



# **SuperStack® 3** Switch Implementation Guide

For units in the SuperStack 3 Switch 4900 Series

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

Part No. DUA1770-0BAA03  
Published October 2001



**3Com Corporation**  
**5400 Bayfront Plaza**  
**Santa Clara, California**  
**95052-8145**

Copyright © 2001, 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, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, 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.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

#### **UNITED STATES GOVERNMENT LEGEND**

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

All technical data and computer software are 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 and SuperStack are registered trademarks of 3Com Corporation. The 3Com logo and CoreBuilder are trademarks of 3Com Corporation.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

All other company and product names may be trademarks of the respective companies with which they are associated.

#### **ENVIRONMENTAL STATEMENT**

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

#### **End of Life Statement**

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

#### **Regulated Materials Statement**

3Com products do not contain any hazardous or ozone-depleting material.

#### **Environmental Statement about the Documentation**

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

# CONTENTS

---

## ABOUT THIS GUIDE

Conventions	10
Related Documentation	11
Documentation Comments	11
Product Registration	12

---

## 1 SWITCH FEATURES OVERVIEW

What is Management Software?	15
Switch Features Explained	15
BOOTP	15
Aggregated Links	16
Auto-negotiation	16
Multicast Filtering	17
Resilient Links	17
Spanning Tree Protocol	17
Switch Database	18
Traffic Prioritization	18
RMON	19
Broadcast Storm Control	19
VLANs	19
IP Routing	20

---

## 2 OPTIMIZING BANDWIDTH

Port Features	21
Duplex	21
Flow Control	22
Auto-negotiation	22
Smart Auto-sensing	22
Aggregated Links	23
Aggregated Links and Your Switch	24
Aggregated Link Example	26

---

### **3 USING MULTICAST FILTERING**

What is an IP Multicast?	27
Benefits of Multicast	28
Multicast Filtering	28
Multicast Filtering and Your Switch	29
IGMP Multicast Filtering	29

---

### **4 USING RESILIENCE FEATURES**

Resilience Feature Overview	31
What are Resilient Links?	32
Spanning Tree Protocol (STP)	33
What is STP?	33
How STP Works	35
STP Requirements	35
STP Calculation	36
STP Configuration	36
STP Reconfiguration	36
STP Example	37
STP Configurations	38
Using STP on a Network with Multiple VLANs	40

---

### **5 USING THE SWITCH DATABASE**

What is the Switch Database?	41
How Switch Database Entries Get Added	41
Switch Database Entry States	42

---

### **6 USING TRAFFIC PRIORITIZATION**

What is Traffic Prioritization?	43
How Traffic Prioritization Works	44
Traffic Prioritization and Your Switch	45
What is Quality of Service (QoS)?	45
QoS Benefits	45
QoS Terminology	46
QoS and Your Switch	46

---

## **7 STATUS MONITORING AND STATISTICS**

- RMON 49
  - What is RMON? 49
    - The RMON Groups 50
  - Benefits of RMON 51
  - RMON and the Switch 52
    - Alarm Events 53
    - The Default Alarm Settings 54
    - The Audit Log 54

---

## **8 SETTING UP VIRTUAL LANS**

- What are VLANs? 55
- Benefits of VLANs 56
- VLANs and Your Switch 57
  - The Default VLAN 57
  - Creating New VLANs 57
  - VLANs: Tagged and Untagged Membership 58
  - Placing a Port in a Single VLAN 58
  - Connecting VLANs to Other VLANs 59
- VLAN Configuration Examples 60
  - Using Untagged Connections 60
  - Using 802.1Q Tagged Connections 61

---

## **9 IP ROUTING**

- What is Routing? 63
  - Routing in a Subnetworked Environment 65
  - Integrating Bridging and Routing 66
  - Bridging and Routing Models 66
- What is IP Routing? 67
- Benefits of IP Routing 68
- IP Routing Concepts 68
  - Router Interfaces 68
  - Routing Tables 69
  - VLAN-based Routing 71
  - Multiple IP Interfaces per VLAN 72
- Implementing IP Routing 73

Configuring Trunks (Optional)	73
Configuring IP VLANs	73
Establishing IP Interfaces	73
IP Routing Protocols	75
Address Resolution Protocol (ARP)	75
ARP Proxy	77
Internet Control Message Protocol (ICMP)	78
Routing Information Protocol (RIP)	81
Domain Name System (DNS)	84
User Datagram Protocol (UDP) Helper	85
Advanced IP Routing Options	86
Access Control Lists	86
How Access Control List Rules Work	87

---

## **A CONFIGURATION RULES**

Configuration Rules for Gigabit Ethernet	91
Configuration Rules for Fast Ethernet	92
Configuration Rules with Full Duplex	93

---

## **B NETWORK CONFIGURATION EXAMPLES**

Network Configuration Examples	96
Improving the Resilience of Your Network	96
Enhancing the Performance of Your Network	97
Utilizing the Traffic Prioritization Features of Your Network	98

---

## **C IP ADDRESSING**

IP Addresses	99
Simple Overview	99
Advanced Overview	100
Subnets and Subnet Masks	102
Default Gateways	104
Standards, Protocols, and Related Reading	105
Requests For Comments (RFCs)	105
Standards Organizations	105

---

## **D ADVANCED IP ROUTING CONCEPTS**

Variable Length Subnet Masks (VLSMs) 107

Supernetting 108

---

## **GLOSSARY**

---

## **INDEX**





# ABOUT THIS GUIDE

This guide describes the features of the SuperStack® 3 Switch 4900 Series and outlines how to use these features to optimize the performance of your network.

Most features detailed in this guide are common to all Switches in the 4900 Series. Refer to the Getting Started Guide that accompanies your Switch for details of the specific features your Switch supports.

This guide is intended for the system or network administrator who is responsible for configuring, using, and managing the Switches. It assumes a working knowledge of local area network (LAN) operations and familiarity with communication protocols that are used to interconnect LANs.



*For detailed descriptions of the web interface operations and the command line interface (CLI) commands that you require to manage the Switch please refer to the Management Interface Reference Guide supplied in HTML format on the 3Com Web site.*



*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.*




Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the 3Com World Wide Web site:

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

## Conventions

[Table 1](#) and [Table 2](#) list conventions that are used throughout this guide.

**Table 1** Notice Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device
	Warning	Information that alerts you to potential personal injury

**Table 2** Text Conventions

Convention	Description
Screen displays	This typeface represents information as it appears on the screen.
Syntax	The word “syntax” means that you must evaluate the syntax provided and then supply the appropriate values for the placeholders that appear in angle brackets. Example:  To change your password, use the following syntax:  <code>system password &lt;password&gt;</code>  In this example, you must supply a password for <password>.
<b>Commands</b>	The word “command” means that you must enter the command exactly as shown and then press Return or Enter. Commands appear in bold. Example:  To display port information, enter the following command:  <b>bridge port detail</b>
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says “type.”
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example:  Press Ctrl+Alt+Del
Words in <i>italics</i>	Italics are used to: <ul style="list-style-type: none"> <li>■ Emphasize a point.</li> <li>■ Denote a new term at the place where it is defined in the text.</li> <li>■ Identify menu names, menu commands, and software button names. Examples:  From the <i>Help</i> menu, select <i>Contents</i>.  Click <i>OK</i>.</li> </ul>

---

## Related Documentation

In addition to this guide, each Switch documentation set includes the following:

- *Getting Started Guide*

This guide contains:

- a list of the features supported by the Switch
- all the information you need to install and set up the Switch in its default state
- information on how to access the management software to begin managing the Switch.

- *Management Interface Reference Guide*

This guide contains information about the web interface operations and CLI (command line interface) commands that enable you to manage the Switch. It contains an explanation for each command and the different parameters available. It is supplied in HTML format on the 3Com Web site.

- *Management Quick Reference Guide*

This guide contains a summary of the web interface operations and CLI commands that enable you to manage the Switch.

- *Release Notes*

These notes provide information about the current software release, including new features, modifications, and known problems.

In addition, there are other publications you may find useful:

- Documentation accompanying the Expansion Modules.
- Documentation accompanying the Advanced Redundant Power System.

---

## Documentation Comments

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 contacting us:

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

Example:

- SuperStack 3 Switch Implementation Guide
- Part number: DUA1770-0BAA02
- Page 25



*Please note that we can only respond to comments and questions about 3Com product documentation at this e-mail address. Questions related to technical support or sales should be directed in the first instance to your network supplier.*

---

## **Product Registration**

You can now register your SuperStack 3 Switch on the 3Com web site:

<http://support.3com.com/registration/frontpg.pl>



# SWITCH FEATURES

- [Chapter 1](#) [Switch Features Overview](#)
- [Chapter 2](#) [Optimizing Bandwidth](#)
- [Chapter 3](#) [Using Multicast Filtering](#)
- [Chapter 4](#) [Using Resilience Features](#)
- [Chapter 5](#) [Using the Switch Database](#)
- [Chapter 6](#) [Using Traffic Prioritization](#)
- [Chapter 7](#) [Status Monitoring and Statistics](#)
- [Chapter 8](#) [Setting Up Virtual LANs](#)
- [Chapter 9](#) [IP Routing](#)





# 1

## SWITCH FEATURES OVERVIEW

This chapter contains introductory information about the SuperStack® 3 Switch management software and supported features. It covers the following topics:

- [What is Management Software?](#)
- [Switch Features Explained](#)

---

### What is Management Software?

Your Switch can operate in its default state. However, to make full use of the features offered by the Switch, and to change and monitor the way it works, you have to access the management software that resides on the Switch. This is known as managing the Switch.

Managing the Switch can help you to improve its efficiency and therefore the overall performance of your network.

There are several different methods of accessing the management software to manage the Switch. These methods are explained in Chapter 3 of the Getting Started Guide that accompanies your Switch.

---

### Switch Features Explained

The management software provides you with the capability to change the default state of some of the Switch features. This section provides a brief overview of these features — their applications are explained in more detail later in this guide.



*For a list of the features supported by your Switch, please refer to Chapter 1 of the Getting Started Guide that accompanies your Switch.*

### BOOTP

If you have a BOOTP server on your network you can input the Switch MAC address on the BOOTP server so it will automatically identify the unit and allocate IP information.

**Aggregated Links** Aggregated links are connections that allow devices to communicate using up to four links in parallel. Aggregated links provide two benefits:

- They can potentially double, triple or quadruple the bandwidth of a connection.
- They can provide redundancy — if one link is broken, the other links share the traffic for that link.



*For more information about aggregated links, see [Chapter 2 “Optimizing Bandwidth”](#).*

**Auto-negotiation** Auto-negotiation allows ports to auto-negotiate port speed, duplex-mode (only at 10 Mbps and 100 Mbps) and flow control. When auto-negotiation is enabled (default), a port “advertises” its maximum capabilities — these capabilities are by default the parameters that provide the highest performance supported by the port.



*1000BASE-SX ports do not support auto-negotiation of port speed.*



*Ports operating at 1000 Mbps only support full duplex mode.*



*For details of the auto-negotiation features supported by your Switch, please refer to the Getting Started Guide that accompanies your Switch.*

### **Duplex**

Full duplex mode allows packets to be transmitted and received simultaneously and, in effect, doubles the potential throughput of a link.

### **Flow Control**

All Switch ports support flow control, which is a mechanism that minimizes packet loss during periods of congestion on the network.

Flow control is supported on ports operating in half duplex mode, and is implemented using the IEEE 802.3x standard on ports operating in full duplex mode.

### **Smart Auto-sensing**

Smart auto-sensing allows auto-negotiating multi-speed ports, such as 10/100 Mbps or 100/1000 Mbps, to monitor and detect high error rates, or problems in the “physical” interconnection to another port. The port



reacts accordingly by tuning the link from its higher speed to the lower supported speed to provide an error-free connection to the network.



*1000BASE-SX ports do not support smart auto-sensing.*



*For more information about auto-negotiation and port capabilities, see [Chapter 2 “Optimizing Bandwidth”](#).*

## Multicast Filtering

Multicast filtering allows the Switch to forward multicast traffic to only the endstations that are part of a predefined multicast group, rather than broadcasting the traffic to the whole network.

The multicast filtering system supported by your Switch uses IGMP (Internet Group Management Protocol) snooping to detect the endstations in each multicast group to which multicast traffic should be forwarded.



*For more information about multicast filtering, see [Chapter 3 “Using Multicast Filtering”](#).*

## Resilient Links

The resilient link feature enables you to protect critical links and prevent network downtime should those links fail. Setting up resilient links ensures that if a main communication link fails, a standby duplicate link automatically takes over the task of the main link. Each main and standby link pair is referred to as a resilient link pair.

Resilient links are a simple method of creating redundancy that provides you with a fast reaction to link failure. Resilient links are quick to set up, you have full control over their configuration, and the port at the other end of the resilient link does not have to support any resilience feature.



*For more information about resilient links, see [Chapter 4 “Using Resilience Features”](#).*

## Spanning Tree Protocol

Spanning Tree Protocol (STP) is a bridge-based system that makes your network more resilient to link failure and also provides protection from network loops — one of the major causes of broadcast storms.

STP allows you to implement alternative paths for network traffic in the event of path failure and uses a loop-detection process to:

- Discover the efficiency of each path.

- Enable the most efficient path.
- Disable the less efficient paths.
- Enable one of the less efficient paths if the most efficient path fails.



*For more information about STP, see [Chapter 4 “Using Resilience Features”](#).*

### **Switch Database**

The Switch Database is an integral part of the Switch and is used by the Switch to determine if a packet should be forwarded, and which port should transmit the packet if it is to be forwarded.



*For more information about the Switch Database, see [Chapter 5 “Using the Switch Database”](#).*

### **Traffic Prioritization**

Traffic prioritization allows time-sensitive and system-critical data, such as digital video and network-control signals, to be transferred smoothly and with minimal delay over a network. This data is assigned a high priority by the transmitting endstation and traffic prioritization allows high priority data to be forwarded through the Switch without being obstructed by lower priority data.

The system works by using the multiple traffic queues that are present in the hardware of the Switch — high priority data is forwarded on a different queue from lower priority data, and is given preference over the lower priority data.

This system is compatible with the relevant sections of the IEEE 802.1D/D17 standard (incorporating IEEE 802.1p).



*For more information about 802.1D and traffic prioritization, see [Chapter 6 “Using Traffic Prioritization”](#).*

### **Quality of Service**

Traffic prioritization can be taken one step further by using the Quality of Service (QoS) feature. Policy-based Quality of Service (QoS) enables you to specify service levels for different traffic classifications. This enables you to prioritize particular applications or traffic types. By default, all traffic is assigned the "normal" QoS policy profile. If needed, you can create other QoS policy profiles and apply them to different traffic types so that they have different priorities across the network.



For more information about Quality of Service, see [Chapter 6 “Using Traffic Prioritization”](#).

**RMON** Remote Monitoring (RMON) is a system that allows you to monitor LANs remotely. The Switch contains RMON probe software that continually collects statistics about the LAN segments connected to the Switch. If you have a management workstation with an RMON management application, the Switch can transfer these statistics to your workstation on request or when a pre-defined threshold is exceeded.



For more information about RMON, see [Chapter 7 “Status Monitoring and Statistics”](#).

**Broadcast Storm Control**

Broadcast Storm Control is a system that monitors the level of broadcast traffic on that port. If the broadcast traffic level rises to a pre-defined number of frames per second (threshold), the broadcast traffic on the port is blocked until the broadcast traffic level drops below the threshold. This system prevents the overwhelming broadcast traffic that can result from network equipment which is faulty or configured incorrectly.

**VLANs** A Virtual LAN (VLAN) is a flexible group of devices that can be located anywhere in a network, but which communicate as if they are on the same physical segment. With VLANs, you can segment your network without being restricted by physical connections — a limitation of traditional network design. As an example, with VLANs you can segment your network according to:

- Departmental groups
- Hierarchical groups
- Usage groups



For more information about VLANs, see [Chapter 8 “Setting Up Virtual LANs”](#).

**IP Routing** Routing is a method for distributing traffic throughout a network. It is used to join LANs at the network layer (Layer 3) of the OSI model. A router provides both filtering and bridging functions across the network and distributes packets over potentially dissimilar networks. Routers are used to:

- Connect enterprise networks.
- Connect subnetworks (or client/server networks) to the main enterprise network.

IP Routing is also referred to as Layer 3 routing as it relates to its place within the OSI model.



*For more information about Layer 3 Routing, see [Chapter 9 “IP Routing”](#).*

# 2

## OPTIMIZING BANDWIDTH

There are many ways you can optimize the bandwidth on your network and improve network performance. If you utilize certain Switch features you can provide the following benefits to your network and end users:

- Increased bandwidth
- Quicker connections
- Faster transfer of data
- Minimized data errors
- Reduced network downtime



*For detailed descriptions of the web interface operations and the command line interface (CLI) commands that you require to manage the Switch please refer to the Management Interface Reference Guide supplied in HTML format on the 3Com Web site.*

---

### Port Features

The default state for all the features detailed below provides the best configuration for a typical user. *In normal operation, you do not need to alter the Switch from its default state.* However, under certain conditions you may wish to alter the default state of these ports, for example, if you are connecting to old equipment that does not comply with the IEEE 802.3x standard.

#### Duplex

Full duplex allows packets to be transmitted and received simultaneously and, in effect, doubles the potential throughput of a link. Half duplex only allows packets to be transmitted or received at any one time.

To communicate effectively, both devices at either end of a link *must* use the same duplex mode. If the devices at either end of a link support auto-negotiation, this is done automatically. If the devices at either end of

a link do not support auto-negotiation, both ends must be manually set to full duplex or half duplex accordingly.



*Ports operating at 1000 Mbps support full duplex mode only.*

### Flow Control

All Switch ports support flow control, which is a mechanism that minimizes packet loss during periods of congestion on the network. Packet loss is caused by one or more devices sending traffic to an already overloaded port on the Switch. Flow control minimizes packet loss by inhibiting the transmitting port from generating more packets until the period of congestion ends.

Flow control is supported on ports operating in half duplex mode, and is implemented using the IEEE 802.3x standard on ports operating in full duplex mode.

### Auto-negotiation

Auto-negotiation allows ports to auto-negotiate port speed, duplex-mode (only at 10 Mbps and 100 Mbps) and flow control. When auto-negotiation is enabled (default), a port “advertises” its maximum capabilities — these capabilities are by default the parameters that provide the highest performance supported by the port.

You can disable auto-negotiation on all fixed ports on the Switch, or on a per port basis. You can also modify the capabilities that a port “advertises” on a per port basis, dependant on the type of port.



*1000BASE-SX ports do not support auto-negotiation of port speed.*



*Ports operating at 1000 Mbps support full duplex mode only.*

Conditions that affect auto-negotiation:

- Ports at both ends of the link must be set to auto-negotiate.
- 1000BASE-SX ports support auto-negotiation, however, the standard defines that 1000BASE-SX can only operate at 1000 Mbps, full duplex mode, so they can only auto-negotiate flow control.

### Smart Auto-sensing

Smart auto-sensing allows auto-negotiating multi-speed ports, such as 10/100 Mbps or 100/1000 Mbps, to monitor and detect a high error rate on a link, or a problem in the “physical” interconnection to another port and react accordingly. In other words, auto-negotiation may “agree”

upon a configuration that the link cannot sustain; smart auto-sensing can detect this and adjust the link accordingly.

For example, smart auto-sensing can detect network problems, such as an unacceptably high error rate or a poor quality cable. If both ends of the link support 100/1000 Mbps auto-negotiation, then auto-sensing tunes the link to 100 Mbps to provide an error-free 100 Mbps connection to the network. An SNMP Trap is sent every time a port is down-rated to a lower speed. Conditions that affect smart auto-sensing:

- Smart auto-sensing will not operate on links that do not support auto-negotiation, or on links where one end is at a fixed speed. The link will reset to the higher speed of operation when the link is lost or the unit is power cycled.
- Smart auto-sensing cannot be configured on a per port basis.



*1000BASE-SX ports do not support smart auto-sensing.*

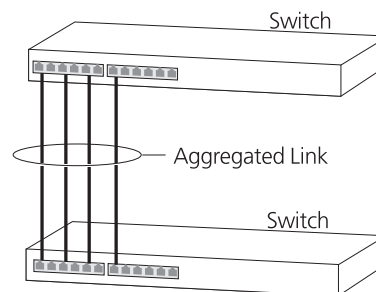
## Aggregated Links

Aggregated links are connections that allow devices to communicate using up to four links in parallel. These parallel links provide two benefits:

- They can potentially double, triple or quadruple the bandwidth of a connection.
- They can provide redundancy — if one link is broken, the other links share the traffic for that link.

[Figure 1](#) shows two Switches connected using an aggregated link containing four links. If all ports on both Switch units are configured as 100BASE-TX and they are operating in full duplex, the potential maximum bandwidth of the connection is 800 Mbps.

**Figure 1** Switch units connected using an aggregated link



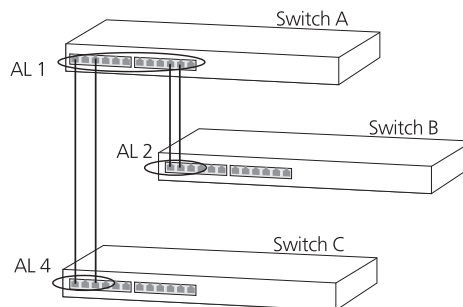
## Aggregated Links and Your Switch

Each Switch supports up to four aggregated links. Each aggregated link can support up to four member links.

When setting up an aggregated link, note that:

- The ports at both ends of a member link must be configured as members of an aggregated link.
- A member link port can only belong to one aggregated link.
- The member link ports can be mixed media, that is fiber and/or twisted pair ports within the same aggregated link.
- The member link ports can have different port configurations within the same aggregated link, that is, auto-negotiation, port speed, and duplex mode. However, please note the following:
  - To be an active participant in an aggregated link the member link ports must operate in full duplex mode. (If a member link port does not operate in full duplex mode it can still be a member of an aggregated link but it will never be activated.)
  - If ports of a different speed are aggregated together, the higher speed links carry the traffic. The lower speed links only carry the traffic if the higher speed links fail.
- The aggregated link does not support security, resilient links, or HTTP traffic (Layer 4) redirection to a Webcache.
- Member links must retain the same groupings at both ends of an aggregated link. For example, the configuration in [Figure 2](#) will not work as Switch A has one aggregated link defined whose member links are then split between two aggregated links defined on Switches B and C.

**Figure 2** An illegal aggregated link configuration





To make this configuration work you need to have two aggregated links defined on Switch A, one containing the member links for Switch B and the other containing those for Switch C.

