module removes the address from the ARP cache immediately. If necessary the Layer 3 Module subsequently uses ARP to find the new MAC address corresponding to that IP address.

### Flushing the ARP Cache

You may want to delete all entries from the ARP cache if the MAC address has changed.

To remove all entries from the ARP cache:

- 1 Enter the following at the top-level menu:

```
ip arp flush
```

The Layer 3 Module removes the entries from the ARP cache immediately.

### Setting the Age Time

The age time for dynamic ARP cache entries determines how long the dynamic entries remain in the ARP cache. When the time expires, the Layer 3 Module automatically flushes the entry from the cache. A value of 0 indicates no age time, and entries remain in the table indefinitely.

The default age time is 15 minutes.

To set the age time:

- 1 Enter the following at the top-level menu:

```
ip arp age
```

The following prompt is displayed:

```
Enter ARP age time in minutes 0 for no ageing (0-1440) [15]:
```

- 2 Enter the age time in minutes, or enter 0 for no ARP ageing.

---

## Administering the Domain Name Server Client

The Domain Name Server (DNS) client provides DNS lookup functionality to the Switch IP ping and traceRoute features. DNS lookup allows you to specify a hostname rather than an IP address when you use ping or traceRoute to contact an IP station.

The DNS commands allow you specify one or more name servers associated with a domain name. Each name server maintains a list of IP addresses and their associated host names. When you use ping or traceRoute with a hostname, the DNS client attempts to locate the name on the name servers you specify. When the DNS client locates the name, it resolves it to the IP address associated with it.

See your DNS documentation for information about how to create and maintain lists of domain names and IP addresses on the name servers.

### Displaying the DNS Configuration

To display the current domain name and the name servers associated with it, enter the following at the top-level menu:

```
ip dns display
```

The following example shows the IP DNS configuration display:

```
Domain Name - dns.org.org
Name Server - 14.4.4.4
```

### Modifying the DNS Domain Name

To change the name of the currently defined domain:

- 1 Enter the following at the top-level menu:

```
ip dns domainName
```

The following prompt is displayed:

```
Enter Domain Name [dns.eg.org]:
```

- 2 Enter the new domain name. The Layer 3 Module displays the current domain name in brackets.

### Defining a New Name Server IP Address

To define a new name server IP address associated with the current domain name:

- 1 Enter the following at the top-level menu:

```
ip dns define
```



The following prompt is displayed:

```
Enter Name Server's IP address:
```

- 2 Enter the new name server IP address at the prompt. When the Layer 3 Module accepts the new IP address, it displays a message similar to the following:

```
Server's IP address 10.0.0.5 is added to the DNS database
```

The Layer 3 Module assigns the new IP address an index number. Use this index number when you want to modify or remove this IP address.

### Modifying a Name Server IP Address

To change a currently defined name server IP address:

- 1 Enter the following at the top-level menu:

```
ip dns modify
```

The Layer 3 Module displays the list of Name Server IP addresses and the index number associated with each one:

```
Index      Name Server IP address
  1         10.0.0.4
  2         10.0.0.5
```

```
Select server index {1-2}:
```

- 2 Enter the index number of the IP address you want to modify.

```
Enter New Server's IP address:
```

- 3 Enter the new IP address.

### Removing a Name Server IP Address

To remove a previously defined Name Server IP address:

- 1 Enter the following at the top-level menu:

```
ip dns remove
```

The Layer 3 Module displays the list of Name Server IP addresses and the index number associated with each one:

```
Index      Name Server IP address
  1         10.0.0.4
  2         10.0.0.5
```

```
Select server index {1-2}:
```

- 2 Enter the index number of the IP address that you want to remove.

**Querying Name Servers** You can check the resolution between IP addresses and host names on a Name Server. You enter either the host name or the IP address, and the DNS client displays the pair.

To query a name server:

- 1 Enter the following at the top-level menu:

```
ip dns nslookup
```

The following prompt is displayed:

```
Enter host information (IP address/name):
```

- 2 Enter the host name or an IP address at the prompt.

The module returns the associated host name or IP address.

---

## Administering UDP Helper

UDP Helper permits the routing of UDP broadcast frames between VLANs when these broadcasts are not normally routed between VLANs. With UDP Helper, protocols such as the Bootstrap Protocol (BOOTP) and the Dynamic Host Configuration Protocol (DHCP) are available so that you can boot hosts through this router.

The UDP services that are mentioned in this section on UDP Helper use the following ports:

- BOOTP and DHCP = 67
- TIME = 37
- DNS = 53

UDP Helper allows you to set the number of times a UDP packet is forwarded between subnetworks. In addition, UDP packets are discarded based on the hop count and the seconds value for BOOTP and DHCP packets. The forwarding address that the UDP Helper uses is either the IP broadcast address, for example, 10.255.255.255, or the IP addresses of the relevant DHCP, BOOTP, TIME or DNS servers.

## Displaying UDP Helper Information

To display the hop count, threshold configuration and list the ports and the IP forwarding addresses that are defined for each port, enter the following at the top-level menu:

```
ip udpHelper display
```

The following example shows a UDP Helper display:

```
BOOTP relay hop count limit is 4, BOOTP relay threshold is 0.  
BOOTP is using the first overlapped interface  
  
UDP port Forwarding address  
67 10.1.0.67
```

### Defining a Port and an IP Forwarding Address

You can define port numbers and IP forwarding addresses for the UDP Helper. You may have up to 32 combinations of port numbers and IP forwarding addresses per router. You may also have multiple IP address entries for the same ports.

To define a port and IP forwarding address:

- 1 Enter the following at the top-level menu:

```
ip udpHelper define
```

The following prompt is displayed:

```
Enter UDP port number (1-65535)[67]:
```

- 2 Enter the UDP port number.

```
Enter forwarding IP address:
```

- 3 Enter the forwarding address.

### Removing a Port or an IP Forwarding Address

You can remove a port number or IP forwarding address defined for UDP Helper.

To remove a port or IP forwarding address:

- 1 Enter the following at the top-level menu:

```
ip udpHelper remove
```

The following prompt is displayed:

```
Enter UDP port number (1-65535):
```

- 2 Enter the UDP port number that you want to remove.

```
Enter forwarding IP address:
```

- 3 Enter the IP forwarding address that you want to remove. The Layer 3 Module removes the port numbers and IP forwarding addresses you specified immediately.

### Setting the BOOTP Hop Count Limit

You can set the maximum hop count for a packet that the Layer 3 Module forwards through the router.

The default hop count limit is 4.

To set the hop count limit:

- 1 Enter the following at the top-level menu:

```
ip udpHelper hopCountLimit
```

The following prompt is displayed:

```
Enter BOOTP relay hop count limit (1-16) [4]:
```

- 2 Enter the BOOTP hop count limit.

### Setting the BOOTP Relay Threshold

You can set the maximum number of times that the Layer 3 Module forwards a packet to the network.

The default BOOTP relay threshold value is 2.

To set the default relay threshold:

- 1 Enter the following at the top-level menu:

```
ip udpHelper threshold
```

The following prompt is displayed:

```
Enter BOOTP relay threshold (0-65535) [2]:
```

- 2 Enter the BOOTP relay threshold value.

---

## Administering IP Multicast Routing

IPv4 uses two types of communication between end stations in a network: unicast for point-to-point communications and multicast for point-to-multipoint communications.

Use of the Internet has seen a rise in the number of new applications that rely on multicast transmission. IP multicast routing conserves bandwidth by forcing the network to replicate packets only when necessary, and offers an alternative to unicast transmission for the delivery of high bandwidth network applications. IP multicast routing is not solely limited to the Internet; it can also play an important role in large distributed commercial networks.

There are two fundamental types of IPv4 addresses, corresponding to the communication methods:

- **Unicast addresses** — Designed to transmit a packet to a single destination.
- **Multicast addresses** — Designed to enable the delivery of datagrams to a set of hosts that have been configured as members of a multicast group in various scattered subnetworks.

A **broadcast address** is a special type of multicast address. It is used to send a datagram to an entire subnetwork; however, a broadcast address is not usually routed beyond the subnetwork.

Multicast routing is not connection-orientated. A multicast datagram is delivered to destination group members with the same “best-effort” reliability as a standard unicast IP datagram. This means that a multicast datagram is not guaranteed to reach all members of the group, or arrive in the same order relative to the transmission of other packets.

The only difference between a multicast IP packet and a unicast IP packet is the presence of a “group address” in the Destination Address field of the IP header. Instead of a Class A, B, or C IP address, multicasting employs a Class D destination address format (224.0.0.0-239.255.255.255).

Multicast routers execute a multicast routing protocol to define delivery paths that enable the forwarding of multicast datagrams across an internetwork. The Distance Vector Multicast Routing Protocol (DVMRP) is a distance-vector routing protocol.



*Before you define any IP multicast interfaces, you must first define IP interfaces and routes.*

### **Enabling and Disabling DVMRP**

Distance Vector Multicast Routing Protocol (DVMRP) is similar to the IP Routing Information Protocol. Multicast routers exchange distance vector updates that contain lists of destinations and the distance in hops to each destination. The routers maintain this information in a routing table.

The default DVMRP mode is *disabled*.



To carry out multicast routing, you must have DVMRP enabled. Doing so enables DVMRP on all active IP interfaces.

To enable or disable DVMRP:

- 1 Enter the following at the top-level menu:

```
ip multicast dvmrp
```

The following prompt is displayed:

```
Enter DVMRP mode (disabled, enabled) [disabled]:
```

- 2 Enable or disable DVMRP as required.

### Enabling and Disabling IGMP

The Internet Group Management Protocol (IGMP) enables a router or switch to find out whether group members exist in a subnetwork. The protocol uses the query mode search method to determine this information. The router or switch with the lowest IP address in the LAN broadcasts a query to all other members of the subnetwork to determine whether they are also in the group. End stations respond to the query with IGMP packets, which report the multicast group to which they belong.

When you select the IGMP option, the interface prompts you to enable or disable the IGMP query mode. Under most conditions, enable IGMP query mode.

IGMP query mode is *enabled* by default.

To enable or disable IGMP query mode:

- 1 Enter the following at the top-level menu:

```
ip multicast igmp
```

The following prompt is displayed:

```
Enter IGMP query mode (disabled, enabled) [enabled]:
```

- 2 Enable or disable the query mode as required.

## Administering IP Multicast Interfaces

The IP multicast interface options allow you to enable and disable multicast characteristics on previously defined IP interfaces.

### Multicast Interface Characteristics

A multicast interface has the following characteristics:

- **DVMRP Metric Value** — Determines the cost of a multicast interface. The higher the cost, the less likely it is that the packets will be routed over the interface. The default value is 1.
- **Time To Live (TTL) Threshold** — Determines whether the interface forwards multicast packets to other switches and routers in the subnetwork. If the interface TTL is greater than the packet TTL, then the interface does not forward the packet. The default value is 1, which means that the interface forwards all packets.

## Displaying Multicast Interface Information

To display information about all the multicast interfaces, enter the following at the top-level menu:

```
ip multicast interface display
```

The following example shows a multicast interface display:

```
DVMRP is disabled
Index Local Address      Metric State
  1   172.16.21.184      1   disabled
  2   172.16.231.97     1   one-way non-querier leaf
                                peers: 140.204.231.99 (3.6) (0xe)
```

## Enabling Multicast Interfaces

Multicast routing is *enabled* on all existing IP interfaces unless you have specifically disabled it. Use the command described in this section to change the characteristics of an existing interface or to enable an interface that you had previously disabled.

To enable or change a multicast interface:

- 1 Enter the following at the top-level menu:

```
ip multicast interface enable
```

The following prompt is displayed:

```
Enter an IP interface index (1-3):
```

- 2 Enter the index numbers of the interfaces that you want to enable.  
`Enter interface DVMRP metric (1-15):`
- 3 Enter the DVMRP metric value of the chosen interfaces.  
`Enter interface TTL threshold (1-255):`
- 4 Enter the Time To Live (TTL) threshold of the chosen interfaces.

### Disabling Multicast Interfaces

To disable multicast routing on a specific interface.

- 1 Enter the following at the top-level menu:  
`ip multicast interface disable`  
The following prompt is displayed:  
`Enter an IP interface index {1-2}:`
- 2 Enter the index number of the IP interface you want to disable.

---

### Administering Multicast Tunnels

A multicast tunnel allows multicast packets to cross several unicast routers to a destination router that supports multicast routing. A tunnel has two end points. The local end point is associated with an interface on the Layer 3 Module.

When you define the tunnel, specify the associated interface on the Layer 3 Module and then the characteristics of the tunnel. Tunnel characteristics are the same as those of an interface. You also specify the IP address of the remote multicast router.



*You only need to define a multicast tunnel if you need to set up a connection between two multicast internetworks through one or more unicast routers.*

### Displaying Multicast Tunnels

To display current IP multicast tunnels on the Layer 3 Module, enter the following at the top-level menu:

```
ip multicast tunnel display
```



The following example shows a IP multicast tunnel display:

```
DVMRP is enabled
Index Local Address      Remote Address  Metric State
  1   10.0.0.1           13.0.0.2       1    one-way querier leaf
      pkts in: 0  pkts out: 275338
```

### Defining a Multicast Tunnel

To define a multicast tunnel from an interface on the Layer 3 Module:

- 1 Enter the following at the top-level menu:

```
ip multicast tunnel define
```

The following prompt is displayed:

```
Enter an IP interface index [1]:
```

- 2 Enter the index numbers of the interfaces with which to associate a multicast tunnel.

```
Enter remote IP address:
```

- 3 Enter the IP address of the destination multicast router.



*The IP address of the destination multicast router must be a remote address. The destination router cannot be directly connected to the same subnetworks as the local IP address.*

```
Enter tunnel DVMRP metric (1-15) [1]:
```

- 4 Enter the DVMRP metric value of the tunnel.

```
Enter tunnel TTL threshold (1-255) [1]:
```

- 5 Enter the Time To Live (TTL) threshold of the tunnel.

### Removing a Multicast Tunnel

To remove multicast tunnels that you have added to the Layer 3 Module:

- 1 Enter the following at the top-level menu:

```
ip multicast tunnel remove
```

The following prompt is displayed:

```
Enter multicast tunnel index [1]:
```

- 2 Enter the index numbers of the interfaces associated with the tunnel that you want to remove. The tunnel is removed.

**Displaying Routes**

To display all available routes in the IP multicast routing table, enter the following at the top-level menu:

```
ip multicast routeDisplay
```

The DVMRP status is displayed. The following example shows a multicast route display:

DVMRP is enabled						
Multicast Routing Table (31 entries)						
Origin-Subnet	From-Gateway	Metric	Tmr	In-If	Out-Ifs	
172.20.24.40/30	172.16.20.20	5	0	I1	I2*	T1* T2*
172.20.24.32/30	172.16.20.20	5	0	I1	I2*	T1* T2*
172.20.22.24/30	172.16.20.20	5	0	I1	I2*	T1* T2*
172.20.22.4/30	172.16.20.20	4	0	I1	I2*	T1* T2*
172.20.21.104/30	172.16.20.20	5	0	I1	I2*	T1* T2*

Table 17 describes the fields in the cache configuration display.

**Table 17** Cache Configuration Display Fields

Field	Field Description
Origin-Subnet	The source address and the number of bits in the subnetwork.
From-Gateway	The interface address of the gateway.
Metric	The hop count.
Tmr	The amount of time, in seconds, since the routing table entry was last reset.
In-If *	Interface number on which that gateway is connected. Traffic is expected to originate from this interface.  T represents the tunnel; P denotes that a prune message has been sent to this tunnel.
Out-Ifs *	Set of interfaces out of which the traffic will be flooded. I indicates interfaces.

**Displaying the Multicast Cache**

The multicast cache contains the IP source address and destination address for packets observed on the Layer 3 Module. It shows how information is routed over interfaces and ports in your Layer 3 Module.

To edit the multicast cache:

- 1 Enter the following at the top-level menu:

```
ip multicast cacheDisplay
```

The following prompt is displayed:

```
Enter multicast source address [255.255.255.255]:
```

- 2 Enter the multicast source address.

Enter multicast group address [255.255.255.255]:

- 3 Enter the multicast group address. The DVMRP status is displayed.

Table 18 describes the fields in the multicast cache display.

**Table 18** Multicast Cache Display Fields

Field	Description
Origin	The source of the incoming packets. Entries preceded by an angle bracket (>) indicate a multicast subnetwork. Entries without an angle bracket are multicast routers within the subnetwork that immediately precedes them in the table.
Mcast-group	The destination multicast group.
CTmr	Cache timer, which is the amount of time that a cache entry has to remain in the cache.
Age	Number of seconds (s), minutes (m), or hours (h) that the cache entry has been in existence.
PTmr	The time remaining, in seconds (s), minutes (m), or hours (h), before another prune message will be sent to the network.
In-If	Interface number on which that gateway is connected. Traffic is expected to originate from this interface. T represents the tunnel; P denotes that a prune message has been sent to this tunnel.
Out-Ifs	Set of interfaces out of which the traffic will be flooded. Ix represents the interface.

## Enabling and Disabling ICMP Router Discovery

The Internet Control Message Protocol (ICMP) Router Discovery protocol (RFC 1256) allows an appropriately configured end station to locate one or more routers on the LAN to which it is attached. The end station then automatically installs a default route to each of the routers running ICMP Router Discovery. You do not need to manually configure a default route. ICMP redirect messages will subsequently channel the IP traffic to the correct router.



*Only certain workstations can be configured to work with the ICMP Router Discovery protocol. Refer to the documentation for your workstation to determine whether it can be configured to work with this protocol.*

ICMP Router Discovery is disabled by default.

To enable or disable ICMP Router Discovery:

- 1 Enter the following at the top-level menu:

```
ip icmpRouterDiscovery
```

The following prompt is displayed:

```
Enter router discovery state (disabled,enabled) [disabled]:
```

- 2 Enable or disable the ICMP Router Discovery mode as required.

## Administering OSPF Areas

Open Shortest Path First (OSPF) is one of the IP interior gateway protocols (IGPs). The Layer 3 Module can use OSPF to configure its routing tables dynamically.

