3com

SuperStack® 3 Switch 3870 Family Implementation Guide

3CR17450-91
3CR17451-91

http://www.3com.com/

Part No. DUA174509-1BAA01
Published October 2005

3Com Corporation
350 Campus Drive
Marlborough, MA
USA 01752-3064

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.

ENCRYPTION

This product contains encryption and may require U.S. and/or local government authorization prior to export or import to another country.

CONTENTS

5 USING RESILIENCE FEATURES

6 USING THE SWITCH DATABASE

7 USING TRAFFIC MANAGEMENT

D ADVANCED IP ROUTING CONCEPTS

GLOSSARY

INDEX

ABOUT THIS GUIDE

This guide describes the features of the 3Com® SuperStack® 3 Switch 3870 (24 Port or 48 Port, Managed 10/100/1000). It outlines how to use these features to optimize the performance of your network.

The terms *Switch* and *Switch 3870* are used when referring to information that applies to both Switches.

Refer to the Management Quick Reference 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, refer to the Management Interface Reference Guide supplied in HTML format on the CD-ROM that accompanies your Switch or 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

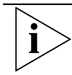
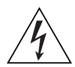
Icon	Notice Type	Description
	Information note	Information that describes important features or instructions
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device
	Warning	Information that alerts you to potential personal injury

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: `system password <password>` In this example, you must supply a password for <password>.
`Commands`	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: **`bridge port detail`**
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 *italics*	Italics are used to: ■ Emphasize a point. ■ Denote a new term at the place where it is defined in the text. ■ Identify menu names, menu commands, and software button names. Examples: From the *Help* menu, select *Contents*. Click *OK*.

Related Documentation

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

- *SuperStack 3 Switch 3870 Family Getting Started Guide*

  This guide contains:

  - 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 your Switch.

- *SuperStack 3 Switch 3870 Family Management Interface Reference Guide*

  This guide provides detailed information about the Web interface and Command Line Interface that enable you to manage your Switch. It is supplied in HTML format on the CD-ROM that accompanies your Switch.

- *SuperStack 3 Switch 3870 Family Management Quick Reference Guide*

  This guide contains:

  - A list of the features supported by your Switch.
  - A summary of the Web interface and Command Line Interface commands for the Switch.

- *Release Notes*

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

There are other publications you may find useful, such as:

- Documentation accompanying 3Com Network Supervisor. This is automatically installed on your workstation when you install 3Com Network Supervisor.

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

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 3870 Family Implementation Guide
- Part number: DUA1745-0BAA02
- Page 12

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.

1 SWITCH FEATURES OVERVIEW

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

- What is Management Software?
- Switch Features Explained

For detailed descriptions of the Web interface operations and the Command Line Interface (CLI) commands that you require to manage the Switch, refer to the Management Interface Reference Guide supplied in HTML format on the CD-ROM that accompanies your Switch.

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, refer to the Management Quick Reference Guide that accompanies your Switch.

Aggregated Links

Aggregated links are connections that allow devices to communicate using multiple links in parallel. Your Switch supports up to 32 aggregated links using the RJ-45 or SFP ports, or the 10 Gigabit Ethernet ports. Aggregated links provide two benefits:

- They can potentially increase the bandwidth of a connection.
- They can provide redundancy — if one link is broken, the other link will still pass traffic.

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.

SFP 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, refer to the Management Quick Reference Guide that accompanies your Switch.

Auto MDI/MDI-X

Auto MDI/MDI-X allows ports to detect whether they are connected to a computer or another switch and configure themselves accordingly. This eliminates the need for crossover cables.

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 Std 802.3-2002 (incorporating 802.3x) on ports operating in full-duplex mode.

For more information about auto-negotiation and port capabilities, see *Chapter 2: Optimizing Bandwidth*.

Configuration Save and Restore

The Configuration Save and Restore feature allows the configuration of your Switch to be saved as a file on a remote server, or to be restored onto the Switch from a remote file. The configuration information is stored in a readable ASCII text file.

All configuration information that can be set using the Switch's Command Line Interface is saved and restored.

You must have *read/write* management access level on the Switch to be able to save and restore the Switch configuration.

Important Considerations

- 3Com recommends the Switch unit is reset to its factory default settings before you restore a configuration onto it. You can reset the Switch using the **`system control initialize`** CLI command or the *System* > *Control* > *Initialize* Web interface operation.
- The configuration can only be restored onto a device of the same type (that is, a 24-port or 48-port Switch 3870) and with the same physical connections, as when the configuration was initially saved. The restore operation will be unsuccessful if the physical configuration of the device is different.
- The configuration of the Switch must only be restored or saved by a single user at a time.
- When using the Configuration Save and Restore feature, 3Com recommends that aggregated links are configured as either:
  - Manual aggregations with Link Aggregation Configuration Protocol (LACP) disabled on the ports that are to be manually placed in the aggregated link.

  or

  - LACP automatic aggregations — that is, LACP enabled on all ports and the aggregated links created automatically. The aggregated link should be enabled and Spanning Tree Protocol enabled.

  Parameters such as VLANs and Fast Start may be set up as required.

  Other combinations of port settings, however, are not recommended as Configuration Restore will only perform a "best effort" restore of the configuration. For example, LACP automatic aggregations with manually defined ports are restored as manual aggregations with manual ports. LACP automatic aggregations with automatic ports where the aggregated link is disabled and Spanning Tree Protocol is disabled are restored as manual aggregations with the aggregated link disabled.

For further information about LACP, see *Chapter 2: Optimizing Bandwidth*

- When restoring a configuration onto a unit over an aggregated link, communication with that unit may be lost because the restore operation disables the aggregated link ports. Communication over the aggregated links is re-established when the restore operation has been completed.

For detailed descriptions of the Configuration Save and Restore Web interface operations and Command Line Interface (CLI) commands, refer to the Management Interface Reference Guide supplied in HTML format on the CD-ROM that accompanies your Switch.

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 and query 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*.

Rapid Spanning Tree Protocol and Multiple Spanning Tree Protocol

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

RSTP 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.

The Multiple Spanning Tree Protocol (MSTP) is an extension to RSTP that supports multiple simultaneous spanning trees. Unlike STP and RSTP, MSTP supports VLANs using a spanning tree for each VLAN. This allows greater flexibility within your network as VLANs can be bridged using separate connections without risk of the Switch blocking one of the connections.

RSTP and MSTP are enhanced versions of STP (Spanning Tree Protocol) and fully compatible with STP systems. RSTP and MSTP can restore network connections quicker than the legacy STP feature. RSTP and MSTP can detect if they are connected to a legacy device that only supports IEEE 802.1D STP and will automatically downgrade to STP on that particular port.

RSTP and MSTP conform to the IEEE Std 802.1w-2001.

For more information about STP, RSTP, and MSTP, see Chapter 5: 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 6: Using the Switch Database.

Traffic Prioritization

The traffic prioritization capabilities of your Switch provides Class of Service (CoS) prioritization to your network. You can prioritize traffic on your network to ensure that high priority data is transmitted with minimum delay.

For more information about traffic prioritization, see Chapter 7: Using Traffic Management.

Rate Limiting

Rate limiting is the restriction of the bandwidth to or from a section of your network. Limiting the rate of network traffic reduces the stress on your network and, when used with traffic prioritization, ensures that important traffic is not held up when the network is busy.

For more information about rate limiting, see Chapter 7: Using Traffic Management.

Roving Analysis

Roving analysis is a feature that allows you to attach a network analyzer to one port and use it to monitor the traffic on other ports of the Switch. The system works by enabling you to define an analysis port (the port that is connected to the analyzer), and a monitor port (the port that is to be monitored). Once the pair is defined, and you start monitoring, the Switch takes all the traffic going in and out of the monitor port and copies it to the analysis port.

You can use roving analysis when you need the functions of a network analyzer, but do not want to change the physical characteristics of the monitored segment by attaching an analyzer to that segment.

For more information about roving analysis, see Chapter 8: Status Monitoring and Statistics.

RMON

Remote Monitoring (RMON) is an industry standard feature for traffic monitoring and collecting network statistics. The Switch software 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.

Event Notification

You can configure your Switch to send you notification when certain events occur. Events can be reported to Network Management Stations using Traps or SNMPv3 informs.

For more information about RMON and Event Notification, see Chapter 8: Status Monitoring and Statistics.

Broadcast Storm Control

Broadcast Storm Control is a system that monitors the level of broadcast traffic on each 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 that is faulty or configured incorrectly.

VLANs

A Virtual LAN (VLAN) is a flexible group of devices that can be located anywhere on 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 9: Setting Up Virtual LANs.

Automatic IP Configuration

Your Switch can have its IP information automatically configured using a DHCP server. Alternatively, you can manually configure the IP information.

For more information about how the automatic IP configuration feature works, see Chapter 10: Using Automatic IP Configuration.

Security

Your Switch has the following security features, which guard against unauthorized users connecting devices to your network:

- Network Login — Controls user access at the network edge by blocking or unblocking access on a per-port basis.
- RADA (RADIUS Authenticated Device Access) — Uses a device MAC address for authentication against a RADIUS server.
- Disconnect Unauthorized Device (DUD) — Disconnects a port or device (depending on the security mode) if an unauthorized device transmits data on it.
- Switch Management Login — User name and password information is stored on a RADIUS server database on your network. Login attempts to the Switch are remotely authenticated by the RADIUS server.
- Trusted IP — Enables you to define the IP host addresses and subnets trusted to access the management interfaces of the Switch.
- SSH (Secure Shell) — Enables secure access to the Command Line Interface of the Switch.