When using an aggregated link, note that:

- To gather statistics about an aggregated link, you must add together the statistics for each port in the aggregated link.
- If you wish to disable a single member link of an aggregated link, you must first physically remove the connection to ensure that you do not lose any traffic, before you disable both ends of the member link separately. If you do this, the traffic destined for that link is distributed to the other links in the aggregated link.

If you do not remove the connection and only disable one end of the member link port, traffic is still forwarded to that port by the aggregated link port at the other end. This means that a significant amount of traffic may be lost.

- Before removing all member links from an aggregated link, you must disable all the aggregated link member ports or disconnect all the links, except one — if you do not, a loop may be created.

### **Traffic Distribution and Link Failure on Aggregated Links**

To maximize throughput, all traffic is distributed across the individual links that make up an aggregated link. Therefore, when a packet is made available for transmission down an aggregated link, a hardware-based traffic distribution mechanism determines which particular port in the link should be used. The mechanism may use the MAC address, IP address, or a combination of both dependant upon the mode of operation. The traffic is distributed among the member links as efficiently as possible.

To avoid the potential problem of out-of-sequence packets (or “packet re-ordering”), the Switch ensures that all the conversations between a given pair of endstations will pass through the same port in the aggregated link. Single-to-multiple endstation conversations, on the other hand, may still take place over different ports.

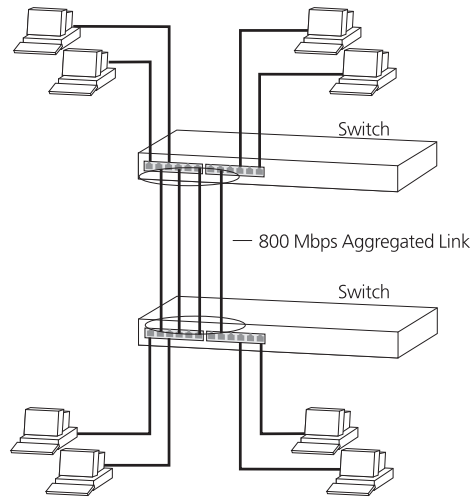
If the link state on any of the ports in an aggregated link becomes inactive due to link failure, then the Switch will automatically redirect the aggregated link traffic to the remaining ports. Aggregated links therefore provide built-in resilience for your network.

The Switch also has a mechanism to prevent the possible occurrence of packet re-ordering when a link recovers too soon after a failure.

### Aggregated Link Example

The example shown in [Figure 3](#) illustrates an 800 Mbps aggregated link between two Switch units.

**Figure 3** An 800 Mbps aggregated link between two Switch units



To set up this configuration:

- 1 Add the ports 2, 4, 6 and 8 on the upper unit to the aggregated link.
- 2 Add the ports 2, 4, 6 and 8 on the lower unit to the aggregated link.
- 3 Connect port 2 on the upper Switch to port 2 on the lower Switch.
- 4 Connect port 4 on the upper Switch to port 4 on the lower Switch.
- 5 Connect port 6 on the upper Switch to port 6 on the lower Switch.
- 6 Connect port 8 on the upper Switch to port 8 on the lower Switch.

# 3

## USING MULTICAST FILTERING

Multicast filtering improves the performance of networks that carry multicast traffic.

This chapter explains multicasts, multicast filtering, and how multicast filtering can be implemented on your Switch. It covers the following topics:

- [What is an IP Multicast?](#)
- [Multicast Filtering](#)
- [IGMP Multicast Filtering](#)



*For detailed descriptions of the web interface operations and the command line interface (CLI) commands that you require to manage the Switch please refer to the Management Interface Reference Guide supplied in HTML format on the 3Com Web site.*

---

### What is an IP Multicast?

A *multicast* is a packet that is intended for “one-to-many” and “many-to-many” communication. Users explicitly request to participate in the communication by joining an endstation to a specific multicast group. If the network is set up correctly, a multicast can only be sent to an endstation or a subset of endstations in a LAN, or VLAN, that belong to the relevant multicast group.

Multicast group members can be distributed across multiple subnetworks; thus, multicast transmissions can occur within a campus LAN or over a WAN. In addition, networks that support IP multicast send only *one* copy of the desired information across the network until the delivery path that reaches group members diverges. It is only at these points that multicast packets are replicated and forwarded, which makes efficient use of network bandwidth.

A multicast packet is identified by the presence of a multicast group address in the destination address field of the packet's IP header.

### Benefits of Multicast

The benefits of using IP multicast are that it:

- Enables the simultaneous delivery of information to many receivers in the most efficient, logical way.
- Reduces the load on the source (for example, a server) because it does not have to produce multiple copies of the same data.
- Makes efficient use of network bandwidth and scales well as the number of participants or collaborators expands.
- Works with other IP protocols and services, such as Quality of Service (QoS).

There are situations where a multicast approach is more logical and efficient than a unicast approach. Application examples include distance learning, transmitting stock quotes to brokers, and collaborative computing.

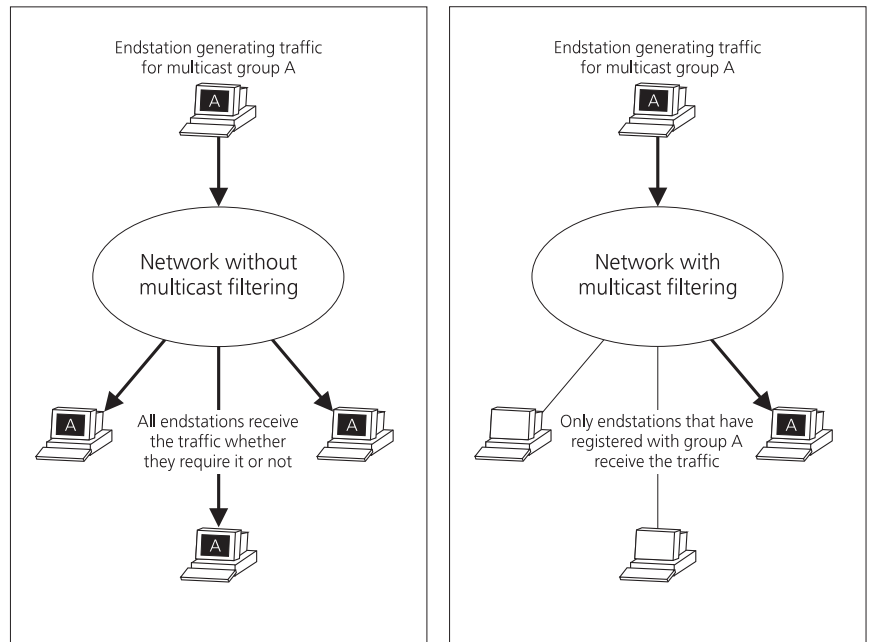
A typical use of multicasts is in video-conferencing, where high volumes of traffic need to be sent to several endstations simultaneously, but where broadcasting that traffic to all endstations would seriously reduce network performance.

---

### Multicast Filtering

Multicast filtering is the system by which endstations only receive multicast traffic if they register to join specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered endstations.

[Figure 4](#) shows how a network behaves without multicast filtering and with multicast filtering.

**Figure 4** The effect of multicast filtering

### Multicast Filtering and Your Switch

Your Switch provides automatic multicast filtering support using IGMP (Internet Group Management Protocol) Snooping.

#### Snooping Mode

Snooping Mode allows your Switch to forward multicast packets only to the appropriate ports. The Switch “snoops” on exchanges between endstations and an IGMP device, typically a router, to find out the ports that wish to join a multicast group and then sets its filters accordingly

---

### IGMP Multicast Filtering

IGMP is the system that all IP-supporting network devices use to register endstations with multicast groups. It can be used on all LANs and VLANs that contain a multicast capable IP router and on other network devices which support IP.

IGMP multicast filtering works as follows:

- 1 The IP router (or querier) periodically sends *query* packets to all the endstations in the LANs or VLANs that are connected to it.  
If your network has more than one IP router, then the one with the lowest IP address becomes the querier. The Switch can be the IGMP querier and will become so if its own IP address is lower than that of any other IGMP queriers connected to the LAN or VLAN.
- 2 When an IP endstation receives a query packet, it sends a *report* packet back that identifies the multicast group that the endstation would like to join.
- 3 When the report packet arrives at a port on a Switch with *IGMP multicast learning* enabled, the Switch learns that the port is to forward traffic for the multicast group and then forwards the packet to the router.
- 4 When the router receives the report packet, it registers that the LAN or VLAN requires traffic for the multicast groups.
- 5 When the router forwards traffic for the multicast group to the LAN or VLAN, the Switch units only forward the traffic to ports that received a report packet.

### Enabling IGMP Multicast Learning

You can enable or disable multicast learning and IGMP querying using the `snoopMode` command on the CLI or the web interface. For more information about enabling IGMP multicast learning, please refer to the Management Interface Reference Guide supplied on the 3Com Web site.

If IGMP multicast learning is not enabled then IP multicast traffic is always forwarded, that is, it floods the network.



*For information about configuring IGMP functionality on an endstation, refer to the user documentation supplied with your endstation or the endstation's Network Interface Card (NIC).*

# 4

## USING RESILIENCE FEATURES

Setting up resilience on your network helps protect critical links against failure, protects against network loops, and reduces network downtime to a minimum.

Features supported by the Switch that provide resilience for your network include:

- Resilient Links
- Spanning Tree Protocol (STP)



*For detailed descriptions of the web interface operations and the command line interface (CLI) commands that you require to manage the Switch please refer to the Management Interface Reference Guide supplied in HTML format on the 3Com Web site.*

---

### Resilience Feature Overview

Resilient links and STP cannot both be used on the network at the same time. [Table 3](#) lists the key differences between each feature, so you can evaluate the benefits of each to determine which feature is most suitable for your network.

**Table 3** Resilient Links and Spanning Tree Protocols — Key Differences

Resilient Links	Spanning Tree Protocol
User configures each Switch separately.	User enables or disables STP on each Switch.
Manual configuration.	Automatic configuration.
Within 5 seconds restores an active connection from a standby link.	Up to 30 second delay on link failure to restoring a network connection.

The Switch also supports aggregated links which increase bandwidth and also provide resilience against individual link failure. Aggregated links will operate with STP enabled, but will not operate on ports that are part of a

resilient link pair. For more information, see [Aggregated Links](#) on [page 23](#).

---

## What are Resilient Links?

The resilient link feature enables you to protect critical links and prevent network downtime if those links fail. A resilient link is comprised of a *resilient link pair* containing a main link and a standby link. If the main link fails, the standby link quickly and automatically takes over the task of the main link.

The resilient link pair is defined by specifying a main port and a standby port at one end of the link. During normal operation, the main port is enabled and the standby port is disabled. If the main link fails, the main port is disabled and the standby port is enabled. If the main link becomes operational, you can then re-enable the main port and disable the standby port again.

There are two user configurable modes of operation for resilient links:

- Symmetric (default) — the standby link remains as the main communication path even if the main link resumes normal operation.
- Switchback — the standby link continues as the main communication path until the main link resumes normal operation. The main communication path then switches back from the standby link to the main link.

When setting up resilient links, note the following:

- Resilient link pairs cannot be set up if the Switch has the Spanning Tree Protocol (STP) enabled.
- A resilient link pair must only be defined at one end of the link.
- A resilient link pair can only be set up if:
  - The ports use the same VLAN tagging system (802.1Q tagging).
  - Neither of the ports have security enabled.
  - Neither of the ports are part of an aggregated link.
  - Neither of the ports belong to another resilient link pair.
- The port state of ports in a resilient link pair cannot be manually changed.



---

## Spanning Tree Protocol (STP)

The Spanning Tree Protocol (STP) makes your network more resilient to link failure and also provides a protection from loops — one of the major causes of broadcast storms.

The following sections explain more about STP and the protocol features supported by your Switch. They cover the following topics:

- [What is STP?](#)
- [How STP Works](#)
- [Using STP on a Network with Multiple VLANs](#)



*The protocol is a part of the IEEE 802.1D bridge specification. To explain STP more effectively, your Switch will be referred to as a bridge.*

---

## What is STP?

STP is a bridge-based system that allows you to implement parallel paths for network traffic and uses a loop-detection process to:

- Find and disable the less efficient paths (that is, the paths that have a lower bandwidth).
- Enable one of the less efficient paths if the most efficient path fails.

As an example, [Figure 5](#) shows a network containing three LAN segments separated by three bridges. With this configuration, each segment can communicate with the others using two paths. Without STP enabled, this configuration creates loops that cause the network to overload.

**Figure 5** A network configuration that creates loops

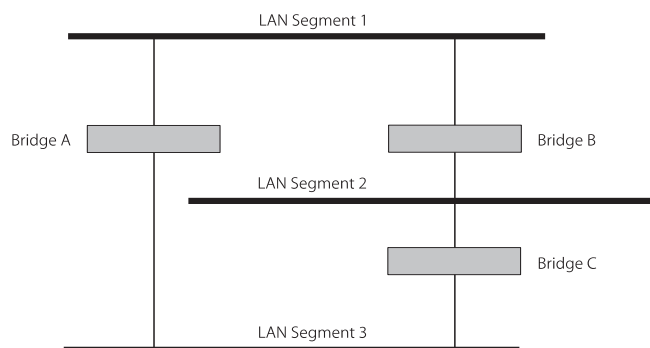
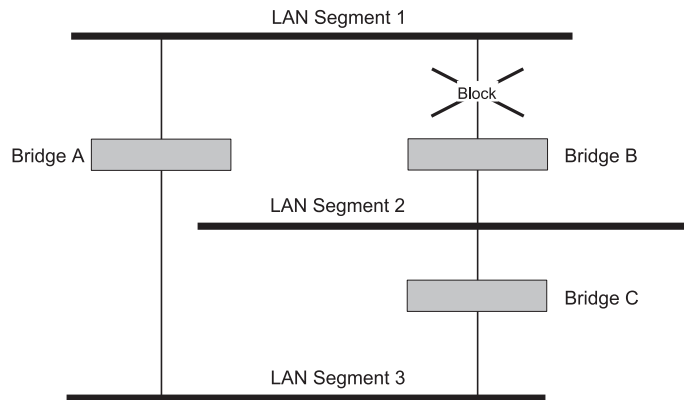


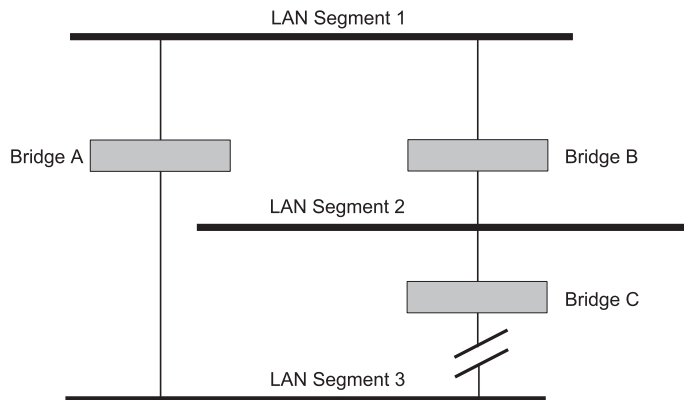
Figure 6 shows the result of enabling STP on the bridges in the configuration. STP detects the duplicate paths and prevents, or *blocks*, one of them from forwarding traffic, so this configuration will work satisfactorily. STP has determined that traffic from LAN segment 2 to LAN segment 1 can only flow through Bridges C and A, because, for example, this path has a greater bandwidth and is therefore more efficient.

**Figure 6** Traffic flowing through Bridges C and A



If a link failure is detected, as shown in Figure 7, the STP process reconfigures the network so that traffic from LAN segment 2 flows through Bridge B.

**Figure 7** Traffic flowing through Bridge B



STP determines which is the most efficient path between each bridged segment and a specifically assigned reference point on the network. Once

the most efficient path has been determined, all other paths are blocked. Therefore, in [Figure 5](#), [Figure 6](#), and [Figure 7](#), STP initially determined that the path through Bridge C was the most efficient, and so blocked the path through Bridge B. After the failure of Bridge C, STP re-evaluated the situation and opened the path through Bridge B.

---

## How STP Works

When enabled, STP determines the most appropriate path for traffic through a network. It does this as outlined in the sections below.

### STP Requirements

Before it can configure the network, the STP system requires:

- Communication between all the bridges. This communication is carried out using Bridge Protocol Data Units (BPDUs), which are transmitted in packets with a known multicast address.
- Each bridge to have a Bridge Identifier. This specifies which bridge acts as the central reference point, or Root Bridge, for the STP system — the lower the Bridge Identifier, the more likely the bridge is to become the Root Bridge. The Bridge Identifier is calculated using the MAC address of the bridge and a priority defined for the bridge. The default priority of your Switch is 32768.
- Each port to have a cost. This specifies the efficiency of each link, usually determined by the bandwidth of the link — the higher the cost, the less efficient the link. [Table 4](#) shows the default port costs for a Switch.

**Table 4** Default port costs

Port Type	Duplex	Cost
10 Mbps	Half	100
	Full	95
	Aggregated Link	90
100 Mbps	Half	19
	Full	18
	Aggregated Link	15
1000 Mbps	Full	4
	Aggregated Link	3

**STP Calculation** The first stage in the STP process is the calculation stage. During this stage, each bridge on the network transmits BPDUs that allow the system to work out:

- The identity of the bridge that is to be the Root Bridge. The Root Bridge is the central reference point from which the network is configured.
- The Root Path Costs for each bridge — that is, the cost of the paths from each bridge to the Root Bridge.
- The identity of the port on each bridge that is to be the Root Port. The Root Port is the one that is connected to the Root Bridge using the most efficient path, that is, the one that has the lowest Root Path Cost. Note that the Root Bridge does not have a Root Port.
- The identity of the bridge that is to be the Designated Bridge of each LAN segment. The Designated Bridge is the one that has the lowest Root Path Cost from that segment. Note that if several bridges have the same Root Path Cost, the one with the lowest Bridge Identifier becomes the Designated Bridge.

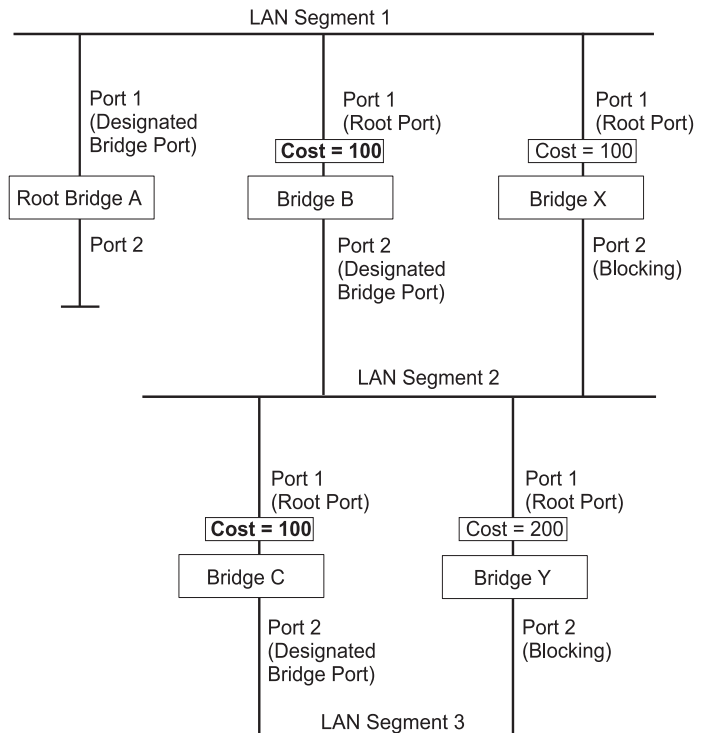
All traffic destined to pass in the direction of the Root Bridge flows through the Designated Bridge. The port on this bridge that connects to the segment is called the Designated Bridge Port.

**STP Configuration** After all the bridges on the network have agreed on the identity of the Root Bridge, and have established the other relevant parameters, each bridge is configured to forward traffic only between its Root Port and the Designated Bridge Ports for the respective network segments. All other ports are blocked, which means that they are prevented from receiving or forwarding traffic.

**STP Reconfiguration** Once the network topology is stable, all the bridges listen for Hello BPDUs transmitted from the Root Bridge at regular intervals. If a bridge does not receive a Hello BPDU after a certain interval (the Max Age time), the bridge assumes that the Root Bridge, or a link between itself and the Root Bridge, has gone down. The bridge then reconfigures the network to cater for the change. If you have configured an SNMP trap destination, when the topology of your network changes, the first bridge to detect the change sends out an SNMP trap.

**STP Example** [Figure 8](#) shows a LAN that has STP enabled. The LAN has three segments, and each segment is connected using two possible links.

**Figure 8** Port costs in a network



- Bridge A has the lowest Bridge Identifier in the network, and has therefore been selected as the Root Bridge.
- Because Bridge A is the Root Bridge, it is also the Designated Bridge for LAN segment 1. Port 1 on Bridge A is therefore selected as the Designated Bridge Port for LAN Segment 1.
- Port 1 of Bridges B, C, X and Y have been defined as Root Ports because they are the nearest to the Root Bridge and therefore have the most efficient path.
- Bridges B and X offer the same Root Path Cost for LAN segment 2, however, Bridge B has been selected as the Designated Bridge for the segment because it has a lower Bridge Identifier. Port 2 on Bridge B is therefore selected as the Designated Bridge Port for LAN Segment 2.

- Bridge C has been selected as the Designated Bridge for LAN segment 3, because it offers the lowest Root Path Cost for LAN Segment 3:
  - the route through Bridges C and B costs 200 (C to B=100, B to A=100)
  - the route through Bridges Y and B costs 300 (Y to B=200, B to A=100).

Port 2 on Bridge C is therefore selected as the Designated Bridge Port for LAN Segment 3.

**STP Configurations** [Figure 9](#) shows three possible STP configurations using SuperStack 3 Switch units.

- **Configuration 1 — Redundancy for Backbone Link**

In this configuration, the Switches both have STP enabled and are connected by two links. STP discovers a duplicate path and blocks one of the links. If the enabled link breaks, the disabled link becomes re-enabled, therefore maintaining connectivity.