OSPF operates between co-operating routers within routing domains (*areas*). Routers communicate to each other the state of each of their links in link state advertisements (*LSAs*). An LSA enables a router to learn the best (shortest) path to a destination network. The Layer 3 Module supports OSPF version 2.

An OSPF *area* is a logical, user-defined group of networks, hosts, and directly-attached routers that have a common view of the OSPF routing table.

A *range* defines networks and hosts within an area. Areas can contain multiple ranges.



*The backbone area 0.0.0.0 is implicitly defined by default.*

## Displaying Areas

To display a list of existing areas according to their area identification (ID) numbers, enter the following at the top-level menu:

```
ip ospf areas display
```

The list of existing areas is displayed. The following example shows an OSPF area list:

Area definitions					
Indx	AreaID	IP Address	Mask	Advertise	Stub
1	0.0.0.1	16.0.0.0	255.255.0.0	y	n

Table 19 describes the fields in the areas display:

**Table 19** Field Attributes for the Areas Display

Field	Description
Indx	Entry index for the area
AreaID	Area identifier
IP Address	Network portion of IP address range
Mask	Subnet mask
Advertise	Should the range be advertised?
Stub	Is the area a stub area?

### Defining an Area

Each OSPF area is a logical group of network entities, including network segments, routers, and nodes. Each area has the following parameters:

- **Area ID** — This number, which is in the form of an IP address, functions as an area identification number to the OSPF autonomous system.
- **Stub Area** — Indicates whether this area is a stub area. Stub areas usually contain routers with limited memory resources and lie on the edge of the network. Stub areas cannot contain *virtual links*.

When you define an area, the module assigns an index number to the area. The module uses the next available index number for the area you define.

To define an OSPF area:

- 1 Enter the following at the top-level menu:

```
ip ospf areas defineArea
```

The following prompt is displayed:

```
Enter Area ID []:
```

- 2 Enter the area identification number (ID).

```
Is this a stub area (yes,no) [no]:
```

- 3 Specify whether this area is a stub area. The default is no.

### Modifying an Area

To modify the attributes of an existing area range:

- 1 Enter the following at the top-level menu:

```
ip ospf areas modifyArea
```

The following prompt is displayed:

```
Select area {1-2}:
```

- 2 Enter the index of the area you want to modify.

```
Enter Area ID [0.0.0.3]:
```

- 3 Enter the area ID.

```
Is this a stub area (yes,no) [no]:
```

- 4 Specify whether this is a stub area.

**Removing an Area** To remove an existing OSPF area:

- 1 Enter the following at the top-level menu:

```
ip ospf areas removeArea
```

The following prompt is displayed:

```
Select areas [1-2]:
```

- 2 Enter the index number of the area you want to remove.

**Adding a Range** You can add a range to a previously defined OSPF area. When you add a range, you specify only the network portion of the IP address.

To add a range:

- 1 Enter the following at the top-level menu:

```
ip ospf areas addRange
```

The following prompt is displayed:

```
Select area [1-2]:
```

- 2 Enter the index number of the area to which you want to add the range.

```
Enter IP address:
```

- 3 Enter the IP address of the range to add to the area.

```
Enter subnet mask [255.255.0.0]:
```

- 4 Enter the subnet mask.

```
Advertise this area range (yes,no) [yes]:
```

- 5 Specify whether to advertise the range on the network. The default is yes.

- Modifying a Range** To modify information associated with a previously defined range:
- 1 Enter the following at the top-level menu:  
**ip ospf areas modifyRange**  
The following prompt is displayed:  
Select area {1-2}:
  - 2 Enter the index number of the area that contains the range to modify.  
Enter IP address of range to modify:
  - 3 Enter the IP address of the range to modify.  
Enter IP address:
  - 4 Enter the new IP address if you want to change it. Press Enter if you do not want to change it.  
Enter subnet mask [255.255.0.0]:
  - 5 Enter the subnet mask. Press Enter if you do not want to change it.  
Advertise this area range (yes,no) [yes]:
  - 6 Specify whether to advertise the range on the network. The default is yes.

- Removing a Range** To remove a previously defined range:
- 1 Enter the following at the top-level menu:  
**ip ospf areas removeRange**  
The following prompt is displayed:  
Select area {1-2}:
  - 2 Enter the index number of the area containing the range you want to remove.  
Enter IP address of range to delete:
  - 3 Enter the IP address of the range you want to delete.

---

## Setting the Default Route Metric

The default route metric value indicates the cost for a default route. If the cost is greater than 0, the router advertises itself as the default router to the area.

The default metric value is 0, which indicates no advertisement.

### Displaying the Default Route Metric

To display the current default route metric value, enter the following at the top-level menu:

```
ip ospf defaultRouteMetric display
```

The default route metric is displayed:

```
Default route metric = 1
```

### Defining the Default Route Metric

To define a default route metric for the router:

- 1 Enter the following at the top-level menu:

```
ip ospf defaultRouteMetric define
```

The following prompt is displayed:

```
Default route metric (1-65535) [1]:
```

- 2 Enter the default route metric value at the prompt.

### Removing a Default Route Metric

To remove a default route metric from the Layer 3 Module, enter the following at the top-level menu:

```
ip ospf defaultRouteMetric remove
```

The designated default route metric is removed immediately.

---

## Configuring OSPF Interfaces

This section describes how to configure OSPF interfaces by adding OSPF characteristics to existing IP Virtual LAN (VLAN) interfaces. You can configure the following OSPF characteristics on existing IP VLAN interfaces:

- Mode
- Priority
- Area ID
- Cost
- Transmit delay
- Hello timer
- Retransmit timer
- Dead interval
- Password



## Displaying OSPF Interface Information

To display information about the module's OSPF interface configuration, enter the following at the top-level menu:

```
ip ospf interface summary
```

or

```
ip ospf interface detail
```

The following example shows an OSPF detail display:

```
IP routing is disabled, ICMP router discovery is disabled, OSPF router id is 0.)
OSPF interface summary information

  Indx  Pri  AreaID          Xmit  Xmit  Hello  Rxmit  Dead
  1     1   0.0.0.0         Cost  Delay Intvl  Intvl  Intvl  Password
  2     1   0.0.0.0         1     1     10    5     40    --

OSPF interface detail information

  Indx  Ip Address      State   DR          BDR          Notes
  1     192.0.1.1      Disabled --          --          --
  2     192.0.4.1      Disabled --          --          --
--Enter <CR> to continue--
```

Table 20 describes the OSPF interface display field attributes:

**Table 20** Field Attributes for the OSPF Interface Displays

Field	Description
Indx	Interface entry index, corresponding to the IP interface index.
Pri	OSPF router priority for the interface.
Area ID	OSPF area that the interface belongs to.
Xmit Cost	Interface transmit cost.
Xmit Delay	Interface transmit delay.
Hello Intvl	OSPF hello packet transmit interval for the interface.
Rxmit Intvl	LSA retransmit interval.
Dead Intvl	Time interval before OSPF declares a neighbor dead.
Password	Used to secure messages between routers in an area. This allows you to prevent attacks on your network.
IP Address	The IP address of the interface on which the area is defined.

(continued)

**Table 20** Field Attributes for the OSPF Interface Displays (continued)

Field	Description
State	Interface state: <ul style="list-style-type: none"> <li>■ Disabled= OSPF is not enabled on the interface.</li> <li>■ Down= The interface is down, but OSPF is enabled on it.</li> <li>■ Loopback= The interface is a loopback interface.</li> <li>■ Waiting= The router is trying to determine the identity of the DR and BDR on the network.</li> <li>■ PTP= The interface is operational and connects to either a point-to-point network or a virtual link. The router attempts to form adjacency with the neighboring router.</li> <li>■ DRother= The interface is on a multi-access network where this router is not the DR or BDR.</li> <li>■ DR= The router is the DR on the attached network.</li> </ul>
DR	Router ID of the designated router (DR).
BDR	Router ID of the backup designated router (BDR).
Notes	When RouterID appears, the interface address is being used as the OSPF router ID.

### Displaying OSPF Interface Statistics

To display statistics associated with specific OSPF interfaces:

- 1 Enter the following at the top-level menu:

```
ip ospf interface statistics
```

The following prompt is displayed:

```
Select IP interfaces (1-2|all):
```

- 2 Select an IP interface.

The following example shows an OSPF interface statistics display:

```
Select IP interfaces (1-3|all|?): all
OSPF interface statistics
Index          receiveHello    transmitHello    receiveDD
1              0               0               0
2             36146          36199           17
3              0               36196           0

Index          transmitDD      receiveLSR       transmitLSR
1              0               0               0
2              13             6               1
3              0               0               0

Index          receiveLSAck    transmitLSAck    receiveLSU
1              0               0               0
2             411            268             272
3              0               0               0

Index          transmitLSU     computeDR        adjacencyUp
1              0               0               0
2             424            18              6
3              0               1               0
--Enter <CR> for more or "q" to quit--
```

Table 21 describes the interface statistics display attributes:

**Table 21** Field Attributes for Interface Statistics Display

Field	Description
receiveHello	Number of hello packets received
transmitHello	Number of hello packets transmitted
receiveDD	Number of database description packets received
transmitDD	Number of database description packets transmitted
receiveLSR	Number of LSA request packets received
transmitLSR	Number of LSA request packets transmitted
receiveLSAck	Number of LSA acknowledgments received
transmitLSAck	Number of LSA acknowledgments transmitted
receiveLSU	Number of link state update packets received
transmitLSU	Number of link state update packets transmitted
computeDR	Number of times the designated router was computed
adjacencyUp	Number of times OSPF adjacencies have been formed
adjacencyDown	Number of times OSPF adjacencies have gone down
transmitError	Number of general transmit errors
receiveError	Number of general receive errors

(continued)

**Table 21** Field Attributes for Interface Statistics Display (continued)

Field	Description
mismatchHello	Number of hello packet interval mismatches detected
mismatchDead	Number of router dead interval mismatches detected
mismatchMask	Number of subnet mask mismatches detected
mismatchAreaID	Number of interface area ID mismatches detected
mismatchAreaType	Number of interface area type mismatches detected
receivedUnknown	Number of unknown LSAs received
authError	Number of authentication errors
packetXsum	Number of packet checksum errors since interface has come up
lsaXsumError	Number of LSA checksum errors detected

### Setting the Mode

You can set the OSPF mode for each interface. The mode can be enabled or disabled. You must set the mode to enabled to run OSPF routing.

The default mode is disabled.

To set the mode for the interface:

- 1 Enter the following at the top-level menu:

```
ip ospf interface mode
```

The following prompt is displayed:

```
Select IP interfaces (1-3|all) [1]:
```

- 2 Select the index number(s) representing the interface(s).

```
Enter OSPF mode {disabled,enabled} [enabled]:
```

- 3 Enable or disable the OSPF mode for each interface as required.

### Setting the Priority

The interface priority is a value that you assign to an OSPF router to determine its status as a designated router. A router can function in one of three ways:

- **Designated router (DR)** — The router with the highest priority value is always the designated router, unless a designated router already exists on the subnetwork.
- **Backup designated router (BDR)** — A router with a lower priority value.
- **Not a designated router** — A router with a priority value of 0.

The default priority value is 1.

To set the interface priority:

- 1 Enter the following at the top-level menu:

```
ip ospf interface priority
```

The following prompt is displayed:

```
Select IP interfaces (1-2|all):
```

- 2 Enter an IP interface.

```
Enter priority (0-255) [1]:
```

- 3 Enter the priority value.

### Setting the Area ID

The interface area ID associates the interface you specify with an OSPF area. See “Defining an Area” on page 85 for more information about OSPF areas.



*Because all routers on the network segment are in the same area, set the area ID to the same value for each router.*

To set the area ID:

- 1 Enter the following at the top-level menu:

```
ip ospf interface areaID
```

The following prompt is displayed:

```
Select IP interfaces (1-3|all) [1-3]:
```

- 2 Select the interface index number(s).

```
Enter Area ID [0.0.0.3]:
```

- 3 Enter the area ID in the form of an IP address.

### Setting the Cost

The interface cost reflects the line speed of the port. To set the cost:

- 1 Enter the following at the top-level menu:

```
ip ospf interface cost
```

The following prompt is displayed:

```
Select IP interfaces (1-2|all):
```

- 2 Enter an IP interface number.

```
Enter cost (1-65535) [1]:
```

- 3 Enter the cost value for the interface. The default is calculated by the Layer 3 Module.

### Setting the Delay

This command sets the OSPF interface transmit delay. The Layer 3 Module adds the value of the transmit delay to all link state advertisements (LSAs) that it sends out to the network. Set the transmit delay according to the link speed: use a longer transmit delay time for slower link speeds.

The default delay is 1 second.

To set the transmit delay:

- 1 Enter the following at the top-level menu:

```
ip ospf interface delay
```

The following prompt is displayed:

```
Select IP interfaces (1-2|all):
```

- 2 Enter an IP interface number.

```
Enter transmit delay (1-65535) [1]:
```

- 3 Enter the interface transmit delay value.

### Setting the Hello Timer

The interface hello timer determines how often the interface transmits hello packets to neighbor routers on the network. Hello packets tell other routers that the sending router is still active on the network. If a router does not send hello packets for a period of time specified by the dead interval, the router is considered inactive by its neighbors and routes from the inactive router are marked as eligible for deletion. See “Setting the Dead Interval” on page 95 for more information.

The default value for the hello timer is 10 seconds.



*Set the hello timer to the same value for all routers on the network segment, because they are in the same area.*

To set the hello timer:

- 1 Enter the following at the top-level menu:

```
ip ospf interface hello
```

The following prompt is displayed:

```
Select IP interfaces (1-2|all):
```

- 2 Enter an IP interface.

```
Enter Hello packet interval (1-65535) [10]:
```

- 3 Enter the hello timer value, in seconds.

### Setting the Retransmit Timer

You can specify the OSPF link state advertisement (LSA) retransmit interval for each interface.

The default value for the retransmit timer is 5 seconds.

To set the retransmit interval:

- 1 Enter the following at the top-level menu:

```
ip ospf interface retransmit
```

The following prompt is displayed:

```
Select IP interfaces (1-2|all):
```

- 2 Enter an IP interface.

```
Enter LSA retransmit time (1-65535) [5]:
```

- 3 Enter the LSA retransmit time, in seconds.

### Setting the Dead Interval

The value of the dead interval determines how long neighbor routers wait for a hello packet before they determine that the transmitting router is inactive. Each time a router receives a hello packet from a neighbor, the router resets the dead interval timer for that neighbor. See “Setting the Hello Timer” on page 94 for more information.



*Use the same dead interval value for all routers in the same area.*

The default value for the dead interval is 40 seconds.

To set the dead interval:

- 1 Enter the following at the top-level menu:

```
ip ospf interface dead
```

The following prompt is displayed:

```
Select IP interfaces (1-2|all):
```

- 2 Enter an IP interface number.  
`Enter dead interval (1-65535) [40]:`
- 3 Enter the value of the dead interval, in seconds.

**Setting the Password** This command allows you to set a security password for a specific OSPF interface.



*Use the same password for all interfaces in the same area.*

By default, no password is assigned.

To set the password:

- 1 Enter the following at the top-level menu:

```
ip ospf interface password
```

The following prompt is displayed:

```
Select IP interfaces (1-2|all):
```

- 2 Enter an IP interface number.  
`Enter interface password [none]:`
- 3 Enter the password. You can use up to eight ASCII characters.



*Use the password **none** to remove a previously assigned password.*

---

## Displaying the Link State Database

The link state database contains information about different link state advertisements (LSAs).

The link state database represents changes to the topology of the network based on information from every router within the areas. If the areas are large, the link state database may change frequently due to geographical events.

When a router is powered up on a network, it takes a short time to learn about other routes in its area. *Router convergence* occurs when the routers in an area agree on the best path to a destination. In very large networks, router convergence may occur infrequently and for short periods only, due to network changes. You can check for router convergence by displaying the link state database.





An asterisk (\*) after the router ID in a display indicates that the LSA originated locally.

**Displaying a Database Summary**

This display summarizes all LSAs in the link state database. To display the database summary:

- 1 Enter the following at the top-level menu:

```
ip ospf linkStateData databaseSummary
```

The following prompt is displayed:

```
Enter Area ID [0.0.0.0]:
```

- 2 Enter the area ID.

```
Enter Area mask [0.0.0.0]:
```

- 3 Enter the area subnet mask.

The following example shows a link state database summary display:

OSPF link state database summary						
Area ID	Checksum Summation	LSA Count	Router LSAs	Network LSAs	Summary LSAs	External LSAs
--	00015DAC	2	--	--	--	2

Table 22 describes the link state database summary display fields:

**Table 22** Field Attributes for Link State Database Summary Display

Field	Description
Checksum Summation	Total of all LSA checksums
LSA Count	Number of LSAs
Router LSAs	Number of router link LSAs
Network LSAs	Number of network link LSAs
Summary LSAs	Number of summary link LSAs
External LSAs	Number of external link LSAs

**Displaying Router LSAs**

This display shows the router LSAs in the link state database. Router LSAs describe the collected states of the router’s interfaces.

To display the router LSAs:

- 1 Enter the following at the top-level menu:

```
ip ospf linkStateData router
```

The following prompt is displayed:

```
Enter Area ID [0.0.0.0]:
```

- 2 Enter the area ID.

```
Enter Area mask [0.0.0.0]:
```

- 3 Enter the area subnet mask.

```
Enter LSID [0.0.0.0]:
```

- 4 Enter the LSID.

```
Enter LSID mask [0.0.0.0]:
```

- 5 Enter the LSID mask.