- SNMPv3 — Addresses the security shortfalls of both SNMPv1 & SNMPv2c and provides secure access to devices by a combination of authenticating and encrypting packets over the network.
- Private Ports — Protects end users from any interference from other end users attached to the same network.

For more information about how the port security features work, see *Chapter 11: "Securing Your Network"*.

Port Security

Your Switch supports the following port security modes, which you can set for an individual port or a range of ports:

- **No Security**

  Port security is disabled and all network traffic is forwarded through the port without any restrictions.
- **Learning Off**

  All currently learned addresses on the port are made permanent. Any packets containing a source address not learned on the port will be dropped.
- **Automatic Learning**

  You can limit the number of addresses that can be learned on individual ports.
- **Network Login**

  Connections are only allowed on a port once the client has been authenticated by a RADIUS server.
- **RADA (RADIUS Authenticated Device Access)**

  Each device is authenticated by MAC address with a list held on a RADIUS server.

The maximum number of permanent addresses on the Switch is 1000.

For more information about how port security works, see *Chapter 11: Securing Your Network*.

IP Routing

IP Routing is a method for distributing traffic throughout an IP network. It is used to join LANs at the network layer, that is Layer 3 of the OSI (Open Systems Interconnection) model. Your Switch is optimized for Layer 3 edge configurations and has only limited functionality as a core switch.

Dynamic Routing

Dynamic routing allows the Switch to adjust automatically to changes in network topology or traffic.

Routing Information Protocol (RIP)

RIP is a dynamic routing protocol that allows the Switch to adjust automatically to changes in network topology or traffic. Routes are calculated between networks automatically.

For more information about Layer 3 Routing, see *Chapter 12: "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, refer to the Management Interface Reference Guide supplied in HTML format on the CD-ROM that accompanies your Switch.

Port Features

The default state for all the features detailed below provides the best configuration for most users. *In normal operation, you do not need to alter the Switch from its default state.* However, under certain conditions you may want 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 prevents 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 prevents packet loss by inhibiting the transmitting port from generating more packets until the period of congestion ends.

Flow control is implemented using the IEEE Std 802.3-2002 (incorporating 802.3x) for ports operating in full-duplex mode, and back pressure for ports operating in half-duplex mode.

Auto-negotiation

Auto-negotiation allows ports to automatically determine the best 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 modify the capabilities that a port "advertises" on a per port basis, dependent on the type of port.

You can disable auto-negotiation for the whole Switch, or per port. You can also modify the capabilities that a port "advertises" on a per port basis, dependent on the type of port.

SFP ports do not support auto-negotiation of port speed.

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

If auto-negotiation is disabled, the auto-MDIX feature does not operate on the ports. Therefore the correct cables, that is, cross-over or straight-through need to be used. For more information, see the Getting Started Guide that accompanies your Switch.

Ports at both ends of the link should be set to auto-negotiate.

Jumbo Frames

The Switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames of up to 9216 bytes for the Gigabit Ethernet ports. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

When the connection is operating at full-duplex, all switches on the network between the two end nodes must be able to accept the extended frame size. For half-duplex connections, all devices in the collision domain would need to support jumbo frames.

Aggregated Links

Aggregated links are connections that allow devices to communicate using two member links in parallel. Aggregated links provide the following benefits:

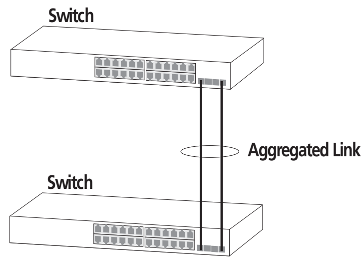
- They can potentially increase the bandwidth of a connection. The capacity of the multiple links is combined into one logical link.
- They can provide redundancy — if one link is broken, the other link will still pass traffic.

A maximum of 32 aggregated links can be created on a unit.

Your Switch supports aggregated links on the 10/100/1000 and SFP ports, and on the 10 Gigabit ports. An aggregation can be created by using two to eight 10/100/1000 ports or SFP ports in any combination from any unit in the stack, or by using two to four 10 Gigabit ports from any unit in the stack.

Figure 1 shows two Switches connected using an aggregated link containing two member links. If both ports on both Switch units are configured as 1000BASE-TX and they are operating in full-duplex, the potential maximum bandwidth of the connection is 2 Gbps.

Figure 1 Switch Units Connected Using an Aggregated Link



3Com recommends that you use IEEE 802.3ad LACP automatic aggregations rather than manual aggregations to ensure maximum resilience on your network. Using manual aggregations to connect to a stack could result in network loops if the cascade fails. By default, LACP is disabled on all Switch ports.

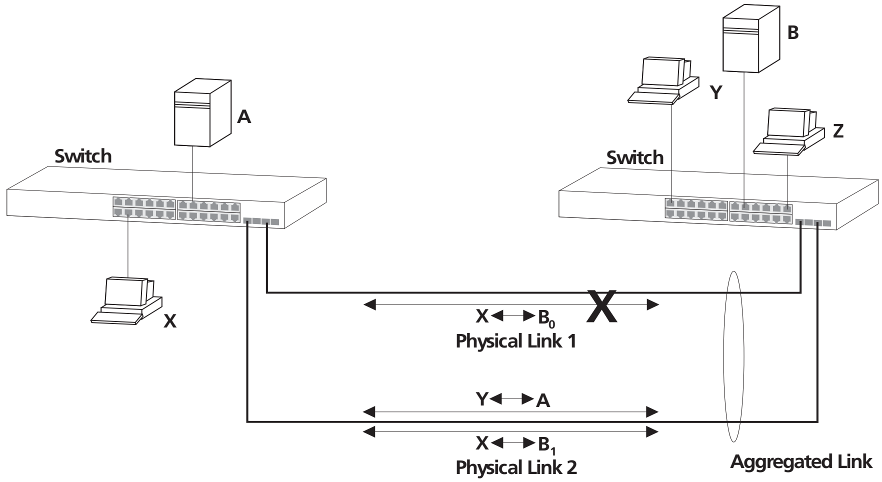
How 802.3ad Link Aggregation Operates

Your Switch supports IEEE Std 802.3-2002 (incorporating 802.3ad) aggregated links that use the Link Aggregation Control Protocol (LACP). LACP provides automatic, point-to-point redundancy between two devices (switch-to-switch or switch-to-server) that have full-duplex connections operating at the same speed.

By default, LACP is disabled on all Switch ports. If LACP is enabled on all Switch ports, this means that your Switch will detect if there is more than one connection to another device and will automatically create an aggregated link consisting of those links.

If a member link in an aggregated link fails, the traffic using that link is dynamically reassigned to the remaining member links in the aggregated link. Figure 2 shows the simplest case: two member links, that is the physical links, form an aggregated link. In this example, if link 1 fails, the data flow between X and B is remapped to physical link 2. The re-mapping occurs as soon as the Switch detects that a member link has failed — almost instantaneously. As a result, aggregated link configurations are extremely resilient and fault-tolerant.

Figure 2 Dynamic Reassignment of Traffic Flows



The key benefits of 802.3ad link aggregation are:

- Automatic configuration — Network management does not need to be used to manually aggregate links.
- Rapid configuration and reconfiguration — Approximately one to three seconds.
- Compatibility — Non-802.3ad devices can interoperate with 802.3ad enabled devices. However, you will need to manually configure the aggregated links as LACP will not be able to automatically detect and form an aggregation with a non-802.3ad device.
- The operation of 802.3ad can be configured and managed via network management.

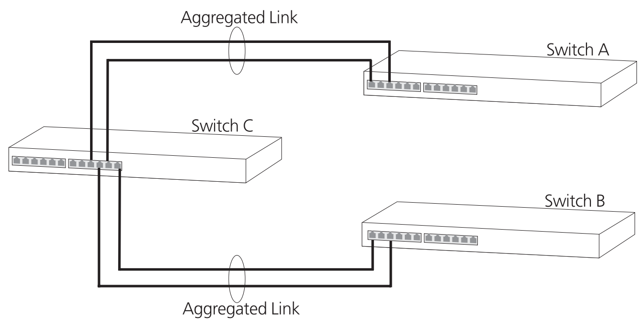
Implementing 802.3ad Aggregated Links

LACP can be enabled or disabled on a per port basis. You can implement 802.3ad aggregated links in two ways:

- Manual Aggregations — You can manually add and remove ports to and from an aggregated link via Web commands. However, if a port has LACP enabled, and if a more appropriate or correct automatic membership is detected by LACP, it will override the manual configuration.

  For example, in Figure 3, if a port on Switch C is physically connected to Switch B, but you manually configure the port on Switch C to be a member of an aggregated link for Switch A in error, LACP (if it is enabled) will detect this and place the port in the aggregated link for Switch B, thus overriding the manual configuration.

Figure 3 Aggregated Link — Example



- LACP Automatic Aggregations — If LACP detects the two active ports are sharing the same partner device, LACP will automatically assign both ports to form an aggregated link with the partner device.

  If you have an existing single port connection between two devices, this automatic behavior allows quick and easy addition of extra bandwidth by simply adding an extra physical link between the units.

The spanning tree costs for a port running LACP is the cost assigned for an aggregated link running at that speed. As required by the IEEE Std 802.3-2002 (incorporating 802.3ad), no changes in cost are made according to the number of member links in the aggregated link.