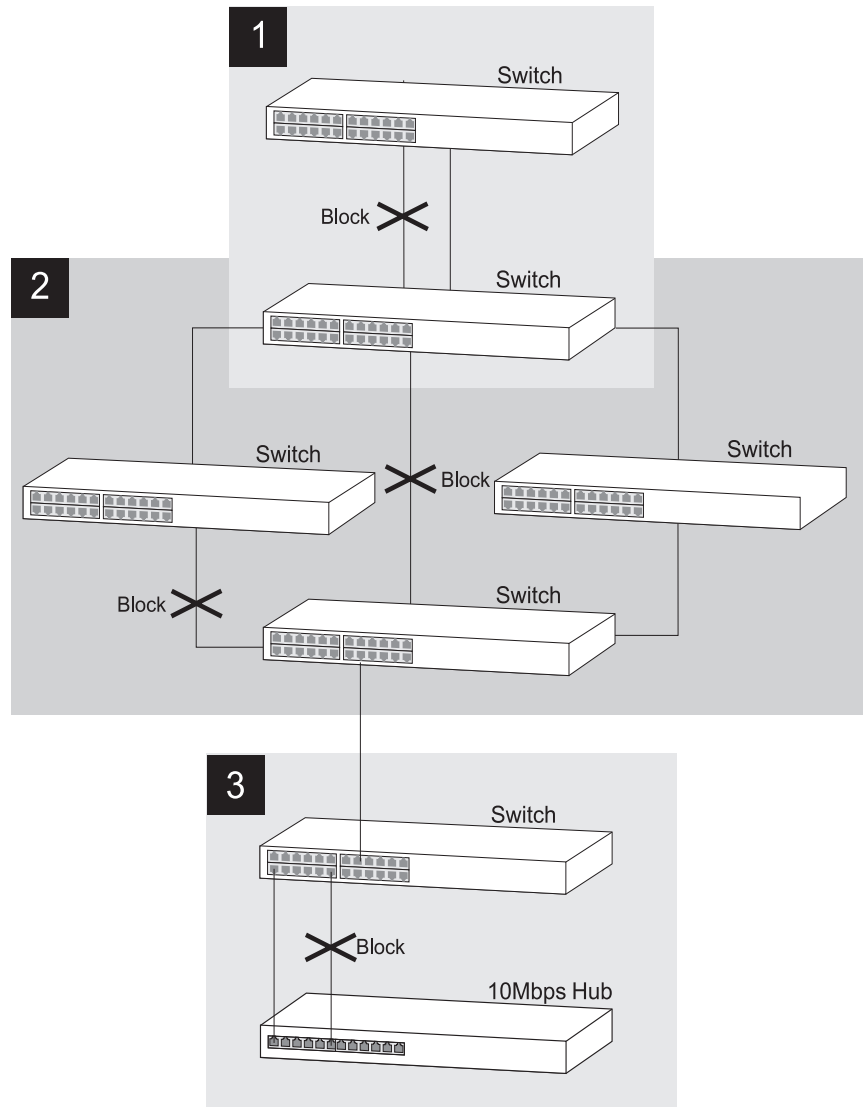
- **Configuration 2 — Redundancy through Meshed Backbone**

In this configuration, four Switch units are connected in a way that creates multiple paths between each one. STP discovers the duplicate paths and blocks two of the links. If an enabled link breaks, one of the disabled links becomes re-enabled, therefore maintaining connectivity.

- **Configuration 3 — Redundancy for Cabling Error**

In this configuration, a Switch has STP enabled and is accidentally connected to a hub using two links. STP discovers a duplicate path and blocks one of the links, therefore avoiding a loop.

Figure 9 STP configurations

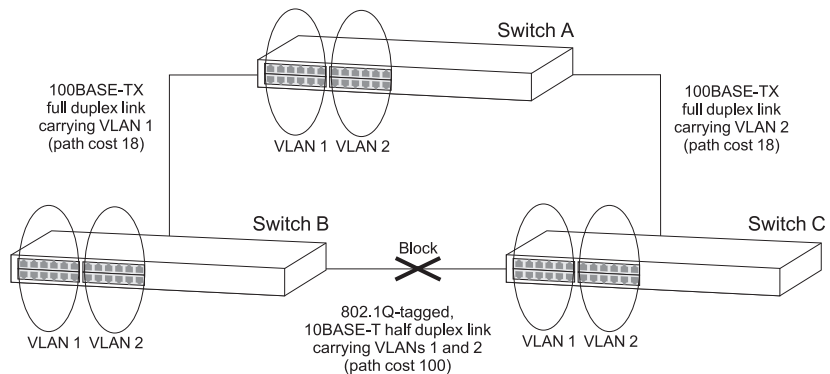


## Using STP on a Network with Multiple VLANs

Your Switch does not take into account VLANs when it calculates STP information — the calculations are only performed on the basis of physical connections. For this reason, some network configurations can result in VLANs being subdivided into a number of isolated sections by the STP system.

For example, [Figure 10](#) shows a network containing VLANs 1 and 2. They are connected using the 802.1Q-tagged link between Switch B and Switch C. By default, this link has a path cost of 100 and is automatically blocked because the other Switch-to-Switch connections have a path cost of 36 (18+18). This means that both VLANs are now subdivided — VLAN 1 on Switch units A and B cannot communicate with VLAN 1 on Switch C, and VLAN 2 on Switch units A and C cannot communicate with VLAN 2 on Switch B.

**Figure 10** Configuration that separates VLANs



To avoid any VLAN subdivision, 3Com recommends that all inter-Switch connections are made members of all available 802.1Q VLANs to ensure connectivity at all times. For example, the connections between Switches A and B, and between Switches A and C should be 802.1Q tagged and carrying VLANs 1 and 2 to ensure connectivity.



For more information about VLAN Tagging, see [Chapter 8 "Setting Up Virtual LANs"](#).



# 5

## USING THE SWITCH DATABASE

---

### What is the Switch Database?

The Switch Database is used by the Switch to determine where a packet should be forwarded to, and which port should transmit the packet if it is to be forwarded.

The database contains a list of entries — each entry contains three items:

- MAC (Ethernet) address information of the endstation that sends packets to the Switch.
- Port identifier, that is the port attached to the endstation that is sending the packet.
- VLAN ID of the VLAN to which the endstation belongs.



*For details of the number of addresses supported by your Switch database, please refer to Chapter 1 of the Getting Started Guide that accompanies your Switch.*



*For detailed descriptions of the web interface operations and the command line interface (CLI) commands that you require to manage the Switch please refer to the Management Interface Reference Guide supplied in HTML format on the 3Com Web site.*

---

### How Switch Database Entries Get Added

Entries are added to the Switch Database in one of two ways:

- The Switch can learn entries. The Switch updates its database with the source MAC address of the endstation that sent the packet, the VLAN ID, and the port identifier on which the packet is received.
- You can enter and update entries using the management interface, or an SNMP Network Manager.

---

## Switch Database Entry States

Databases entries can have three states:

- *Learned* — The Switch has placed the entry into the Switch Database when a packet was received from an endstation. Note that:
  - Learned entries are removed (aged out) from the Switch Database if the Switch does not receive further packets from that endstation within a certain period of time (the *aging time*). This prevents the Switch Database from becoming full with obsolete entries by ensuring that when an endstation is removed from the network, its entry is also removed from the database.
  - Learned entries are removed from the Switch Database if the Switch is reset or powered-down.
- *Non-aging learned* — If the aging time is set to 0 seconds, all learned entries in the Switch Database become non-aging learned entries. This means that they are not aged out, but they are still removed from the database if the Switch is reset or powered-down.
- *Permanent* — The entry has been placed into the Switch Database using the management interface. Permanent entries are not removed from the Switch Database unless they are removed using the Switch management interface or the Switch is initialized.

# 6

## USING TRAFFIC PRIORITIZATION

Using the traffic prioritization capabilities of your Switch allows you to prioritize your network traffic to ensure that high priority data is transmitted with minimum delay.

This chapter explains more about traffic prioritization.

- [What is Traffic Prioritization?](#)
- [What is Quality of Service \(QoS\)?](#)



*For a list of the features supported by your Switch, please refer to Chapter 1 of the Getting Started Guide that accompanies your Switch.*



*For detailed descriptions of the web interface operations and the command line interface (CLI) commands that you require to manage the Switch please refer to the Management Interface Reference Guide supplied in HTML format on the 3Com Web site.*

---

### What is Traffic Prioritization?

Traffic prioritization allows high priority data, such as time-sensitive and system-critical data to be transferred smoothly and with minimal delay over a network.



*The traffic prioritization feature supported by the Switch is compatible with the relevant sections of the IEEE 802.1D/17 standard (incorporating IEEE 802.1p).*

Traffic prioritization is most useful for critical applications that require a high Class of Service (CoS) from the network. These could include:

- **Converged network applications** — Used by organizations with a converged network, that is, a network that uses the same infrastructure for voice and video data and traditional data. Organizations that require high quality voice and video data transmission at all times can ensure this by maximizing bandwidth and providing low latency.

- **Resource planning applications** — Used by organizations that require predictable and reliable access to enterprise resource planning applications such as SAP.
- **Financial applications** — Used by Accounts departments that need immediate access to large files and spreadsheets.
- **CAD/CAM design applications** — Design departments that need priority connections to server farms and other devices for transferring large files.

### How Traffic Prioritization Works

Traffic prioritization ensures that high priority data is forwarded through the Switch without being delayed by lower priority data. It differentiates traffic into classes and prioritizes those classes automatically.

Traffic prioritization uses the multiple traffic queues that are present in the hardware of the Switch to ensure that high priority traffic is forwarded on a different queue from lower priority traffic, and is given preference over that traffic. This ensures that time-sensitive traffic gets the highest level of service.

The 802.1D standard specifies eight distinct levels of priority (0 to 7), each of which relates to a particular type (class) of traffic. The priority levels and their traffic types are shown in [Table 5](#).



*You cannot alter the mapping of the priorities as this is fixed (as defined in IEEE 802.1D).*

**Table 5** IEEE 802.1D Priority levels and traffic types

IEEE 802.1D Priority Level	IEEE 802.1D Traffic Type
0 (Default)	Best Effort
1	Background
2	Standard (spare)
3	Excellent Effort (business critical)
4	Controlled Load (streaming multimedia)
5	Video (Interactive media), less than 100 milliseconds latency and jitter.
6	Voice (Interactive voice), less than 10 milliseconds latency and jitter.
7	Network Control Reserved traffic

The transmitting endstation sets the priority of each packet. The Switch receives the packet from the endstation and is able to recognize and sort the packet into the appropriate queue depending on its priority level for onward transmission across the network. The Switch determines which queue to service next through its queuing mechanism.

### Traffic Prioritization and Your Switch

The Switch 4900 Series only has one priority queue set as default when QoS is disabled. This assumes that a network does not require any traffic prioritization, therefore all traffic is mapped to the same queue. This allows all the buffering to be allocated to the single queue.

When the Switch 4900 has QoS enabled the number of priority queues is automatically set to four.



*Queues cannot be enabled on a per-port basis.*

---

### What is Quality of Service (QoS)?

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic.

QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of your data and allows you to prioritize certain applications across your network. You can define exactly how you want your Switch to treat selected applications and types of traffic.



*QoS can be configured on your Switch via the Command Line Interface or the 3Com Network Supervisor application, which you can download from the following URL: <http://www.3com.com/tns>. 3Com recommends that for ease of use you configure QoS via the 3Com Network Supervisor application.*

### QoS Benefits

You can use QoS on your system to:

- Control a wide variety of network traffic by:
  - Classifying traffic based on packet attributes.
  - Assigning priorities to traffic (for example, to set higher priorities to time-critical or business-critical applications).
  - Applying security policy through traffic filtering.

- Provide predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improve performance for specific types of traffic and preserve performance as the amount of traffic grows.
- Reduce the need to constantly add bandwidth to the network.
- Manage network congestion.

### QoS Terminology

**Classifier** — classifies the traffic on the network. Traffic classifications are determined by protocol, application, source, destination, and so on. You can create and modify classifications. The Switch then groups classified traffic in order to schedule them with the appropriate service level.

**DiffServ Code Point (DSCP)** — is the traffic prioritization bits within an IP header that are encoded by certain applications and/or devices to indicate the level of service required by the packet across a network.

**Policy** — comprises a set of “rules” that are applied to a network so that a network meets the needs of the business. That is, traffic can be prioritized across a network according to its importance to that particular business type.

**QoS Profile** — consists of multiple sets of rules (classifier plus service level combinations). The QoS profile is assigned to a port(s).

**Rules** — comprises a service level and a classifier to define how the Switch will treat certain types of traffic. Rules are associated with a QoS Profile (see above).

**Service Level** — defines the priority that will be given to a set of classified traffic. You can create and modify service levels.

### QoS and Your Switch

Your Switch’s implementation of QoS focuses on policy-management. This means that you can select and prioritize particular applications. The Switch provides multiple service levels (mapped to transmit queues), and classification of traffic types.



*QoS can be configured on your Switch via the Command Line Interface or the 3Com Network Supervisor application, which you can download from the following URL: <http://www.3com.com/tns>. 3Com recommends that for ease of use you configure QoS via the 3Com Network Supervisor application.*

To implement QoS on your network, you need to carry out the following actions:

- 1 Define a service level to determine the priority that will be applied to traffic.
- 2 Apply a classifier to determine how the incoming traffic will be classified, and thus treated by the Switch.
- 3 Create a QoS profile which associates a service level and a classifier.
- 4 Apply a QoS profile to a port(s).

It is this QoS profile that constitutes the “rules” that determine how a particular traffic type is treated by your Switch.

### Using QoS Profiles

The Switch uses QoS profiles to determine how different traffic classifications should be treated, for example, how the traffic should be prioritized, remarked, and so on.

The QoS profile is set up on a per-Switch basis and is applied to each packet received on every port of that Switch. Only one QoS profile can be applied to each Switch.

A QoS profile should contain a minimum of one service level and classifier pair. However, a QoS profile may contain multiple service level and classifier pairs that can be applied to a port together.

The Switch 4900 Series only supports application-based classifiers. Application-based classifiers describe how to deal with packets for a specific application, for example, Voice over IP calls, Lotus Notes, and so on. Typically the application-based classifiers are the same on all ports in the network.

To disable QoS simply apply the “No Classifiers” profile.



*The active profile is the actual profile being applied to the hardware. The default profile is the profile that is applied to the hardware by default on power-up. When the Switch 4900 is reset, the active profile becomes the same as the default profile. Only the default profile is stored and only the active profile is applied to the device. This feature is useful when an external client changes the active profile regularly and requires that a well-known default be applied. Note that these two profiles can be*

accessed separately using SNMP only. The command line interface (CLI) treats the profiles as one.

See [“Utilizing the Traffic Prioritization Features of Your Network”](#) on [page 98](#) for a further network example.

## QoS Profile Components

**Traffic Classifiers** Traffic can be classified using one or more of the types of traffic classifiers listed in [Table 6](#) that the Switch recognizes. A classifier detects the packet attributes and classifies the traffic accordingly.

**Table 6** Types of Traffic Classifiers

Classifier	Packet Attributes
Layer 4 ports	Identifies application protocols, such as HTTP, SNMP (4 classifiers max).
DiffServ Code Point (DSCP)	Identifies packets by their DSCP

**Service Levels** Once traffic is classified, service levels can be applied to determine how the Switch treats classified packets. The Switch offers some predefined standard service levels, for example, best effort, business critical, network control, and so on.



# 7

## STATUS MONITORING AND STATISTICS

This chapter contains details of the Remote Monitoring ([RMON](#)) feature that assists you with status monitoring and statistics.



*For a list of the features supported by your Switch, please refer to Chapter 1 of the Getting Started Guide that accompanies your Switch.*

---

### RMON

Using the RMON capabilities of a Switch allows you to improve your network efficiency and reduce the load on your network.

This section explains more about RMON. It covers the following topics:

- [What is RMON?](#)
- [Benefits of RMON](#)
- [RMON and the Switch](#)



*You can only use the RMON features of the Switch if you have a management application that supports RMON, for example 3Com Network Supervisor.*

---

### What is RMON?

RMON is a system defined by the IETF (Internet Engineering Task Force) that allows you to monitor the traffic of LANs or VLANs.

RMON is an integrated part of the Switch software agent and continually collects statistics about a LAN segment or VLAN, and transfers the information to a management workstation on request or when a pre-defined threshold is crossed. The workstation does not have to be on the same network as the Switch and can manage the Switch by in-band or out-of-band connections.

**The RMON Groups** The IETF define groups of Ethernet RMON statistics. This section describes seven groups supported by the Switch, and details how you can use them.

### **Statistics**

The Statistics group provides traffic and error statistics showing packets, bytes, broadcasts, multicasts and errors on a LAN segment or VLAN.

Information from the Statistics group is used to detect changes in traffic and error patterns in critical areas of your network.

### **History**

The History group provides historical views of network performance by taking periodic samples of the counters supplied by the Statistics group.

The group is useful for analyzing the traffic patterns and trends on a LAN segment or VLAN, and for establishing the normal operating parameters of your network.

### **Alarms**

The Alarms group provides a mechanism for setting thresholds and sampling intervals to generate events on any RMON variable.

Alarms are used to inform you of network performance problems and they can trigger automated responses through the Events group.

### **Hosts**

The Hosts group specifies a table of traffic and error statistics for each host (endstation) on a LAN segment or VLAN. Statistics include packets sent and received, octets sent and received, as well as broadcasts, multicasts, and error packets received.

The group supplies a list of all hosts that have transmitted across the network.

### **Hosts Top N**

This group requires implementation of the Hosts group. The Hosts Top N group extends the Hosts table by providing sorted host statistics, such as the top 20 hosts sending packets or an ordered list of all hosts according to the errors they sent over the last 24 hours.

### Matrix

The Matrix group shows the amount of traffic and number of errors between pairs of devices on a LAN segment or VLAN. For each pair, the Matrix group maintains counters of the number of packets, number of octets, and number of error packets between the hosts.

The conversation matrix helps you to examine network statistics in more detail to discover, for example, who is talking to whom or if a particular PC is producing more errors when communicating with its file server. Combined with Hosts Top N, this allows you to view the busiest hosts and their primary conversation partners.

### Events

The Events group provides you with the ability to create entries in an event log and send SNMP traps to the management workstation. Events are the action that can result from an RMON alarm. In addition to the standard five traps required by SNMP (link up, link down, warm start, cold start, and authentication failure), RMON adds two more: rising threshold and falling threshold.

Effective use of the Events group saves you time; rather than having to watch real-time graphs for important occurrences, you can depend on the Event group for notification. Through the SNMP traps, events can trigger other actions, therefore providing a way to automatically respond to certain occurrences.

---

## Benefits of RMON

Using the RMON features of your Switch has three main advantages:

- **It improves your efficiency**

Using RMON allows you to remain at one workstation and collect information from widely dispersed LAN segments or VLANs. This means that the time taken to reach a problem site, set up equipment, and begin collecting information is largely eliminated.

- **It allows you to manage your network in a more proactive manner**

If configured correctly, RMON can deliver information before problems occur. This means that you can take action before they affect users. In addition, probes record the behavior of your network, so that you can analyze the causes of problems.

- **It reduces the load on the network and the management workstation**

Traditional network management involves a management workstation polling network devices at regular intervals to gather statistics and identify problems or trends. As network sizes and traffic levels grow, this approach places a strain on the management workstation and also generates large amounts of traffic.

RMON, however, autonomously looks at the network on behalf of the management workstation without affecting the characteristics and performance of the network. RMON reports by exception, which means that it only informs the management workstation when the network has entered an abnormal state.

---

## RMON and the Switch

The RMON support provided by your Switch is detailed in [Table 7](#).

**Table 7** RMON support supplied by the Switch

RMON group	Support supplied by the Switch
<b>Statistics</b>	A new or initialized Switch has one Statistics session per port and one default Statistics session for VLAN 1.
<b>History</b>	<p>A new or initialized Switch has two History sessions per port, and one default History session for VLAN 1.</p> <p>These sessions provide the data for the web interface history displays:</p> <ul style="list-style-type: none"> <li>■ 30 second intervals, 120 historical samples stored</li> <li>■ 2 hour intervals, 96 historical samples stored</li> </ul>
<b>Alarms</b>	<p>A new or initialized Switch has two alarms defined for each port:</p> <ul style="list-style-type: none"> <li>■ Broadcast bandwidth used.</li> <li>■ Percentage of errors over one minute</li> </ul> <p>You can modify these alarms using an RMON management application, but you cannot create or delete them.</p> <p>You can define up to 200 alarms for the Switch.</p> <p>For more information about the alarms setup on the Switch, see <a href="#">“Alarm Events”</a> on <a href="#">page 53</a> and <a href="#">“The Default Alarm Settings”</a> on <a href="#">page 54</a>.</p>
<b>Hosts</b>	Although Hosts is supported by the Switch, Hosts sessions are defined on VLANs only (default VLAN 1). There are no Hosts sessions defined on a new or initialized Switch.
<b>Hosts Top N</b>	Although Hosts Top N is supported by the Switch, there are no Hosts Top N sessions defined on a new or initialized Switch.

**Table 7** RMON support supplied by the Switch

RMON group	Support supplied by the Switch
<b>Matrix</b>	Although Matrix is supported by the Switch, Matrix sessions are defined on VLANs only (default VLAN 1). There are no Matrix sessions defined on a new or initialized Switch.
<b>Events</b>	A new or initialized Switch has Events defined for use with the default alarm system. See <a href="#">“The Default Alarm Settings”</a> on <a href="#">page 54</a> for more information.

When using the RMON features of the Switch, note the following:

- After the default sessions are created, they have no special status. You can delete or change them as required.
- The greater the number of RMON sessions, the greater the burden on the management resources of the Switch. If you have many RMON sessions, the forwarding performance of the Switch is not affected but you may experience slow response times from the web interface.

## Alarm Events

You can define up to 200 alarms for the Switch. The events that you can define for each alarm and their resulting actions are listed in [Table 8](#).

**Table 8** Alarm Events

Event	Action
<b>No action</b>	
<b>Notify only</b>	Send Trap.
<b>Notify and filter port</b>	Send Trap. Block broadcast and multicast traffic on the port. Recovers with the <i>unfilter port</i> event.
<b>Notify and disable port</b>	Send Trap. Turn port off.
<b>Notify and enable port</b>	Send Trap. Turn port on.
<b>Disable port</b>	Turn port off.
<b>Enable port</b>	Turn port on.
<b>Notify and switch resilient port</b>	Send Trap. If port is the main port of a resilient link pair then move to standby.
<b>Notify and unfilter port</b>	Send Trap. Stop blocking broadcast and multicast traffic on the port.
<b>System started</b>	
<b>Software Upgrade report</b>	

### The Default Alarm Settings

A new or initialized Switch has two alarms defined for each port:

- Broadcast bandwidth used.
- Percentage of errors over one minute

The default values and actions for each of these alarms are given in [Table 9](#).

**Table 9** Values for the default alarms

Statistic	High Threshold	Low Threshold Recovery	Period
Broadcast bandwidth used	Value: 20% Action: Notify and filter	Value: 10% Action: Notify and unfilter	30 secs
Number of errors over 10 seconds	Value: 8 errors per 10 seconds Action: Smart auto-sensing will reduce port speed	Value: 8 errors per 10 seconds Action: None. (Speed can only be increased upon link loss, for example by removing and replacing the cable, or by triggering the port to perform another auto-negotiation on that link.)	10 secs

### The Audit Log

The Switch keeps an audit log of all management user sessions, providing a record of a variety of changes, including ones relating to RMON. The log can only be read by users at the *security* access level using an SNMP Network Management application.