Table 23 describes the fields in the link state database router display:

**Table 23** Field Attributes for Link State Database Router Display

Field	Description
LSID	ID of the router originating the LSI
Router ID	Remote router ID
LS Seq	Sequence number of the LSA (used to detect older duplicate LSAs)
LS Age	Time in seconds since LSA was originated
Flags	<ul style="list-style-type: none"> <li>■ V= Router is the endpoint of an active virtual link that is using the area as a transmit area</li> <li>■ ASBR= Router is an autonomous system boundary router</li> <li>■ ABR= Router is an area border router</li> </ul>
Link Type	<ul style="list-style-type: none"> <li>■ PTP= Connection is point-to-point to another router</li> <li>■ Transit= Connection is to a transit network (one with more than one OSPF router on it)</li> <li>■ Stub= Connection is to a stub network</li> <li>■ Virtual link= Connection is to a far-end router that is the endpoint of a virtual link</li> </ul>
Link ID	<ul style="list-style-type: none"> <li>■ PTP= Router ID for the neighboring router</li> <li>■ Transit= Address of designated router</li> <li>■ Stub= IP network/subnetwork number</li> <li>■ Virtual link= Router ID for the neighboring router</li> </ul>

(continued)

**Table 23** Field Attributes for Link State Database Router Display (continued)

Field	Description
Link Data	<ul style="list-style-type: none"> <li>■ PTP= MIB II index value for an unnumbered point-to-point interface</li> <li>■ Transit= IP interface address of designated router</li> <li>■ Stub= Network IP address mask</li> <li>■ Virtual link= IP interface address of neighboring router</li> </ul>
Metric	Cost of the link

**Displaying Network LSAs**

This display shows the network LSAs in the link state database. Network LSAs describe the set of routers attached to the network.

To display the network LSAs:

- 1 Enter the following at the top-level menu:

```
ip ospf linkStateData network
```

The following prompt is displayed:

```
Enter Area ID [0.0.0.0]:
```

- 2 Enter the ID of the OSPF area.

```
Enter Area mask [0.0.0.0]:
```

- 3 Enter the area mask.

```
Enter LSID [0.0.0.0]:
```

- 4 Enter the LSID.

```
Enter LSID mask [0.0.0.0]:
```

- 5 Enter the LSID mask.

Table 24 describes the fields in the link state database network display:

**Table 24** Field Attributes for Link State Database Network Display

Field	Description
LSID	Interface address of designated router.
Router ID	Originating router ID.
LS Seq	Sequence number of the LSA (used to detect older duplicate LSAs).
LS Age	Time in seconds since LSA was originated.

(continued)

**Table 24** Field Attributes for Link State Database Network Display

Field	Description
Network Mask	IP address mask for the network.
Attached Routers	List of routers that are fully adjacent to the designated router (DR). The ID of the DR is also listed here.

### Displaying Summary Network LSAs

This display summarizes all network LSAs in the link state database. Summary LSAs describe inter-area routes, and enable the condensing of routing information at area borders. Originating from area border routers, Type 3 summary-LSAs describe routes to networks while Type 4 summary-LSAs describe routes to AS (autonomous system) boundary routers.

To display a network LSA summary:

- 1 Enter the following at the top-level menu:

```
ip ospf linkStateData summary
```

The following prompt is displayed:

```
Enter Area ID [0.0.0.0]:
```

- 2 Enter the ID of the OSPF area.

```
Enter Area mask [0.0.0.0]:
```

- 3 Enter the area mask.

```
Enter LSID [0.0.0.0]:
```

- 4 Enter the LSID.

```
Enter LSID mask [0.0.0.0]:
```

- 5 Enter the LSID mask.

Table 25 describes the fields in the link state database network summary display:

**Table 25** Field Attributes for Link State Database Network Summary Display

Field	Description
LSID	<ul style="list-style-type: none"> <li>■ Type 3= IP network number</li> <li>■ Type 4= ASBR's OSPF router ID</li> </ul>
Router ID	Originating router ID

(continued)

**Table 25** Field Attributes for Link State Database Network Summary Display

Field	Description
LS Seq	Sequence number of the LSA (used to detect older duplicate LSAs)
LS Age	Time in seconds since LSA was originated
Network Mask	<ul style="list-style-type: none"> <li>■ Type 3= destination network's IP address mask</li> <li>■ Type 4= this type is not used, must be 0</li> </ul>
Metric	Cost to reach the network

### Displaying External Network LSAs

This display shows the external network LSAs in the link state database. Originating from AS boundary routers, they describe routes to destinations external to the Autonomous System.

To display external network LSAs:

- 1 Enter the following at the top-level menu:

```
ip ospf linkStateData external
```

The following prompt is displayed:

```
Enter LSID [0.0.0.0]:
```

- 1 Enter the LSID.

```
Enter LSID mask [0.0.0.0]:
```

- 2 Enter the LSID mask.

Table 26 describes the fields in the link state database external display:

**Table 26** Field Attributes for the Link State Database External Display

Field	Description
LSID	IP network number.
Router ID	Originating router ID.
LS Seq	Sequence number of the LSA (used to detect older duplicate LSAs).
LS Age	Time in seconds since LSA was originated.
Network Mask	IP address mask for the advertised destination.
Fwd Address	Forwarding address for data traffic to the advertised destination.
Metric	Cost to reach advertised destination.

(continued)

**Table 26** Field Attributes for the Link State Database External Display

Field	Description
Type	<ul style="list-style-type: none"> <li>■ Type 1= normal link state metric</li> <li>■ Type 2= metric is larger than any local link state path</li> </ul>
RouteTag	Not used by OSPF, these 32 bits may be used to communicate other information between boundary routers. Tag contents generally defined by application systems.

## Administering Neighbors

Neighbor routers are physically attached to the same network segment and exchange OSPF routing tables.

### Displaying Neighbors

To display information about the currently defined neighbors in an OSPF area, enter the following at the top-level menu:

```
ip ospf neighbors display
```

The following example shows an OSPF neighbors display:

OSPF neighbor information								
Indx	Neighbor Addr	Router ID	State	Pri	RxQ	SumQ	ReqQ	Flags
1	10.0.0.2	0.0.0.0	Down	0	0	0	0	S
1	10.0.0.3	0.0.0.0	Down	0	0	0	0	S
2	11.0.0.2	0.0.0.0	Down	0	0	0	0	S

Table 27 describes the fields in the neighbors display:

**Table 27** Field Attributes for Neighbors Display

Field	Description
Indx	Interface index that a neighbor belongs to.
Neighbor Addr	Interface address of neighbor.
Router ID	Neighbor's OSPF router ID.

(continued)

**Table 27** Field Attributes for Neighbors Display (continued)

Field	Description
State	Neighbor's adjacency: <ul style="list-style-type: none"> <li>■ <code>Down</code>= No recent data received from neighbor, connection is down</li> <li>■ <code>Attempt</code>= Only used on non-broadcast networks. No recent data received from neighbor (will attempt to contact)</li> <li>■ <code>Init</code>= Have recently seen hello packet from neighbor, however two-way communication has not been established</li> <li>■ <code>Two-way</code>= Bidirectional communication has been established</li> <li>■ <code>ExStart</code>= Taking initial step to create adjacency between neighboring routers</li> <li>■ <code>Exchange</code>= Database descriptions are being exchanged</li> <li>■ <code>Loading</code>= LSA databases are being exchanged</li> <li>■ <code>Full</code>= Neighboring routers are fully adjacent</li> </ul>
Pri	Neighbor's OSPF router priority.
RxQ	Number of LSAs in local retransmit queue to the neighbor.
SumQ	Number of LSAs in LSA summary queue for the neighbor.
ReqQ	Number of LSAs being requested from neighbor.
Flags	Neighbor identification flags: <ul style="list-style-type: none"> <li>■ <code>D</code>= dynamic neighbor</li> <li>■ <code>S</code>= static neighbor</li> <li>■ <code>BDR</code>= backup designated router</li> <li>■ <code>DR</code>= designated router</li> </ul> <p>Example: <code>[S, BDR] + [D, DR]</code> is a static neighboring backup designated router and a dynamic neighboring designated router.</p>

**Adding a Neighbor** You can add a neighbor static IP address to an existing interface. This may speed up the process of router convergence.

To add a neighbor:

- 1 Enter the following at the top-level menu:

```
ip ospf neighbors add
```

The following prompt is displayed:

```
Select IP interface {1-4} [3]:
```

- 2 Enter the interface to which to add the OSPF neighbor.

```
Enter static neighbor address:
```

- 3 Enter the static IP address of the neighbor.

**Removing a Neighbor** To remove a static neighbor address from an existing interface:

- 1 Enter the following at the top-level menu:

```
ip ospf neighbors remove
```

The following prompt is displayed:

```
Select IP interface {1-4} [3]:
```

- 2 Enter the IP interface.

```
Enter static neighbor address:
```

- 3 Enter the IP address of the neighbor to remove.

The module removes the neighbor from that IP interface.

---

## Setting the OSPF Router ID

The OSPF router ID identifies the router to other routers within an autonomous system. Three types of router identifiers are available, and all three take the form of an IP address, but are not necessarily an actual IP address:

- **Default** — A unique ID that the module generates and uses as the default router ID
- **Interface** — The index of an IP interface on the router
- **Address** — An ID that you define in the form of an IP address





*The router ID must be unique for every router for OSPF to operate correctly. To make sure that the router ID is unique, choose the default setting. The default setting uses the Layer 3 Module ID, which is unique to each Layer 3 Module.*

OSPF routing must be inactive before you can add or modify an OSPF router ID.

To make OSPF routing inactive by setting the OSPF mode to disabled, see “Setting the Mode” on page 92. After you add the router ID, you can set the OSPF mode to enabled on the interface.

To set the router ID:

- 1 Enter the following at the top-level menu:

```
ip ospf routerID
```

The module displays the current router ID and the router ID type.

```
Current OSPF router id = 172.16.142.1 (interface)
```

```
Enter router ID type {default,interface,address}[default]:
```

- 2 Enter the required router ID type.
- 3 Do one of the following:
  - a If you selected the default router ID, you do not need to enter any further information
  - b If you selected the interface router ID, enter the interface number of the interface you want to use.
  - c If you selected the address router ID, enter the address for the router ID.

---

## Administering Memory Partitions

You can display information about how much memory the OSPF protocol can use for its data processing and storage. You typically do not have to change OSPF memory allocation; however, you can do so if necessary.

### Displaying Memory Partitions

To display the current OSPF memory allocation, enter the following at the top-level menu:

```
ip ospf partition display
```

The following example shows an OSPF memory partition summary display:

```
Current partition maximum size = 500000 (bytes).
Configured partition maximum size = 500000 (bytes).
Allocated partition size = 100000 (bytes).
```

This display shows three partition parameters:

- **Current partition maximum size** (500000 in this example) — The OSPF memory limit implemented at the last system reboot.
- **Configured partition maximum size** (500000 in this example) — The last value that you entered, which becomes the current partition maximum size at system reboot.
- **Allocated partition size** (100000 in this example) — The module's current working memory. OSPF dynamically allocates memory in 100,000-byte chunks up to the current partition maximum size.

## Modifying Memory Partitions

This command changes the OSPF memory allocation. This change takes effect at system reboot.



*In normal circumstances, you are unlikely to have to modify the OSPF memory allocation.*

To modify a memory partition:

- 1 Enter the following at the top-level menu:

```
ip ospf partition modify
```

The following prompt is displayed:

```
Maximum partition size is 8443220 bytes
Enter new partition maximum size (in bytes) [500000]:
```

- 2 Enter the new partition size (in bytes).

```
New partition size will take effect after reboot.
```



*The maximum partition size (8443220 in this example) shows how much total memory is available to define as the OSPF maximum partition.*

---

## Administering the Stub Default Metric

The stub default metric value determines if the router will generate the default route into the stub areas of the network. This value applies to area border routers (ABRs) that have attached stub areas.

### Displaying the Stub Default Metric

To display the current stub default metric value, enter the following at the top-level menu:

```
ip ospf stubDefaultMetric display
```

A message similar to the following appears:

```
Stub default metric = 20
```

### Defining a Stub Default Metric

You can set the stub default metric value on an area border router with an attached stub area.

The default value is 1.

To define a default stub metric:

- 1 Enter the following at the top-level menu:

```
ip ospf stubDefaultMetric define
```

The following prompt is displayed:

```
Enter stub default metric (1-65535) [1]:
```

- 2 Enter the stub default metric value.

### Removing a Stub Default Metric

To disable the stub default metric value on the router, enter the following at the top-level menu:

```
ip ospf stubDefaultMetric remove
```

The module removes the stub default metric immediately.

---

## Administering Virtual Links

Virtual Links provide connections to areas in the autonomous system that are not directly connected to the backbone. You can define, remove, modify, and display the virtual links on your module.

You must establish a virtual link in the following situations:

- When an area border router (ABR) has an interface that is not in the backbone area (an area ID of 0.0.0.0)

- When an ABR is connected to the backbone and provides access to the other ABRs that do not have access to the network

When you define a virtual link, you specify the Transit Area ID and the Target Router ID. The module also allocates default values for the following characteristics associated with a virtual link. Table 28 lists these characteristics and their default values.

**Table 28** Virtual Link Characteristics

Characteristic	Default Value
areaID	
delay timer	1 second
hello timer	10 seconds
Rxmit Intvl	50 seconds
dead interval	40 seconds
password	no password

You can change the default values of these characteristics with the commands in this section.

### Displaying Virtual Links

To display information about the virtual links associated with the interface you specify:

- 1 Enter one of the following commands at the top-level menu:
  - `ip ospf virtualLinks summary`
  - `ip ospf virtualLinks detail`

The following prompt is displayed:

```
Select virtual link (1-32|?) [1]:
```

- 2 Select the virtual link.

The following example shows a summary display:

```
IP routing is disabled, ICMP router discovery is disabled, OSPF router id is 0.)
OSPF virtual link summary information

  Indx  Transit      Target      Xmit  Hello  Rxmit  Dead  Password
      Area      Router      Delay Intvl Intvl Intvl
  1     0.0.0.5    192.168.168.168  1    10    50    40    --
--Enter <CR> to continue--
```

The following example shows a detailed display:

```

IP routing is disabled, ICMP router discovery is disabled, OSPF router id is 0.)
OSPF virtual link summary information

  Indx  Transit      Target          Xmit  Hello  Rxmit  Dead
   Area                Router          Delay Intvl  Intvl  Intvl  Password
  1    0.0.0.5        192.168.168.168  1    10    50    40    --

OSPF virtual link detail information

  Indx  State      Local Address  Remote Address  Cost
  1    Down      --            --              Unreachable

OSPF virtual link neighbor information

  Indx  State  RxQ  SumQ  ReqQ
  1    Down   0    0    0
--Enter <CR> to continue--

```

Table 29 describes the virtual links display fields:

**Table 29** Field Attributes for Virtual Links Display

Field	Description
Indx	Index of the local interface that the virtual link is connected to
Interface Address	Local interface address
Router ID	Remote router's OSPF router ID
Rxmit Intvl	LSA retransmit interval for the virtual link
Router Address	Remote router's interface address (changes dynamically)
Link State	Virtual link state
Link Cost	Cost of virtual link (computed dynamically)

### Displaying Virtual Link Statistics

To display statistics associated with virtual links:

- 1 Enter one of the following commands at the top-level menu:

```
ip ospf virtualLinks statistics
```

The following prompt is displayed:

```
Select virtual link (1-32|?) [1]:
```

- 2 Select the virtual link.

The following example shows a virtual link statistics display:

OSPF virtual link statistics		
receiveHello	transmitHello	receiveDD
0	0	0
transmitDD	receiveLSR	transmitLSR
0	0	0
receiveLSAck	transmitLSAck	receiveLSU
0	0	0
transmitLSU	computeDR	adjacencyUp
0	0	0
adjacencyDown	transmitError	receiveError
0	0	0
mismatchHello	mismatchDead	mismatchMask
0	0	0
mismatchAreaId	mismatchAreaType	receivedUnknown

### Defining a Virtual Link

You must configure a virtual link for each area border router that has an interface outside the backbone area.



*You can define up to 32 virtual links per Layer 3 Module.*

To define a virtual link:

- 1 Enter the following at the top-level menu:

```
ip ospf virtualLinks define
```

The following prompt is displayed:

```
Enter transit area:
```

- 2 Enter the transit area in the form of an IP address. This is the area that the virtual link is going through.

```
Enter target router:
```

- 3 Enter the router ID of the target router. This is the OSPF border router where the virtual link will terminate.

### Removing a Virtual Link

To remove a virtual link that you have added previously:

- 1 Enter the following at the top-level menu:

```
ip ospf virtualLinks remove
```

The following prompt is displayed:

```
Select virtual link (1-2|all):
```

- 2 Specify the virtual link(s) you want to remove.

**Modifying an AreaID** To modify the area ID of the transit area associated with the virtual link:

- 1 Enter the following at the top-level menu:

```
ip ospf virtualLinks areaID
```

The following prompt is displayed:

```
Select virtual link (1-2|all):
```

- 2 Specify the virtual link required.

```
Enter target area [0.0.0.1]:
```

- 3 Specify the new area ID.

**Modifying the Target Router** To modify the target router associated with the virtual link:

- 1 Enter the following at the top-level menu:

```
ip ospf virtualLinks router
```

The following prompt is displayed:

```
Select virtual link (1-2|all):
```

- 2 Specify the virtual link required.

```
Enter target router [16.6.6.6]:
```

- 3 Enter the IP address of the new target router.

**Modifying the Transmit Delay** You can set the virtual link transmit delay.

The default value for the transmit delay is 1 second.

To modify the transmit delay:

- 1 Enter the following at the top-level menu:

```
ip ospf virtualLinks delay
```

The following prompt is displayed:

```
Select virtual link (1-2|all):
```

- 2 Enter the virtual link ID.  
`Enter transmit delay (1-65535) [1]:`
- 3 Enter the value of the transmit delay.

### Setting the Hello Timer

The hello timer determines how often the virtual link transmits hello packets to neighbor routers on the network. Hello packets tell other routers that the sending router is active on the network. If a router does not send hello packets for a period of time specified by the dead interval, the router is considered inactive.

The default value for the hello interval is 10 seconds.

To set the hello timer:

- 1 Enter the following at the top-level menu:  
`ip ospf virtualLinks hello`
- 2 The following prompt is displayed:  
`Select virtual link (1-2|all):`
- 3 Enter the virtual link ID.  
`Enter Hello packet interval (1-65535) [10]:`
- 4 Enter the hello timer value, in seconds.

### Setting the Retransmit Interval

You can set the virtual link retransmit interval, in seconds.

The default value for the retransmit interval is 50 seconds.

To set the retransmit interval:

- 1 Enter the following at the top-level menu:  
`ip ospf virtualLinks retransmit`  
The following prompt is displayed:  
`Select virtual link (1-2|all):`
- 2 Enter the virtual link ID.  
`Enter LSA retransmit time (1-65535) [50]:`
- 3 Enter the retransmit interval.