Aggregated Links and Your Switch

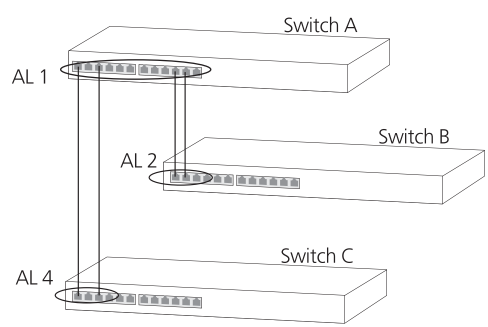
When any port is assigned to an aggregated link (either manually or via LACP), it will adopt the configuration settings of the aggregated link. When a port leaves an aggregated link, its original configuration settings are restored.

- Your Switch supports up to 32 aggregated links comprising any combination of 10/100/1000 or SFP ports from any unit in the stack, or comprising 10 Gigabit ports from any unit in the stack.
- A LinkUp / LinkDown trap will be sent for individual links or for an aggregation. Traps will not be sent for members of an aggregation.

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, if you are manually configuring aggregated links.
- 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 must have the same configuration.
- Aggregated links and the analyzer port used by roving analysis are mutually exclusive, that is, a port cannot be configured both as a member of an aggregated link and as an analyzer port.
- Aggregated links and port security are mutually exclusive, that is, you cannot have both these features operating on the same ports.
- Aggregated links and port privacy are mutually exclusive, that is, you cannot have both these features operating on the same ports.
- Member links must retain the same groupings at both ends of an aggregated link. For example, the configuration in Figure 4 will not work because Switch A has one aggregated link defined whose member links are then split between two aggregated links defined on Switches B and C. Note that this invalid configuration could not occur if LACP is enabled.

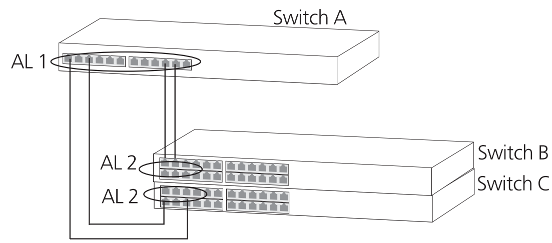
Figure 4 An Invalid Aggregated Link Configuration



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.

Alternatively, if Switches B and C are, for example, stacked Switch 3870 Family units and their member link ports defined as part of the same aggregated link as shown in Figure 5, the configuration will operate correctly as aggregated links are supported stack-wide by the Switch 3870 Family.

Figure 5 A Valid Aggregated Link Configuration



When using an aggregated link, note that:

- You can display statistics for an aggregated link or for individual port members within an aggregated link. Statistics displayed for an aggregated link are the sum of statistics for its current members. However, the collection of members may change over time, and therefore may not accurately reflect the accumulated statistics of the aggregated link over its lifetime.
- If you want 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 an entire aggregated link, you must disable all the aggregated link ports or disconnect all the links, except one — if you do not, a loop may be created.
- When manually creating an aggregated link between two devices, the ports in the aggregated link must not be physically connected together until the aggregated link has been correctly configured at both ends of the link. Failure to configure the aggregated link at both

ends before physically connecting the ports can result in a number of serious network issues such as lost packets and network loops.

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 through an aggregated link, a hardware-based traffic distribution mechanism determines which particular port in the link should be used. 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.

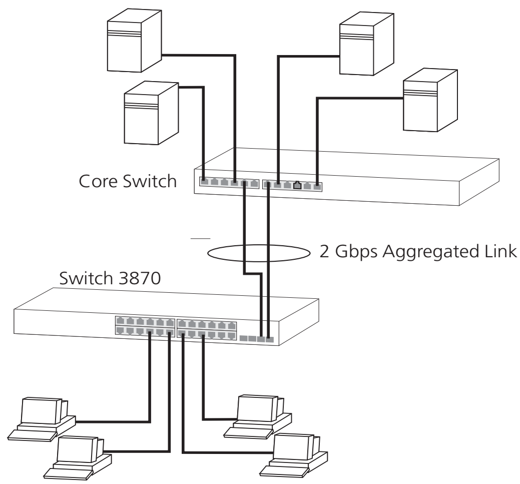
If the link state on any of the ports in an aggregated link becomes inactive due to link failure, then the Switch will automatically redirect the aggregated link traffic to the remaining ports. Aggregated links therefore provide built-in resilience for your network.

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 — Manual Configuration Example

The example shown in Figure 6 illustrates a 2 Gbps aggregated link between two Switch units, (that is, each port is operating at 1000 Mbps, full-duplex).

Figure 6 A 2 Gbps Aggregated Link Between Two Switch Units



To manually set up this configuration:

1 Prepare ports 5 and 7 on the core Switch for aggregated links. To do this:

   a Check that the ports have an identical configuration using your preferred management interface.

   b Add ports 5 and 7 on the specified unit to the aggregated link.

2 Prepare ports 23 and 24 on the Switch 3870 (or ports 47 and 48 if you are configuring a 48-Port Switch) for aggregated links. To do this:

   a Check that the ports have an identical configuration using your preferred management interface.

   b Add ports 23 and 24 on the 24-Port Switch (or ports 47 and 48 if you are configuring a 48-Port Switch) to the aggregated link.

3 Connect port 5 on the core Switch to port 23 on the 24-Port Switch or port 47 if you are configuring a 48-Port Switch.

4 Connect port 7 on the core Switch to port 24 on the 24-Port Switch or port 48 if you are configuring a 48-Port 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:

For detailed descriptions of the Web interface operations and the Command Line Interface (CLI) commands that you require to manage the Switch, refer to the Management Interface Reference Guide supplied in HTML format on the CD-ROM that accompanies your Switch.

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 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.

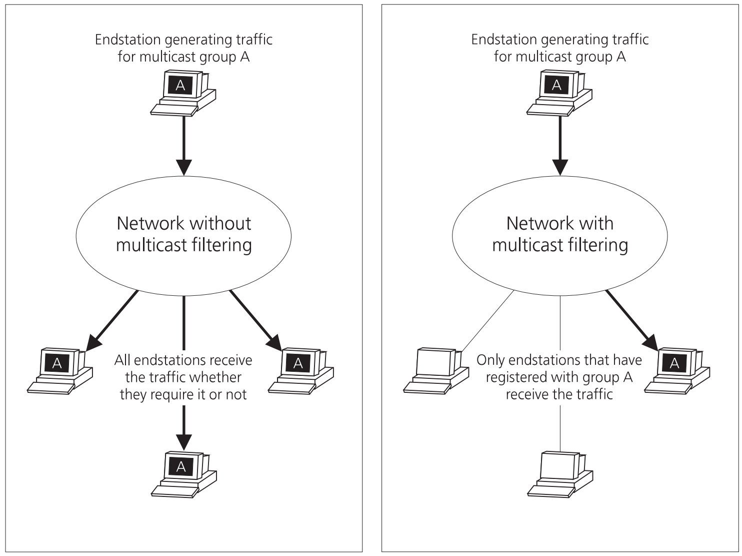
Multicast Filtering

Multicast filtering is the process that ensures that 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.

Multicast filtering is used to restrict multicasts within a VLAN. It does not route multicasts between different VLANs.

Figure 7 shows how a network behaves without multicast filtering and with multicast filtering.

Figure 7 The Effect of Multicast Filtering



Multicast Filtering and Your Switch

Your Switch provides automatic multicast filtering support using IGMP (Internet Group Management Protocol) Snooping. It also supports IGMP query mode.

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 want to join a multicast group and then sets its filters accordingly.

The Switch 3870 is compatible with any device that conforms to the IGMP v1 or v2. The Switch does not support IGMP v3. If you have an IGMP v3 network, you should disable IGMP snooping for the Switch using the **`snoopMode`** *command on the Web Interface.*

Query Mode

Query mode allows the Switch to function as the Querier on the management VLAN, if it has a lower IP address than any other Querier in the subnetwork to which it belongs and there is no IGMP v3 querier present.

IGMP querying is disabled by default on the Switch 3870. This helps prevent interoperability issues with core products that may not follow the lowest IP address election method.

You can enable or disable IGMP query mode for all Switch units in the stack using the `queryMode` command on the Command Line Interface IGMP menu.

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 that 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.
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 snooping enabled, the Switch learns that the port is to forward traffic for the multicast group and then forwards the IGMP report 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 snooping and IGMP querying using the `snoopMode` and `queryMode` commands on the Web interface. For more information about enabling IGMP multicast processes, refer to the Management Interface Reference Guide supplied on your Switch CD-ROM.

If IGMP multicast learning is not enabled, then IP multicast traffic is flooded to all ports in the VLAN.

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).

IGMP Versions

The Switch 3870 Family switches support IGMPv1 and IGMPv2 snooping.

The following describes the main purpose for each version:

- IGMPv1 provides the support for IP multicast routing. IGMPv1 specifies the mechanism for communicating IP multicast group membership requests from a host to its locally attached routers.
- IGMPv2 extends the features in IGMPv1 by quickly reporting group membership termination to the routing protocol. This feature is important for multicast groups in which the members are frequently changing.

The Switch 3870 Family is compatible with any device that conforms to the IGMP v1 or v2 protocol. If you have an IGMP v1 or v2 network, you should enable IGMP snooping for all Switch units in the stack using the **`snoopMode`** *command on the Command Line Interface.*

The Switch does not support IGMP v3. If you have an IGMP v3 network, you should disable IGMP snooping for the Switch using the **`snoopMode`** *command on the Web Interface.*

How IGMP Supports IP Multicast

IGMP provides a way for routers and switches to learn where group members exist on a network, and thus provides a critical function in the IP multicast packet delivery process.

Electing the Querier

On each subnetwork or broadcast domain (VLAN), the communication between routers, switches, and group members begins with one IGMP-capable device being elected as the querier – that is, the device that asks all hosts to respond with a report of the IP multicast groups that they want to join or to which they already belong. The querier is always the device with the lowest IP address on the subnetwork. It can be a router or a Layer 2 switch. The network traffic flows most efficiently if the querier is the closest device to the sources of IP multicast traffic.