Each entry in the log contains information in the following order:

- Entry number
- Timestamp
- User ID
- Item ID (including qualifier)
- New value of item

The last 16 operations are stored in the audit log. The oldest records are overwritten first.

# 8

## SETTING UP VIRTUAL LANs

Setting up Virtual LANs (VLANs) on your Switch reduces the time and effort required by many network administration tasks, and increases the efficiency of your network.

This chapter explains more about the concept of VLANs and explains how they can be implemented on your Switch. It covers the following topics:

- [What are VLANs?](#)
- [Benefits of VLANs](#)
- [VLANs and Your Switch](#)
- [VLAN Configuration Examples](#)



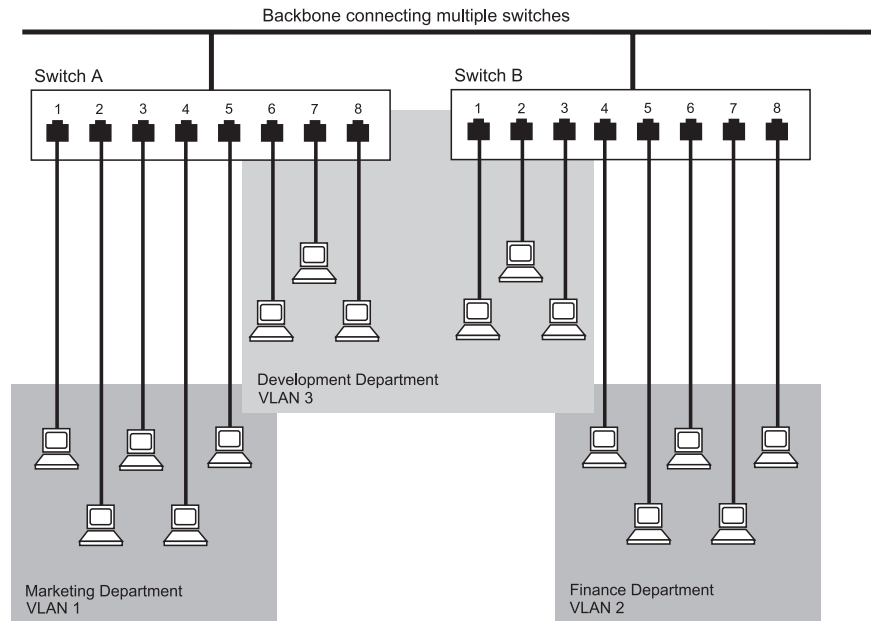
*For detailed descriptions of the web interface operations and the command line interface (CLI) commands that you require to manage the Switch please refer to the Management Interface Reference Guide supplied in HTML format on the 3Com Web site.*

---

### What are VLANs?

A VLAN is a flexible group of devices that can be located anywhere in a network, but which communicate as if they are on the same physical segment. With VLANs, you can segment your network without being restricted by physical connections — a limitation of traditional network design. As an example, with VLANs you can segment your network according to:

- **Departmental groups** — For example, you can have one VLAN for the Marketing department, another for the Finance department, and another for the Development department.
- **Hierarchical groups** — For example, you can have one VLAN for directors, another for managers, and another for general staff.
- **Usage groups** — For example, you can have one VLAN for users of e-mail, and another for users of multimedia.

**Figure 11** A network setup showing three VLANs

## Benefits of VLANs

The main benefit of VLANs is that they provide a network segmentation system that is far more flexible than any traditional network. Using VLANs also provides you with three other benefits:

- **VLANs ease the movement of devices on networks**

With traditional networks, network administrators spend much of their time dealing with moves and changes. If users move to a different subnetwork, the addresses of each endstation must be updated manually.

With a VLAN setup, if an endstation in VLAN *Marketing* for example is moved to a port in another part of the network, and retains its original subnet membership, you only need to specify that the new port is in VLAN *Marketing*. You do not need to carry out any re-cabling.

- **VLANs provide extra security**

Devices within each VLAN can only communicate with other devices in the same VLAN. If a device in VLAN *Marketing* needs to communicate with devices in VLAN *Finance*, the traffic must pass through a routing device or Layer 3 switch.



- **VLANs help to control traffic**

With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices whether they require it or not. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that need to communicate with each other.

---

## **VLANs and Your Switch**

Your Switch provides support for VLANs using the IEEE 802.1Q standard. This standard allows traffic from multiple VLANs to be carried across one physical link.

The IEEE 802.1Q standard allows each port on your Switch to be placed in:

- Any one VLAN defined on the Switch.
- Several VLANs at the same time using 802.1Q tagging.

The standard requires that you define the following information about each VLAN on your Switch before the Switch can use it to forward traffic:

- *VLAN Name* — This is a descriptive name for the VLAN (for example, Marketing or Management).
- *802.1Q VLAN ID* — This is used to identify the VLAN if you use 802.1Q tagging across your network.

### **The Default VLAN**

A new or initialized Switch contains a single VLAN, the Default VLAN. This VLAN has the following definition:

- *VLAN Name* — Default VLAN
- *802.1Q VLAN ID* — 1 (if tagging required)

All the ports are initially placed in this VLAN, and it is the only VLAN that allows you to access the management software of the Switch over the network.

### **Creating New VLANs**

If you want to move a port from the Default VLAN to another VLAN, you must first define information about the new VLAN on your Switch.

### **VLANs: Tagged and Untagged Membership**

Your Switch supports 802.1Q VLAN tagging, a system that allows traffic for multiple VLANs to be carried on a single physical (backbone) link.

When setting up VLANs you need to understand when to use untagged and tagged membership of VLANs. Quite simply, if a port is in a single VLAN it can be an untagged member but if the port needs to be a member of multiple VLANs tagged membership must be defined. Typically endstations (for example, clients or servers) will be untagged members of one VLAN, while inter-Switch connections will be tagged members of all VLANs.

The IEEE 802.1Q standard defines how VLANs operate within an open packet-switched network. An 802.1Q compliant packet carries additional information that allows a switch to determine to which VLAN the port belongs. If a frame is carrying the additional information, it is known as *tagged*.

To carry multiple VLANs across a single physical (backbone) link, each packet must be tagged with a VLAN identifier so that the Switches can identify which packets belong in which VLANs. To communicate between VLANs a router must be used.

### **Placing a Port in a Single VLAN**

Once the information for a new VLAN has been defined, you can place a port in that VLAN.

#### **Creating an IEEE 802.1Q Tagged Link**

This method of tagging is defined in the IEEE 802.1Q standard, and allows a link to carry traffic for any of the VLANs defined on your Switch. 802.1Q tagging can only be used if the devices at both ends of a link support IEEE 802.1Q.

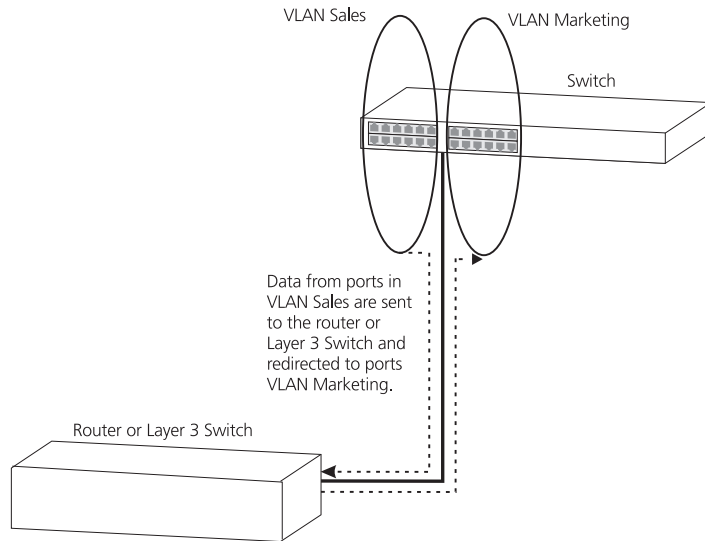
To create an 802.1Q tagged link:

- 1** Ensure that the device at the other end of the link uses the same 802.1Q tags as your Switch, that is, the same VLAN IDs are configured (note that VLAN IDs are global across the network).
- 2** Place the Switch ports in the required VLANs as tagged members.
- 3** Place the port at the other end of the link as a tagged member of the same VLANs as the port on your Switch.

## Connecting VLANs to Other VLANs

If the devices placed in a VLAN need to communicate to devices in a different VLAN, each VLAN requires a connection to a router or Layer 3 switching device. Communication between VLANs can only take place if they are all connected to a routing or Layer 3 switching device.

**Figure 12** Two VLANs connected via a router



## VLAN Configuration Examples

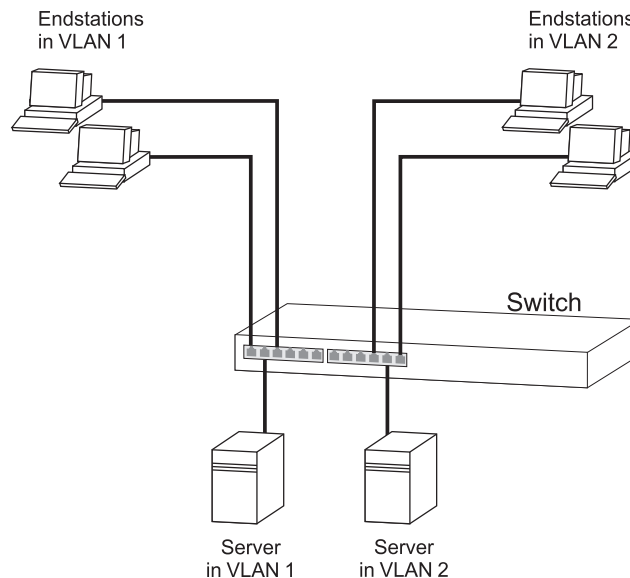
### Using Untagged Connections

This section contains examples of simple VLAN configurations. It describes how to set up your switch to support simple untagged and tagged connections.

The simplest VLAN operates in a small network using a single switch. In this network there is no requirement to pass traffic for multiple VLANs across a link. All traffic is handled by the single Switch and therefore untagged connections can be used.

The example shown in [Figure 13](#) illustrates a single Switch connected to endstations and servers using untagged connections. Ports 1, 2 and 3 of the Switch belong to VLAN 1, ports 10, 11 and 12 belong to VLAN 2. VLANs 1 and 2 are completely separate and cannot communicate with each other. This provides additional security for your network.

**Figure 13** VLAN configuration example: Using untagged connections



To set up the configuration shown in [Figure 13](#):

#### 1 Configure the VLANs

Create VLAN 2 on the Switch. VLAN 1 is the default VLAN and already exists.

## 2 Add ports to the VLANs

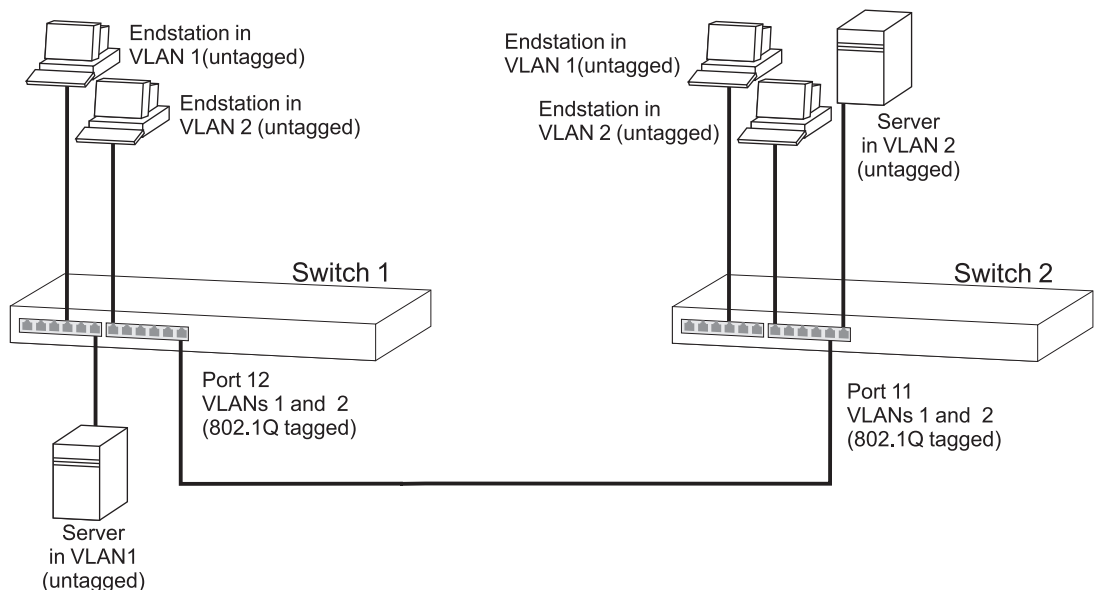
Add ports 10, 11 and 12 of the Switch as untagged members to VLAN 2.

### Using 802.1Q Tagged Connections

In a network where the VLANs are distributed amongst more than one Switch, you must use 802.1Q tagged connections so that all VLAN traffic can be passed along the links between the Switches.

The example shown in [Figure 14](#) illustrates two Switch units. Each switch has endstations and a server in VLAN 1 and VLAN 2. All endstations in VLAN 1 need to be able to connect to the server in VLAN1 which is attached to Switch 1 and all endstations in VLAN 2 need to connect to the server in VLAN2 which is attached to Switch 2.

**Figure 14** VLAN configuration example: 802.1Q tagged connections



To set up the configuration shown in [Figure 14](#):

### 1 Configure the VLANs on Switch 1

Define VLAN 2. VLAN 1 is the default VLAN and already exists.

### 2 Add endstation ports on Switch 1 to the VLANs

Place the endstation ports in the appropriate VLANs as untagged members.

**3 Add port 12 on Switch 1 to the VLANs**

Add port 12 on Switch 1 as a tagged member of both VLANs 1 and 2 so that all VLAN traffic is passed over the link to Switch 2.

**4 Configure the VLANs on Switch 2**

Define VLAN 2. VLAN 1 is the default VLAN and already exists.

**5 Add endstation ports on Switch 2 to the VLANs**

Place the endstation ports in the appropriate VLANs as untagged members.

**6 Add port 11 on Switch 2 to the VLANs**

Add port 11 on Switch 2 as a tagged member of both VLANs 1 and 2 so that all VLAN traffic is passed over the link to Switch 1.

**7 Check the VLAN membership for both switches**

The relevant ports should be listed in the VLAN members summary.

**8 Connect the switches**

Connect port 12 on Switch 1 to port 11 on Switch 2.

The VLANs are now configured and operational and the endstations in both VLANs can communicate with their relevant servers.

# 9

## IP ROUTING

Routing is a method for distributing traffic throughout a network. It is used to join LANs at the network layer (Layer 3) of the Open Systems Interconnection (OSI) model. A router provides both filtering and bridging functions across the network.

This chapter explains routers, protocols, and how your Switch allows bridges and routers to interoperate. It covers the following topics:

- [What is Routing?](#)
- [What is IP Routing?](#)
- [Benefits of IP Routing](#)
- [IP Routing Concepts](#)
- [Implementing IP Routing](#)
- [IP Routing Protocols](#)
- [Access Control Lists](#)

---

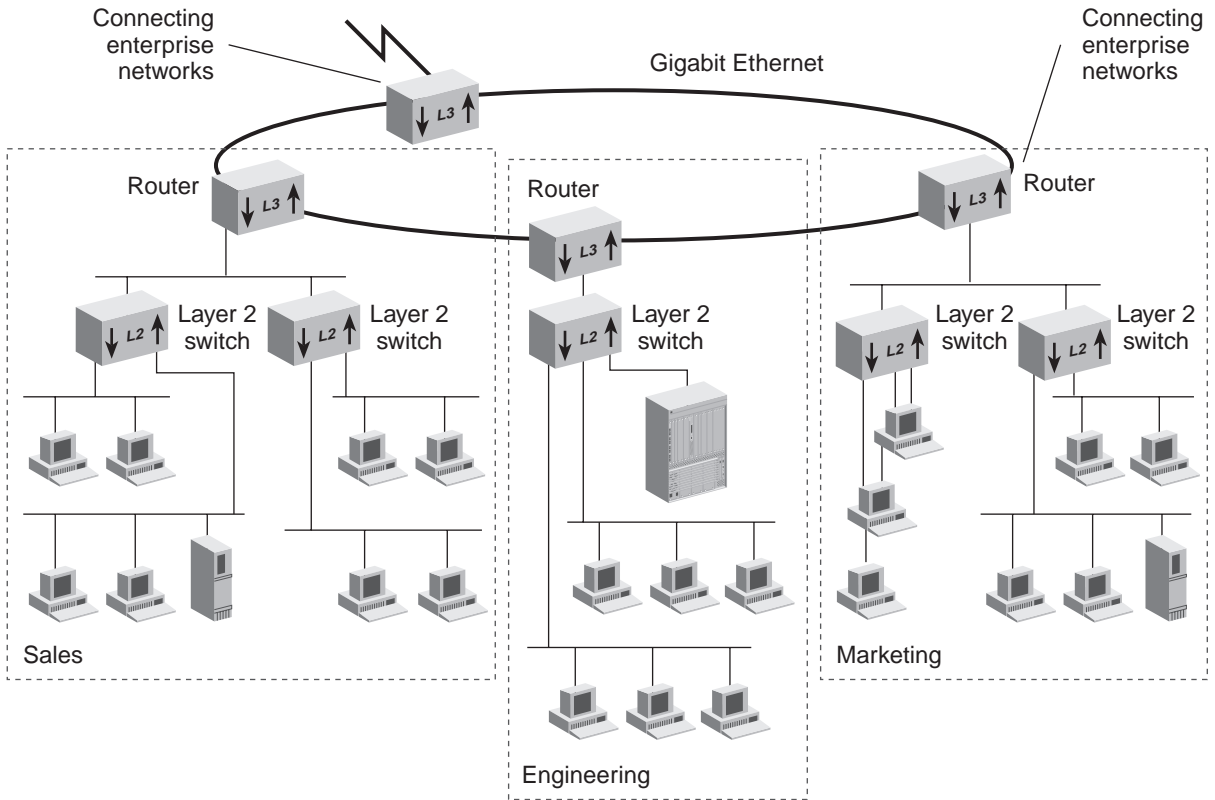
### What is Routing?

Routing distributes packets over potentially dissimilar networks. A router is the device that accomplishes this task. Your Switch, as a Layer 3 device, can act as a router. Routers typically:

- Connect enterprise networks.
- Connect subnetworks (or client/server networks) to the main enterprise network.

[Figure 15](#) shows where routers are typically used in a network. Routing connects subnetworks to the enterprise network, providing connectivity between devices within a workgroup, department, or building.

**Figure 15** Typical Routing Architecture

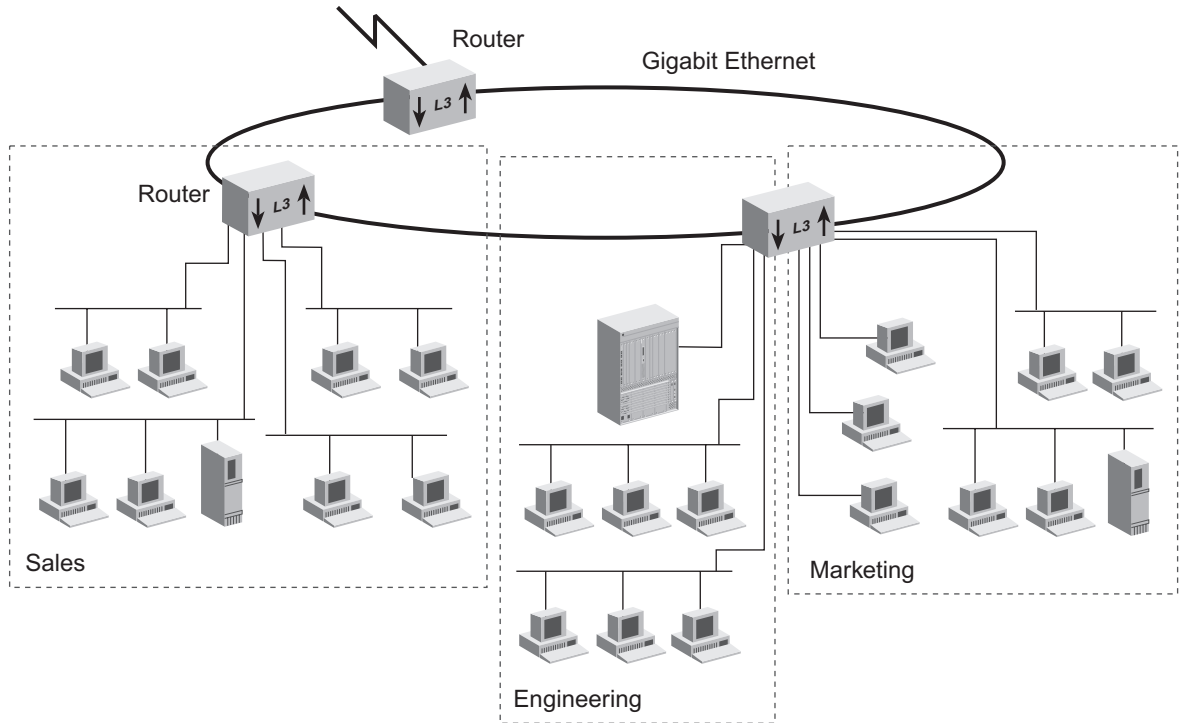




**Routing in a Subnetworked Environment**

Your Switch allows you to both perform routing and switching within your network. You can streamline your network architecture by routing between subnetworks and switching within subnetworks. See [Figure 16](#) for an example configuration.