### Modify the Dead Interval

You can modify the virtual link dead interval.

The default dead interval is 40 seconds.

To modify the dead interval:

- 1 Enter the following at the top-level menu:

```
ip ospf virtualLinks dead
```

The following prompt is displayed:

```
Select virtual link (1-2|all):
```

- 2 Enter the virtual link ID.

```
Enter dead interval (1-65535) [40]:
```

- 3 Enter the value of the dead interval, in seconds.

### Setting the Password

You can set the virtual link password, which allows you to ensure that only routers with the correct password can use a virtual link.

To set the password:

- 1 Enter the following at the top-level menu:

```
ip ospf virtualLinks password
```

The following prompt is displayed:

```
Select virtual link (1-2|all):
```

- 2 Enter the virtual link ID.

```
Enter virtual link password [none]:
```

- 3 Enter the password.

---

### Displaying OSPF General Statistics

To display general OSPF statistics, enter the following at the top-level menu:

```
ip ospf statistics
```

The following example shows an OSPF statistics display:

OSPF general statistics		
SPFComputations	memoryFailures	LSAsTransmitted
1	0	2
LSAsReceived	routeUpdateErrors	recvErrors
0	0	15477
extLsaChanges	softRestarts	
2	0	

Table 30 describes OSPF statistics display fields:

**Table 30** Field Attributes for OSPF Statistics Display

Field	Description
SPFComputations	Number of shortest-path-first computations done
memoryFailures	Number of nonfatal memory-allocation failures
LSAsTransmitted	Number of link state advertisements transmitted
extLsaChanges	Number of external LSA changes made to database
softRestarts	Number of OSPF router soft restarts due to insufficient memory resources (implies that a fatal memory-allocation failure has happened).



*To resolve insufficient memory resource problems, indicated by memory failure or software restart errors, change the OSPF memory partition, or reconfigure the network topology to generate smaller OSPF databases.*

## Administering RIP

The Routing Information Protocol (RIP) is one of the IP Interior Gateway Protocols (IGPs). The Layer 3 Module uses RIP to dynamically configure its routing tables.

RIP operates in terms of active and passive devices. The *active devices*, usually routers, broadcast their RIP messages to all devices in a network or subnetwork; they update their own routing tables when they receive a RIP message from another device. The *passive devices*, usually hosts, listen for RIP messages and update their routing tables; they do not send RIP messages.



*Only RIP version 1.0 is supported.*

An active router sends a RIP message every 30 seconds. This message contains both the IP address and a metric (the distance to the destination from that router) for each destination. In RIP, each router that a packet must travel through to reach a destination equals one *hop*.

## Displaying RIP Interface Information

To display information about RIP interfaces on the module, enter the following at the top-level menu:

```
ip rip display
```

The following example shows a RIP interface display:

```
IP routing is enabled, ICMP router discovery is disabled
RIP interface information:
```

Index	Mode	Cost	PoisonReverse	AdvertisementAddress
1	learn	1	enabled	10.255.255.255
2	learn	1	enabled	11.255.255.255

## Setting the RIP Mode

You can select one of the following RIP modes on an interface:

- **Disabled** — The module ignores all incoming RIP packets and does not generate any RIP packets of its own.
- **Enabled** — The module processes all incoming RIP packets, responds to explicit requests for routing information, and broadcasts periodic and triggered RIP updates.
- **Learn** — The module processes all incoming RIP packets and responds to explicit request for routing information, but it does *not* broadcast periodic or triggered RIP updates.
- **Advertise** — The module processes all incoming RIP packets and advertises RIP routes to other routers but does not learn RIP routes from other modules.

The default RIP mode is passive.

To set the RIP mode:

- 1 Enter the following at the top-level menu:

```
ip rip mode
```

The following prompt is displayed:

```
Select IP interfaces (1-4|all) [1]:
```

- 2 Select the interface you require.

```
Interface 2 - Enter RIP mode
(disabled,learn,advertise,enabled) [enabled]:
```

- 3 Enter the RIP mode as required.

### Enabling and Disabling Poisoned Reverse

When the Poisoned Reverse mode is enabled, RIP does the following:

- Advertises route updates it receives back through the receiving interfaces
- Sets the route metric to 16 (meaning “route not reachable”)

By disabling the Poisoned Reverse mode, you can stop RIP from advertising routes back through the originating ports.

Poisoned Reverse mode is enabled by default.

To enable Poisoned Reverse mode:

- 1 Enter the following at the top-level menu:

```
ip rip poisonReverse
```

The following prompt is displayed:

```
Select IP interfaces (1-4|all) [4]:
```

- 2 Select the interface you require.

```
Interface 2 - Enter RIP poison reverse mode
(disabled,enabled) [enabled]:
```

- 3 Enable or disable the Poisoned Reverse mode as required.

### Adding an Advertisement Address

You can add an advertisement address to an IP RIP interface. This defines the IP addresses of specific hosts or routers to receive RIP updates. An advertisement address is usually the IP broadcast address for a network, for example, 10.255.255.255, but in certain environments, it may be useful to restrict advertisements to the IP address of the router.

To add an advertisement address:

- 1 Enter the following at the top-level menu:

```
ip rip addAdvertisement
```

The following prompt is displayed:

```
Select IP interface {1-4|?} [1]:
```

- 2 Enter the IP interface index number, or specify ? to get a list of the selectable IP interface indexes.

Interface 1 - Enter advertisement address:

- 3 Enter an advertisement address. You can specify up to 64 advertisement addresses in separate iterations.

### Removing an Advertisement Address

To remove an advertisement address from the advertisement address list that is associated with the interface:

- 1 Enter the following at the top-level menu:

```
ip rip removeAdvertisement
```

The following prompt is displayed:

```
Select IP interface {1-4} [2]:
```

- 2 Select the interface from the available interfaces, or specify ? to get a list of the selectable interfaces.

Interface 2 - Enter advertisement address:

- 3 Enter the index interface number and the advertisement address that you want to remove, or specify ? to get a list of the selec

### Displaying RIP Statistics

To display RIP statistics, enter the following at the top-level menu:

```
ip rip statistics
```

The following example shows a RIP statistics display:

```
RIP general statistics
      routeChanges      queries
              0              0
```

- 4 IP interface indexes.

### Displaying RIP Statistics

To display RIP statistics, enter the following at the top-level menu:

```
ip rip statistics
```

The following example shows a RIP statistics display:

```
RIP general statistics
      routeChanges      queries
              0              0
```

**Setting the Cost** You can set the RIP cost option.

The default cost value is 1, which is appropriate for most networks.

To set the RIP cost:

- 1 Enter the following at the top-level menu:

```
ip rip cost
```

The following prompt is displayed:

```
Select IP interfaces (1-4|all) [2]:
```

- 2 Select the interface from the available interfaces, or specify ? to get a list of the selectable interfaces.

```
Interface 2 - Enter RIP cost (1-15) [1]:
```

- 3 Enter the cost value for the specified interfaces.

---

## Using ping

The ping feature is a useful tool for network testing, performance measurement and management. The ping command sends ICMP echo request packets, using the ICMP echo facility, to the IP destination you specify. See “Enabling and Disabling ICMP Router Discovery” on page 83 for more information about ICMP.

When a router sends an echo request packet to an IP station using ping, the router waits for an ICMP echo reply packet. The response from the remote IP station indicates whether it is available, unreachable, or not responding.

There are two ping commands available and several options you can set up for the advanced command.

- **ping** — Uses the hostname or IP address to contact a host using the default settings
- **advancedPing** — Uses the hostname or IP address to contact a host using the advanced ping options that you specify

You can enter either the host name or the IP address of the destination you want to ping. If you specify a hostname, the hostname and its associated IP address must be configured on a network name server. You must also add the IP address on the name server to the list of name server addresses associated with the network domain name. See “Administering the Domain Name Server Client” on page 72 for information about this task.

The following are possible responses to a ping:

- If the host is reachable, the Layer 3 Module displays information about the ICMP reply packets and the response time to the ping. The amount of information depends on whether the quiet option is enabled or disabled.
- If the host does not respond, the Layer 3 Module displays the ICMP packet information and the message, `Host is Not Responding`.
- If the packets cannot reach the host, the Layer 3 Module displays the ICMP packet information and the message, `Host is Unreachable`. A host is unreachable when there is no route to that host.

### Using the ping Command

Use the `ping` command to ping a destination using the default ping options (see Table 31 on page 120). To change the default ping options, use the `advancedPing` command and press [Enter] until you see the prompt for the option you want to change.

To ping a host with the default ping options:

- 1 Enter the following at the top-level menu:  
`ip ping`
- 2 At the prompt, specify the destination hostname or IP address.

The following example shows a successful ping with the default options:

```
Select menu option (ip): ping
Enter host name/IP address [0.0.0.0]: 10.204.20.75
Press "Enter" key to interrupt.

PING 10.204.20.75: 64 byte packets
64 bytes from 10.204.20.75: icmp_seq=0. time=16. ms
64 bytes from 10.204.20.75: icmp_seq=1. time=19. ms
64 bytes from 10.204.20.75: icmp_seq=2. time=24. ms

---- 10.204.20.75 PING Statistics ----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms) min/avg/max = 16/20/24
```

Table 31 lists the default values for a ping command.

**Table 31** Default Values for Ping Options

Option	Default Value
count	3 packets
wait	1 second
packetSize	64 bytes
quiet	disabled
burst	disabled
sourceAddress	determined by the router

### Using the advancedPing command

Use the `ip advancedPing` command to ping a host with one or more of the advanced ping options.

Table 32 describes the advanced ping options.

**Table 32** Advanced Ping Options

Option	Description
count	The number of ICMP echo request packets that the system sends to ping a host. If the destination host does not respond after it is pinged by the number of packets that you specify, the system displays a <code>Host is Unreachable</code> or a <code>Host is not Responding</code> message.
wait	The number of seconds that the system waits before it sends out successive ICMP echo request packets. You may want to set this option to a high value if network traffic is heavy and you choose not to add to the network traffic with pings in fast succession.
packetSize	The number of bytes in each ICMP echo request packet. The packet size includes both the IP and the ICMP headers.
quiet	Determines how much packet information the system displays after a ping.  When the quiet option is enabled, the system displays summary information about the number of packets that the system sent and received, any loss of packets, and the average time that it took a packet to travel to and from the host.  When the quiet option is disabled, the system displays more detailed status information about each ICMP echo request packet. If the burst option is enabled, it overrides the value that is set with the quiet option.

(continued)



**Table 32** Advanced Ping Options (continued)

Option	Description
burst	<p>When this option is enabled, the system sends out the ICMP echo request packets as rapidly as possible.</p> <p>When this option is enabled, it overrides the values set for the quiet option and for the wait option.</p> <p>The Layer 3 Module displays a period (.) on the screen each time that it receives an ICMP echo relay packet. Use this display to determine how many packets are being dropped during the burst. This output is unique to the burst option and overrides the value set in the quiet option.</p>
sourceAddress	<p>Use this option to force the source address of the ICMP packets to be something other than the IP address of the interface from which the packet originated. You can use this option if you have more than one IP interface defined on the system.</p> <p>When you enter this command, the system displays a list of the currently defined interfaces and their index numbers. Select the number of the interface that you want to use.</p>



**CAUTION:** *The burst option floods the network with ICMP echo packets, and can cause network congestion. It may also affect your ability to manage the Layer 3 Module. Consequently, avoid using the burst option during periods of heavy network traffic.*

To ping a host using the advanced options:

- 1 Enter the following at the top-level menu:

```
ip advancedPing
```

- 2 At the prompt, enter the host name or the IP address of the destination host.

At the following prompts, enter the appropriate settings. Press [Enter] to use the default value for an option and move onto the next option.

See Table 31 on page 120 for the default values and Table 32 on page 120 for the range of valid values for an option.

- 3 Enter the number of ICMP request packets to send during a ping.
- 4 Enter the packet size, in bytes.
- 5 Enter the burst mode.
- 6 Enter the quiet mode.
- 7 Enter the wait value, in seconds.

- 8 If you have more than one interface defined, you can select a particular ICMP source IP address (**n** or **y**). The default is **y**.
- 9 Enter the index number of the ICMP source IP address that you want to use or enter **?** to list the index values.

You can press [Enter] at any time to interrupt the ping.

The following example shows a successful advanced ping:

```
Select menu option (ip): advancedPing
Enter host IP address [0.0.0.0]: 10.204.20.75
Enter number of ICMP request packets (1-9999) [3]:
Enter packet size (bytes) (28-4096) [64]:
Enter Burst Transmit Ping mode (disabled, enabled)
[disabled]:
Enter Quiet mode (disabled, enabled) [disabled]:
Enter time (sec) waits between sending each packet (1-20)
[1]: 2
Configure ICMP sourceAddress? (n,y) [y]:
  Index  Interface Address
    0    Best interface (default)
    1    10.204.20.70
    2    10.204.20.79
Select interface index {0-2|?} [0]: 1
Press "Enter" key to interrupt.

PING 10.204.20.75 from 10.204.20.83: 64 byte packets
64 bytes from 10.204.20.75: icmp_seq=0. time=26. ms
64 bytes from 10.204.20.75: icmp_seq=1. time=18. ms
64 bytes from 10.204.20.75: icmp_seq=2. time=18. ms

---- 10.204.20.75 PING Statistics ----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms) min/avg/max = 19/21/26
```

---

## Using traceRoute

The traceRoute feature allows you to track the route of an IP packet through the network. TraceRoute information includes all the nodes in the network that a packet passes through to get from its origin to its destination. The traceRoute feature uses the IP time-to-live (TTL) field in UDP probe packets to elicit an ICMP “Time Exceeded” message from each gateway to a particular host.

There are two traceRoute commands available:

- **traceRoute** — Uses the host name or IP address to trace a route to a host using the default options.
- **advancedTraceRoute** — Uses the host name or IP address to trace a route to a host using the advanced options that you specify.

You can enter the host name as part of the command string or you can supply the name in response to the prompt.

To track the route of an IP packet, the traceRoute feature launches UDP probe packets with a small TTL value and then listens for an ICMP “Time Exceeded” reply from a gateway. Probes start with a small TTL of one and increase the value by one until one of the following events occurs:

- The Layer 3 Module receives a “Port Unreachable” message, indicating that the packet reached the host.
- The probe exceeds the maximum number of hops (the default is 30 hops).

At each TTL setting, the Layer 3 Module launches three UDP probe packets, and the traceRoute display prints a line showing the TTL value, the address of the gateway, and the round trip time of each probe. If a probe answers from different gateways, the traceRoute feature prints the address of each responding system. If no response occurs in the three second time-out interval, traceRoute prints an asterisk \* for that probe. Other characters that can appear in the display are:

- **!N** — Indicates that the network is unreachable
- **!H** — Indicates that the host is unreachable
- **!P** — Indicates that the protocol is unreachable
- **!F** — Indicates that fragmentation is needed
- **!<n>** — Indicates an unknown packet type

## Using the traceRoute Command

Use the `ip traceRoute` command to trace a route to a destination using the default traceRoute options (see Table 33 on page 125). To change the default traceRoute options, use the **advancedTraceroute** command and press [Enter] until you see the prompt for the option you want to change.



*You can specify a host name or an IP address as the destination in the traceRoute command. If you specify a hostname, the hostname and its associated IP address must be configured on a network name server. Also, you must add the IP address on the name server to the list of name server addresses associated with the network domain name. See “Administering the Domain Name Server Client” on page 72 for further information.*

To trace a route to a host:

- 1 Enter the following at the top-level menu:  
**ip traceRoute**
- 2 At the prompt, specify the host name or IP address of the destination to which you want to trace a route.

The system begins the trace and then displays the IP address and host name (if available) of the gateways and routers through which the UDP probe packets pass on the way to the destination.

The following example shows a successful traceRoute using the default values automatically (see Table 33 on page 125 for the default values):

```
Select menu options (ip): traceRoute  
Enter host name/IP address [0.0.0.0]: 10.0.1.2  
Press "Enter" key to interrupt.
```

```
Traceroute to 10.0.1.2: 30 hops max, 28 bytes packet
```

```
1 10.0.2.2      9 ms 22 ms 5 ms  
2 10.0.3.2      8 ms 22 ms 8 ms  
3 10.0.24.3     7 ms 22 ms 7 ms  
4 10.0.10.1     7 ms 23 ms 6 ms
```

Table 33 lists the default values for the traceRoute options:

**Table 33** Default Values for traceRoute Options

Option	Default Value
ttl	30 hops
port	port 33434
probeCount	3 probes
wait	3 seconds
packetSize	28 bytes
sourceAddress	determined by the router
numeric	disabled

### Using the advancedTraceRoute Command

Use the `ip advancedTraceRoute` command to trace a route to a host using one or more of the advanced traceRoute options.

Table 34 describes the advanced traceRoute options.

**Table 34** Advanced traceRoute options

Option	Description
ttl	Determines the maximum number of hops that the system can use in outgoing probe packets.
port	The destination (or base) UDP port number that the system uses in probe packets. Set the destination UDP port number to a very high value to make sure that an application at the destination is not using that port. The valid port numbers are numbers greater than 30,000 which makes it unlikely that an application would be using this port.
probeCount	The maximum number of probes that the system sends out at each TTL level.
wait	The wait interval determines the maximum amount of time, in seconds, that the module waits for a response to a probe. Valid values are 1 through 10.
packetSize	The number of bytes in each UDP probe packet. Valid packet sizes are 28 through 4096.

(continued)

**Table 34** Advanced traceRoute options (continued)

Option	Description
sourceAddress	Use this option to specify a source address other than the one from which the probe packets originate. This option is available if you have more than one IP interface defined on your system. When you use this option, the module lists all the currently defined interfaces and their index numbers. To choose an address, select the index number given for that address.
numeric	When you enable this option, the system shows the hop addresses in numeric format, rather than symbolic format.