Query Messages

The querier normally sends messages called IGMP Host Membership Query Messages, or queries, every 125 seconds. All the hosts hear the query because it is addressed to 224.0.0.1, which is a Class D address for all systems on the subnetwork. A query is not forwarded beyond the subnetwork from which it originates.

Host Messages

Hosts use IGMP to build their own types of IP multicast messages, as described in this section.

Response to Queries

Hosts respond to queries with IGMP Host Membership Report messages, or simply IGMP reports. These reports do not travel beyond their origin subnetworks, and hosts send them at random intervals to prevent the querier from being overwhelmed.

A host sends a separate report for each group that it wants to join or to which it currently belongs. Hosts do not send reports if they are not group members.

If a router does not receive at least one host report for a particular group after two queries, the router assumes that members no longer exist and it prunes the interface for that source-group spanning tree.

Join Message

Rather than wait for a query, a host can also send an IGMP report on its own initiative to inform the querier that it wants to begin receiving a transmission for a specific group (perhaps by clicking a *Go* or *Start* button on the client interface). This is called a join message. The benefit is faster transmission linkages, especially if the host is the first group member on the subnetwork.

Leave-Group Messages

Leave-group messages are a type of host message defined in IGMP version 2. If a host wants to leave an IP multicast group, it issues a leave-group message addressed to 224.0.0.2, which is a Class D address for all routers on this subnetwork. Upon receiving such a message, the querier determines whether that host is the last group member on the subnetwork by issuing a group-specific query.

Leave-group messages lower leave latency – that is, the time between when the last group member on a given subnetwork sends a report and when a router stops forwarding traffic for that group onto the subnetwork. This process conserves bandwidth. The alternative is for the router to wait for at least two queries to go unanswered before pruning that subnetwork from the delivery tree.

Role of IGMP in IP Multicast Filtering

To further refine the IP multicast delivery process and maximize bandwidth efficiency, a Layer 3 module filters IP multicast packets on appropriate ports using a process called IGMP snooping. Both bridged interfaces and routed interfaces record which ports receive host IGMP reports and then set their filters accordingly so that IP multicast traffic for particular groups is not forwarded on ports or VLANs that do not require it.

4 STACK MANAGEMENT

This chapter describes how to use the stack management capabilities of your Switch. The Switch 3870 can create mixed stacks of up to eight units high, which can be managed as a single system when connected together. The stack system is based on a centralized stacking topology whereby one master unit represents the whole stack.

Some combinations of stacked 24-port and 48-port units restrict the number of 10G modules supported by the stack. Table 3 *shows which stack configurations restrict the number of supported modules.*

Table 3 Maximum Stack Configurations

Type of Unit		Total Units in the Stack	Maximum Modules
48-Port	**24-Port**		
0	8	8	8
8	0	8	0
7	1	8	2
7	0	7	4
6	2	8	4
6	1	7	6
6	0	6	6

This chapter covers the following topics:

Master Election

When the stack is powered on and completes the startup process, the master unit is determined through the Master Election process.

The master unit election is based on the following rules:

- If a unit has previously been elected as the master unit and it has been running for more than 20 seconds, then it enters 'non-preemptive mode'. This means that the unit will remain the master unit and the other units in the stack will be backup master units.
- If no units are in non-preemptive mode or if multiple units are in non-preemptive mode, the unit with the lowest MAC address is elected as the master unit. This could occur if multiple master units are connected to form a stack.

Backup Master Units

All non-master units in the stack are considered backup master units and can perform the functions of a master unit if the elected master unit is no longer available.

If the master unit fails, is power cycled, or a stack topology change is detected, then the system will perform the following tasks:

- Re-elect a new master unit.
- Synchronize all units in the stack with the latest configuration information that is stored on the master unit.

Topology Discovery

Once the master unit has been elected, it performs a Topology Discovery to find the connected stack units and build up a database containing information about each unit.

The information collected from each unit is as follows:

- Unit Configuration (model and description)
- Software Version
- Hardware Version
- CPU Version
- Device MAC Address
- Device Serial Number
- EPLD version (if any)

If an expansion module is fitted, the information collected also includes:

- Module Type and Status
- Module Software Version

Auto Unit ID Assignment

Once the Topology Discovery is complete, the master unit does the following:

- **Assigns a Unit ID —** This is assigned to each unit in the stacking system and is used for system configuration and simple management. Only the master unit can assign an ID to each unit in the stack. If a unit already has a Unit ID stored in the master unit's flash memory, then the master unit will re-assign this same Unit ID to the unit. If the unit does not already have a Unit ID, then the master unit will assign it the next available Unit ID.
- **Generates a Unit ID Table** — This is generated by the master unit to map MAC addresses and Unit IDs. The master unit maintains and updates the Unit ID table when the Unit ID assignment is completed and saves it to its flash memory. The table is updated if a new unit is added to the stack.

Image Checking

After the Unit IDs have been assigned, the master unit performs a consistency check to ensure that all the units and expansion modules in the stack are running the same version of firmware. Units and expansion modules run different firmware. However, the unit firmware and expansion module firmware are combined into a single downloadable image. This is achieved using the information gathered during Topology Discovery.

If the 'next boot firmware' version of any unit in the stack (that is, the image to run after the next reboot) is not the same as the combined download image referenced above, it will be replaced during TFTP download.

If the current runtime version of any unit in the stack is not the same as the master unit's, the stack will operate in Special Stacking Mode in which all backup units and expansion modules are disabled as described below:

- The master unit starts normal operation mode in standalone mode.

- The master unit can see all units in the stack and maintain stack topology.
- None of the other units can function (all ports will be disabled).
- All user-initiated commands to configure the non-functioning units are dropped. The master unit, however, will be able to communicate the following information to the non-functioning units:
  - Image downloads
  - Stack topology information
  - System configuration information already stored on the master

System Initialization

If the master unit determines during image checking that all units and expansion modules are running the same version of firmware, the system will be initialized for Normal Stacking Mode. If not, then the system will be initialized for Special Stacking Mode.

System Initialization for Normal Stacking Mode

The master unit initializes the stack using the last saved system configuration that is stored in its local flash memory. To conserve flash space, the configuration is stored as a plain text file containing only those settings that differ from the system default settings.

The master unit looks for changes to the configuration (for example, port settings, VLAN settings, and parameter changes) and saves these changes to its flash memory. Two 'rotating' files are used in flash memory so that only the two most recent sets of changes are available. Changes are saved to one file and the next time are saved to the next file. If the configuration changes again, the first file is overwritten.

If the configuration file contains information (such as the MAC address and Unit ID) for units that appear in the Unit ID table, then the system will apply the configuration to those units. The system will apply default settings to any units that do not have configuration information in the file.

If a system file is corrupted, the master unit will initialize the stack and set it to the Factory Default Configuration.

System Initialization for Special Stacking Mode

In this mode, only the master unit is initialized with system configuration information. The other units are not initialized and are forced to remain in non-operational mode, where all ports are disabled by default.

Operating in Special Stacking Mode

With the stack running in Special Stacking mode, your use of management commands is limited. 3Com recommends that you monitor and upgrade the stack in one of the following ways:

- CLI/Telnet/Web Interface
- 3Com Network Supervisor (3NS)

CLI/Telnet/Web Interface

In Special Stacking mode, the master unit displays warning messages whenever you log into the system through CLI, Telnet or Web, that inform you that an image download is required.

You can use a CLI, Web or SNMP command to download the run-time image from a remote server to the master unit. The master unit stores the image as its 'Next boot image' and downloads the image to those backup units that are running a different image version.

3Com Network Supervisor (3NS)

During its Network Discovery process, 3NS runs a report that detects stack misconfigurations. If you notice inconsistent firmware versions on the report, then you will need to upgrade the device via the 3NS agent upgrade. The image is downloaded to the master, which automatically downloads this version of the software to all the other units.

When the image download has completed, the whole stack is automatically rebooted and each image in the new stack boots up with the new image.

Recovering from a Master Unit Failure

During normal operation, the master unit sends 'heartbeat' messages to each unit in the stack to indicate that it is still running. If the master unit fails, the other units in the stack will detect this and the stack will go through another master election process, where the unit with the lowest MAC address becomes the new master unit. During the election process and the associated follow-on operations (topology discovery, unit ID assignment, image checking, system initialization), traffic on the network will be disrupted for up to two minutes while the stack recovers.

Recovering from a Change in Stacking Topology

To ensure minimal disruption to the stack in case of a break in the stacking cable, always connect a wrap-around cable from the bottom unit back up to the top unit in the stack. If the stack is connected in this manner, a break in the stacking cable will not affect the operation of other units in the stack.

Regardless of whether you configure the stack in a ring or line topology, any changes to a backup unit, such as the removal or insertion of a unit, will force the master unit to rediscover the new stack topology.

If you do not connect the stack in a ring topology, a break in the stack cable will cause the stack to break into two separate segments. In this case, a master unit will be elected for both of the stacks. However, backup information inherited from the previous master unit will cause the same IP address to be used by both master units in the two stacks. You must therefore manually reconfigure the IP address of the management interface on one of the master units.

5 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.

The Switch provides resilient links using the Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP). The spanning tree protocols respond to changes in the network infrastructure, preventing network loops and network outages by starting and stopping redundant links. The Switch is compatible with other switches that use MSTP, RSTP, or the 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, refer to the Management Interface Reference Guide supplied in HTML format on the CD-ROM that accompanies your Switch.