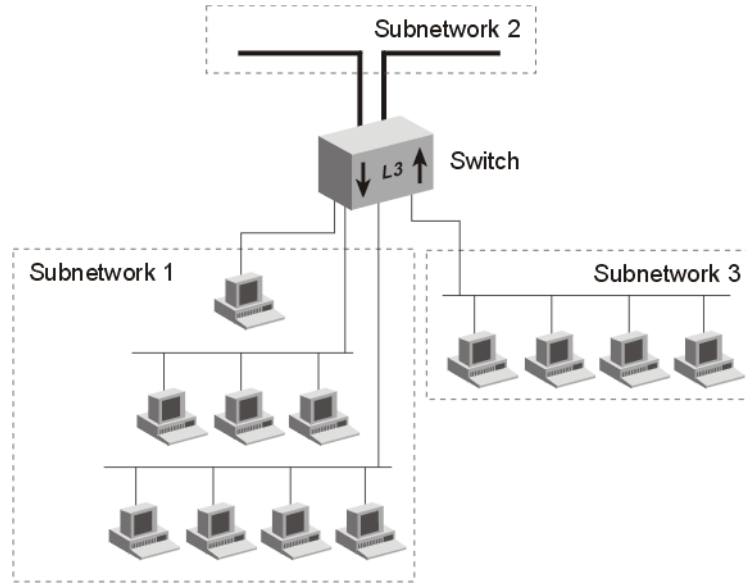
**Figure 16** Subnetwork Routing Architecture



## Integrating Bridging and Routing

Your Switch integrates bridging and routing. You can assign multiple ports to each subnetwork. See [Figure 17](#) for an example configuration.

**Figure 17** Multiple Ethernet Ports Per Subnetwork



Bridging switches traffic between ports that are assigned to the same subnetwork. Traffic traveling to different subnetworks is routed using one of the supported routing protocols.

## Bridging and Routing Models

Your Switch implements routing differently from the way bridges and routers usually coexist.

Traditionally, network systems first try to route packets that belong to recognized protocols; all other packets are bridged.

Your Switch first tries to determine if the packet is to be routed or switched. If the destination MAC address matches the MAC address of a router port on this Switch and the packet is not a protocol request to the Switch itself, then the packet is routed. However, if the destination MAC address is not the internal address for a port on this Switch, the packet is further examined to determine if it can be switched according to the IEEE 802.1D protocol.

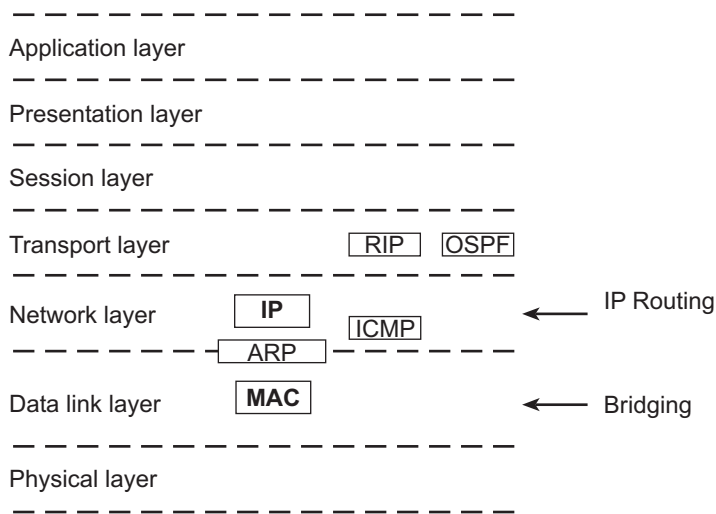
Route calculations are triggered during initialization and when changes are made in the network configuration. At that point the router determines the appropriate route and forwards to the switch information describing the path that is to be taken. Once the route has been determined, all packets in the current flow are simply switched or forwarded across the chosen path. This takes advantage of the high throughput and low latency characteristics of switching by enabling the traffic to bypass the routing software once path calculation has been performed.

**What is IP Routing?**

An IP router, unlike a bridge, operates at the network layer of the OSI Reference Model. The network layer is also referred to as Layer 3. An IP router routes packets by examining the network layer address (IP address). Bridges use data link layer MAC addresses to perform forwarding. See [Figure 18](#).

**Figure 18** OSI Reference Model and IP Routing

**OSI Reference Model**



When an IP router sends a packet, it does not know the complete path to a destination — only the next hop (the next device on the path to the destination). Each hop involves three steps:

- 1 The IP routing algorithm computes the *next hop* IP address and the next router interface, using routing table entries.
- 2 The Address Resolution Protocol (ARP) translates the next hop IP address into a physical MAC address.
- 3 The router sends the packet over the network across the next hop.

---

## Benefits of IP Routing

IP routing provides the following features and benefits:

- **Economy** — Because you can connect several segments to the same subnetwork with routing, you can increase the level of segmentation in your network without creating new subnetworks or assigning new network addresses. Instead, you can use additional Ethernet ports to expand existing subnetworks.
- **Optimal routing** — IP routing can be the most powerful tool in a complex network setup for sending devices to find the best route to receiving devices. (The best route here is defined as the shortest and fastest route.)
- **Resiliency** — If a router in the network goes down, the other routers update their routing tables to compensate for this occurrence; in a typical case, there is no need for you to manually intervene.

---

## IP Routing Concepts

IP routers use the following elements to transmit packets:

- [Router Interfaces](#)
- [Routing Tables](#)
- [VLAN-based Routing](#)
- [Multiple IP Interfaces per VLAN](#)

## Router Interfaces

A router interface connects the router to a subnetwork. On your Switch, more than one port can connect to the same subnetwork.

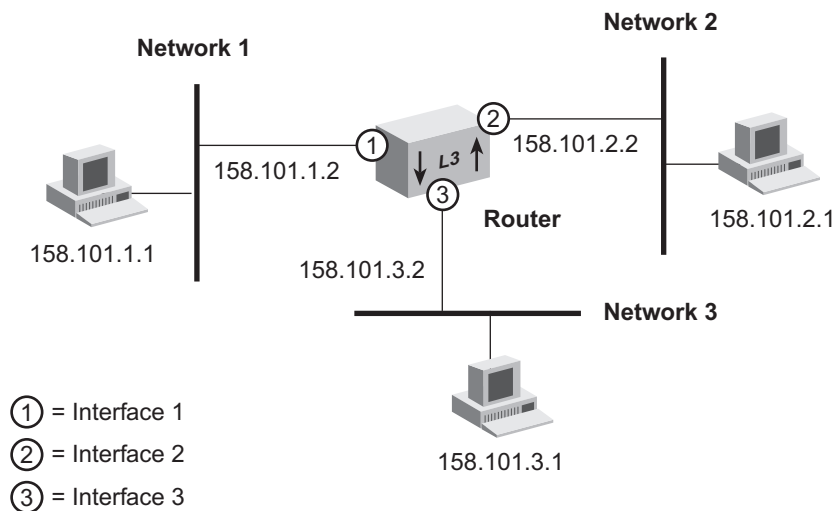
Each router interface has an IP address and a subnet mask. This router interface address defines both the number of the network to which the

router interface is attached and its host number on that network. A router interface IP address serves two functions:

- Sends IP packets to or from the router.
- Defines the network and subnetwork numbers of the segment that is connected to that interface.

Figure 19 shows an example of a router interface configuration.

**Figure 19** Routing Interfaces



To gain access to the Switch using TCP/IP or to manage the Switch using the Simple Network Management Protocol (SNMP), set up an IP interface to manage your system and at least one virtual LAN (VLAN). See [Chapter 8](#) for information about how to define a VLAN.

**Routing Tables** With a routing table, a router or host determines how to send a packet toward its ultimate destination. The routing table contains an entry for every learned and locally defined network. The size of the routing table is dynamic and can hold at least 2,000 entries.

A router or host uses the routing table when the destination IP address of the packet is not on a network or subnetwork to which it is directly connected. The routing table provides the IP address of a router that can forward the packet toward its destination.

The routing table consists of the following elements:

- **Destination IP address** — The destination network, subnetwork, or host.
- **Subnet mask** — The subnet mask for the destination network.
- **Metric** — A measure of the distance to the destination. In the Routing Information Protocol (RIP), the metric is the number of hops through routers.
- **Gateway** — The IP address of the router interface through which the packet travels on its next hop.
- **Status** — Information that the routing protocol has about the route, such as how the route was put into the routing table.

[Figure 20](#) shows the routing table contents of the router in Figure 19.

**Figure 20** Sample Routing Table

Routing table						
Destination	Subnet mask	Metric	Gateway	Status	TTL	
default route	255.255.255.0	2	160.1.1.254	learned - RIP	170	
158.101.1.0	255.255.255.0	2	160.1.1.254	learned - OSPF - INTRA	---	
158.101.2.0	255.255.255.0	2	160.1.1.254	learned - OSPF - INTRA	---	
158.101.3.0	255.255.255.0	2	160.1.1.254	learned - OSPF - INTRA	---	

Routing table data is updated statically or dynamically:

- **Statically** — You manually enter static routes in the routing table. Static routes are useful in environments where no routing protocol is used or where you want to override some of the routes that are generated with a routing protocol. Because static routes do not automatically change in response to network topology changes, manually configure only a small number of reasonably stable routes. Static routes do not time out, but they can be learned.
- **Dynamically** — Routers use a protocol such as RIP or OSPF to automatically exchange routing data and to configure their routing tables dynamically. Routes are recalculated at regular intervals. This process helps you to keep up with network changes and allows the Switch to reconfigure routes quickly and reliably. Interior Gateway

Protocols (IGPs), which operate within networks, provide this automated method.

### Default Route

In addition to the routes to specific destinations, a routing table can contain a *default route*. The router uses the default route to forward packets that do not match any other routing table entry.

A default route is often used in place of static routes to numerous destinations that all have the same gateway IP address and interface number. The default route can be configured statically, or it can be learned dynamically.

A drawback to implementing a default static route is that it is a single point of failure on the network.

### VLAN-based Routing

VLAN-based routing is used to control how a bridge and a router interact within the same Switch. The Switch uses a routing over bridging scheme, first trying to determine if the packet will be switched or routed. The Switch does this by examining the destination MAC address:

- If the destination MAC address is the internal MAC address for a port on this Switch, then the packet must be switched and is forwarded according to the IEEE 802.1D protocol.
- If the destination MAC address is not the internal MAC address for a port on this Switch, the packet is further examined to determine if the packet is a routed packet (Layer 3) or a request to the Switch itself (Layer 2).

This model allows the Switch to give the packet first to Layer 2 to be bridged by the VLAN, and then given to the router only if the packet cannot be bridged. This scheme gives you the flexibility to define router interfaces on top of several bridge ports.

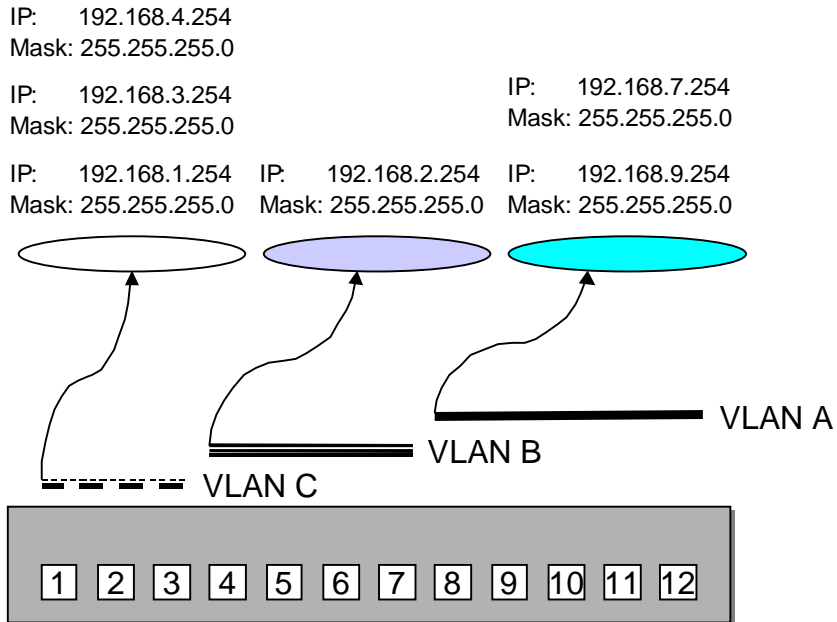
The “routing over bridging” scheme requires a VLAN-based IP Interface. To create this kind of interface you must first configure a VLAN and then create a router interface over that VLAN.

See [Chapter 8](#) for more information on VLANs.

**Multiple IP Interfaces per VLAN**

You can overlap IP interfaces without configuring a separate VLAN for each subnet. Multiple IP interfaces can share the same VLAN, allowing multiple subnets to be routed on the same 802.1Q VLAN. You can define up to 64 IP interfaces on the Switch, that is, IP routing interfaces for static VLANs. See [Figure 21](#).

**Figure 21** Multiple IP Interfaces per VLAN





---

## Implementing IP Routing

To route network traffic using IP, you must perform these tasks in the following order:

- 1 Configure Trunks (Optional)
- 2 Configure IP VLANs
- 3 Establish IP Interfaces

### Configuring Trunks (Optional)

*Trunks* (also known as aggregated links) work at Layer 2 and allow you to combine multiple Fast Ethernet or Gigabit Ethernet into a single high-speed link between two switches.

If you intend to use trunking on an IP device, configure your trunks *before* you set up VLANs and IP interfaces. In this case, you must specify the index number of the trunk. For example, if ports 5 through 8 are associated with a trunk, specifying “Aggregated Link 1” defines the VLAN to include all of the physical ports in the trunk (ports 5 through 8).

### Configuring IP VLANs

If you want to use IP routing, you must first configure the VLAN to use IP. You can create network-based VLANs, which are IP VLANs that are grouped according to the IP network address and mask.

See [Chapter 8](#) in this guide to learn about VLANs.

### Establishing IP Interfaces

To establish an IP interface:

- 1 Determine your interface parameters.
- 2 Define the IP interfaces.

#### Interface Parameters

Each IP routing interface has these standard characteristics:

- **IP address** — An address from the range of addresses that the Internet Engineering Task Force (IETF) assigns to your organization. This address is specific to your network and Switch. Refer to [Appendix C](#) for details on IP Addressing.
- **Subnet mask** — The 32-bit number that uses the same format and representation as an IP address. The subnet mask determines which bits in the IP address are interpreted as the network number/subnetwork number and the host number. Each IP address bit

that corresponds to a 1 in the subnet mask is in the network/subnetwork part of the address. Each IP address bit that corresponds to a 0 is in the host part of the IP address.

- **State** — The status of the IP interface. It indicates whether the interface is available for communications (UP) or unavailable (DOWN).
- **VLAN interface index (for in-band management)** — The number of the VLAN that is associated with the IP interface. When the Switch prompts you for this option, the menu identifies the available VLAN indexes.

### Important Consideration

Consider the following issue before you establish an IP interface:

- Before you assign IP addresses, map out the entire network and subnetwork IP addressing scheme. Plan for future expansion of address numbers as well.

### Defining an IP Interface

After you determine the VLAN index, IP address, and subnet mask for each IP interface, you can define each interface. Use the Command Line Interface or the Web interface to define an IP interface.



*Remember that you must define a VLAN before you define the IP (routing) interface. VLANs are described in [Chapter 8](#).*

To define your IP interface, you should understand the following IP features:

- [ARP Proxy](#)
- [ICMP Redirect](#)
- [ICMP Router Discovery](#)
- [Routing Information Protocol \(RIP\)](#)
- [User Datagram Protocol \(UDP\) Helper](#)

These features are discussed later in this chapter.



*You can use the Routing Information Protocol (RIP) protocol to take advantage of routing capabilities. RIP is discussed in this chapter.*

### Administering IP Routing

Keep these points in mind while you administer the IP network:

- Flush the ARP cache regularly if you set the age time to 0.
- Set up a default route.

The Switch 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. If you do not use a default route, ICMP is more likely to return an `address not found` error.
- Before you can define static routes, you must define at least one IP interface. See [“Defining an IP Interface”](#) on [page 74](#) for more information. Remember the following guidelines:
  - Static routes remain in the routing table until you remove them or the corresponding interface.
  - Static routes take precedence over dynamically learned routes to the same destination.
  - Static routes are included in periodic RIP updates sent by your Layer 3 Switch.

---

## IP Routing Protocols

IP protocols are a set of uniquely defined interactions that allow data communications to occur. Protocols are the rules by which networks must adhere in order to successfully operate. Protocols that are discussed in this section include:

- [Address Resolution Protocol \(ARP\)](#)
- [Internet Control Message Protocol \(ICMP\)](#)
- [Routing Information Protocol \(RIP\)](#)
- [Domain Name System \(DNS\)](#)
- [User Datagram Protocol \(UDP\) Helper](#)

### Address Resolution Protocol (ARP)

ARP is a low-level protocol that locates the MAC address that corresponds to a given IP address. This protocol allows a host or router to use IP addresses to make routing decisions while it uses MAC addresses to forward packets from one hop to the next.

You do not need to implement ARP — the Switch has ARP capability built in, but you can change and display the contents of the ARP cache.

When the host or router knows the IP address of the *next* hop towards the packet destination, the host or router translates that IP address into a MAC address before sending the packet. To perform this translation, the host or router first searches its *ARP cache*, which is a table of IP addresses with their corresponding MAC addresses. Each device that participates in IP routing maintains an ARP cache. See Figure 22.

**Figure 22** Example of an ARP Cache

ARP cache	
IP address	MAC address
158.101.1.1	00308e3d0042
158.101.2.1	0080232b00ab

If the IP address does not have a corresponding MAC address, the host or router broadcasts an *ARP request* packet to all the devices on the network. The ARP request contains information about the target and source addresses for the protocol (IP addresses). See Figure 23.

**Figure 23** Example of an ARP Request Packet

00802322b00ad	Source hardware address
158.101.2.1	Source protocol address
?	Target hardware address
158.101.3.1	Target protocol address

When devices on the network receive this packet, they examine it. If their address is not the target protocol address, they discard the packet. When a device receives the packet and confirms that its IP address matches the target protocol address, the receiving device places its MAC address in

the target hardware address field and exchanges both source and target fields. This packet is then sent back to the source device.

When the originating host or router receives this *ARP reply*, it places the new MAC address in its ARP cache next to the corresponding IP address. See [Figure 24](#).

**Figure 24** Example of ARP Cache Updated with ARP Reply

ARP cache	
IP address	MAC address
158.101.1.1	00308e3d0042
158.101.2.1	0080232b00ab
158.101.3.1	0134650f3000

After the MAC address is known, the host or router can send the packet directly to the next hop.

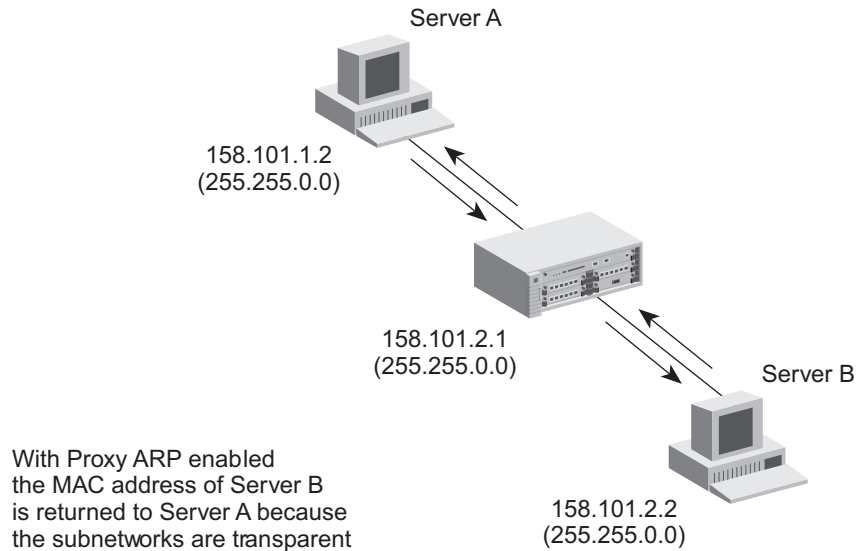
**ARP Proxy** ARP proxy allows a host that has no routing ability to determine the MAC address of a host on another network or subnet.

When ARP proxy is enabled and a workstation sends an ARP request for a remote network, the Switch determines if it has the best route and then answers the ARP request by sending its own MAC address to the workstation. The workstation then sends the frames for the remote destination to the Switch, which uses its own routing table to reach the destination on the other network.

### Example

In the following example, Server A cannot use the router as a gateway to Server B because Server A has its subnet mask set to broadcast (using ARP) its IP network address as 158.101.0.0, while the IP network address of the router is 158.101.1.0.

However, if the router answers the request of Server A with its own MAC address — thus, all traffic sent to Server B from Server A is addressed to the corresponding IP interface on the router and forwarded appropriately.

**Figure 25** ARP Proxy

### Internet Control Message Protocol (ICMP)

Because a router knows only about the next network hop, it is not aware of problems that may be closer to the destination. Destinations may be unreachable if:

- Hardware is temporarily out of service.
- You specified a nonexistent destination address.
- The routers do not have a route to the destination network.

To help routers and hosts discover problems in packet transmission, a mechanism called Internet Control Message Protocol (ICMP) reports errors back to the source when routing problems occur. With ICMP, you can determine whether a delivery failure resulted from a local or a remote problem.

ICMP performs these tasks:

- **Determines which router to use as the default gateway (ICMP Router Discovery)** — ICMP Router Discovery is useful if you have multiple gateways that connect a particular subnet to outside networks.
- **Creates more efficient routing (ICMP Redirect)** — Often the host route configuration specifies the minimum possible routing data that

is needed to communicate (for example, the address of a single router). The host relies on routers to update its routing table. In the process of routing packets, a router may detect that a host is not using the best route. The router sends an ICMP Redirect to this host, requesting that the host use a different gateway when it sends packets to a destination. The host then sends packets to that destination using the new route if it is able to interpret ICMP Redirect directives.

### ICMP Router Discovery

ICMP Router Discovery enables hosts that are attached to multicast or broadcast networks to discover the IP addresses of their neighboring routers and determine which router to use for a default gateway.

ICMP Router Discovery is permanently enabled on the Switch.

### Important Considerations

Keep the following points in mind with ICMP Router Discovery:

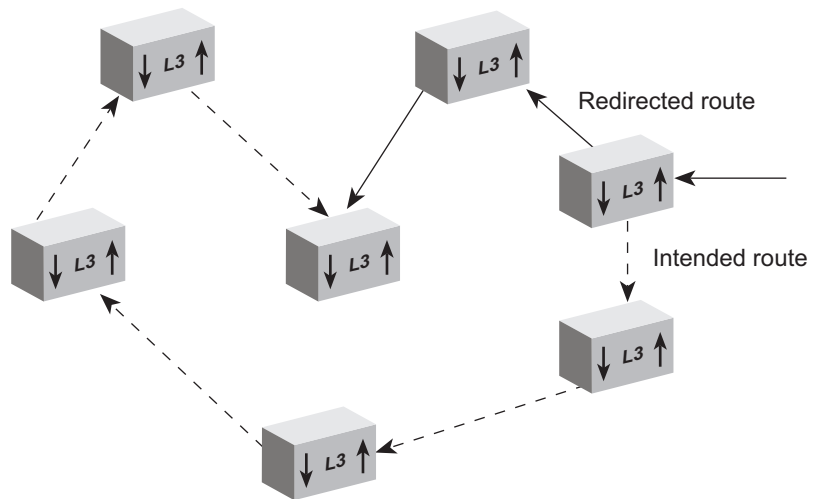
- You need not manually configure a default route.  
Although IP traffic may initially be directed to any of the routers on the LAN, ICMP Redirect messages subsequently channel IP traffic to the correct router.
- ICMP Router Discovery is useful on large networks, or when the network topology has undergone a recent change.
- If you are on a small network that is relatively stable, consider using a static route to the gateway instead of ICMP Router Discovery to reduce network traffic.