To trace a route to a host using the advanced options:

- 1 Enter the following at the top-level menu:  
**ip advancedTraceRoute**
- 2 At the prompt, enter the host name or IP address of the destination host. See Table 33 for the default values and Table 34 for valid values to enter at the following prompts.
- 3 Enter the maximum time-to-live (TTL) value (the maximum number of hops).
- 4 Enter the destination port number.
- 5 Enter the number of probes to send at each TTL level.
- 6 Enter the wait value in seconds.
- 7 Enter the packet size in bytes.
- 8 If you have more than one interface defined, you can choose to change the source address. Enter **y** to change the source or address or **n** to leave the source address set to the default.
- 9 If you are changing the source address, do one of the following:
  - a Enter the index number for the ICMP source address that you want to use.
  - b Enter **?** to display a list of the index numbers and then enter the number you want to use.
- 10 Enter the numeric mode: **disabled** or **enabled**.

You can press [Enter] at any time to interrupt the trace route.

The following example shows a successful advanced traceRoute command, specifying a TTL value of 10:

```
Select menu options (ip): advancedTraceRoute
Enter host name/IP address [0.0.0.0]: 10.0.1.2
Enter maximum Time-to-Live (ttl) (1-255 [30]): 10
Enter Destination Port number (30000-65535) [33434]:
Enter the number of probes to be sent at each ttl level
(1-10) [3]:
Enter time (sec) to wait for a response (1-10) [3]
Enter the packet size (bytes) (28-4096) [28]:
Configure TRACEROUTE sourceAddress? (n,y) [y]:
  Index   Interface address
    0     Best interface (default)
    1     10.0.5.43
    2     10.0.7.1
Select interface index {0-2|?} [0]:
Enter Numeric mode (disabled,enabled) [disabled]:
Press "Enter" key to interrupt.
```

Traceroute to 10.0.1.2: 30 hops max, 28 bytes packet

```
1 10.0.17.3    12 ms 7 ms 5 ms
2 10.0.3.1     51 ms 9 ms 7ms
3 10.0.24.22  21 ms 15 ms 6 ms
4 10.0.0.2    18 ms 90ms 80 ms
```





# 9

## PROBLEM SOLVING

This chapter describes how to identify the cause of problems you may encounter with the SuperStack® II Switch Layer 3 Module and suggests possible solutions. It contains the following sections:

- Introduction
- Interpreting LEDs
- Identifying the Problem



*This chapter deals with problems specific to the Layer 3 Module. For more general problem solving tips, see the Problem Solving section of your Switch user guide.*

---

### Introduction

This problem solving section describes how to identify the cause of a problem and suggests possible solutions. It contains the following sections:

- **Interpreting LEDs**  
The two module status LEDs on the Switch provide valuable status information that can be used for troubleshooting. You may find it useful to familiarize yourself with these LEDs before reading the troubleshooting suggestions in the following sections.
- **Identifying the Problem**  
Use this section when you do not know the cause of the problem.



*If you have problems that are not addressed by the problem solving information in this guide, contact 3Com Technical Support, or your service personnel. See Appendix C for information about contacting Technical Support.*



**CAUTION:** *The Layer 3 Module does not contain any parts that can be serviced by the user.*

## Interpreting LEDs

Table 35 describes the LEDs on the Switch.

**Table 35** Switch Module Status LEDs

LED Name	Color/State	Indicates
Packet	Yellow	Packets are being routed.
	Off	No packets are being routed.
Status	Yellow	The Layer 3 Module is functioning.
	Yellow flashing	An unrecognized or faulty module is installed in the Switch.
	Off	There is no module installed in the Switch.



**CAUTION:** *The absence of lit LEDs does not necessarily mean that the device is not powered up.*

## Identifying the Problem

This section describes how to identify problems, and suggests possible solutions.

**Table 36** Identifying Problems with the Layer 3 Module

Problem	Cause	Solution
The module status LED on the front panel of the Switch is not lit when the Layer 3 Module is present.	Power supply problem.	<p>Try the following troubleshooting procedures:</p> <ol style="list-style-type: none"> <li>1 Check that the power supply is plugged into the device, using a power outlet that is known to be working.</li> <li>2 Check that the main power supply switch on the wall is set to the <i>ON</i> position.</li> <li>3 Replace the power cable with a cable known to be working, and power-up the Switch.</li> <li>4 Contact 3Com Technical Support. See Appendix C.</li> </ol>
	Layer 3 Module is not correctly installed.	Remove and then reinstall the Layer 3 Module. See Chapter 3 for more information about installing the Layer 3 Module.

(continued)

**Table 36** Identifying Problems with the Layer 3 Module (continued)

Problem	Cause	Solution
The module status LED on the front panel of the Switch flashes slowly when the Layer 3 Module is present.	Switch software version in your Switch does not support the Layer 3 Module.	<p>Upgrade the Switch software to a version that supports the Layer 3 Module.</p> <p>The software on the Switch must be version 2.4 or later.</p> <p>To determine the version of software installed on the Switch, do one of the following:</p> <ul style="list-style-type: none"> <li>■ Use the Unit Status page on the Web interface of the Switch.</li> <li>■ Use the <b>system display</b> command on the Switch. The software version is identical to the Operational Version.</li> </ul> <p>For further information, see your Switch management guide.</p>
Cannot contact any Layer 3 Module IP address.	Layer 3 Module is disabled on the Switch.	Use the <b>system module mode</b> command on the Switch to enable the Layer 3 Module. You may have to restart the Switch if you change the enabled/disabled state of the module.
Cannot ping or Telnet to the Layer 3 Module VLAN 1 IP address.	Layer 3 Module has not finished booting.	The Layer 3 Module takes up to 90 seconds to start after the Switch has been powered up. Check to see if the module packet LED is blinking, indicating that the module is receiving packets from the network.
	Layer 3 Module does not have a VLAN 1 IP address.	<p>The Layer 3 Module must have a VLAN 1 IP address. Define a VLAN 1 IP address on the Switch. The IP address is then allocated to the module each time the unit is powered up. The Layer 3 module VLAN 1 IP address must be on the same network and subnet as the Switch management IP address.</p> <p>See step 3 on page 31 for more information about setting IP addresses on the Switch.</p>

(continued)

**Table 36** Identifying Problems with the Layer 3 Module (continued)

Problem	Cause	Solution
Cannot ping or Telnet to the Layer 3 Module VLAN 1 IP address.	Switch or stack does not have an IP address.	Configure the Switch, or stack, that contains the Layer 3 Module to have a management IP address, and then ensure that the Layer 3 Module also has an IP address. Both addresses must be on the same network and subnet.  You can configure the Switch management IP address using the <b>ip interface define</b> command on the Switch.
	Switch management IP address is on a different network from Layer 3 Module IP address.	The Layer 3 Module VLAN 1 IP address must be on the same network and subnet as the Switch management IP address.  You can change the Switch management IP address using the <b>ip interface define</b> command on the Switch.
	Layer 3 Module non-volatile configuration is in an invalid state, and the module is continually rebooting.	Follow the procedure in “Resetting the Module to the Factory Default Values” in Appendix B.
bridge vlan summary on the Layer 3 Module does not show any of the VLANs that have been defined on the Switch, apart from VLAN 1.	Layer 3 Module is not receiving VLAN update messages from the Switch.	The Switch does not have a management IP address, or has a management IP address that is not on the same subnet as the Layer 3 Module VLAN 1 IP address.  Configure the Switch to have an IP address on the same network as the Layer 3 Module VLAN 1 IP address. You can do this using the <b>ip interface define</b> command on the Switch.
After removing a VLAN from the Switch, the VLAN remains in the bridge vlan summary on the Layer 3 Module.	Layer 3 Module only receives updates about VLAN changes every 30 seconds.	Wait for at least 60 seconds for the VLAN update to be sent to the Layer 3 Module from the Switch, and then try again.

(continued)

**Table 36** Identifying Problems with the Layer 3 Module (continued)

Problem	Cause	Solution
After removing a VLAN from the Switch, the VLAN remains in the <code>bridge vlan summary</code> on the Layer 3 Module.	If the removed VLAN has an IP address configured, the Layer 3 Module does not remove the VLAN until the IP address has been removed.	Remove the IP address from the deleted VLAN using the <code>ip interface remove</code> command, and the VLAN will be removed when the next VLAN update is received from the Switch.
The Layer 3 Module is not routing. If you Telnet to the Layer 3 Module VLAN 1 IP address, you can see the Configuration Application menu, as described in Appendix B.	Main application image has become corrupted; for example, because a software upgrade was interrupted.	Obtain the main application software image from the 3Com Web site. To reinstall the application image, follow the procedure described in "Downloading a Software Update" in Appendix B.
After moving the Layer 3 Module from one switch to another, you cannot contact the module on the configured Layer 3 Module VLAN 1 IP address.	Layer 3 Module must be reset to the factory default values when moved from switch to switch.	Follow the procedure in "Resetting the Module to the Factory Default Values" in Appendix B.
After saving a configuration on one Layer 3 Module, and restoring the same configuration on a different Layer 3 Module using the <code>system nvdata restore</code> command, you cannot contact the second module on the same VLAN 1 IP address.	Layer 3 Module that the configuration was restored on does not have the same VLAN 1 IP address as the module that the configuration was saved from.	<p>The configuration may only be restored onto a Layer 3 Module with the same VLAN 1 IP address as the module it was restored from.</p> <p>To solve this problem, try one of the following workarounds:</p> <ul style="list-style-type: none"> <li>■ Telnet to a different VLAN address of the Layer 3 Module, and remove the duplicate VLAN 1 IP address that was restored. You may have to remove some static routes.</li> <li>■ Follow the procedure in "Resetting the Module to the Factory Default Values" in Appendix B. Then set the VLAN 1 IP addresses of the Switch and the Layer 3 Module to match the configuration, and restore the configuration again.</li> </ul>

(continued)

**Table 36** Identifying Problems with the Layer 3 Module (continued)

Problem	Cause	Solution
After changing the VLAN 1 IP address of the Layer 3 Module, you may still be able to contact the module on VLAN 1 on the old IP address, or you may not be able to contact the module on VLAN 1 at all.	Under some circumstances, the Layer 3 Module cannot remove the old VLAN 1 IP address. For example, the Layer 3 Module may not be able to remove the old VLAN 1 IP address if any of the following apply: <ul style="list-style-type: none"> <li>■ OSPF is on VLAN 1.</li> <li>■ There is a multicast tunnel terminating on VLAN 1.</li> <li>■ There are static routes over VLAN 1 interfaces.</li> <li>■ There are static ARP entries on VLAN 1.</li> </ul>	Follow the procedure in “Resetting the Module to the Factory Default Values” in Appendix B, and reconfigure the Layer 3 Module.
	New VLAN 1 IP address is on the same IP network as an existing Layer 3 Module IP address.	Try one of the following: <ul style="list-style-type: none"> <li>■ Remove the duplicate IP interface.</li> <li>■ Follow the procedure in “Resetting the Module to the Factory Default Values” in Appendix B, and reconfigure the Layer 3 Module.</li> </ul>
You can ping or Telnet to the Layer 3 Module from hosts on VLAN 1, but not from any of the hosts on other VLANs.	Main application image has become corrupted, and the module is running the Configuration Application.	Obtain the main application software image from the 3Com Web site. To reinstall the application image, follow the procedure described in “Downloading a Software Update” in Appendix B.
	You may have inadvertently configured the Switch ports for 802.1Q tagging, using the VLAN page on the Switch Web interface, instead of placing the ports into specific VLANs using the port setup by clicking on the Switch mimic.	Use the Switch Web interface or command line interface to verify that the corresponding front panel Switch ports have the correct configuration.
You have configured a multicast tunnel, but multicast traffic is not being routed through it.	DVMRP is not enabled on the Layer 3 Module.	Enable DVMRP using the <b>ip multicast dvmrp</b> command. See “Enabling and Disabling DVMRP” on page 77.

(continued)

**Table 36** Identifying Problems with the Layer 3 Module (continued)

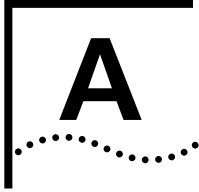
<b>Problem</b>	<b>Cause</b>	<b>Solution</b>
You have configured a multicast tunnel, but multicast traffic is not being routed through it.		Check the IP addresses of the routers at both ends of the multicast tunnel. The <b>ip multicast tunnel display</b> command should indicate that they have the remote router as the peer.
	If the multicast tunnel display shows the correct IP address in the peer field, but no multicast traffic is being routed through the tunnel, the tunnel endpoints may not be on the interfaces that are closest to the destination.	Use the <b>ip multicast tunnel remove</b> and <b>define</b> commands to create a multicast tunnel. The multicast tunnel endpoints must be on two interfaces that are as close to each other on the network as possible.
Multicasts are being routed to other routers, but not to your hosts.	Layer 3 Module is not the IGMP querier on the VLAN.	Ensure that IGMP is enabled using the <b>ip multicast igmp</b> command. See “Enabling and Disabling IGMP” on page 78. Verify that the Layer 3 Module is the IGMP querier for the VLAN by checking the <b>ip multicast interface display</b> command.
OSPF network is unstable.	Layer 3 Module fails to converge because it is out of memory. This is indicated by soft restarts, or memoryFailure errors by the <b>ip ospf statistics</b> command.	Increase the system resources available to OSPF using the <b>ip ospf partition modify</b> command. See “Modifying Memory Partitions” on page 106.
	On networks with a large amount of multicast traffic, the intra-router OSPF multicasts may become lost. This causes HELLO and LSA messages to be missed and the network to destabilize.	If appropriate for your network, try enabling IGMP snooping on the Switch stack. This reduces multicast traffic across the network as a whole, and prioritizes the router protocol multicasts over other multicast traffic.

(continued)

**Table 36** Identifying Problems with the Layer 3 Module (continued)

Problem	Cause	Solution
If RIP is the routing protocol and you are using variable length subnet masks of class A, B or C network addresses (for example, an address with a subnet mask of 255.255.255.0 of a Class B network), your other routers are not getting correct advertisements for these networks.	<p>Layer 3 Module supports RIP version 1.</p> <p>RIP version 1 does not support the advertisement of variable length subnet masks. It only correctly advertises unsubnetted class A (mask 255.0.0.0), class B (mask 255.255.0.0) and class C (mask 255.255.255.0) networks in the corresponding network ranges.</p>	<p>Where you have subnets, try one of the following procedures:</p> <ul style="list-style-type: none"> <li>■ Turn off RIP and define static routes on your Layer 3 Module and the other routers to your subnets.</li> <li>■ Use OSPF instead of RIP between the Layer 3 Module and other routers.</li> <li>■ Only use unsubnetted class A, B or C network addresses with your Layer 3 Module.</li> </ul>
When you try to access those features of the Layer 3 Module that do not have their own Web pages, you get errors mentioning URL.DLL from the Web interface.	URL.DLL is used from some Web browsers to invoke Telnet. If the URL.DLL is not installed, Telnet does not work.	Run Telnet manually instead.
Although you have no front panel ports up on a VLAN, the <code>ip interface summary</code> display reports the corresponding IP interface as <i>UP</i> . In addition, other routers are still having routes to that network advertised to them by the Layer 3 Module.	Layer 3 Module always reports all of its IP interfaces as <i>UP</i> . This is because the Layer 3 Module is (in effect) directly connected to the Switch infrastructure through a tagged-link, and that link to the Switch fabric never goes down.	
You have forgotten your admin password setting, and therefore cannot manage your Layer 3 Module.		Follow the procedure in “Resetting the Module to the Factory Default Values” in Appendix B, and reconfigure the Layer 3 Module.
When you access the Web interface, you can see the banner and the tab panel, but nothing in the Menu tree or workspace.		Click the Web Console button on the tab panel to bring up the menu tree and workspace.
The fonts in the Web interface are too small to read easily.	Fonts used in the Layer 3 Module Web pages are configured to be small in order to include as much information as possible on each page.	Reconfigure your browser to override the document-specified fonts with your own choice of fonts and point sizes.





# LAYER 3 MODULE TECHNICAL SPECIFICATIONS

---

## Environmental Requirements

---

Operating Temperature	0° to 50°C (32° to 122°F)
Storage Temperature	-10° to 70°C (14° to 158°F)
Operating Humidity	0 to 95% non-condensing
Environmental Standard	EN60068 (IEC 68)

---

## Safety

Agency Certifications	UL 1950, EN60950, CSA22.2 No.950, IEC950
-----------------------	--

---

## EMC

Emissions	EN55022 Class B, FCC Part 15 Subpart B Class A, ICES-003 Class A, AS/NZS 3548 Class B, VCCI Class B
Immunity	EN50082-1

---

## Power Consumption

Current Rating	(@ 5V DC) 7A maximum (35W maximum)
----------------	------------------------------------

---

## Standards Supported

### SNMP

- SNMP protocol (RFC 1157)
- MIB-II (RFC 1213)
- BOOTP (RFC 951)

### Terminal Emulation

- Telnet (RFC 854)

### Protocols

- IP (RFC 791)
  - ICMP (RFC 792)
  - RIP (RFC 1058)
  - DVMP (RFC 1075)
  - IGMP (RFC 1112)
  - OSPF Protocol Analysis (RFC 1245)
  - Requirements for IP Version 4 routers (RFC 1812)
- 

## Year 2000 Compliance

This product is Year 2000 compliant. For information on Year 2000 Compliance and 3Com products, visit the 3Com Year 2000 Web page:

<http://www.3Com.com/products/yr2000.html>

---

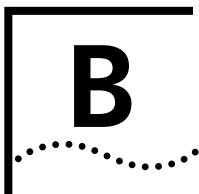
---

**EMC Statements**

**FCC Statement:** This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference to radio communications, in which case the user will be required to correct the interference at their own expense.

**CSA Statement:** This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.



# CONFIGURATION APPLICATION

This appendix contains the following sections:

- About the Configuration Application
- Accessing the Configuration Application
- Downloading a Software Update
- Resetting the Module to the Factory Default Values

---

## About the Configuration Application

The Configuration Application is an additional application provided with the Layer 3 Module boot code. You can use it to provide an alternative method of installing new system software, and to restore the Layer 3 Module to its factory default values.

---

## Accessing the Configuration Application

The Configuration Application can only be accessed via Telnet, from hosts on VLAN 1.