Rapid Spanning Tree Protocol

The Rapid Spanning Tree Protocol makes your network more resilient to link failure and provides protection from loops — one of the major causes of broadcast storms. RSTP is enabled by default on your Switch.

To be fully effective, RSTP or STP must be enabled on all Switches on your network.

RSTP provides the same functionality as STP. For details on how the two systems differ, see "How RSTP Differs from STP" on page 55.

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
- Multiple Spanning Tree Protocol
- Using STP on a Network with Multiple VLANs

The protocol is a part of the IEEE Std 802.1w-2001, bridge specification. To explain RSTP more effectively, your Switch will be referred to as a bridge.

Rapid Spanning Tree Protocol (RSTP)

The Rapid Spanning Tree Protocol (RSTP) is an enhanced Spanning Tree feature. RSTP implements the Spanning Tree Algorithm and Protocol, as defined in the IEEE Std 802.1w-2001.

Some of the benefits of RSTP are:

- Faster determination of the Active Spanning Tree topology throughout a bridged network.
- Support for bridges with more than 256 ports.
- Support for the Fast-Forwarding configuration of edge ports provided by the 'Fast Start' feature. Fast Start allows a port that is connected to an endstation to begin forwarding traffic after only four seconds. During this four seconds RSTP (or STP) will detect any misconfiguration that may cause a temporary loop and react accordingly.

  If you have Fast Start disabled on a port, the Switch will wait up to 30 seconds before RSTP (or STP) lets the port forward traffic. However, this delay is not incurred if another bridge is connected to the port and both ends of the link are operating in RSTP mode.

If Fast Start is enabled on a port and the Switch receives a Bridge Protocol Data Units (BPDU) from the connected device, it will stop using Fast Start on this port because it is connected to another bridging device (such as a switch or router). Note that the Switch will continue to show that Fast Start is enabled for this port, but it will not be operational under these circumstances.

- Easy deployment throughout a legacy network, through backward compatibility:
  - It will default to sending 802.1D style BPDUs on a port if it receives packets of this format.
  - It is possible for some ports on a Switch to operate in RSTP (802.1w) mode and other ports, for example those connected to a legacy Switch, to operate in STP (802.1D) mode.
  - You have an option to force your Switch to use the legacy 802.1D version of Spanning Tree, if required.

What is STP?

STP (802.1D) 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.

RSTP provides the same functionality as STP. For details on how the two systems differ, see *"How RSTP Differs from STP" on page 55**.*

As an example, Figure 8 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 8 A Network Configuration that Creates Loops

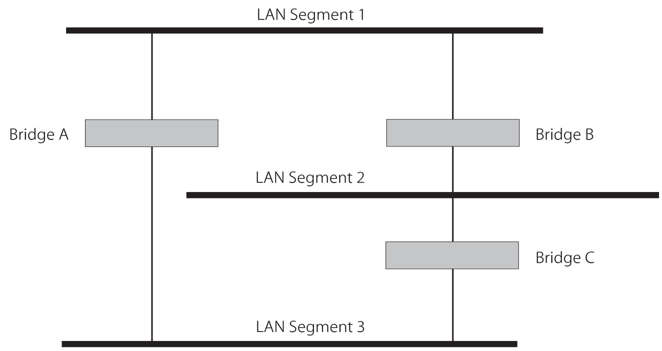
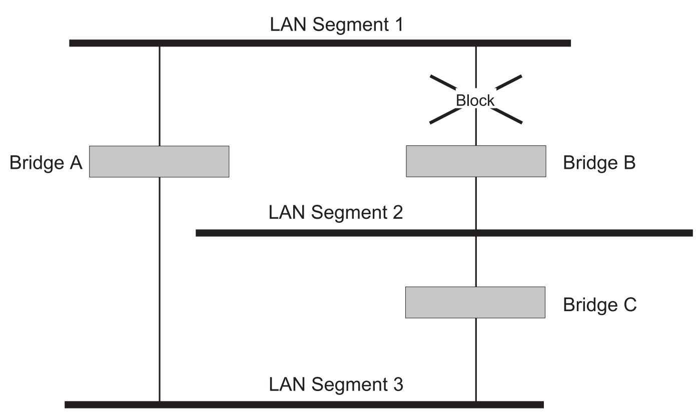


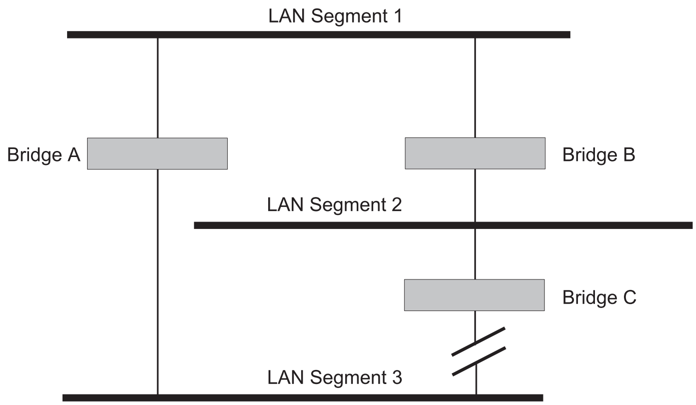
Figure 9 shows the result of enabling STP on the bridges in the configuration. STP detects the duplicate paths and prevents, or *blocks*, one of them from forwarding traffic, so this configuration will work satisfactorily. STP has determined that traffic from LAN segment 2 to LAN segment 1 can only flow through Bridges C and A, because, for example, this path has a greater bandwidth and is therefore more efficient.

Figure 9 Traffic Flowing through Bridges C and A



If a link failure is detected, as shown in Figure 10, the STP process reconfigures the network so that traffic from LAN segment 2 flows through Bridge B.

Figure 10 Traffic Flowing through Bridge B



STP determines 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 8, Figure 9, and Figure 10, 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 Speed	Link Type	Path Cost 802.1D, 1998 Edition	Path Cost 802.1w-2001
10 Mbps	Half-duplex Full-duplex Aggregated Link	100 99 100	2,000,000 1,999,999 2,000,000
100 Mbps	Half-duplex Full-duplex Aggregated Link	19 18 19	200,000 199,999 200,000
1000 Mbps	Full-duplex Aggregated Link	4 5	20,000 20,000
10000 Mbps	Full-duplex Aggregated Link	2 2	2,000 2,000

The default path cost for an aggregated link depends on the number of member ports.

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 adjust to 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.

CAUTION: *Network loops can occur if aggregated links are manually configured incorrectly, that is, the physical connections do not match the assignment of ports to an aggregated link. RSTP and STP may not detect these loops. So that RSTP and STP can detect all network loops, you must ensure that all aggregated links are configured correctly.*

How RSTP Differs from STP

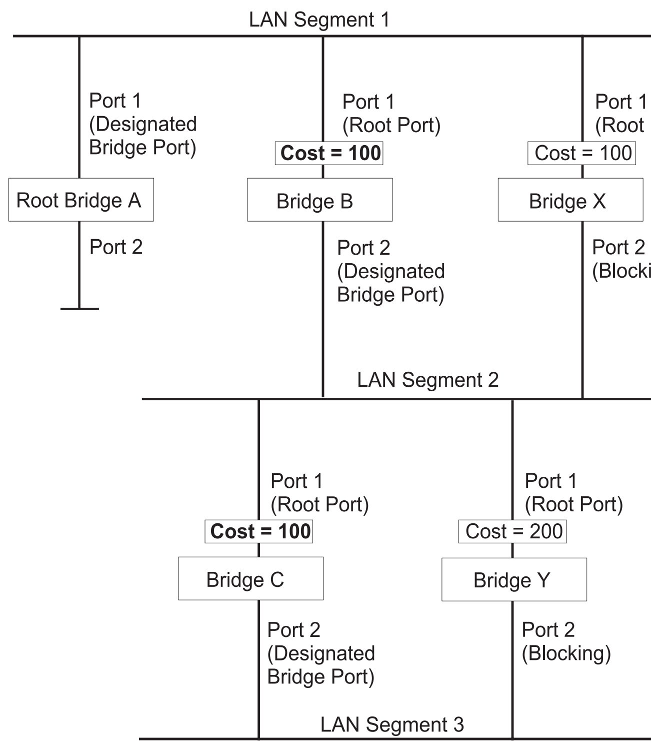
RSTP works in a similar way to STP, but it includes additional information in the BPDUs. This information allows each bridge to confirm that it has taken action to prevent loops from forming when it wants to enable a link to a neighbouring bridge. This allows adjacent bridges connected via point-to-point links to enable a link without having to wait to ensure all other bridges in the network have had time to react to the change.

So the main benefit of RSTP is that the configuration decision is made locally rather than network-wide, which is why RSTP can carry out automatic configuration and restore a link faster than STP.

STP Example

Figure 11 shows a LAN that has STP enabled. The LAN has three segments, and each segment is connected using two possible links.

Figure 11 Port Costs on a Network



- Bridge A has the lowest Bridge Identifier on 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 12 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.