*See the documentation for your workstation to determine whether you can configure your workstation to use this protocol.*

See RFC 1256 for detailed information about ICMP Router Discovery.

[Figure 26](#) shows how ICMP can dynamically determine a router to act as the default gateway.

**Figure 26** ICMP Router Discovery**ICMP Redirect**

ICMP Redirect adds another layer of intelligence to routing. ICMP Redirect:

- Informs the sending device of the frame that there is a more efficient route to the destination.
- Routes the frame via the more efficient route.

ICMP Redirect is permanently enabled on the Switch.

**Important Considerations**

Keep the following things in mind with ICMP Redirect:

- ICMP Redirect determines if the sending interface is the same as the receiving interface.
- ICMP Redirect determines if the source device of the frame is on a direct-connect network.
- Performance can be affected if the sending device ignores the recommendations of ICMP Redirect, in which case the performance cost of ICMP Redirect is incurred while the benefits are wasted.



## Routing Information Protocol (RIP)

RIP is the protocol that implements routing. RIP does this by using Distance Vector Algorithms (DVAs) to calculate the route with the fewest number of hops to the destination of a route request. Each device keeps its own set of routes in its routing table. RIP is an Interior Gateway Protocol (IGP) for TCP/IP networks.

RIP operates using both active and passive devices.

- *Active* devices, usually routers, broadcast RIP messages to all devices in a network or subnetwork and update their internal routing tables when they receive a RIP message.
- *Passive* devices, usually hosts, listen for RIP messages and update their internal routing tables, but do not send RIP messages.

An active router sends a broadcast RIP message every 30 seconds. This message contains the IP address and a metric (distance) from the router to each destination in the routing table. In RIP, each router through which a packet must travel to reach a destination counts as one network *hop*.

### Basic RIP Parameters

There are several parameters to consider when you set up RIP for your network. When you configure an IP interface, the Switch already has the RIP parameters set to the defaults listed in [Table 10](#).

**Table 10** RIP Parameters

RIP Parameter	Default Value
Router Mode	disabled
Cost	1
Update Time	30 seconds
Send Mode	RIPv1Compatible
Receive Mode	RIPv1OrRIPv2
Poison Reverse	disabled
Advertisement Address	limited broadcast address (255.255.255.255)

### Router Mode

The available settings for router mode are as follows:

- **Disabled** — The Switch ignores all incoming RIP packets and does not generate any RIP packets of its own.
- **Enabled** — The Switch broadcasts RIP updates and processes incoming RIP packets.

### Cost

RIP calculates the route metrics (the *cost*) for you. The cost is the number of hops that the packet needs to get to its destination. The RIP cost is a number between 1 and 15. (A number higher than 15 is not allowed, because RIP cannot negotiate more than 15 hops.) This Switch assigns a default cost of 1 to all interfaces.

Most facilities assign a cost of 1 to all interfaces. However, if you have two links with differing speeds, such as a dial-up link versus a direct link, you may want to raise the cost of the dial-up link so that the direct link is more likely to be used.

### Update Time

This Switch sends a RIP message every 30 seconds (by default) with both the IP address and a *metric* (the distance to the destination from that router) for each destination. You can modify the update time if needed to adjust performance.

### Send and Receive Modes

The following RIP send and receive modes are supported by the Switch:

**Table 11** Send and Receive Modes

Send Mode	Receive Mode
RIPv1	RIPv1
RIPv1Compatible	RIPv2
RIPv2	RIPv1OrRIPv2
doNotSend	doNotReceive

- RIPv1 – Route information is broadcast periodically to other routers on the network using the advertisement list for RIP-1 updates.
- RIPv2 – Route information is multicast periodically to other routers on the network using the multicast address of 224.0.0.9. This method reduces the load on hosts that are not configured to listen to RIP-2 messages.
- RIPv1 Compatible – Route information is broadcast to other routers on the network using the advertisement list for RIP-2 updates.
- RIPv1OrRIPv2 – Both RIP-1 and RIP-2 route information can be received by the Switch.

- doNotSend – The Switch processes (or passively learns) all incoming RIP packets, but does not transmit RIP updates.
- doNotReceive – The Switch broadcasts (or advertises) RIP updates, but does not process incoming RIP packets.

The doNotSend and doNotReceive modes are also referred to as one-way learn and advertise modes.

### Poison Reverse

Poison Reverse is a RIP feature that you use specifically with a scheme called *Split Horizon*. The Switch disables Poison Reverse by default.

Split Horizon avoids the problems that reverse-route updates can cause. Reverse-route updates are sent to a neighboring router and include the routes that are learned from that router. Split Horizon omits the routes that are learned from one neighbor in the updates that are sent to that neighbor (the reverse routes).

Poison Reverse is essentially another layer of protection against advertising reverse routes.

- When you enable Poison Reverse, the Switch advertises reverse routes in updates, but it sets the metrics to 16 (infinity). Setting the metric to infinity breaks the loop immediately when two routers have routes that point to each other.
- When you disable (default mode) Poison Reverse, such reverse routes are not advertised.

You can disable Poison Reverse because it augments what Split Horizon already does, and it puts additional information that you may not need into RIP updates.

### Advertisement Address

The Switch uses the advertisement address to advertise routes to other stations on the same network. Each interface that you define uses a fixed broadcast address (255.255.255.255) as the advertisement address. The Switch uses this address for sending updates.

### RIP-1 Versus RIP-2

Like RIP-1, RIP-2 allows the Switch to dynamically configure its own routing table. RIP-2 is much more flexible and efficient than RIP-1,

however, because RIP-2 advertises using the multicast method, which can advertise to a subset of the network (RIP-1 uses the broadcast method, which advertises to the whole network). RIP-2 can do this because it includes a subnet mask in its header.

If your Switch receives a RIP-2 packet, your Switch puts the route into the routing table with the subnet mask that was advertised.

### Important Considerations

Consider the following issues when you implement RIP on your Switch:

- Use RIP-2 rather than RIP-1 if possible, because RIP-2 uses subnet masking and the next hop field. Subnet mask advertising allows you to use VLSM. (See [“Variable Length Subnet Masks \(VLSMs\)”](#) earlier in this chapter for more information.)
- Where possible, set RIP as follows:
  - **Send Mode** — `RIPv2`
  - **Receive Mode** — `RIPv1OrRIPv2`

In this way, the Switch keeps track of the RIP-1 and RIP-2 address routes in its routing table and forwards the routes as well.

- When using Spanning Tree (STP) and Routing Information Protocol (RIP) all Switches must communicate with each other on the same VLAN.

## Domain Name System (DNS)

The Domain Name System (DNS) client allows you to specify a hostname rather than an IP address when you perform various operations (for example, when you use `ping` to contact an IP station).

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

You can resolve an IP address to a host name or a host name to an IP address on a name server. Enter either the host name or the IP address; the DNS client displays the pair.

### Important Considerations

When you set up DNS servers on your LAN, remember the following:

- Always set up more than one DNS name server (a primary and secondary server) so that the lookup service does not have a single point of failure.
- If your ISP changes the Classes of Internetwork Service, change the DNS setting on each host that the ISP services.

### User Datagram Protocol (UDP) Helper

User Datagram Protocol (UDP) Helper allows TCP/IP applications to forward broadcast packets from one part of the network to another. The most common uses of UDP are:

- **Bootstrap Protocol (BOOTP)**

BOOTP allows you to boot a host through the router using a logical port. This can be done even when the host is on another part of the network. UDP packets that rely on the BOOTP relay agent are modified and then forwarded through the router.

- **Dynamic Host Configuration Protocol**

A host can retrieve its own configuration information including IP address, from a DHCP server through the IP network. DHCP makes it easier to administer the IP network. With DHCP you can dynamically configure a host with new information.

Your Switch implements a generic UDP Helper agent that applies to any port.

### Implementing UDP Helper

You have to set the following UDP Helper parameters:

- **UDP Port Number** A logical address, not a port (interface) on your device. BOOTP (including DHCP) uses UDP port 67.
- **IP forwarding address** The IP address to which the packets are forwarded. You can have up to 32 combinations of port numbers and IP forwarding addresses. You can also have up to 4 IP address entries for the same ports.

You need to have a thorough understanding of your network configuration to use UDP Helper. Review the network topology before you implement UDP Helper.

### Important Considerations

Consider the following points when you use UDP Helper:

- Overlapped IP interfaces are multiple logical interfaces that are defined for a single VLAN. UDP Helper forwards packets from overlapped IP interfaces by assigning each overlapped IP interface, in turn, as the source network for forwarded packets.
- The BOOTP hop count (how many steps the Switch uses to forward a packet) is fixed at 16.
- You can always add or remove a port number or IP forwarding address defined for UDP Helper.

---

### Advanced IP Routing Options

Your Switch has several features which further extend the networking capabilities of the device. Refer to Appendix D for more information on the following:

- [Variable Length Subnet Masks \(VLSMs\)](#)
- [Supernetting](#)

---

### Access Control Lists

Access Control Lists are a set of instructions that can be applied to filter traffic on VLANs. They can be used to limit access to certain segments of the network and therefore, are useful for network security.

Access Control Lists can be used to:

- Prevent unnecessary network traffic.
- Restrict access to proprietary information within the network.

Access Control Lists are based on a series of rules. Rules are applied to VLANs and determine the path or access limitations for packets received on a VLAN. When a packet is received or sent on a VLAN, it is compared to an access list for this VLAN. If a match is found; meaning the packet falls under the rule, it will be blocked or forwarded to the appropriate VLAN depending on the action.

Rules are established based on IP addressing. A packet matches an access list rule when it's destination IP address falls with the values of the rule. When a match is found, the path the packet takes is determined by the rule and is either forwarded (permitted) or dropped (denied).

There are a maximum of 100 access lists that can be applied under the current operating system. Access list rules can be applied and traffic is forwarded at wire speed using layer 3 destination IP addresses and VLANs.

### How Access Control List Rules Work

When a packet is received it is compared against the VLAN access list. The access list rules are applied to a range of IP addresses and are defined by the destination IP address and a mask. If a match is found in the access list the appropriate action is taken. By default, if no access list has been defined for a VLAN, all IP traffic will be permitted. Denial is based on a pre-defined rule.

For example:

Packet destination IP address: 10.101.67.45

Rule destination address: 10.101.67.0

Rule destination mask: 255.255.255.0

Rule action: deny

As a result of the above rule, the packet matches the parameters of the rule and will be blocked.



*A destination mask of 0.0.0.0 will match all packets.*







# APPENDICES AND INDEX

- [Appendix A](#)    [Configuration Rules](#)
- [Appendix B](#)    [Network Configuration Examples](#)
- [Appendix C](#)    [IP Addressing](#)
- [Appendix D](#)    [Advanced IP Routing Concepts](#)
- [Glossary](#)
- [Index](#)





# A

## CONFIGURATION RULES

---

### Configuration Rules for Gigabit Ethernet

Gigabit Ethernet is designed to run over several media:

- Single-mode fiber optic cable, with connections up to 5 km (3.1 miles). Support for distances over 5 km is supported depending on the module specification.
- Multimode fiber optic cable, with connections up to 550 m (1804 ft).
- Category 5 cabling, with connections up to 100 m (328 ft).

The different types of Gigabit Ethernet media and their specifications are detailed in [Table 12](#).

**Table 12** Gigabit Ethernet cabling

Gigabit Ethernet Transceivers	Fiber Type	Modal Bandwidth (MHz/km)	Lengths Supported Specified by IEEE (meters)
1000BASE-LX	62.5 $\mu$ m MM	500	2–550
	50 $\mu$ m MM	400	2–550
	50 $\mu$ m MM	500	2–550
	10 $\mu$ m SM	N/A	2–5000
1000BASE-SX	62.5 $\mu$ m MM	160	2–220
	62.5 $\mu$ m MM	120	2–275
	50 $\mu$ m MM	400	2–500
	50 $\mu$ m MM	500	2–550
1000BASE-T	N/A	N/A	100

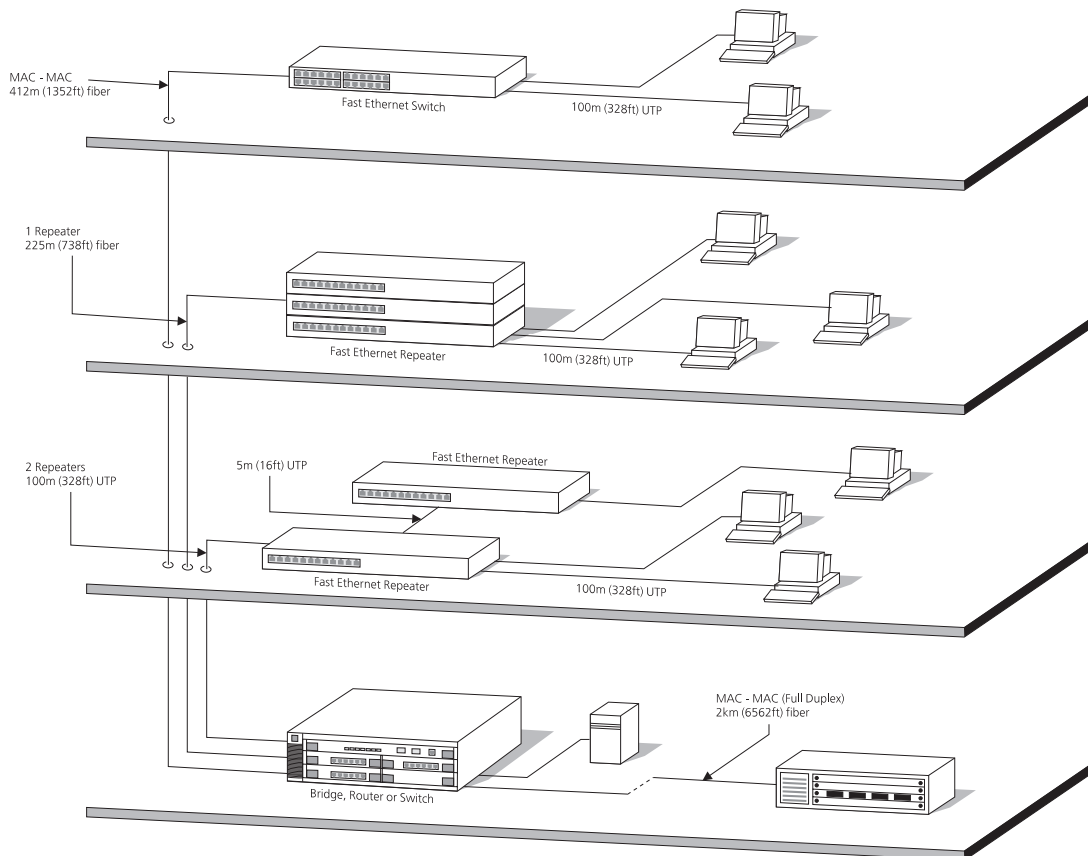
*MM = Multimode SM = Single-mode*

---

## Configuration Rules for Fast Ethernet

The topology rules for 100 Mbps Fast Ethernet are slightly different to those for 10 Mbps Ethernet. [Figure 27](#) illustrates the key topology rules and provides examples of how they allow for large-scale Fast Ethernet networks.

**Figure 27** Fast Ethernet configuration rules



The key topology rules are:

- Maximum UTP cable length is 100 m (328 ft) over Category 5 cable.
- A 412 m (1352 ft) fiber link is allowed for connecting switch-to-switch, or endstation-to-switch, using half-duplex 100BASE-FX.
- A total network span of 325 m (1066 ft) is allowed in single-repeater topologies (one hub stack per wiring closet with a fiber link to the

collapsed backbone). For example, a 225 m (738 ft) fiber link from a repeater to a router or switch, plus a 100 m (328 ft) UTP link from a repeater out to the endstations.

**Configuration Rules  
with Full Duplex**

The Switch provides full duplex support for all its ports, including Expansion Module ports. Full duplex allows packets to be transmitted and received simultaneously and, in effect, doubles the potential throughput of a link.

With full duplex, the Ethernet topology rules are the same, but the Fast Ethernet rules are:

- Maximum UTP cable length is 100 m (328 ft) over Category 5 cable.
- A 2 km (6562 ft) fiber link is allowed for connecting switch-to-switch, or endstation-to-switch.



# B

## NETWORK CONFIGURATION EXAMPLES

This chapter contains the following sections:

- [Network Configuration Examples](#)
  - [Improving the Resilience of Your Network](#)
  - [Enhancing the Performance of Your Network](#)
  - [Utilizing the Traffic Prioritization Features of Your Network](#)



*Where a Switch 4900 is shown, this is interchangeable with the Switch 4900 SX.*

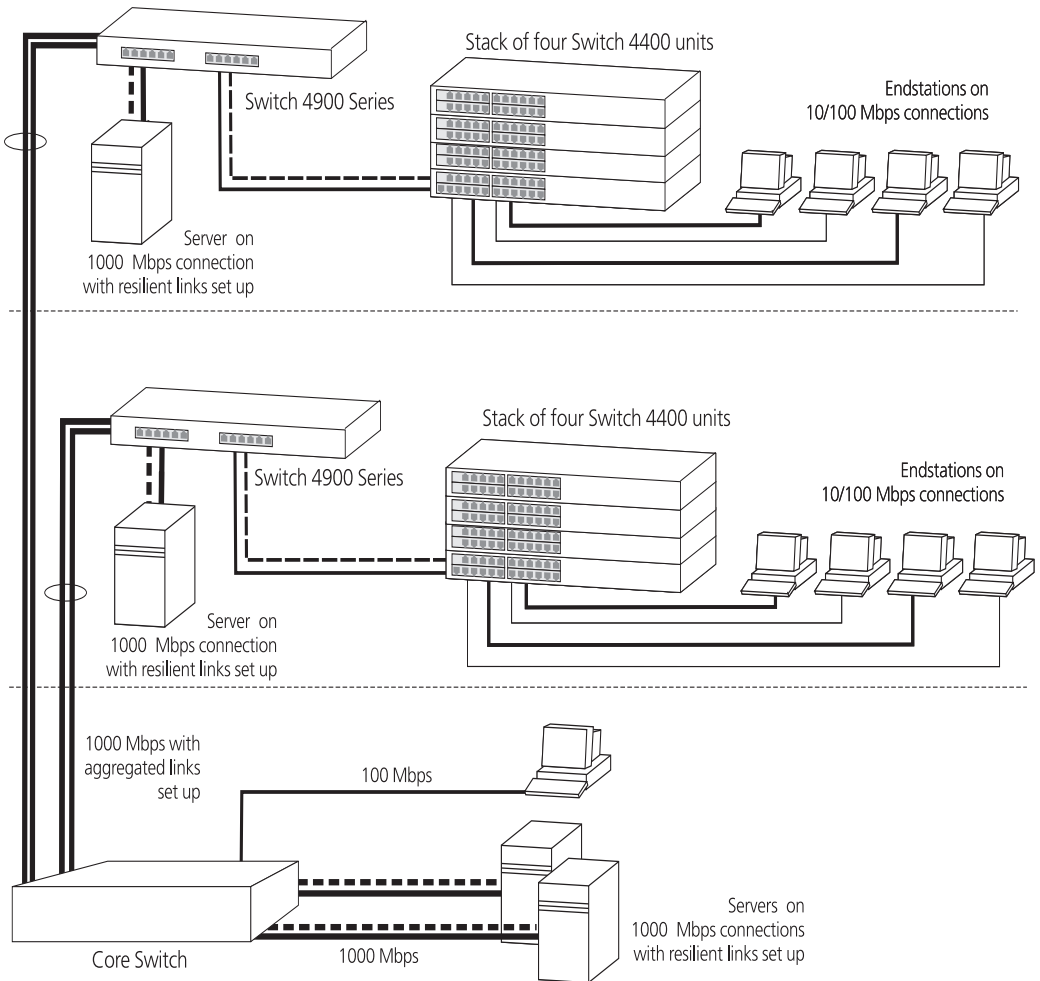
## Network Configuration Examples

This section shows some network examples that illustrate how you can set up your network for optimum performance using some of the features supported by your Switch.

### Improving the Resilience of Your Network

[Figure 28](#) shows how you can set up your network to improve its resilience using resilient links. Alternatively, instead of setting up resilient links, you can enable Spanning Tree Protocol (STP). Aggregated links have also been setup from the Core Switch, this increases the bandwidth available for the backbone connection, and also provides extra resilience.