To start the Layer 3 Module running with the Configuration Application:

- 1** Use the Switch Web interface or command line interface to ensure that the Layer 3 Module has an IP address, subnet mask and default gateway, and that the module is enabled. See step 3 on page 31 for more information.
- 2** Turn off the power to the Switch and disconnect the Switch from the main power supply.
- 3** Use a sharp non-metallic object (but *not* a graphite pencil), to press and hold in the recessed configuration switch.
- 4** Continue to hold in the configuration switch, and power up the Switch. The Switch does not have an On/Off button, so you must power it up by reconnecting it to the main power supply using a power cable.

- 5 Continue to hold in the configuration switch until the front panel link status LEDs have lit up. This is usually about 10 seconds after you power up the Switch.
- 6 Release the configuration switch.
- 7 Telnet to the Layer 3 Module IP address from any host on VLAN 1.  
You will see a menu display similar to the one in Figure 12.

**Figure 12** Configuration Application Menu Display

```
SuperStack II Switch Layer 3 Module Configuration System
Copyright (c) 1998,1999 3Com Technologies. ALL RIGHTS RESERVED

Serial Number:                               7D6B147E9C0
Mac Address:                                  00:90:04:47:e9:c0

Boot Version:                                1.00 - Tue Sep 21 19:45:37 1999
App Version:                                 1.00 - Tue Sep 21 19:45:37 1999

IP Address:                                   192.168.132.101
Subnet Mask:                                  255.255.255.0
Default Gateway IP Address:                   192.168.132.101

1 Download software update ->
2 Reset to factory defaults
3 Exit

Enter one of: 1 2 3 ? █
```

---

## Downloading a Software Update

Enter 1 in the Configuration Application menu display (Figure 12), to open the Download Software Update menu, as shown in Figure 13.

**Figure 13** Download Software Update Menu

```
Download Software Update Menu

1 TFTP Server IP address                0.0.0.0
2 Install file name
3 Download software upgrade (.bin files)
4 Download software to run immediately (.ram files)
0 Return to previous menu

IP Address:                            192.168.132.101
Subnet Mask:                            255.255.255.0
Default Gateway IP address:             192.168.132.101

Enter one of: 1 2 3 4 0 ? █
```

To download a new application image, you need to have a TFTP server installed on VLAN 1. The application image that you want to download must be installed on this TFTP server.

- 1** Enter **1** and the IP address of the TFTP server.

The menu now refreshes to display this change.

- 2** Enter **2** and the filename of the application image that you want to download.

The menu now refreshes to display this change, as shown in Figure 14.

**Figure 14** Download Software Update Menu with IP Address and Filename

```

                                Download Software Update Menu

1 TFTP Server IP address                      192.168.132.83
2 Install file name                          13m01_01.bin
3 Download software upgrade (.bin files)
4 Download software to run immediately (.ram files)
0 Return to previous menu

IP Address:                                192.168.132.101
Subnet Mask:                               255.255.255.0
Default Gateway IP address:                192.168.132.101

Enter one of: 1 2 3 4 0 ? █

```

- 3** Enter 3 to download the application image and load it into the non-volatile storage on the Layer 3 Module.

The following prompt is displayed:

```

Enter one of: 1 2 3 4 0? 3
Starting tftp download. Please wait a few
moments.....
.....
Image read done, 4458064 bytes OK

```

If the image loaded into the Layer 3 Module is corrupt, you receive an error message, similar to the following:

This image has an invalid checksum

This may be because the image was not transferred in binary mode when FTPed between hosts.



**CAUTION:** During the programming of the application image, you must not do any of the following:

- Power down and power up the Switch.
- Reset the Switch.
- Close the Telnet session to the Configuration Application.

These actions prevent the application image from being loaded into the Layer 3 Module.



*If an incomplete or corrupt application image is loaded into the Layer 3 Module, the module boots up into the Configuration Application.*

When the image is read it is applied to the non-volatile storage on the Layer 3 Module.

The following prompt is displayed:

```
Applying software update.....
Download operation completed successfully.
Press RETURN key to continue
```

The application image has now been downloaded.



*Option 4 is provided for 3Com support purposes only.*

- 4 Enter **0** to return to the Configuration Application Menu Display.

## Restarting the Module

- 1 Enter **3** to exit the Layer 3 Module.
- 2 To restart the module, do one of the following:
  - Power down and then power up the Switch.
  - Use the **system reset** command on the Switch.

To use this command:

  - a Use Telnet to access the command line interface for the Switch.
  - b Enter the following at the top-level menu:

```
system reset yes
```

This command restarts the Switch and module immediately.

---

## Resetting the Module to the Factory Default Values

To reset the configuration to its factory default values:

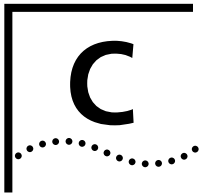
- 1 Enter **2** in the Configuration Application Menu Display, as shown in Figure 12.
- 2 Enter **y** to reset the module to its factory default values.



*Resetting the module to the factory defaults also removes any passwords that have been set, and resets the SNMP community strings.*







# TECHNICAL SUPPORT

3Com provides easy access to technical support information through a variety of services. This appendix describes these services.

Information contained in this appendix is correct at time of publication. For the very latest information, 3Com recommends that you access the 3Com Corporation World Wide Web site.

---

## Online Technical Services

3Com offers worldwide product support 24 hours a day, 7 days a week, through the following online systems:

- World Wide Web site
- 3Com Knowledgebase Web Services
- 3Com FTP site
- 3Com Bulletin Board Service (3Com BBS)
- 3ComFacts<sup>SM</sup> automated fax service

## World Wide Web Site

Access the latest networking information on the 3Com Corporation World Wide Web site by entering the URL into your Internet browser:

<http://www.3com.com/>

This service provides access to online support information such as technical documentation and software library, as well as support options ranging from technical education to maintenance and professional services.

## 3Com Knowledgebase Web Services

This interactive tool contains technical product information compiled by 3Com expert technical engineers around the globe. Located on the World Wide Web at <http://knowledgebase.3com.com>, this service gives all 3Com customers and partners complementary, round-the-clock access to technical information on most 3Com products.

**3Com FTP Site** Download drivers, patches, software, and MIBs across the Internet from the 3Com public FTP site. This service is available 24 hours a day, 7 days a week.

To connect to the 3Com FTP site, enter the following information into your FTP client:

- Hostname: **ftp.3com.com**
- Username: **anonymous**
- Password: **<your Internet e-mail address>**



*A user name and password are not needed with Web browser software such as Netscape Navigator and Internet Explorer.*

**3Com Bulletin Board Service** The 3Com BBS contains patches, software, and drivers for 3Com products. This service is available through analog modem or digital modem (ISDN) 24 hours a day, 7 days a week.

#### **Access by Analog Modem**

To reach the service by modem, set your modem to 8 data bits, no parity, and 1 stop bit.

#### **Access by Digital Modem**

ISDN users can dial in to the 3Com BBS using a digital modem for fast access up to 64 Kbps.

Use the following number to access the 3Com BBS with an analog or a digital modem:

**1 847 262 6000**

**3ComFacts Automated Fax Service** The 3ComFacts automated fax service provides technical articles, diagrams, and troubleshooting instructions on 3Com products 24 hours a day, 7 days a week.

Call 3ComFacts using your Touch-Tone telephone:

**1 408 727 7021**

---

## Support from Your Network Supplier

If additional assistance is required, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

---

## Support from 3Com

If you are unable to obtain assistance from the 3Com online technical resources or from your network supplier, 3Com offers technical telephone support services. To find out more about your support options, please call the 3Com technical telephone support phone number at the location nearest you.

When you contact 3Com for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

Below is a list of worldwide technical telephone support numbers:

Country	Telephone Number	Country	Telephone Number
<b>Asia Pacific Rim</b>			
Australia	1 800 678 515	P.R. of China	10800 61 00137 or 021 6350 1590
Hong Kong	800 933 486	Singapore	800 6161 463
India	61 2 9937 5085	S. Korea	
Indonesia	001 800 61 009	From anywhere in S. Korea:	82 2 3455 6455
Japan	0031 61 6439	From Seoul:	00798 611 2230
Malaysia	1800 801 777	Taiwan, R.O.C.	0080 611 261
New Zealand	0800 446 398	Thailand	001 800 611 2000
Pakistan	61 2 9937 5085		
Philippines	1235 61 266 2602		
<b>Europe</b>			
From anywhere in Europe, call: +31 (0)30 6029900 phone +31 (0)30 6029999 fax			
From the following European countries, you may use the toll-free numbers:			
Austria	0800 297468	Netherlands	0800 0227788
Belgium	0800 71429	Norway	800 11376
Denmark	800 17309	Poland	0800 3111206
Finland	0800 113153	Portugal	0800 831416
France	0800 917959	South Africa	0800 995014
Germany	0130 821502	Spain	900 983125
Hungary	00800 12813	Sweden	020 795482
Ireland	1 800 553117	Switzerland	0800 55 3072
Israel	1800 9453794	U.K.	0800 966197
Italy	1678 79489		
<b>Latin America</b>			
Argentina	AT&T +800 666 5065	Mexico	01 800 CARE (01 800 2273)
Brazil	0800 13 3266	Peru	AT&T +800 666 5065
Chile	1230 020 0645	Puerto Rico	800 666 5065
Colombia	98012 2127	Venezuela	AT&T +800 666 5065
<b>North America</b>			
	1 800 NET 3Com (1 800 638 3266)		
	Enterprise Customers: 1 800 876 3266		

## Returning Products for Repair

Before you send a product directly to 3Com for repair, you must first obtain a Return Materials Authorization (RMA) number. Products sent to 3Com without RMA numbers will be returned to the sender unopened, at the sender's expense.

To obtain an RMA number, call or fax:

Country	Telephone Number	Fax Number
Asia, Pacific Rim	65 543 6500	65 543 6348
Europe, South Africa, and Middle East	+ 44 1442 435860	+ 44 1442 435718
Latin America	1 408 326 2927	1 408 326 3355
From the following European countries, you may call the toll-free numbers; select option 2 and then option 2:		
Austria	0800 297468	
Belgium	0800 71429	
Denmark	800 17309	
Finland	0800 113153	
France	0800 917959	
Germany	0130 821502	
Hungary	00800 12813	
Ireland	1800553117	
Israel	1800 9453794	
Italy	1678 79489	
Netherlands	0800 0227788	
Norway	800 11376	
Poland	00800 3111206	
Portugal	0800 831416	
South Africa	0800 995014	
Spain	900 983125	
Sweden	020 795482	
Switzerland	0800 55 3072	
U.K.	0800 966197	
U.S.A. and Canada	1 800 NET 3Com (1 800 638 3266)	1 408 326 7120 (not toll-free)
	Enterprise Customers: 1 800 876 3266	



# GLOSSARY

**802.1p and 802.1Q** 802.1p and 802.1Q are IEEE standards that have been developed to address the problems of multimedia traffic delivery and VLAN partitioning across a bridged network.

**ABR** Area Border Router — a border router for an OSPF area. An ABR is located on the border of one or more OSPF areas that connects those areas to the backbone network. ABRs are treated as members of both the OSPF backbone and the attached areas. They therefore maintain routing tables that list both the backbone topology and the topology of the other areas in the network.

**ANSI** American National Standards Institute. A United States technology standards organization.

**ARP** Address Resolution Protocol — ARP is a TCP/IP Interior Gateway Protocol for dynamically mapping Internet addresses to physical hardware addresses on LANs; limited to LANs that support hardware broadcast.

**ASBR** Autonomous System Boundary Router — an area border router located between an OSPF area and a non-OSPF network. As well as the OSPF protocol, ASBRs run another routing protocol, such as RIP. ASBRs cannot reside in a stub OSPF area.

**autonomous system** In Internet (TCP/IP) terminology, a series of gateways or routers that fall under a single administrative entity and cooperate using the same Interior Gateway Protocol (IGP).

**backbone** The part of a network used as the primary path for transporting traffic between network segments.

- backbone area** A special OSPF Area 0 (often written as Area 0.0.0.0, since OSPF Area IDs are typically formatted as IP addresses). The OSPF backbone always contains all area border routers. The backbone is responsible for distributing routing information between non-backbone areas.
- backbone router** A backbone router only has interfaces in the OSPF backbone area.
- BOOTP** The BOOTP protocol allows you to automatically map an IP address to a given MAC address each time a device is started. In addition, the protocol can assign the subnet mask and default gateway to a device.
- border router** A border router has interfaces in more than one OSPF area, in other words, it is positioned between two or more OSPF areas.
- class A network** An IP network in the range of 0.0.0.0 to 127.0.0.0 with a subnet mask of 255.0.0.0.
- class B network** An IP network in the range of 128.0.0.0 to 191.255.0.0 with a subnet mask of 255.255.0.0.
- class C network** An IP network in the range of 192.0.0.0 to 223.255.255.0 with a subnet mask of 255.255.255.0.
- designated router** In OSPF, each multiaccess network with at least two attached routers has a designated router. The designated router has special duties in the running of the protocol, such as generating a link state advertisement for the multiaccess network.
- distance-vector routing** In distance-vector routing, each device calculates the best path to all destinations using a simple metric (for example, the number of hops to a destination) and then shares that information with neighboring routers. The devices continually update their tables as soon as they learn of better routes to their destinations.
- DHCP** Dynamic Host Configuration Protocol — DHCP is a protocol which allows dynamic allocation of IP addresses to IBM PCs running on a Microsoft Windows local area network. The system administrator assigns a range of IP addresses to DHCP. Each client PC on the LAN can use its TCP/IP software to request an IP address from the DHCP server. DHCP uses a lease concept to respond to a request for an IP address and to grant an IP address to client PC. The system administrator can control for how long a client can use a particular IP address.



- DVMRP** Distance Vector Multicast Routing Protocol — DVMRP (RFC 1075) is an Internet routing protocol that provides multicast routing. It supports IP multicast routing by broadcasting data to each router in an internetwork when users join or leave multicast groups.
- dynamic route** Dynamic routes are IP routes learned using a routing information protocol, such as OSPF or RIP.
- firewall** A combination of specifically configured network hardware and software products that limit access to the network by unauthorized individuals from outside the firewall. For example, a firewall can enforce an access control policy between an internal network and the Internet.
- flash EPROM** Erasable Programmable Read-Only Memory. Programmable Read-Only Memory Technology providing nonvolatile storage that can be electrically erased in the circuit and reprogrammed.
- flat network** A network that consists of a single backbone domain. The connections between devices are only at the Layer 2 level, and do not contain routers.
- host** An IP end-station, such as a UNIX workstation, a personal computer or a network-connected device.
- GARP** Generic Attribute Registration Protocol — GARP is a system outlined by the IEEE 802.1D standard that allows endstations in a network to register that they would like to receive traffic with certain attributes.
- gateway** A device that can interconnect networks with different, incompatible communications protocols. The gateway performs a layer-7 protocol-conversion to translate one set of protocols to another (for example, from TCP/IP to SNA or from TCP/IP to X.25). A gateway operates at Open Systems Interconnection (OSI) layers up through the Session Layer.
- GVRP** GARP VLAN Registration Protocol — GVRP is a specific use of GARP that allows endstations to register that they would like to receive traffic for certain VLANs.
- HTTP** HyperText Transfer Protocol — HTTP is a protocol used for transferring text and images over an intranet or the Internet.

- ICMP** Internet Control Message Protocol (RFC 792) — ICMP allows hosts to find the routers attached to their segments and provides certain diagnostic capabilities to the hosts when the routers are unable to deliver packets to addressed destinations.
- IEEE** Institute of Electrical and Electronics Engineers — committees that develop and propose computer standards, such as the 802 protocols, which define the physical and data link protocols of communication networks. Members represent an international cross section of users, vendors and engineering professionals.
- IGMP** Internet Group Management Protocol (RFC 1112) is used by IP hosts to report their multicast group memberships to any adjacent multicast routers. It lets all the systems on a physical network know which hosts currently belong to which multicast groups.
- IGMP querier** The device on a network that sends out IGMP query requests, in order to identify which hosts are members of multicast groups.
- IGMP snooping** A Layer 2 switch uses IGMP snooping to identify which hosts have requested multicasts. The switch can therefore identify which hosts should receive a multicast stream, and also prevent the multicast stream from going to those hosts that have *not* requested multicasts.
- IP Address** Internet Protocol address — a unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with full-stops (periods), and is made up of a network part, identifying what network the device resides on, and a host part, identifying individual devices on a given network.
- IPv4** IPv4 (RFC 791) is a Layer 3 connectionless, datagram delivery service. Information about the organization of IPv4 networks and how to pass datagrams within those networks is controlled by the routing protocol. IPv4 defines two distinct communications methods for end stations:
- Unicast  
A point-to-point method for communicating between two end-stations.
  - Multicast  
A point-to-multipoint method for communication from one end-station to one or more end stations.
- Layer 2** The datalink (or MAC) layer in the OSI 7-layer model.

<b>Layer 3</b>	The network layer in the OSI 7-layer model. This layer controls communication links and data routing across one or more links. It receives data that has been framed by the Data Link layer below it, converts this data into packets, and passes the result to the Transport layer that directs the packets to their destination.
<b>Layer 3 switch</b>	A high-performance router that operates at Layer 3 of the OSI 7-layer model.
<b>link-state routing</b>	In link-state routing, each device maintains a part of a replicated, distributed database of routing information. Each device monitors the state of each active link to its local IP networks. All connected devices collect this local link-state information from all other devices, which allows them to run a shortest path calculation to determine the best routes to any given destination network.
<b>link-state advertisement</b>	The mechanism by which OSPF routing information is exchanged.
<b>MAC address</b>	The hardware address of a device connected to a shared network medium.
<b>multicast</b>	A message sent to a specific group of nodes on a network simultaneously.
<b>multicast routing</b>	Multicast routing allows packets to be routed between specific groups of hosts on different VLANs.
<b>multicast tunnel</b>	A mechanism by which multicast traffic may be routed through a non-multicast routing domain. The tunnel is defined by two endpoints which reside within multicast routing domains, but which connect through a non-multicast routing domain.
<b>neighbor</b>	A router's neighbors (or peers) are those routers with which the router will directly exchange routing information.
<b>nonvolatile data</b>	Data which is persistent even when the device where the data is stored is not switched on.
<b>OSI 7-layer model</b>	The Open Systems Interconnection model is a 7-layer framework within which communications protocols and standards have been defined.