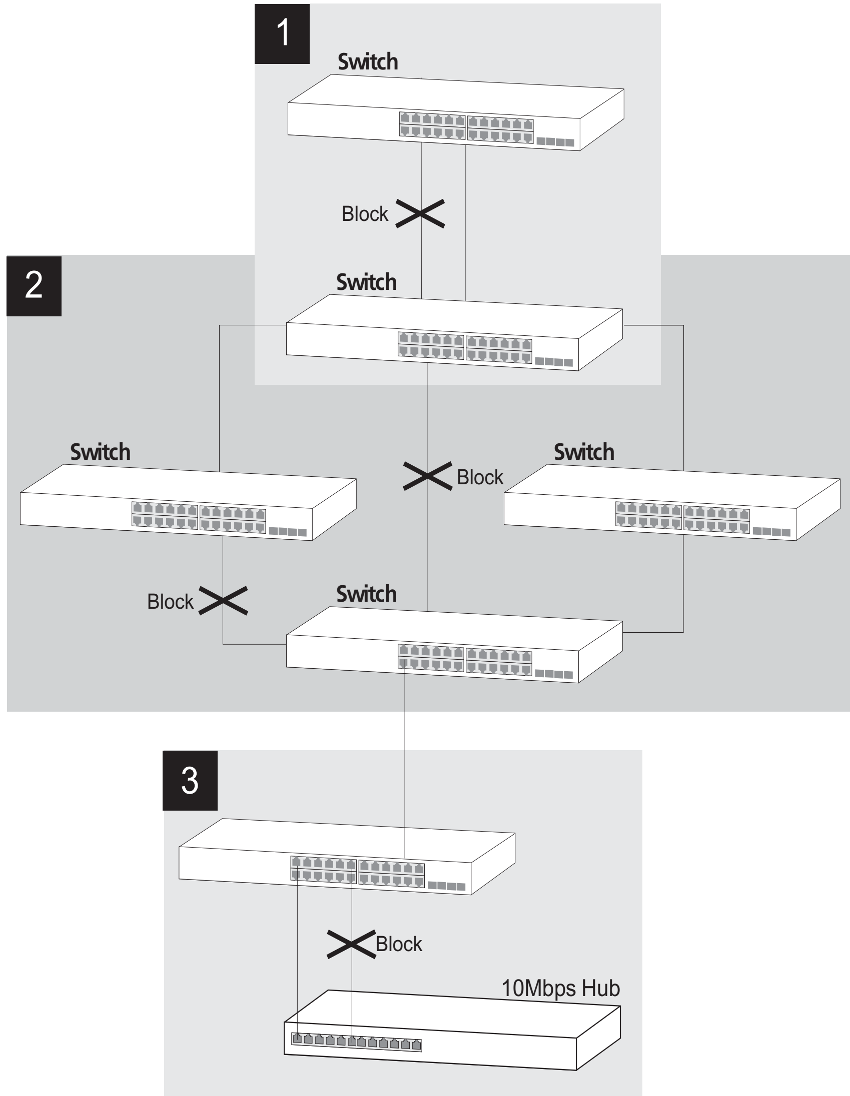
- **Configuration 2 — Redundancy through Meshed Backbone**

  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 12 STP Configurations



Multiple Spanning Tree Protocol

The Multiple Spanning Tree Protocol (MSTP) is an extension to RSTP that supports multiple simultaneous spanning trees. Unlike STP and RSTP, MSTP supports VLANS using a spanning tree for each VLAN. This allows greater flexibility within your network as VLANs can be bridged using separate connections without risk of the Switch blocking one of the connections.

Setting up an MSTP Region

MSTP architecture is based on regions. An MSTP Region is defined by a name, revision number and a maximum hop size. For devices to share MSTP information, they must have the same Region Name, Revision Number and be within the maximum number of allowed hops of the MSTP Master.

To set up a single MSTP region on your network:

- Assign all MSTP devices the same *Region Name*.
- Assign all the same *Revision Number*.
- Ensure that the *Region Maximum Hop* is larger than the maximum hops across your network.

Figure 13 Single MSTP Region

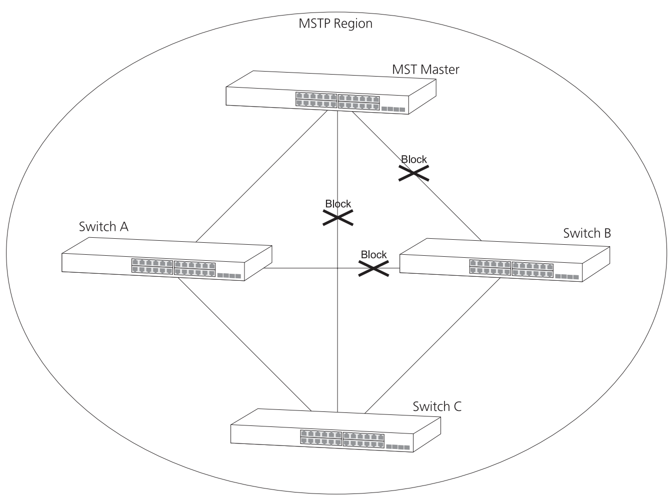


Figure 13 shows a network that is part of a single MSTP Region.The switches share the same Region Name and Revision Number. The Region Maximum Hops is set to at least 3 to allow the MSTP information to propagate across the region.

Using Multiple MSTP Regions

MSTP allows you to create separate independent regions within your network. You may want to use separate regions:

- To improve the efficiency of your network.
- To manage parts of your network independently.
- To overcome any hardware limitations on the number of VLANS or the number of Multiple Spanning Tree Instances supported by a device on your network.

Figure 14 Multiple MSTP Regions

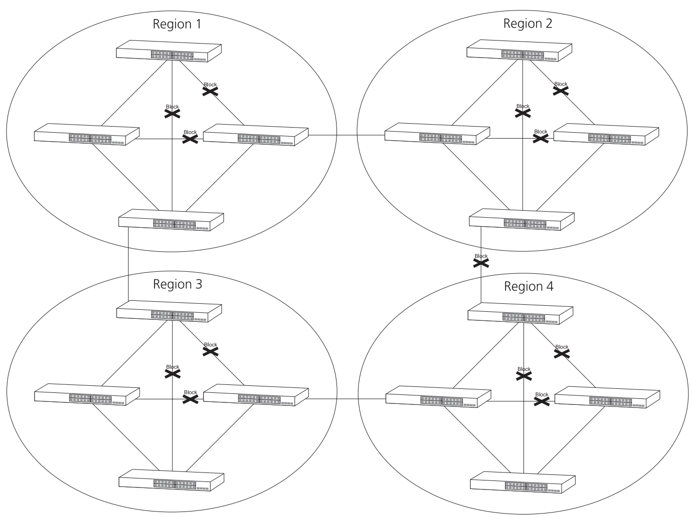


Figure 14 shows a network consisting of four separate MSTP Regions. Spanning tree links are still possible between the MSTP Regions but can only be of STP/RSTP, as a single switch can only belong to a single MSTP region. Ensure that the connections obey the rules for STP connections and VLANS (see "Using STP on a Network with Multiple VLANs" on page 61).

MSTP and VLANs

MSTP is not only more scalable than RSTP but supports VLANs by putting each VLAN into its own spanning tree. Each spanning tree supported by an MSTP Region is known as a Multiple Spanning Tree Instance (an MSTI). This isolation of each VLAN allows MSTP to correctly preserve multiple links between switches if those links serve different VLANS.

Figure 15 MSTP and VLANs

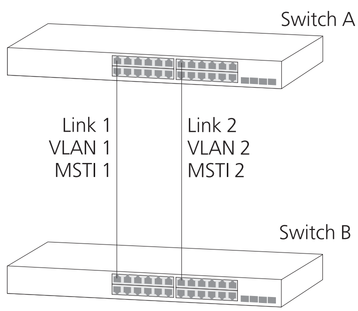


Figure 15 shows two switches in the same MST Region with two links bound to different VLANs. In this situation, STP and RSTP would block one of the links, isolating the VLAN from the rest of the network. Fortunately, MSTP recognizes that they are separate VLANs because they belong to different MST Instances and allows both links.

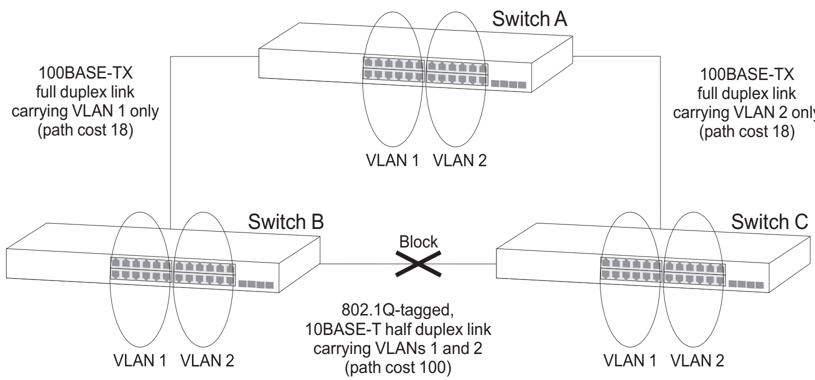
Using STP on a Network with Multiple VLANs

When using the Switch with other legacy devices or when connecting MSTP Regions together, STP or RSTP will be used instead of MSTP. STP and RSTP do not take VLANs into account when they calculate 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. Therefore, you must ensure that any VLAN configuration on your network takes into account the expected STP topology and alternative topologies that may result from link failures.

Figure 16 shows an example of a network that contains 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 16 Configuration that Separates VLANs



To avoid any VLAN subdivision, it is recommended 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 9: "Setting Up Virtual LANs"**.*

6 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, 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, refer to the Management Interface Reference Guide supplied in HTML format on the CD-ROM that accompanies your Switch.

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 via the `bridge addressDatabase` CLI command, the *Bridge > Address Database* Web interface operation, or an SNMP Network Manager, for example 3Com Network Supervisor.

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 turned off, 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 via the `bridge addressDatabase` remove CLI command, the *bridge* > *addressDatabase* > *remove* Web operation, or the Switch is initialized.

7 USING TRAFFIC MANAGEMENT

Using the traffic management capabilities of your Switch allows your network traffic to be controlled and prioritized to ensure that high priority data is transmitted with minimum delay.