**Figure 28** Network set up to provide resilience



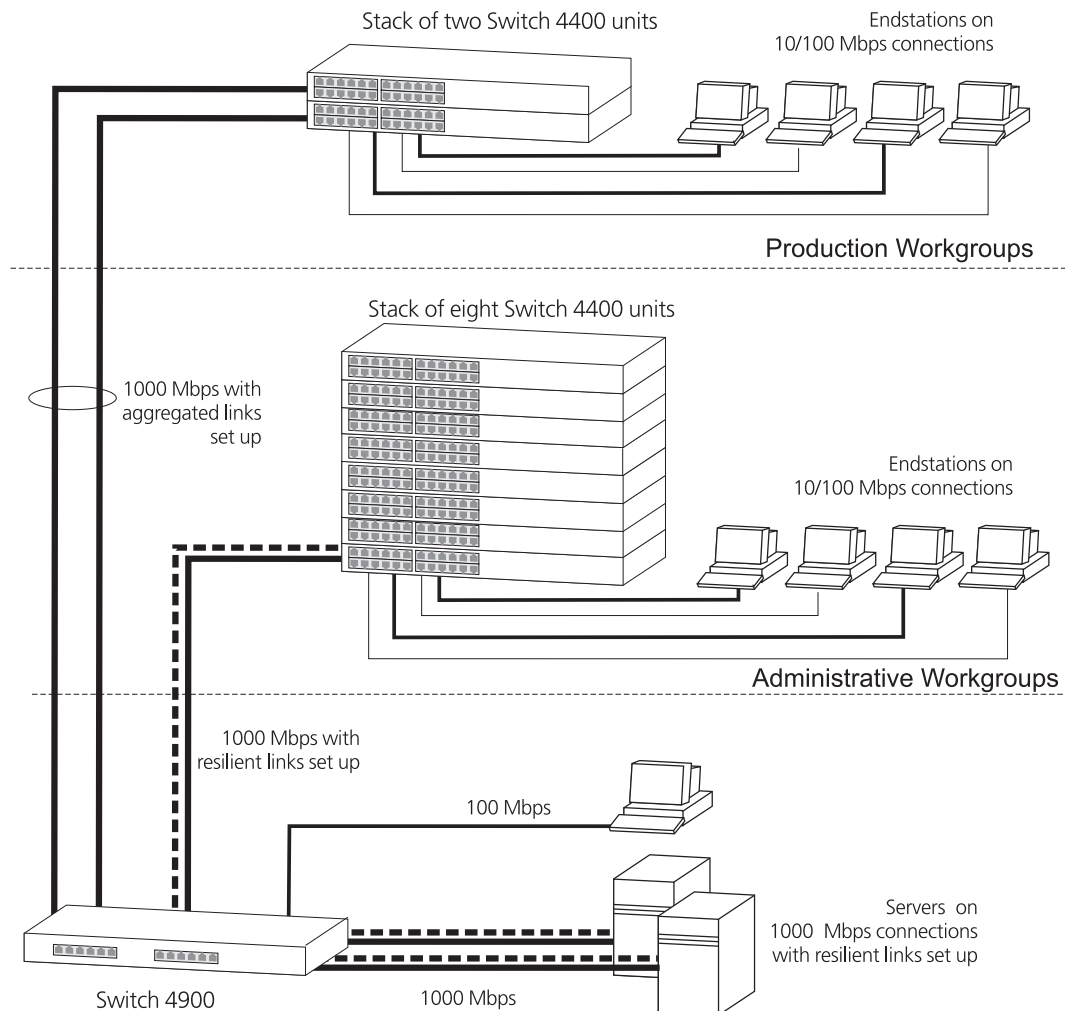


## Enhancing the Performance of Your Network

[Figure 29](#) shows how you can set your network up to enhance its performance.

All ports are auto-negotiating and smart auto-sensing and will therefore pass data across the network at the optimum available speed and duplex mode. Flow control will help avoid packet loss during periods of network congestion. A Gigabit Ethernet backbone is set up between the Switch 4900 and each Switch in the workgroups to increase the bandwidth, and therefore the overall network performance.

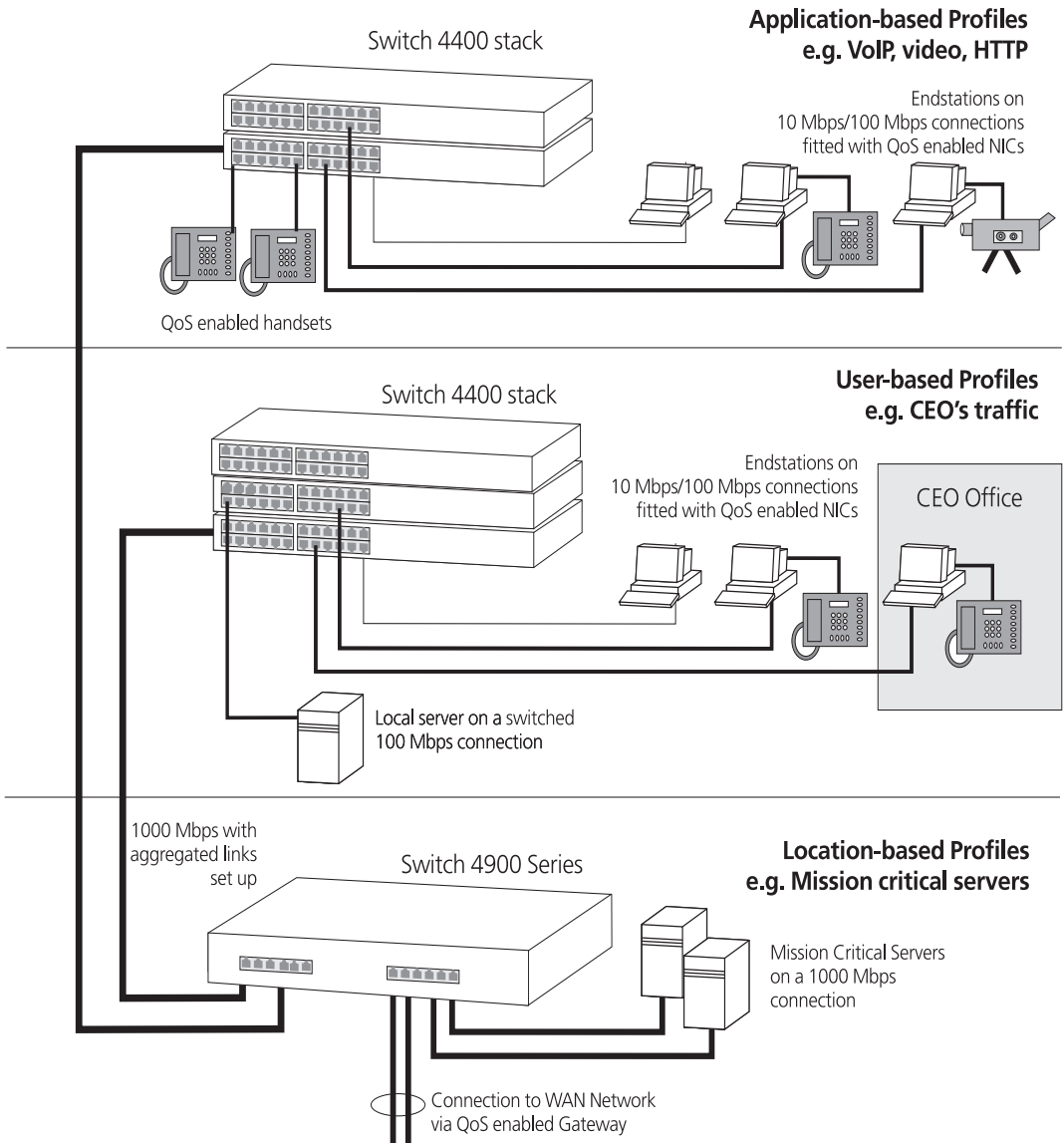
**Figure 29** Network set up to enhance performance



### Utilizing the Traffic Prioritization Features of Your Network

The example in [Figure 30](#) shows a network configuration that demonstrates how you can utilize the different types of Quality of Service (QoS profiles) to ensure a high level of service and prioritization across the network for certain applications, users, or locations. For more information on using QoS, see [Chapter 6 “Using Traffic Prioritization”](#).

**Figure 30** Network set up to utilize traffic prioritization



# C

## IP ADDRESSING

This chapter provides some background detail on the IP information that needs to be assigned to your Switch to enable you to manage it across a network. The topics covered are:

- [IP Addresses](#)
- [Subnets and Subnet Masks](#)
- [Default Gateways](#)
- [Standards, Protocols, and Related Reading](#)



IP addressing is a vast topic and there are white papers on the World Wide Web and publications available if you wish to learn more about IP addressing.

---

### IP Addresses

This IP address section is divided into two parts:

- [Simple Overview](#) — Gives a brief overview of what an IP address is.
- [Advanced Overview](#) — Gives a more in depth explanation of IP addresses and the way they are structured.

### Simple Overview

To operate correctly, each device on your network must have a unique IP address. IP addresses have the format  $n.n.n.n$  where  $n$  is a decimal number between 0 and 255. An example IP address is '192.168.100.8'.

The IP address can be split into two parts:

- The first part, called the network part, ('192.168' in the example) identifies the network on which the device resides.
- The second part, called the host part, ('100.8' in the example) identifies the device within the network.

If your network is internal to your organization only, you may use any arbitrary IP address. 3Com suggests you use addresses in the series 192.168.100.X (where X is a number between 1 and 254) with a subnet mask 255.255.255.0. If you are using SLIP, use the default SLIP address of 192.168.101.1 with a subnet mask of 255.255.255.0.



*These suggested IP addresses are part of a group of IP addresses that have been set aside specially for use “in house” only.*



**CAUTION:** *If your network has a connection to the external IP network, you must apply for a registered IP address. This registration system ensures that every IP address used is unique; if you do not have a registered IP address, you may be using an identical address to someone else and your network will not operate correctly.*

### Obtaining a Registered IP Address

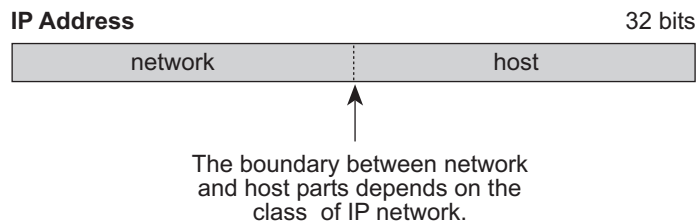
InterNIC Registration Services is the organization responsible for supplying registered IP addresses. The following contact information is correct at time of publication:

World Wide Web site: <http://www.internic.net>

### Advanced Overview

IP addresses are 32-bit addresses that consist of a *network part* (the address of the network where the host is located) and a *host part* (the address of the host on that network).

**Figure 31** IP Address: Network Part and Host Part



IP addresses differ from Ethernet MAC addresses, which are unique hardware-configured 48-bit addresses. A central agency, such as the InterNIC Registration Services mentioned above, assigns the network part of the IP address, and you assign the host part. All devices that are connected to the same network share the same network part (also called the *prefix*).

## Dotted Decimal Notation

The actual IP address is a 32-bit number that is stored in binary format. These 32 bits are segmented into 4 groups of 8 bits — each group is referred to as a *field* or an *octet*. Decimal notation converts the value of each field into a decimal number, and the fields are separated by dots.

**Figure 32** Dotted Decimal Notation for IP Addresses

10011110.01100101.00001010.00100000 = Binary notation

158.101.10.32 = Decimal notation



*The decimal value of an octet whose bits are all 1s is 255.*

## Network Portion

The location of the boundary between the network part and the host part depends on the class that the central agency assigns to your network. The three primary classes of IP addresses are as follows:

- **Class A address** — Uses 8 bits for the network part and 24 bits for the host part. Although only a few Class A networks can be created, each can contain a very large number of hosts.
- **Class B address** — Uses 16 bits for the network part and 16 bits for the host part.
- **Class C address** — Uses 24 bits for the network part and 8 bits for the host part. Each Class C network can contain only 254 hosts, but many such networks can be created.

The high-order bits of the network part of the address designate the IP network class. See [Table 13](#).

**Table 13** How Address Class Corresponds to the Address Number

Address Class	High-order Bits	Address Number (Decimal)
A	0nnnnnnn	0-127
B	10nnnnnn	128-191
C	11nnnnnn	192-254

## Subnets and Subnet Masks

You can divide your IP network into sub-networks also known as subnets. Support for subnets is important because the number of bits assigned to the device part of an IP address limits the number of devices that may be addressed on any given network. For example, a Class C address is restricted to 254 devices.

The IP address can also contain a *subnetwork part* at the beginning of the host part of the IP address. Thus, you can divide a single Class A, B, or C network internally, allowing the network to appear as a single network to other external networks. The subnetwork part of the IP address is visible only to hosts and gateways on the subnetwork.

When an IP address contains a subnetwork part, a *subnet mask* identifies the bits that constitute the subnetwork address and the bits that constitute the host address. A subnet mask is a 32-bit number in the IP address format. The *1* bits in the subnet mask indicate the network and subnetwork part of the address. The *0* bits in the subnet mask indicate the host part of the IP address, as shown in [Figure 33](#).

**Figure 33** Subnet Masking

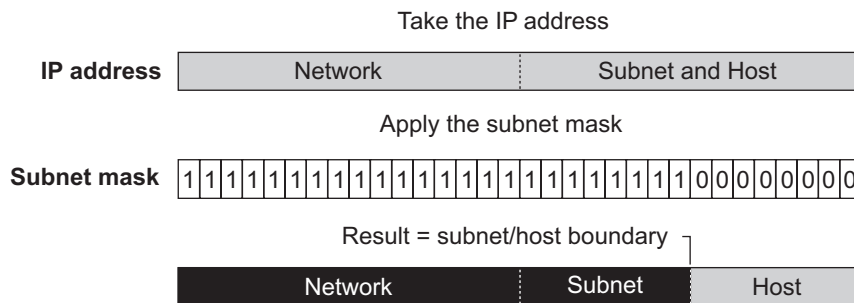


Figure 34 shows an example of an IP address that includes network, subnetwork, and host parts. Suppose the IP address is *158.101.230.52* with a subnet mask of *255.255.255.0*. Since this is a Class B address, this address is divided as follows:

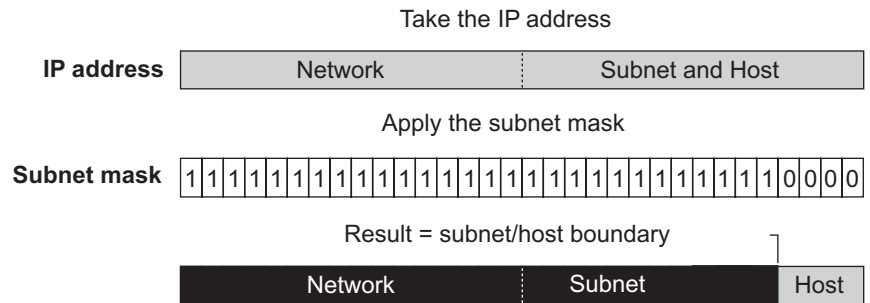
- *158.101* is the network part
- *230* is the subnetwork part
- *52* is the host part



As shown in this example, the 32 bits of an IP address and subnet mask are usually written using an integer shorthand. This notation translates four consecutive 8-bit groups (octets) into four integers that range from 0 through 255. The subnet mask in the example is written as 255.255.255.0.

Traditionally, subnet masks were applied to octets in their entirety. However, one octet in the subnet mask can be further subdivided so that part of the octet indicates an *extension* of the network number, and the rest of the same octet indicates the host number, as shown in [Figure 34](#).

**Figure 34** Extending the Network Prefix



Using the Class B IP address from Figure 33 (158.101.230.52), the subnet mask is 255.255.255.240.

The number that includes both the Class B natural network mask (255.255) and the subnet mask (255.240) is sometimes called the *extended network prefix*.

Continuing with the previous example, the subnetwork part of the mask uses 12 bits, and the host part uses the remaining 4 bits. Because the octets are actually binary numbers, the number of subnetworks that are possible with this mask is 4,096 ( $2^{12}$ ), and the number of hosts that are possible in each subnetwork is 16 ( $2^4$ ).

### Subnet Mask Numbering

An alternate method to represent the subnet mask numbers is based on the number of bits that signify the network portion of the mask. Many Internet Service Providers (ISPs) now use this notation to denote the subnet mask. See [Table 14](#).

**Table 14** Subnet Mask Notation

Standard Mask Notation	Network Prefix Notation
100.100.100.100 (255.0.0.0)	100.100.100.100/8
100.100.100.100 (255.255.0.0)	100.100.100.100/16
100.100.100.100 (255.255.255.0)	100.100.100.100/24



*The subnet mask 255.255.255.255 is reserved as the default broadcast address.*

## Default Gateways

A gateway is a device on your network which is used to forward IP packets to a remote destination. An alternative name for a gateway is a Router. “Remote” refers to a destination device that is not directly attached to the same network segment as the source device.

The source device cannot send IP packets directly to the destination device because it is in a different network segment. Instead you configure it to send the packets to a gateway which is attached to multiple segments.

When it receives the IP packets, the gateway determines the next network hop on the path to the remote destination, and sends the packets to that hop. This could either be the remote destination or another gateway closer towards the destination.

This hop-by-hop process continues until the IP packets reach the remote destination.

If manually configuring IP information for the Switch, enter the IP address of the default gateway on the local subnet in which the Switch is located. If no default gateway exists on your network, enter the IP address 0.0.0.0 or leave the field blank.



---

## Standards, Protocols, and Related Reading

This section describes how to obtain more technical information about IP.

### Requests For Comments (RFCs)

Documents called Requests for Comments (RFCs) contain information about the entire set of protocols that make up IP. Some of the RFCs that pertain to the discussions in this chapter are:

- **RFC 791** — Internet Protocol
- **RFC 1219** — Subnetwork Numbers
- **RFC 1878** — VLSMs
- **RFC 1519** — Supernetting
- **RFC 1256** — ICMP Router Discovery Messages
- **RFC 1058** — RIP
- **RFC 1723** — RIP Version 2
- **RFC 1786** — IP Routing Policies
- **RFC 2400** — Internet Official Protocol Standards

You can obtain RFCs from the Internet using the following URL:

<http://sunsite.auc.dk/RFC>

### Standards Organizations

Standards organizations ensure interoperability, create reports, and recommend solutions for communications technology. The most important standards groups are:

- International Telecommunications Union (ITU)
- Electronic Industry Association (EIA)
- American National Standards Institute (ANSI)
- International Standards Organization (ISO)
- Institute of Electrical and Electronic Engineers (IEEE)
- Internet Engineering Task Force (IETF)
- National Institute of Standards and Technology (NIST)



# D

## ADVANCED IP ROUTING CONCEPTS

This chapter provides some additional background detail on the IP information that can be assigned to your Switch to enable you to manage it across a network. These are advanced features and are not required for operating your switch in your network. The topics covered are:

- [Variable Length Subnet Masks \(VLSMs\)](#)
- [Supernetting](#)

---

### Variable Length Subnet Masks (VLSMs)

With Variable Length Subnet Masks (VLSMs), each subnetwork under a network can use its own subnet mask. Therefore, with VLSM, you can get more subnetwork space out of your assigned IP address space.

#### How VLSMs Work

VLSMs get beyond the restriction that a single subnet mask imposes on the network. One subnet mask per IP network address fixes the number of subnetworks and the number of hosts per subnetwork.

For example, if you decide to configure the 158.100.0.0/16 network with a /23 extended-network prefix, you can create 128 subnetworks with each having up to 510 hosts. If some of the subnetworks do not need that many hosts, you would assign many host IP addresses but not use them.

With VLSMs, you can assign another subnet mask, for instance, /27, to the same IP address. So you can assign a longer subnet mask that consequently uses fewer host IP addresses. As a result, routing tables are smaller and more efficient.



*This method of further subdividing addresses using VLSMs is being used increasingly more as networks grow in size and number. However, be aware that this method of addressing can greatly increase your network*

*maintenance and the risk of creating erroneous addresses unless you plan the addressing scheme properly.*

### Guidelines for Using VLSMs

Consider the following guidelines when you implement VLSMs:

- When you design the subnetwork scheme for your network, do not estimate the number of subnetworks and hosts that you need. Work from the top down until you are sure that you have accounted for all the hosts, present and future, that you need.
- Make sure that the routers forward routes based on what is known as the *longest match*.

For example, assume that the destination IP address of a packet is 158.101.26.48 and that the following four routes are in the routing table:

- 158.101.26.0/24
- 158.101.3.10/16
- 158.101.26.32/16
- 158.95.80.0/8

The router selects the route to 158.101.26.0/24 because its extended network prefix has the greatest number of bits that correspond to the destination IP address of the packet.

See RFCs 1219 and 1878 for information about understanding and using VLSMs.

---

## Supernetting

Because Class B Internet addresses are in short supply, larger networks are now usually granted a contiguous block of several Class C addresses. Unfortunately, this creates very large routing tables since multiple Class C routes have to be defined for each network containing more than 254 nodes. Larger routing tables mean more work for the routers and, therefore, poorer performance.



*Supernetting is only supported by RIPv2.*

With traditional IP, each class C network must have a routing table entry.

Supernetting, or CIDR (Classless InterDomain Routing), is a technique that allows each of these larger networks to be represented by a single

routing table entry. (See RFC 1519 for detailed information about Supernetting.)

To do this, supernet addressing does something very different from traditional TCP/IP routing (which allows only one netmask per network). In supernet routing, each supernet can be assigned its own netmask.

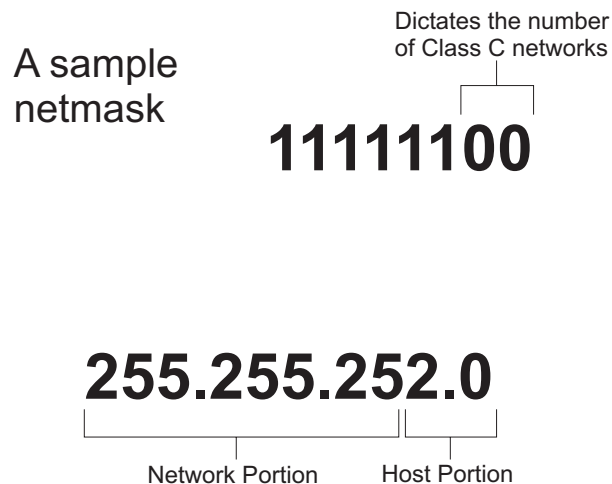
Since supernet addressing is a fairly complex mechanism, the easiest way to understand it is to step through the setup process.

### Step 1 - Select a netmask for each supernet

Each supernet must have a netmask assigned to it. The netmask for an individual supernet can be, but does not have to be, the same as the netmask for any other supernet.

As in subnetting, a netmask creates a division between the network portion of an address and the host portion of an address. However, since the network you are defining is larger than a Class C network, the division you are creating is not in the fourth octet of the address. This example creates supernets composed of fewer than 254 Class C networks. So, their netmasks are actually splitting up the third octet in their IP addresses. See [Figure 35](#).

**Figure 35** Sample CIDR Netmask



Notice that the number of zero bits in the third octet actually dictates the number of Class C networks in the supernet. Each zero bit makes the

supernet twice as large. So, a supernet composed of 8 Class C networks would actually have 3 zeroes ( $8 = 2^3$ ).

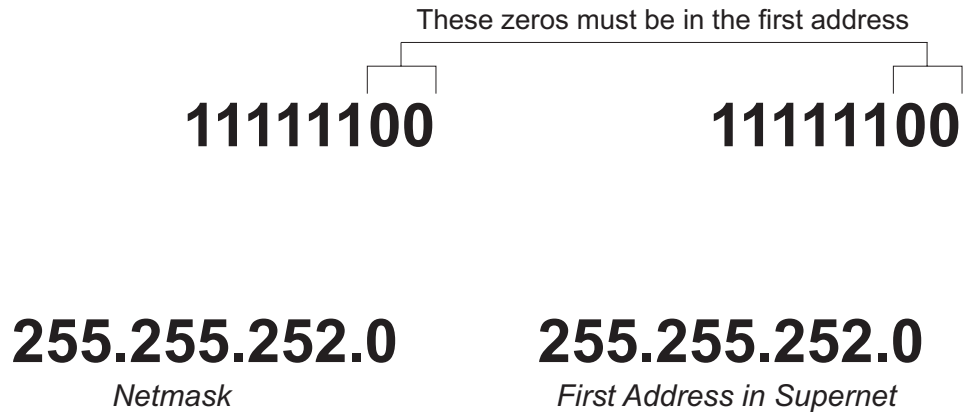
This would seem very limited since it restricts you to using groups that nicely fit into a power of 2 (1, 2, 4, 8, 16...). However, inconveniently-sized supernets can be accommodated because of a simple fact: a netmask with more 1 bits will override a netmask with fewer 1 bits.