- OSPF** Open Shortest Path First — OSPFv1 (RFC 1245) is an alternative to RIP that overcomes many of its limitations; limited network size, slow to stabilize and network traffic load. OSPFv1 in the Layer 3 Module supports 32 areas, 32 virtual links and 64 neighbors.
- OSPF area** An OSPF area is a logical, user-defined group of networks, hosts, and directly attached routers. All routers in an area converge onto the same OSPF routing table.
- OSPF stub area** A type of OSPF area that contains routers with limited resources, such as memory. The stub area cannot support virtual links or Autonomous System boundary routers (ASBRs) and is at the outside edge of the OSPF routing domain. Designating an OSPF area as a stub area allows routers in the stub area to work successfully without being able to route to the whole of the network.
- RIPv1** Routing Information Protocol Version 1 — a simple protocol used to exchange information between routers.
- router convergence** This occurs when all of the routers in a given OSPF area agree on the best path to a destination.
- routing** A network management function responsible for forwarding packets from their source to their destination. A number of routing algorithms exist to suit different network topologies and requirements.
- routing domain** A collection of routers.
- routing table** A routing table contains various routing information including destination/next hop associations and path desirability.
- SNMP** Simple Network Management Protocol — a protocol originally designed to be used in managing TCP/IP internets. SNMP is presently implemented on a wide range of computers and networking equipment and may be used to manage many aspects of network and endstation operation.
- static route** Static routes are entered manually into the routing table, and are used to reach networks not advertised by routers.
- subnet mask** A subnet mask distinguishes the network ID part of an IP address from the host ID part. A subnet mask is a 32-bit number expressed as four decimal numbers, in the range 0 to 255, separated by periods.

- switch** A device which filters, forwards and floods packets based on the packet's destination address. The switch learns the addresses associated with each switch port and builds tables based on this information to be used for the switching decision.
- TCP** A layered set of communications protocols providing Telnet terminal emulation, FTP file transfer, and other services for communication among a wide range of computer equipment.
- Telnet** A TCP/IP application protocol that provides virtual terminal service, letting a user log in to another computer system and access a host as if the user were connected directly to the host.
- TELNET** An asynchronous, virtual terminal protocol that allows for remote access.
- TFTP** Trivial File Transfer Protocol — allows you to transfer files (such as software upgrades and configuration files) to and from a remote device.
- UDP** User Datagram Protocol — a protocol enabling an application to send individual messages to other applications. Delivery is not guaranteed, and messages need not be delivered in the same order as they were sent.
- UDP Helper** The UDP helper forwards specific protocol broadcasts that would not normally be forwarded by the router. The broadcast will be forwarded to a set of specific IP addresses. Typically, the Bootstrap Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP) will be forwarded to a suitable server. The Layer 3 Module supports 32 UDP helpers.
- unicast** A message sent to an individual node on a network.
- unicast routing** Unicast routing allows packets to be routed between individual hosts on different VLANs.
- variable length subnet mask** More than one subnet mask (of different lengths) can be configured for a Class A, B or C network. This allows these networks to be divided into smaller subnetworks. A longer subnet mask than that which the network class specifies, is used to group hosts into smaller networks. The subnet masks are stored in routing tables so that the longest subnet mask takes precedence over the shortest.

- virtual link** Virtual Links provide connections to those areas in the OSPF autonomous system that are not directly connected to the backbone.
- VLAN** Virtual Local Area Network — a group of location and topology independent devices that communicate as if they are on the same physical LAN.

# INDEX

---

## Numerics

- 3Com bulletin board service (3Com BBS) 146
  - 3Com Knowledgebase Web Services 145
  - 3Com URL 145
  - 3ComFacts 146
  - 802.1Q tagged links 23
- 

## A

- access levels
  - user interface 39
- accessing
  - configuration application 29, 139
  - user interface 39
- active devices 114
- adding
  - OSPF neighbors 104
  - ranges to OSPF areas 86
  - RIP advertisement address 116
- Address Resolution Protocol. *See* ARP
- addresses
  - for SNMP trap reporting 46
- administering
  - ARP cache 70
  - DNS client 72
  - IP interfaces 63
  - IP multicast interfaces 79
  - IP multicast routing 76
  - IP multicast tunnels 80
  - IP routes 66
  - neighbors 102
  - OSPF areas 84
  - OSPF memory partitions 105
  - RIP 114
  - stub default metric value 107
  - UDP helper 74
  - virtual links 107
- administration console
  - password access 50
- advanced options
  - ping 120
  - traceRoute 125
- advertise mode

- RIP 115
  - advertisement addresses
    - adding 116
    - IP interface characteristics 64
    - removing 117
  - age time
    - setting 71
  - allocating
    - memory for OSPF 106
  - area IDs
    - modifying for virtual links 111
    - OSPF areas 85
    - OSPF interfaces 93
  - ARP
    - administering ARP cache 70
    - defining static ARP entry 70
    - displaying ARP cache 70
    - flushing ARP cache 71
    - removing ARP cache entry 71
    - setting age time 71
  - assigning
    - Layer 3 module IP address 31
- 

## B

- backing up
    - NV data 52
  - backup designated routers 92
  - baseline
    - reasons for 84
  - BOOTP 14, 74
    - setting BOOTP relay threshold 76
    - setting hop count limit 76
  - Bootstrap Protocol. *See* BOOTP
  - bridge menu commands
    - vlan summary 57, 132
  - broadcast addresses 77
  - bulletin board service 146
  - burst option
    - ping command 121
- 

## C

- changing
  - DNS domain names 72
  - IP interfaces 65
  - multicast interfaces 79
  - name server IP address 73
  - OSPF area ranges 87
  - OSPF areas 85
  - OSPF memory partition 106
  - virtual link area IDs 111
  - virtual link dead interval 113

- virtual link target routers 111
- virtual link transmit delay 111
- characteristics
  - IP interfaces 63
  - IP multicast interfaces 79
  - OSPF area 85
  - routing table entries 66
- checking
  - IP address resolution 74
- commands
  - bridge vlan summary 57
  - ip advancedPing 121
  - ip advancedTraceRoute 126
  - ip arp age 71
  - ip arp display 70
  - ip arp flush 71
  - ip arp remove 71
  - ip arp static 70
  - ip dns define 72
  - ip dns display 72
  - ip dns domainName 72
  - ip dns modify 73
  - ip dns nslookup 74
  - ip dns remove 73
  - ip icmpRouterDiscovery 84
  - ip interface define 65
  - ip interface modify 65
  - ip interface remove 65
  - ip interface summary 64
  - ip multicast cacheDisplay 82
  - ip multicast dvmrp 78
  - ip multicast igmp 78
  - ip multicast interface disable 80
  - ip multicast interface display 79
  - ip multicast interface enable 79
  - ip multicast routeDisplay 82
  - ip multicast tunnel define 81
  - ip multicast tunnel display 80
  - ip multicast tunnel remove 81
  - ip ospf areas addRange 86
  - ip ospf areas defineArea 85
  - ip ospf areas display 84
  - ip ospf areas modifyArea 85
  - ip ospf areas modifyRange 87
  - ip ospf areas removeArea 86
  - ip ospf areas removeRange 87
  - ip ospf defaultRouteMetric 88
  - ip ospf defaultRouteMetric define 88
  - ip ospf defaultRouteMetric display 88
  - ip ospf interface areaID 93
  - ip ospf interface dead 95
  - ip ospf interface delay 94
  - ip ospf interface hello 94
  - ip ospf interface mode 92
  - ip ospf interface retransmit 95
  - ip ospf interface statistics 90
  - ip ospf interface summary 89
  - ip ospf linkStateData databaseSummary 97
  - ip ospf linkStateData external 101
  - ip ospf linkStateData network 99
  - ip ospf linkStateData router 97
  - ip ospf linkStateData summary 100
  - ip ospf neighbors add 104
  - ip ospf neighbors display 102
  - ip ospf neighbors remove 104
  - ip ospf partition display 105
  - ip ospf partition modify 106
  - ip ospf routerID 105
  - ip ospf stubDefaultMetric define 107
  - ip ospf stubDefaultMetric display 107
  - ip ospf stubDefaultMetric remove 107
  - ip ospf virtualLinks areaID 111
  - ip ospf virtualLinks dead 113
  - ip ospf virtualLinks define 110
  - ip ospf virtualLinks delay 111
  - ip ospf virtualLinks detail 108
  - ip ospf virtualLinks hello 112
  - ip ospf virtualLinks remove 110
  - ip ospf virtualLinks retransmit 112
  - ip ospf virtualLinks router 111
  - ip ospf virtualLinks statistics 109
  - ip ospf virtualLinks summary 108
  - ip ping 119
  - ip rip addAdvertisement 116
  - ip rip cost 118
  - ip rip display 115
  - ip rip mode 115
  - ip rip poisonReverse 116
  - ip rip removeAdvertisement 117
  - ip rip statistics 117
  - ip route display 67
  - ip route flush 69
  - ip route remove 68
  - ip route static 68
  - IP statistics 63
  - ip traceRoute 124
  - ip udpHelper define 75
  - ip udpHelper display 74
  - ip udpHelper hopCountLimit 76
  - ip udpHelper remove 75
  - ip udpHelper threshold 76
  - SNMP community 45
  - SNMP context 44
  - snmp display 45
  - snmp trap addModify 46
  - snmp trap display 46



- snmp trap flush 47
- snmp trap remove 47
- system consoleTimeout timeOut 50
- system display 48
- system initialize 55
- system name 51
- system nvData restore 54
- system nvData save 53
- system password 51
- system reset 56, 143
- system softwareUpgrade 49
- community strings
  - setting 45
  - values 45
- configuration application 139 to 143
  - accessing 29, 139
  - downloading software 140
  - menu display 140
  - overview 139
- configuration button. See configuration switch.
- configuration switch 29
- configuring
  - essential configuration 30
  - IP interfaces 64
  - telnet timeout 50
  - trap reporting destinations 46
- conventions
  - notice icons 8
  - text 8
- cost
  - IP interface characteristics 64
  - setting for RIP 118
- count
  - ping command 120

---

## D

- dead interval
  - OSPF interfaces 95
  - virtual links 113
- default gateways 17, 32
- default passwords 33
- default route metric
  - displaying 88
  - OSPF 87
  - removing 88
- default routers 32
- default routes 17, 66
  - learning 69
  - removing 69
  - setting 69
- default values
  - IP configuration 34
  - ping 119
  - resetting for NV data 55, 143
  - route metric 87
  - SNMP 32
  - system 33
  - system console timeout 50
  - traceRoute 125
- defining
  - default route metric 88
  - IP interfaces 64
  - multicast tunnels 81
  - name server IP address 72
  - OSPF areas 85
  - static ARP cache entries 70
  - static routes 68
  - stub default metric 107
  - UDP helper forwarding addresses 75
  - UDP helper port numbers 75
  - virtual links 110
- deleting
  - ARP cache entries 71
  - default route metric 88
  - default routes 69
  - IP interfaces 65
  - multicast tunnels 81
  - name server IP address 73
  - OSPF area ranges 87
  - OSPF areas 86
  - OSPF neighbors 104
  - RIP advertisement address 117
  - routes 68
  - stub default metric 107
  - UDP helper forwarding address 75
  - UDP helper port numbers 75
  - virtual links 110
- designated routers 92
- destination address
  - for SNMP trap reporting 47
- DHCP 14, 74
- disabled mode
  - RIP 115
- disabling
  - DVMRP 77
  - ICMP router discovery 83
  - IGMP 78
  - IP multicast interfaces 80
  - OSPF interface mode 92
  - poisoned reverse mode 116
- disconnecting remote sessions 50
- displaying
  - ARP cache 70
  - default route metric value 88
  - DNS configuration 72

- external network LSAs 101
- IP interface summaries 64
- IP multicast interfaces 79
- IP multicast tunnels 80
- link state database summary 97
- multicast cache 82
- multicast routes 82
- network LSA summary 100
- network LSAs 99
- OSPF areas 84
- OSPF interface statistics 90
- OSPF interfaces 89
- OSPF memory allocation 105
- OSPF neighbors 102
- OSPF statistics 113
- RIP information 115
- RIP statistics 117
- router LSAs 97
- routing tables 67
- SNMP settings 45
- stub default metric 107
- system configuration 48
- trap reporting configuration 46
- UDP helper 74
- virtual links 108
- VLAN summary 57

Distance Vector Multicast Routing Protocol. See DVMRP

DNS

- client 72
- displaying 72
- modifying the domain name 72
- name server
  - defining 72
  - modifying 73
  - removing 73
- querying with nslookup 74

DNS client

- administering 72

Domain Name Server. See DNS

DVMRP 14, 77

- disabling 77
- enabling 77

DVMRP metric value 79

Dynamic Host Configuration Protocol. See DHCP

dynamic routes 16

**E**

- enabled mode
  - RIP 115
- enabling
  - DVMRP 77

- ICMP router discovery 83
- IGMP 78
- IP multicast routing 79
- multicast interfaces 79
- OSPF interface mode 92
- poisoned reverse mode 116
- remote session timeout 50

Ethernet port

- management through 44

external network LSAs 101

**F**

- fax service (3ComFacts) 146
- flash memory
  - loading software into 49
- flushing
  - ARP cache 71
  - routes 69
  - trap reporting addresses 47

**G**

- gateways
  - default 17, 32
  - routing table entry 66

**H**

- hello timer
  - OSPF interfaces 94
  - virtual links 112
- hop count limit 76
- hops 115

**I**

- ICMP router discovery
  - disabling 83
  - enabling 83
- IGMP 14, 78
  - disabling 78
  - enabling 78
- improving router convergence 104
- installing
  - Layer 3 module hardware 29
  - post installation checks 35
  - pre-installation 28
  - through TFTP 49
  - troubleshooting 49, 130
- integrating
  - Layer 3 module with a network 26
- Interior Gateway Protocols 114

- Internet Control Message Protocol. See ICMP
- Internet Group Management Protocol. See IGMP
- Internet Protocol. See IP
- interpreting LEDs 130
- IP
  - time-to-live 123
- IP addresses
  - assigning 31
  - defining for the name server 72
  - forwarding gateway 66
  - IP interface characteristics 63
  - removing for name servers 73
  - removing for UDP helper 75
  - resolution 74
  - routing table entry 66
  - UDP helper forwarding addresses 75
- IP configuration
  - default values 34
- IP context
  - available commands 60
- IP interfaces
  - administering 63
  - advertisement address 64
  - characteristics 63
  - cost 64
  - defining 64
  - displaying 64
  - IP address 63
  - modifying 65
  - removing 65
  - state 64
  - subnet mask 63
  - VLAN index 64
- IP management interface
  - using 39
- IP menu commands
  - advancedPing 121
  - advancedTraceRoute 126
  - arp age 71
  - arp display 70
  - arp flush 71
  - arp remove 71
  - arp static 70
  - dns define 72
  - dns display 72
  - dns domainName 72
  - dns modify 73
  - dns nslookup 74
  - dns remove 73
  - icmpRouterDiscovery 84
  - interface define 65
  - interface modify 65
  - interface remove 65
  - interface summary 64
  - multicast cacheDisplay 82
  - multicast dvmrp 78
  - multicast igmp 78
  - multicast interface disable 80
  - multicast interface display 79
  - multicast interface enable 79
  - multicast routeDisplay 82
  - multicast tunnel define 81
  - multicast tunnel display 80
  - multicast tunnel remove 81
  - ospf areas addRange 86
  - ospf areas defineArea 85
  - ospf areas display 84
  - ospf areas modifyArea 85
  - ospf areas modifyRange 87
  - ospf areas removeArea 86
  - ospf areas removeRange 87
  - ospf defaultRouteMetric define 88
  - ospf defaultRouteMetric display 88
  - ospf defaultRouteMetric remove 88
  - ospf interface areaID 93
  - ospf interface dead 95
  - ospf interface delay 94
  - ospf interface hello 94
  - ospf interface mode 92
  - ospf interface priority 93
  - ospf interface retransmit 95
  - ospf interface statistics 90
  - ospf interface summary 89
  - ospf linkStateData databaseSummary 97
  - ospf linkStateData external 101
  - ospf linkStateData network 99
  - ospf linkStateData router 97
  - ospf linkStateData summary 100
  - ospf neighbors add 104
  - ospf neighbors display 102
  - ospf neighbors remove 104
  - ospf partition display 105
  - ospf partition modify 106
  - ospf routerID 105
  - ospf statistics 113
  - ospf stubDefaultMetric define 107
  - ospf stubDefaultMetric display 107
  - ospf stubDefaultMetric remove 107
  - ospf virtualLinks areaID 111
  - ospf virtualLinks dead 113
  - ospf virtualLinks define 110
  - ospf virtualLinks delay 111
  - ospf virtualLinks detail 108
  - ospf virtualLinks hello 112
  - ospf virtualLinks remove 110
  - ospf virtualLinks retransmit 112

- ospf virtualLinks router 111
- ospf virtualLinks statistics 109
- ospf virtualLinks summary 108
- ping 119
- rip addAdvertisement 116
- rip cost 118
- rip display 115
- rip mode 115
- rip poisonReverse 116
- rip removeAdvertisement 117
- rip statistics 117
- route display 67
- route flush 69
- route remove 68
- route static 68
- traceRoute 124
- udpHelper define 75
- udpHelper display 74
- udpHelper hopCountLimit 76
- udpHelper remove 75
- udpHelper threshold 76
- IP multicast cache
  - displaying 82
- IP multicast interfaces
  - administering 79
  - characteristics 79
  - disabling 80
  - displaying 79
  - DVMRP metric value 79
  - enabling 79
  - TTL threshold 79
- IP multicast routes
  - displaying 82
- IP multicast routing
  - administering 76
- IP multicast routing table
  - displaying routes 81
- IP multicast tunnels
  - administering 80
  - defining 81
  - displaying 80
  - removing 81
  - uses 80
- IPv4 addresses
  - types 77
- contacting from VLANs 134
- contacting IP address 131
- downloading software using TFTP 49
- essential configuration 30
- handling 28
- hardware features 13
- in switch stacks 24
- installing 29
- integrating with a network 26
- moving between switches 133
- naming 51
- network scenarios 18
- pre-installation checks 28
- rebooting 56
- required version of switch software 13
- resetting to factory defaults 55, 143
- routing table 67
- running with configuration application 139
- safety information 27
- software features 13
- troubleshooting status LED 131
- VLAN indexes 57
- Layer 3 switching
  - background concepts 15
  - benefits 17
- learn mode
  - RIP 115
- LEDs
  - interpreting 130
  - summary 35, 130
- line speed
  - OSPF interfaces 93
- Link State Advertisements. See LSAs
- link state database
  - external network LSAs 101
  - network LSAs 99
  - router LSAs 97
  - summary network LSAs 100
- LSAs 95
  - external 101
  - network 99
  - network summary 100
  - router 97
  - transmit delay 94