The Switch 3870 has two features that allow you to manage the traffic on your network:

- Traffic Prioritization — Ensures that important data is forwarded promptly by the Switch without delay. See "What is Traffic Prioritization?" on page 66.
- Rate Limiting — Keeps your core network traffic down by setting a maximum traffic rate on a port by port basis. See "Limiting the Rate of a Port" on page 70.

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.

Traffic prioritization is most useful for critical applications that require a high level of service 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** — Used by design departments that need priority connections to server farms and other devices for transferring large files.

Traffic Prioritization and Your Switch

The traffic should be marked as it enters the network; the marking can be achieved in two ways:

- The original device can apply DSCP (DiffServ code point) or 802.1p markings to the packet before transmission.
- The edge port on the Switch connecting the originating device can mark or re-mark the packets using 802.1p, before sending the packets to the network.The Switch does not support DSCP marking or remarking.

The transmitting endstation sets the priority of each packet. When the packet is received, the Switch places 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 according to the queuing mechanism selected, see "Traffic Queues" on page 69.

How Traffic Is Processed To Provide Class of Service

A received packet at the ingress port is checked for its DSCP and IEEE 802.1D attributes to determine the level of service that the packet should receive.

802.1D packets are categorized into the eight traffic classes defined by IEEE 802.1D; the higher the class, the higher the priority given the packet on transmission.

DSCP packets are categorized into the eight service levels as shown in Figure 18 and mapped to the appropriate queue.

The priority defined in the service level directs the packet to the appropriate egress queue. When a packet comes in with both 802.1D and DSCP priority markings, the higher of the priorities will be used.

How Traffic Prioritization Works

Traffic prioritization ensures that high priority data is forwarded through the Switch without being delayed by lower priority data. Traffic prioritization uses the eight 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. High priority traffic is given preference over low priority traffic to ensure that the most critical traffic gets the highest level of service.

The Switch employs three methods of classifying traffic for prioritization. Traffic classification is the means of identifying which application generated the traffic, so that a service level can be applied to it.

The three supported methods for classifying traffic are:

- 802.1D (classification is done at layer 2 of the OSI model).
- DiffServ code point (classification is done at layer 3 of the OSI model).
- IP Port (classification is done at layer 4 of the OSI model).

These methods can be used together. If a packet is prioritized differently by the two methods, then it will be tagged with the higher priority.

802.1D Traffic Classification

At layer 2, a traffic service class is defined in 802.1Q frame, which is able to carry VLAN identification and user priority information. The information is carried in a header field immediately following the destination MAC address and source MAC address.

802.1D Priority Levels

The traffic prioritization feature supported by the Switch at layer 2 is compatible with the relevant sections of the IEEE 802.1D/D17 standard (incorporating IEEE 802.1p). Once a packet has been classified, the level of service relevant to that type of packet is applied to it.

The 802.1D standard specifies eight distinct levels of priority (0 to 7), each of which relates to a particular type of traffic. The priority levels and their traffic types are shown in Figure 17 in order of increasing priority.

You cannot alter the mapping of priority levels 0 - 7 to the traffic queues. These priority levels are fixed to the traffic queues as shown in Figure 17.

Figure 17 IEEE 802.1D Traffic Types

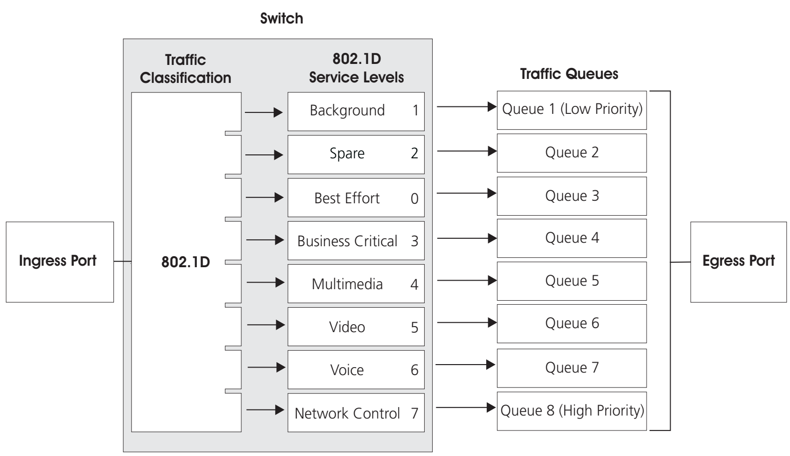


Figure 17 illustrates IEEE 802.1D traffic types as well as associated priority levels and how they are mapped to the eight supported traffic queues.

DiffServ Traffic Classification

DiffServ is an alternative method of classifying traffic so that different levels of service can be applied to it on a network. DiffServ is a layer 3 function; and the service to be applied is contained within the DSCP field, which is in the IP header of a packet.

Figure 18 DSCP Service Level Mapping

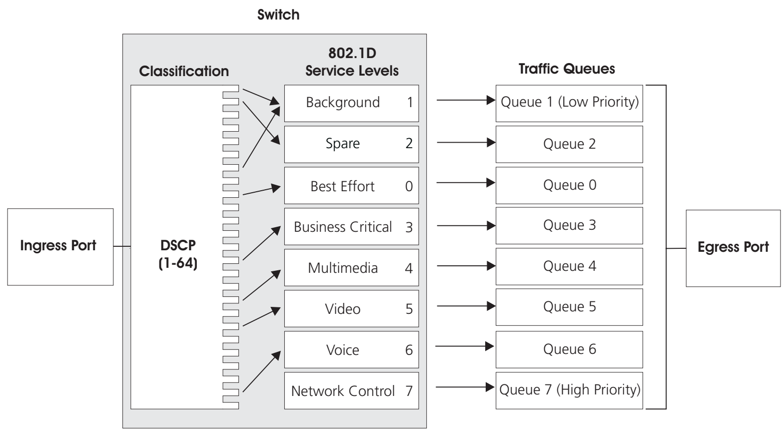


Figure 18 illustrates how DiffServ code point (DSCP) service levels are mapped to the eight traffic queues.

IP Port Traffic Classification

The Switch supports classification of traffic from legacy devices according to its IP port number.

When an IP packet is transmitted, it is always tagged with an IP port number. (When an IP packet is transmitted, it is always tagged with a source IP address and IP port number, and a destination IP address and IP port number.) This number represents the type of application that created the packet and can be used to prioritize traffic originating from different applications.

The transmitting endstation tags a packet with an IP port number. When the packet is received, the Switch places the packet in the queue that corresponds to the IP port number of the packet. If there is no priority set against the IP port number then the packet will be sent out with the default priority.

Traffic Queues

It is the multiple traffic queues within the Switch hardware that allow packet prioritization to occur. Higher priority traffic can pass through the Switch without being delayed by lower priority traffic. As each packet arrives in the Switch, it passes through any ingress processing (which includes classification), and is then sorted into the appropriate queue. The Switch then forwards packets from each queue. Note that each egress port has its own set of queues, so that if one port is congested, it does not interfere with the queue operation of other ports.

The Switch uses the following queuing mechanisms:

- Weighted Round Robin (WRR) — This method services all the traffic queues, giving priority to the higher priority queues. Under most circumstances, this method gives high priority precedence over low-priority, but in the event that high-priority traffic exceeds the link capacity, lower priority traffic is not blocked. This is the default method.
- Strict Priority Queuing (SPQ) — This method guarantees that traffic on a higher priority queue will always be serviced ahead of traffic waiting on a lower priority queue. This can have the disadvantage that lower priority queues may become starved of bandwidth when the higher priority queues are heavily utilized.

Traffic queues cannot be enabled on a per-port basis on the Switch 3870.

Limiting the Rate of a Port

Limiting the rate at which a port can receive or send traffic can be used to ease congestion on bottlenecks on your network and provide simple prioritization when the network is busy.

Rate limiting is commonly used in the following situations:

- To prevent a high bandwidth client or group of clients from dominating the traffic on your network.
- To balance the traffic at a bottleneck, such as an external-facing router, so that different departments or parts of your network get similar access across the bottleneck.

The advantage of rate limiting is that it is a simple solution: it is easy to set up and maintain. It can be used to effectively keep the traffic on your network to a manageable level.

Traffic Prioritization and Rate Limiting

Traffic prioritization and rate limiting can be used together to effectively manage the traffic on your network:

- Rate limiting will ensure that the traffic on a connection never exceeds the rate you specify.

- Traffic prioritization will ensure that any packets dropped at times of network congestion are of the lowest priority.

Traffic prioritization and rate limiting are best used together if the egress rate rather than the ingress rate is limited on a port; in other words, if the traffic rate leaving the Switch is limited rather than the traffic arriving at the Switch. This ensures that the traffic is prioritized before rate limiting is applied and the lowest priority packets are dropped first.

Rate limiting on ingress, as the packets arrive at the port, is not as effective. The Switch cannot determine the order in which packets will arrive and will not filter by priority.

8 STATUS MONITORING AND STATISTICS

This chapter contains details of the features that assist you with status monitoring and statistics. It covers the following topics:

- Roving Analysis Port
- RMON

For detailed descriptions of the Web interface operations and the Command Line Interface (CLI) commands that you require to manage the Switch, refer to the Management Interface Reference Guide supplied in HTML format on the CD-ROM that accompanies your Switch.

Roving Analysis Port

Roving analysis is a feature that allows you to attach a network analyzer to one port and use it to monitor the traffic on other ports of the Switch. The system works by enabling you to define an analysis port (the port that is connected to the analyzer) and a monitor port (the port that is to be monitored). Once the pair is defined, and you start monitoring, the Switch takes all the traffic going in and out of the monitor port and copies it to the analysis port.