This allows a smaller supernet to share the address space of a larger supernet. If, for example, you had a supernet of size 6 and a supernet of size 2, you could assign the larger supernet an 8 network address space and assign the smaller supernet the portion of that address space that the larger supernet was not using.

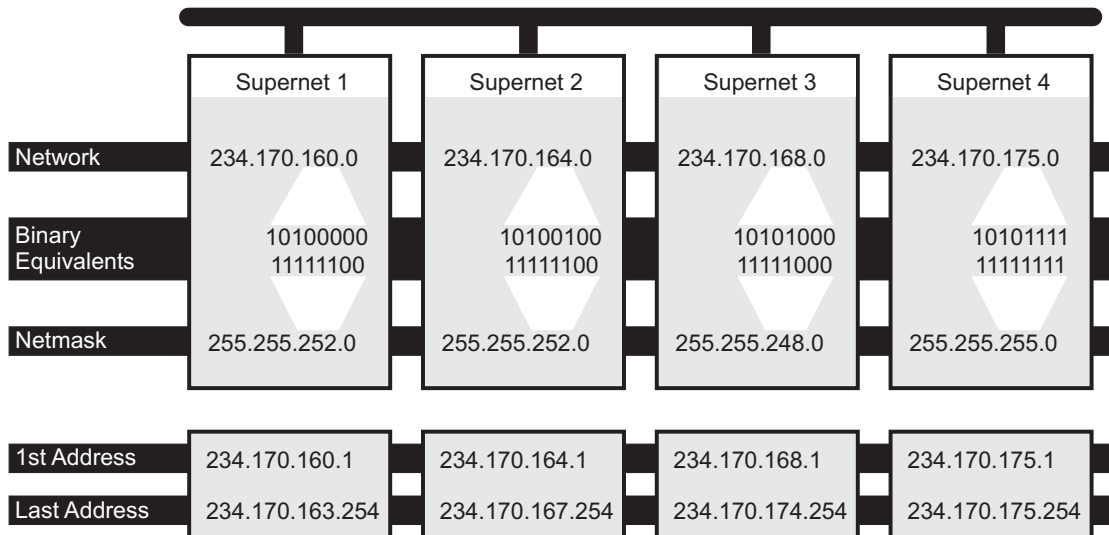
Because the smaller supernet netmask has more 1 bits, packets whose address was part of its address space would be routed to the smaller supernet even though the address is also part of the address space dictated by the larger supernet netmask.

### **Step 2 - Select a range of addresses for each supernet**

The range of addresses in a supernet must fit exactly into a space that can be described by its netmask. This means that the zero bits in the netmask must also appear in the first address of the supernet block. For this to be true, the third octet in the address must be an even multiple of the same power of 2 used to form the netmask. For example, if you had created a block of 8 networks, the third octet in the first address will be an even multiple of 8. See [Figure 36](#).

**Figure 36** Selecting a Range of Addresses**Supernet Example**

The four networks in [Figure 37](#) are all connected to the same Internet service provider (ISP). The ISP has decided to use supernetting to reduce the size of the routing tables and improve throughput.

**Figure 37** Supernet example

- Supernets 1 and 2 each require four Class C networks, so they require a netmask with 2 zero bits ( $4 = 2^2$ ) in the third octet. This yields a netmask of 255.255.252.0.

- Supernet 3 requires 7 Class C address spaces. Since 7 isn't a power of 2, we have to round it up to eight. This gives it a netmask of 255.255.248.0.
- Supernet 4 is a single Class C network, making its netmask 255.255.255.0

Now, assign ranges of addresses. Assume that the ISP is responsible for the network 234.170.0.0 and that its first free addresses are at 234.170.158.0.

The third octet of Supernet 1 has to be an even multiple of 4, so the ISP grants an address range starting at 234.170.160.0 and hopes that the block between 158 and 160 can be filled in later.

Supernet 2 must also begin on an even multiple of 4. The first available address after Supernet 1 conveniently fits the bill. So, supernet 2 extends from 234.170.164.1 to 234.170.167.254.

Supernet 3 requires an even multiple of 8. It also can begin on the next available address.

Since supernet 4 can fit entirely in a single Class C address space, it can use the supernet 3 surplus space. It is therefore given the last Class C address space in the Supernet 3 territory, effectively reducing supernet 3 to only the 7 class C networks it needs.



# GLOSSARY

<b>10BASE-T</b>	The IEEE specification for 10 Mbps Ethernet over Category 3, 4 or 5 twisted pair cable.
<b>100BASE-FX</b>	The IEEE specification for 100 Mbps Fast Ethernet over fiber-optic cable.
<b>100BASE-TX</b>	The IEEE specification for 100 Mbps Fast Ethernet over Category 5 twisted-pair cable.
<b>1000BASE-T</b>	The IEEE specification for 1000 Mbps Gigabit Ethernet over four-pair Category 5 twisted-pair cable.
<b>1000BASE-SX</b>	The IEEE specification for 1000 Mbps Gigabit Ethernet over fiber-optic cable.
<b>aging</b>	The automatic removal of dynamic entries from the Switch Database which have timed-out and are no longer valid.
<b>Aggregated Links</b>	Aggregated links allow a user to increase the bandwidth and resilience between switches by using a group of ports to carry traffic between the switches.
<b>auto-negotiation</b>	A feature on twisted pair ports that allows them to advertise their capabilities for speed, duplex and flow control. When connected to a port that also supports auto-negotiation, the link can automatically configure itself to the optimum setup.
<b>backbone</b>	The part of a network used as a primary path for transporting traffic between network segments.
<b>bandwidth</b>	The information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10 Mbps, the bandwidth of Fast Ethernet is 100 Mbps, and the bandwidth of Gigabit Ethernet is 1000 Mbps.

- baud** The signalling rate of a line, that is, the number of transitions (voltage or frequency changes) made per second. Also known as *line speed*.
- 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.
- bridge** A device that interconnects two LANs of a different type to form a single logical network that comprises of two network segments.  
Bridges learn which endstations are on which network segment by examining the source addresses of packets. They then use this information to forward packets based on their destination address. This process is known as filtering.
- broadcast** A packet sent to all devices on a network.
- broadcast storm** Multiple simultaneous broadcasts that typically absorb all the available network bandwidth and can cause a network to fail. Broadcast storms can be due to faulty network devices.
- collision** A term used to describe two colliding packets in an Ethernet network. Collisions are a part of normal Ethernet operation, but a sudden prolonged increase in the number of collisions can indicate a problem with a device, particularly if it is not accompanied by a general increase in traffic.
- CSMA/CD** Carrier-sense Multiple Access with Collision Detection. The protocol defined in Ethernet and IEEE 802.3 standards in which devices transmit only after finding a data channel clear for a period of time. When two devices transmit simultaneously, a collision occurs and the colliding devices delay their retransmissions for a random length of time.
- endstation** A computer, printer or server that is connected to a network.
- Ethernet** A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks use CSMA/CD to transmit packets at a rate of 10 Mbps over a variety of cables.
- Ethernet address** See *MAC address*.
- Fast Ethernet** An Ethernet system that is designed to operate at 100Mbps.
- forwarding** The process of sending a packet toward its destination using a networking device.

- Forwarding Database** See *Switch Database*.
- filtering** The process of screening a packet for certain characteristics, such as source address, destination address, or protocol. Filtering is used to determine whether traffic is to be forwarded, and can also prevent unauthorized access to a network or network devices.
- flow control** A mechanism that prevents packet loss during periods of congestion on the network. Packet loss is caused when devices send traffic to an already overloaded port on a Switch. Flow control prevents packet loss by inhibiting devices from generating more traffic until the period of congestion ends.
- full duplex** A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.
- Gigabit Ethernet** IEEE standard 802.3z for 1000 Mbps Ethernet; it is compatible with existing 10/100 Mbps Ethernet standards.
- half duplex** A system that allows packets to be transmitted and received, but not at the same time. Contrast with *full duplex*.
- hub** A device that regenerates LAN traffic so that the transmission distance of that signal can be extended. Hubs are similar to repeaters, in that they connect LANs of the same type; however they connect more LANs than a repeater and are generally more sophisticated.
- IEEE** Institute of Electrical and Electronics Engineers. This American organization was founded in 1963 and sets standards for computers and communications.
- IEEE 802.1D** A standard that defines the behavior of bridges in an Ethernet network.
- IEEE 802.1p** A standard that defines traffic prioritization. 802.1p is now incorporated into the relevant sections of the IEEE 802.1D/D17 standard.
- IEEE 802.1Q** A standard that defines VLAN tagging.
- IEEE 802.3x** A standard that defines a system of flow control for ports that operate in full duplex.
- IETF** Internet Engineering Task Force. An organization responsible for providing engineering solutions for TCP/IP networks. In the network

management area, this group is responsible for the development of the SNMP protocol.

**IFM** Intelligent Flow Management. A flow control mechanism that prevents packet loss during periods of congestion on the network.

**Internet Group Management Protocol** Internet Group Management Protocol (IGMP) is a protocol that runs between hosts and their immediate neighboring multicast routers. The protocol allows a host to inform its local router that it wishes to receive transmissions addressed to a specific multicast group. Based on group membership information learned from the IGMP, a router is able to determine which if any multicast traffic needs to be forwarded to each of its subnetworks.

**IGMP snooping** A mechanism performed by intermediate systems that optimizes the flow of multicast traffic; these intermediate systems (such as Layer 2 switches) listen for IGMP messages and build mapping tables and associated forwarding filters, in addition to reducing the IGMP protocol traffic.

**IP** Internet Protocol. IP is a layer 3 network protocol that is the standard for sending data through a network. IP is part of the TCP/IP set of protocols that describe the routing of packets to addressed devices.

**IPX** Internetwork Packet Exchange. IPX is a layer 3 and 4 network protocol designed for networks that use Novell® Netware®.

**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 periods (full-stops), and is made up of a network section, an optional subnet section and a host section.

**Jitter** An expression often used to describe the end-to-end delay variations during the course of a transmission. See also *latency*.

**LAN** Local Area Network. A network of endstations (such as PCs, printers, servers) and network devices (hubs and switches) that cover a relatively small geographic area (usually not larger than a floor or building). LANs are characterized by high transmission speeds over short distances (up to 1000 m).

**LLC** Logical Link Control. A sublayer of the IEEE data link layer that is located above the MAC sublayer. The LLC sublayer is responsible for MAC sublayer addressing, flow control, error control, and framing.

<b>latency</b>	The delay between the time a device receives a packet and the time the packet is forwarded out of the destination port.
<b>line speed</b>	See <i>baud</i> .
<b>loop</b>	An event that occurs when two network devices are connected by more than one path, thereby causing packets to repeatedly cycle around the network and not reach their destination.
<b>MAC</b>	Media Access Control. A protocol specified by the IEEE for determining which devices have access to a network at any one time.
<b>MAC address</b>	Media Access Control address; also called hardware or physical address. A layer 2 address associated with a particular network device. Most devices that connect to a LAN have a MAC address assigned to them as they are used to identify other devices in a network. MAC addresses are 6 bytes long.
<b>main port</b>	The port in a resilient link that carries data traffic in normal operating conditions.
<b>MDI</b>	Medium Dependent Interface. An Ethernet port connection where the transmitter of one device is connected to the receiver of another device.
<b>MDI-X</b>	Medium Dependent Interface Cross-over. An Ethernet port connection where the internal transmit and receive lines are crossed.
<b>MIB</b>	Management Information Base. A collection of information about the management characteristics and parameters of a networking device. MIBs are used by the Simple Network Management Protocol (SNMP) to gather information about the devices on a network. The Switch contains its own internal MIB.
<b>multicast</b>	A packet sent to a specific group of endstations on a network.
<b>multicast filtering</b>	A system that allows a network device to only forward multicast traffic to an endstation if it has registered that it would like to receive that traffic.
<b>Network-Layer Address</b>	The network-layer address refers to a logical address that applies to a specific protocol. A network-layer address exists at Layer 3 of the OSI reference model.

- NIC** Network Interface Card. A circuit board installed in an endstation that allows it to be connected to a network.
- OSI** Open Systems Interconnection. A reference to the protocols used when interconnecting computers. These protocols relate specifically to networking and are comprised of seven layers: physical, data link, network, transport, session, presentation, and application layer. For more information on the OSI model, refer to "What is IP Routing?"
- POST** Power On Self Test. An internal test that a Switch carries out when it is powered-up.
- protocol** A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.
- repeater** A simple device that regenerates LAN traffic so that the transmission distance of that signal can be extended. Repeaters are used to connect two LANs of the same network type.
- resilient link** A pair of ports that can be configured so that one takes over data transmission should the other fail. See also *main port* and *standby port*.
- RMON** IETF Remote Monitoring MIB. A MIB that allows you to remotely monitor LANs by addressing up to nine different groups of information.
- router** A device that provides WAN links between geographically separate networks.
- roving analysis port (RAP)** A system that allows you to copy the traffic from one port on a Switch to another port on the Switch. Roving Analysis is used when you want to monitor the physical characteristics of a LAN segment without changing the characteristics by attaching a monitoring device.
- RPS** Redundant Power System. A device that provides a backup source of power when connected to a Switch.
- SAP** Service Access Point. A well-defined location that identifies the user of services of a protocol entity.
- segment** A section of a LAN that is connected to the rest of the network using a switch or bridge.
- server** A computer in a network that is shared by multiple endstations. Servers provide endstations with access to shared network services such as computer files and printer queues.

- SLIP** Serial Line Internet Protocol. A protocol that allows IP to run over a serial line (console port) connection.
- SNMP** Simple Network Management Protocol. The current IETF standard protocol for managing devices on an TCP/IP network.
- Spanning Tree Protocol (STP)** A bridge-based system for providing fault tolerance on networks. STP works by allowing you to implement parallel paths for network traffic, and ensure that redundant paths are disabled when the main paths are operational and enabled if the main paths fail.
- stack** A group of network devices that are integrated to form a single logical device.
- standby port** The port in a resilient link that takes over data transmission if the main port in the link fails.
- STP** See *Spanning Tree Protocol (STP)*.
- switch** A device that interconnects several LANs to form a single logical LAN that comprises of several LAN segments. Switches are similar to bridges, in that they connect LANs of a different type; however they connect more LANs than a bridge and are generally more sophisticated.
- Switch Database** A database that is stored by a switch to determine if a packet should be forwarded, and which port should forward the packet if it is to be forwarded. Also known as Forwarding Database.
- TCP/IP** Transmission Control Protocol/Internet Protocol. This is the name for two of the most well-known protocols developed for the interconnection of networks. Originally a UNIX standard, TCP/IP is now supported on almost all platforms, and is the protocol of the Internet. TCP relates to the content of the data travelling through a network — ensuring that the information sent arrives in one piece when it reaches its destination. IP relates to the address of the endstation to which data is being sent, as well as the address of the destination network.
- Telnet** A TCP/IP application protocol that provides a virtual terminal service, letting a user log into another computer system and access a device as if the user were connected directly to the device.
- TFTP** Trivial File Transfer Protocol. Allows you to transfer files (such as software upgrades) from a remote device using the local management capabilities of the Switch.

**traffic prioritization** A system which allows data that has been assigned a high priority to be forwarded through a switch without being obstructed by other data.

**Transcend®** The 3Com umbrella management system used to manage all of 3Com's networking solutions.

**unicast** A packet sent to a single endstation on a network.

**VLAN** Virtual LAN. A group of location- and topology-independent devices that communicate as if they are on the same physical LAN.

**VLAN tagging** A system that allows traffic for multiple VLANs to be carried on a single link.

**WAN** Wide Area Network. A communications network that covers a wide area. A WAN can cover a large geographic area, and may contain several LANs within it.



# INDEX

---

## Numbers

802.1D 44  
802.1Q tagging 58

---

## A

Access Control Lists 86  
addresses  
    classes 101  
    IP 73, 99  
advertise RIP mode 81  
advertisement address 83  
aggregated links 16, 23  
aging time, definition 42  
alarm events 53  
alarm settings, default 54  
Alarms (RMON group) 50, 52  
ARP (Address Resolution Protocol)  
    cache 75  
    defined 75  
    location in OSI Reference Model 67  
    reply 76  
    request 76  
audit log 54  
auto-negotiation 16, 22

---

## B

bandwidth 21  
BOOTP 15  
BPDUs. *See* Bridge Protocol Data Units  
Bridge Identifier 35  
Bridge Protocol Data Units 35  
broadcast storm control 19

---

## C

cable  
    maximum length 92, 93  
cache, ARP 75  
Capture (RMON group) 52  
conventions  
    notice icons, About This Guide 10

text, About This Guide 10

---

## D

data link layer  
    IP 67  
default gateway 104  
default route, IP 71  
    gateway address 75  
Default VLAN 57  
defining IP interfaces 74  
Designated Bridge 36  
Designated Bridge Port 36  
DiffServ Code Point 46  
disabled  
    RIP mode 81  
DSCP (see DiffServ Code Point) 46  
dynamic route, IP 70

---

## E

enabled RIP mode 81  
errors  
    ICMP redirect 78  
    routing interface 74  
    VLAN 74  
Events (RMON group) 51, 52  
extended network prefix 103

---

## F

Fast Ethernet configuration rules 92  
Filter (RMON group) 51, 52  
flow control 22  
full duplex configuration rules 93

---

## G

gateway address 70  
Gigabit Ethernet configuration rules 91  
glossary 113

---

## H

Hello BPDUs 36  
History (RMON group) 50, 52  
Hosts (RMON group) 50, 52  
Hosts Top N (RMON group) 50, 52

---

## I

ICMP (Internet Control Message Protocol)  
    description 78

- location in OSI Reference Model 67
- ICMP Redirect, description 80
- ICMP Router Discovery 79
  - guidelines 79
- IEEE 802.1Q 57
- IEEE 802.3x flow control 16
- IGMP multicast filtering 29
- index, VLAN interface 74
- interfaces
  - IP 74
- Interior Gateway Protocols (IGPs) 70
- Internet
  - addresses 99
- InterNIC 100
- intranetwork routing 64
- IP (Internet Protocol)
  - addresses 73, 100
  - interfaces 74
- IP address 99
  - classes of 101
  - defined 100
  - derivation 100
  - division of network and host 100
  - example 102
  - netmask for supernet 108
  - network layer 67
  - next hop 68
  - obtaining 100
  - RIP 81
  - routing table 70
  - subnet mask 102
  - subnet portion 102
  - supernet portion 108
- IP interfaces
  - defining 74
  - parameters 74
- IP multicast
  - addressing 27
- IP routing
  - address classes 101
  - administering 74
  - defining static routes 75
  - features and benefits 68
  - OSI reference model 67
  - router, interface 68
  - routing table 69, 71
  - transmission process 68
  - types of routes 75

**L**

- learn RIP mode 81
- learned SDB entries 42

- link aggregation
  - configuring before establishing IP interfaces 73

**M**

- MAC (Media Access Control)
  - addresses
    - IP address 100
    - located with ARP 75
    - use in IP routing 77
- management
  - IP interface 69
- masks
  - subnet 74, 102
- Matrix (RMON group) 51, 52
- Max Age 36
- metric, RIP 70
- multicast filtering 27
  - IGMP 29
- multicasts, description 27
- multiple IP interfaces 72

**N**

- netmask for supernet 108
- network
  - addresses 99
  - layer 67
  - segmentation 68
- network configuration examples 96
- non-aging learned SDB entries 42

**O**

- obtaining
  - registered IP address 100
- OSI Reference Model 67
- OSPF (Open Shortest Path First)
  - location in OSI Reference Model 67

**P**

- path costs. See port costs
- permanent SDB entries 42
- poison reverse 83
- port costs, default 35
- port trunks
  - example 26
- priority in STP 35

**Q**

- QoS

- classifier 46
- DiffServ Code Point (DSCP) 46
- policy 46
- rules 46
- QoS (see Quality of Service) 45
- QoS Profile 46
- Quality of Service 45

---

## R

- registered IP address, obtaining 100
- Remote Monitoring. See RMON
- resilient links 32
- RIP (Routing Information Protocol)
  - advertisement address 83
  - defined 81
  - location in OSI Reference Model 67
  - poison reverse 83
  - route configuration 70
  - router mode 81
- RMON 19
  - alarm events 53
  - benefits 51
  - default alarm settings 54
  - groups 50
- Root Bridge 35
- Root Path Cost 36
- Root Port 36
- routers
  - interface 68
- routing
  - and bridging 66
  - overview 63
  - system 66
- routing architecture 63
- routing table, IP
  - contents 69
  - default route 71, 75
  - described 69
  - dynamic routes 70
  - metric 70
  - static routes 70, 75
  - status 70

---

## S

- SDB. See Switch Database
- segment, maximum length 92
- segmentation, network 68
- Service Level 46
- smart auto-sensing 22
- Spanning Tree Protocol, see STP 33
- static route, IP 70, 75

- Statistics (RMON group) 50, 52
- status, routing table 70
- STP 33
  - avoiding the subdivision of VLANs 40
  - Bridge Identifier 35
  - Bridge Protocol Data Units 35
  - default port costs 35
  - default priority 35
  - Designated Bridge 36
  - Designated Bridge Port 36
  - example 37
  - Hello BPDUs 36
  - Max Age 36
  - priority 35
  - Root Bridge 35
  - Root Path Cost 36
  - Root Port 36
  - using on a network with multiple VLANs 40
- subnet mask 102
  - defined 102
  - example 102
  - IP interface parameter 74
  - numbering 103
  - routing table 70
- subnets 102
- subnetting
  - defined 102
  - subnet mask 102
- sub-networks. See subnets
- supernet 108
- supernet mask
  - example 109
  - range of addresses 110
- supernet, example 111
- supernetting
  - defined 108
  - netmask 108
- Switch 4005
  - supernetting 108
- Switch Database 41

---

## T

- topology rules for Fast Ethernet 92
- topology rules with full duplex 93
- traffic prioritization 43
  - 802.1D 44
  - Quality of Service (QoS) 45

---

## V

- VLANs 55
  - 802.1Q tagging 58

- benefits 56
- Default 57
- defining the information for 57
- IEEE 802.1Q 57
- placing ports in multiple 58
- VLANs (virtual LANs)
  - errors 74
  - interface index 74
- VLSMs (Variable Length Subnet Masks) 107