---

## L

- Layer 3 module
  - assigning IP addresses 31
  - changing VLAN 1 IP address 134
  - configuration application 139 to 143
  - configuration switch 29

---

## M

- management
  - configuring system access 39
  - IP interface 39
  - naming the system 51
  - SNMP community strings 45
  - system name 51

- maximum hop count
    - BOOTP 76
  - memory
    - OSPF usage 105
  - MIBs 146
  - modes
    - poisoned reverse 116
    - RIP 115
  - modifying
    - DNS domain names 72
    - IP interfaces 65
    - name server IP address 73
    - OSPF area ranges 87
    - OSPF areas 85
    - OSPF memory partitions 106
    - virtual link area IDs 111
    - virtual link dead interval 113
    - virtual link target routers 111
    - virtual link transmit delay 111
  - multicast addresses 77
  - multicast interfaces
    - changing 79
    - enabling 79
  - multicast routing 76
    - troubleshooting 134, 135
  - multicast routing protocol 77
- 
- N**
- name servers
    - defining 72
    - modifying 73
    - removing 73
  - naming the Layer 3 module 51
  - neighbors
    - administering 102
  - network LSAs 99
    - external 101
    - summary 100
    - summary types 100
  - network supplier support 147
  - next hop
    - routing table entry 66
  - next hop routers 16
  - NonVolatile data. *See* NV data
  - numeric format
    - traceRoute command 125, 126
  - NV data
    - backup 52
    - contents saved 52
    - file information 52
    - parameters 52
    - resetting 55
    - resetting default values 55, 143
    - restoring 54
    - saving 52
    - transferring 52
- 
- O**
- online technical services 145
  - Open Shortest Path First protocol. *See* OSPF
  - OSI reference model 15
  - OSPF 16, 84
    - area border routers 107
    - areas 156
    - available memory 105
    - defining stub default metric 107
    - defining virtual links 110
    - displaying stub default metric 107
    - external network LSAs 101
    - link state advertisement 95
    - link state database 96
    - link state database summary 97
    - memory partitions 105
    - network LSA summary 100
    - network LSAs 99
    - removing stub default metric 107
    - router ID 104
    - router LSAs 97
    - setting default route metrics 87
    - statistics 113
    - stub default metric 107
    - troubleshooting 135
    - virtual links 107
  - OSPF areas
    - adding ranges 86
    - administering 84
    - area ID 85
    - characteristics 85
    - defining 85
    - displaying 84
    - modifying 85
    - modifying ranges 87
    - ranges 86
    - removing 86
    - removing ranges 87
    - stub area 85
  - OSPF interfaces
    - area ID 93
    - backup designated routers 92
    - characteristics 88
    - cost 93
    - dead interval 95
    - delay 94
    - designated routers 92

- disabling the mode 92
- displaying 89
- enabling the mode 92
- hello timer 94
- mode 92
- password 96
- priority 92
- retransmit timer 95
- statistics 90
- OSPF memory partitions
  - administering 105
  - displaying 105
  - modifying 106
- OSPF neighbors
  - adding 104
  - administering 102
  - displaying 102
  - removing 104
- OSPF virtual links
  - dead interval 113
  - displaying 108
  - displaying statistics 109
  - hello timer 112
  - modifying area ID 111
  - modifying the target router 111
  - modifying the transmit delay 111
  - password 113
  - removing 110
  - retransmit interval 112
  - target router 111
  - transmit delay 111

---

## P

- packet size
  - ping command 120
  - traceRoute command 125
- packets
  - traceRoute probe 123
- parameters
  - NV data 52
- passive devices 114
- passwords
  - configuring 50
  - default 33
  - OSPF interfaces 96
  - recovering 143
  - setting 50
  - SNMP community 34
  - virtual links 113
- ping
  - advanced options 120
  - burst 121

- commands 118
  - count 120
  - default values 119
  - packet size 120
  - quiet 120
  - responses 119
  - source address 121
  - wait 120
- poisoned reverse
  - RIP 116
- port numbers
  - defining for UDP helper 75
  - removing for UDP helper 75
  - traceRoute command 125
- POST 30
- Power On Self Test. See POST
- priority
  - OSPF interfaces 92
- probe count
  - traceRoute command 125
- probe packets
  - traceRoute command 123
- problem solving. See troubleshooting

---

## Q

- querying
  - IP address resolution 74
- quiet option
  - ping command 120

---

## R

- ranges
  - adding to OSPF areas 86
  - modifying for OSPF areas 87
- reboot
  - resetting the system 56
- relay threshold
  - setting for BOOTP 76
- remote sessions
  - enabling timeout 50
- removing
  - ARP cache entries 71
  - default route metric 88
  - default routes 69
  - IP interfaces 65
  - multicast tunnels 81
  - name server IP address 73
  - OSPF area ranges 87
  - OSPF areas 86
  - OSPF neighbors 104
  - RIP advertisement address 117

- routes 68
    - stub default metric 107
    - trap reporting destinations 47
    - UDP helper forwarding address 75
    - UDP helper port numbers 75
    - virtual links 110
  - resetting
    - NV data default values 55, 143
  - restoring
    - NV data 54
  - retransmit interval
    - virtual links 112
  - retransmit timer
    - OSPF interfaces 95
  - retrieving
    - NV data 54
  - returning products for repair 149
  - RIP 16
    - active devices 114
    - adding advertisement addresses 116
    - administering 114
    - advertise mode 115
    - disabled mode 115
    - displaying information 115
    - displaying statistics 117
    - enabled mode 115
    - hops 115
    - learn mode 115
    - modes 115
    - poisoned reverse 116
    - removing advertisement addresses 117
    - setting cost 118
    - setting mode 115
    - supported version 114
  - RIP passive devices 114
  - rlogin
    - and rebooting the system 56
  - router convergence
    - improving 104
  - router ID
    - OSPF 104
  - routers
    - default 32
    - multicast 77
    - router convergence 96
  - routes
    - administering 66
    - default 17
    - defining static 68
    - dynamic 16
    - flushing 69
    - multicast 82
    - removing 68
    - removing the default 69
    - setting default 69
    - static 17
  - routing
    - multicast 14, 76
    - protocols 16
    - unicast 14
  - Routing Information Protocol. *See* RIP
  - routing metric
    - routing table entry 66
  - routing table entries
    - characteristics 66
    - destination IP address 66
    - gateway IP address 66
    - next hop 66
    - routing metric 66
    - status 66
    - subnet mask 66
  - routing tables
    - default route 66
    - displaying 67
    - function 16
    - how it works 67
- 
- ## S
- sending
    - ping packets 118
  - setting
    - ARP age time 71
    - BOOTP hop count limit 76
    - BOOTP relay threshold 76
    - community strings 45
    - default route metric 87
    - default routes 69
    - OSPF interface area ID 93
    - OSPF interface cost 93
    - OSPF interface dead interval 95
    - OSPF interface delay 94
    - OSPF interface hello timer 94
    - OSPF interface mode 92
    - OSPF interface password 96
    - OSPF interface priority 92
    - OSPF interface retransmit timer 95
    - OSPF router ID 104
    - RIP cost 118
    - RIP mode 115
    - system name 51
    - system passwords 50
    - system timeout interval 50
    - traceRoute trace option 124
    - virtual link hello timer 112
    - virtual link passwords 113

- virtual link retransmit interval 112
  - setting up
    - SNMP 44
  - Simple Network Management Protocol. *See* SNMP
  - SNMP
    - agent 44
    - community strings 45
    - configuring trap reporting destinations 46
    - default values 32
    - displaying current settings 45
    - displaying trap reporting configuration 46
    - flushing trap reporting addresses 47
    - removing trap reporting destinations 47
    - setting up 44
  - SNMP community
    - default passwords 34
  - SNMP context
    - available commands 44
  - SNMP menu commands
    - community 45
    - display 45
    - trap addModify 46
    - trap display 46
    - trap flush 47
    - trap remove 47
  - SNMP traps
    - problem solving 47
  - software
    - backing up NV data 52
    - build date and time 48
    - switch version 13, 28
    - upgrade 28, 140
  - source address
    - ping command 121
    - traceRoute command 126
  - state
    - IP interface characteristics 64
  - static routes 16
    - advantages 17
    - defining 68
    - disadvantages 17
  - statistics
    - baselining 84
    - general OSPF 113
    - RIP 117
  - status
    - routing table entry 66
  - stub area
    - default metric value 107
    - OSPF areas 85
  - subnet masks
    - IP interface characteristics 63
    - routing table entry 66
  - troubleshooting 136
  - SuperStack II Switch Matrix module 23
  - switches
    - stacking 24
  - system
    - default console timeout value 50
    - default values 33
  - system commands
    - consoleTimeout interval 50
    - consoleTimeout timeOut 50
    - display 48
    - initialize 55
    - name 51
    - nvData restore 54
    - nvData save 53
    - password 51
    - reset 56, 143
    - softwareUpgrade 49
  - system configuration
    - displaying 48
  - system consoleTimeout interval 50
  - system context
    - available commands 48
  - system name
    - setting 51
- 
- T**
- target router ID 108
  - target routers
    - modifying for virtual links 111
  - technical support
    - 3Com Knowledgebase Web Services 145
    - 3Com URL 145
    - bulletin board service 146
    - fax service 146
    - network suppliers 147
    - product repair 149
  - telnet
    - default password 33
    - rebooting the system 56
  - telnet timeout 50
    - interval 50
  - terminology 9
  - testing
    - layer 3 module self test 30
  - TFTP
    - using to install 49
  - Time To Live. *See* TTL
  - timeout
    - enabling for remote sessions 50
  - timeout interval
    - setting 50



- traceRoute
    - advanced options 125
    - commands 123
    - default values 125
    - numeric format 125, 126
    - packet size 125
    - port 125
    - probe count 125
    - responses 123
    - source address 126
    - ttl 125
    - using 123
    - wait 125
  - transit area ID 108
  - transmit delay
    - modifying for virtual link 111
    - OSPF interfaces 94
  - trap reporting
    - configuring destinations 46
    - displaying 46
    - flushing addresses 47
    - removing destinations 47
  - Trivial File Transfer Protocol. See TFTP
  - troubleshooting
    - admin password setting 136
    - bridge vlan summary 132
    - changing VLAN 1 IP address on Layer 3 module 134
    - contacting Layer 3 Module from VLANs 134
    - contacting Layer 3 module IP address 131
    - ip interface summary 136
    - Layer 3 module 129 to 136
    - module status LED 131
    - moving the module between switches 133
    - multicast routing 134, 135
    - OSPF network 135
    - restoring configurations 133
    - URL.DLL errors 136
    - using LEDs 35, 130
    - variable length subnet masks 136
  - TTL
    - threshold 79
  - ttl option
    - traceRoute command 125
    - removing forwarding addresses 75
    - removing port numbers 75
    - setting BOOTP hop count limit 76
    - setting BOOTP relay threshold 76
  - unicast addresses 77
  - Uniform Resource Locator. See URL
  - upgrading
    - system software 49
  - URL 145
  - URL.DLL errors 136
  - User Datagram Protocol. See UDP
  - user interface
    - access levels 39
    - accessing 39
  - using
    - IP management interface 39
    - LEDs 130
    - NV data 52
    - traceRoute 123
- 
- V**
- variable length subnet masks 136
  - Virtual LANs. See VLANs
  - virtual links 107
    - dead interval 113
    - defining 110
    - displaying 108
    - displaying statistics 109
    - modifying area IDs 111
    - modifying target routers 111
    - modifying transmit delay 111
    - passwords 113
    - removing 110
    - retransmit interval 112
    - setting hello timer 112
  - VLAN indexes 57
    - IP interface characteristics 64
  - VLANs 63
    - adding 19, 21
    - contacting Layer 3 module from 134
    - displaying summary 57
    - heavy traffic 24
    - index 64
- 
- U**
- UDP 123
  - UDP helper 14
    - administering 74
    - defining forwarding addresses 75
    - defining port numbers 75
    - displaying information 74
- 
- W**
- wait interval
    - ping command 120
    - traceRoute command 125
  - web
    - default password 33
  - web interface

menu tree 42  
overview 41  
tabs panel 42  
workspace 42  
World Wide Web (WWW) 145

---

**Y**

Year 2000 compliance 137

# 3Com Corporation LIMITED WARRANTY

The duration of the warranty for the SuperStack® II Switch Layer 3 Module (3C16968) is 1 year.

---

## HARDWARE

3Com warrants its hardware products to be free from defects in workmanship and materials, under normal use and service, for the following lengths of time from the date of purchase from 3Com or its authorized reseller:

Network Interface Cards	Lifetime
Other hardware products *unless otherwise specified above	1 year*
Spare parts and spares kits	90 days

If a product does not operate as warranted above during the applicable warranty period, 3Com shall, at its option and expense, repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of 3Com. Replacement products may be new or reconditioned. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

---

## SOFTWARE

3Com warrants that the software programs licensed from it will perform in substantial conformance to the program specifications therefor for a period of ninety (90) days from the date of purchase from 3Com or its authorized reseller. 3Com warrants the media containing software against failure during the warranty period. No updates are provided. 3Com's sole obligation with respect to this express warranty shall be (at 3Com's discretion) to refund the purchase price paid by Customer for any defective software products, or to replace any defective media with software which substantially conforms to applicable 3Com published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. 3Com makes no warranty or representation that its software products will meet Customer's requirements or work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third party products listed in the 3Com software product documentation or specifications as being compatible, 3Com will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a "bug" or defect in the third party's product.

---

## YEAR 2000 WARRANTY

In addition to the Hardware Products Warranty and Software Products Warranty identified above, 3Com warrants that all Heritage 3Com products sold or licensed to Customer on and after January 1, 1998 that are date sensitive will continue performing properly with regard to such date data on and after January 1, 2000, provided that all other products used by Customer in connection or combination with the 3Com products, including hardware, software, and firmware, accurately exchange date data with the 3Com products, with the exception of those products identified at 3Com's Web site, <http://www.3com.com/products/yr2000.html>, as not meeting this standard. A product is considered a "Heritage 3Com product" if it is a member of a product family which was manufactured by 3Com prior to its merger with US Robotics Corporation. This Year 2000 limited warranty does not apply to Heritage US Robotics Corporation products. If it appears that any such product does not perform properly with regard to such date data on and after January 1, 2000, and Customer notifies 3Com before the later of April 1, 2000, or ninety (90) days after purchase of the product from 3Com or its authorized reseller, 3Com shall, at its option and expense, provide a software update which would effect the proper performance of such product, repair such product, deliver to Customer an equivalent product to replace such product, or if none of the foregoing is feasible, refund to Customer the purchase price paid for such product.

Any software update or replaced or repaired product will carry a Year 2000 Warranty for ninety (90) days or until April 1, 2000, whichever is later.

---

## OBTAINING WARRANTY SERVICE

Customer must contact 3Com's Corporate Service Center or an Authorized 3Com Service Center within the applicable warranty period to obtain warranty service authorization. Dated proof of purchase may be required. Products returned to 3Com's Corporate Service Center must be pre-authorized by 3Com with a Return Material Authorization (RMA) number marked on the outside of the package, and sent prepaid and packaged appropriately for safe shipment, and it is recommended that they be insured. The repaired or replaced item will be shipped to Customer, at 3Com's expense, not later than thirty (30) days after receipt of the defective product by 3Com.

*Dead- or Defective-on-Arrival.* In the event a product completely fails to function or exhibits a defect in materials or workmanship within the first forty-eight (48) hours of installation but no later than thirty (30) days after the date of purchase, and this is verified by 3Com, it will be considered dead- or defective-on-arrival (DOA) and a replacement shall be provided by advance replacement. The replacement product will normally be shipped not later than three (3) business days after 3Com's verification of the DOA product, but may be delayed due to export or import procedures. When an advance replacement is provided and Customer fails to return the defective product to 3Com within fifteen (15) days after shipment of the replacement, 3Com will charge Customer for the replacement product, at list price.

3Com shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to 3Com for repair, whether under warranty or not.

---

## **ADDITIONAL SERVICES**

*Telephone Support:* This OfficeConnect® or SuperStack® product comes with telephone technical support for ninety (90) days. The ninety (90) day period begins on the date of Customer's product purchase.

The telephone technical support is available from 3Com from 9 a.m. to 5 p.m., local time, Monday through Friday, excluding local holidays. Telephone technical support is limited to the 3Com products designated above and may include assistance with installation, product-specific configuration and identification of equipment problems. Please refer to the Technical Support Appendix in the User Guide for telephone numbers.

Response to requests for telephone technical support will be in the form of a return call from a 3Com representative by close of business on the *following* business day.

To qualify for this 90 days of telephone technical support, you must register on the 3Com Web site at: <http://support.3com.com/index.htm>

and provide your date of purchase, product number, and serial number. 3Com reserves the right to modify or cancel this telephone support offering at any time, without advance notice. This offer is not available where prohibited or restricted by law.

---

## **WARRANTIES EXCLUSIVE**

IF A 3COM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND SATISFACTORY QUALITY. 3COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

3COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

---

## **LIMITATION OF LIABILITY**

TO THE FULL EXTENT ALLOWED BY LAW, 3COM ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF 3COM OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

---

## **DISCLAIMER**

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

---

## **GOVERNING LAW**

This Limited Warranty shall be governed by the laws of the State of California, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

**3Com Corporation**, 5400 Bayfront Plaza, Santa Clara, CA 95052-8145 (408) 326-5000