Roving analysis is used when you need the functions of a network analyzer, but do not want to change the physical characteristics of the monitored segment by attaching an analyzer to that segment.

Roving Analysis and Your Switch

Roving analysis is supported:

- In a standalone Switch 3870 unit.
- In a single Switch 3870 unit within a stack or across a stack of Switch 3870 units.

Roving analysis is not supported for a monitor port that is configured as a member of an aggregated link.

RMON

Using the Remote Network Monitoring (RMON) capabilities of a Switch allows you to improve 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

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.

RMON Groups

The IETF defines groups of Ethernet RMON statistics. This section describes the four 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.

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.

The Switch can be configured to send a combination of SNMP events. please refer to Table 5 for more information.

Table 5 Combination of SNMP Events

Protocol	Type of Event
SNMPv1	Traps
SNMPv3	Traps
SNMPv3	Informs

Benefits of RMON

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

- **It improves network management 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 3870 is detailed in Table 6.

Table 6 RMON Support Supplied by the Switch

RMON Group	Support Supplied by the Switch
Statistics	General network statistics — Gathers statistics such as bandwidth utilization, counters for network traffic, or errors and collisions. A new or initialized Switch has one Statistics session per port.
History	Statistics for trend analysis — Periodically samples and saves information from the statistics group. A new or initialized Switch has two History sessions per port. These sessions provide the data for the Web interface history displays: ■ 1-hour intervals, 6 historical samples stored ■ 6-hour intervals, 6 historical samples stored

Table 6 RMON Support Supplied by the Switch

RMON Group	Support Supplied by the Switch
Alarms	Sets thresholds for system variables — Alarms are triggered when counters reach predefined thresholds, and can be used to generate response events. For more information about the alarm setup on the Switch, see "Alarm and Event Groups" on page 77.
Events	Reporting mechanism for alarms — Defines the action to take when an alarm is triggered, including logging the alarm, or generating a trap message. For more information about the event setup on the Switch, see "Alarm and Event Groups" on page 77.

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

- 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 and Event Groups

The Alarm and Event Groups allow you to record important events or to immediately respond to critical network problems. These groups are used together to define specific criteria that will generate response events.

Alarms can be set to test data over any specified time interval, and can monitor absolute or changing values (such as a statistical counter reaching a specific value, or a statistic changing by a certain amount over the set interval). Alarms can be set to respond to either rising or falling thresholds. However, note that after an alarm is triggered, it will not be triggered again until the statistical value crosses the opposite bounding threshold.

An Event determines the action to take when an alarm is triggered. The response to an alarm can include logging the alarm into the RMON Event's log table or sending a trap to a trap manager.

9 SETTING UP VIRTUAL LANS

Setting up Virtual LANs (VLANs) on your Switch increases the efficiency of your network by dividing the LAN into logical, rather than physical, segments that are easier to manage.

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

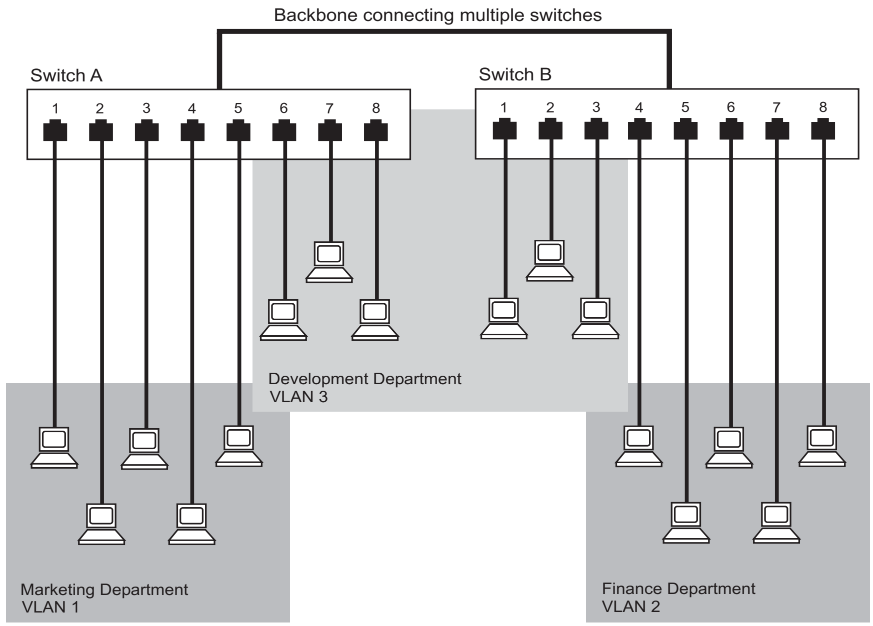
For detailed descriptions of the Web interface operations and the Command Line Interface (CLI) commands that you require to manage the Switch, refer to the Management Interface Reference Guide supplied in HTML format on the CD-ROM that accompanies your Switch.

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 19 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 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 Std 802.1Q-1998. This standard allows traffic from multiple VLANs to be carried across one physical link.

The IEEE Std 802.1Q-1998 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.

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

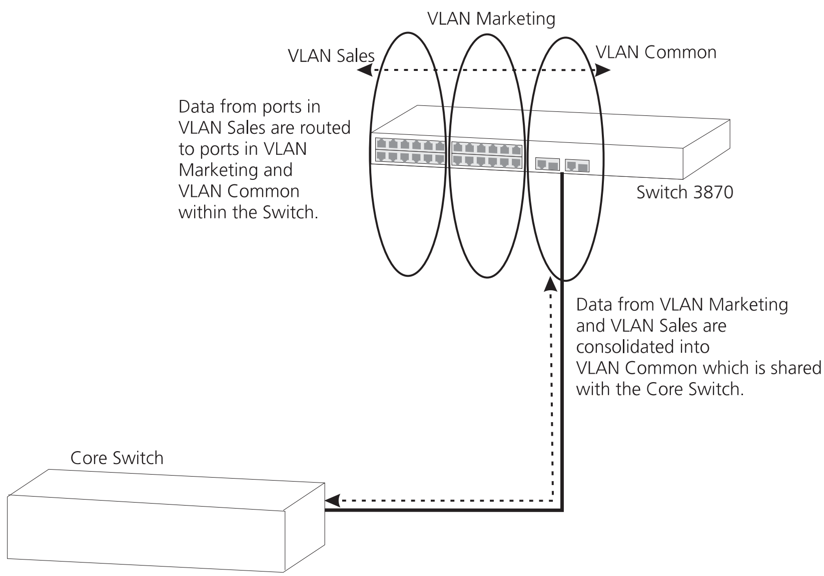
All the ports are initially placed in this VLAN.

Communication Between VLANs

If the devices placed in a VLAN need to communicate with devices in a different VLAN, a router or Layer 3 switching device with connections to both VLANs needs to be present. Your Switch will act as a Layer 3 switching device provided that it has an IP interface on each VLAN. See Chapter 12: "IP Routing" for information about IP routing.

Figure 20 shows how a Layer 3 switch can be used to route between VLANs on the Switch and how an additional VLAN can be used to aggregate two VLANs.

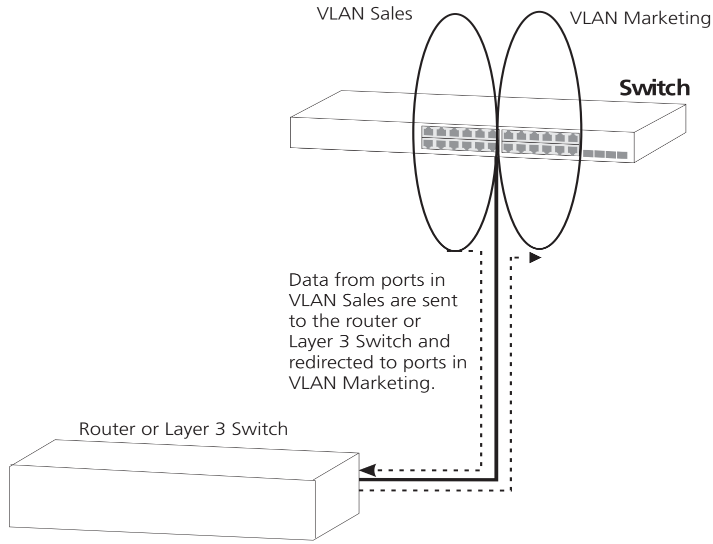
Figure 20 Two VLANs Connected to a Core Switch Using a Third VLAN



The Switch can also be used to route traffic between VLANs on a Layer 2 switch. Figure 21 shows how a Layer 3 switch can be used to redirect traffic from one VLAN to another.

The Switch 3870 is optimized for edge switching and is not suitable as a core switch in large or complex networks.

Figure 21 Two VLANs Connected via a Router



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, it must be a tagged member of all those VLANs except for one. Typically, endstations (for example, clients) will be untagged members of one VLAN, while inter-Switch connections will be tagged members of all VLANs.

A port must always be an untagged member of one VLAN. If a port has its untagged membership removed via the Web interface or CLI, it will be assigned untagged membership of VLAN 1. Untagged inbound traffic is assigned to this VLAN. However, note that if a port has its untagged membership removed via SNMP, it will not be an untagged member of any VLAN. In this case, all untagged inbound traffic will be dropped.

The IEEE Std 802.1Q-1998 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 Switch can identify which packets belong in which VLANs. To communicate between VLANs, a router must be used. Your Switch will act as a Layer 3 switching device provided that it has an IP interface on each VLAN. See Chapter 12: for information about IP routing.

VLAN Configuration Examples

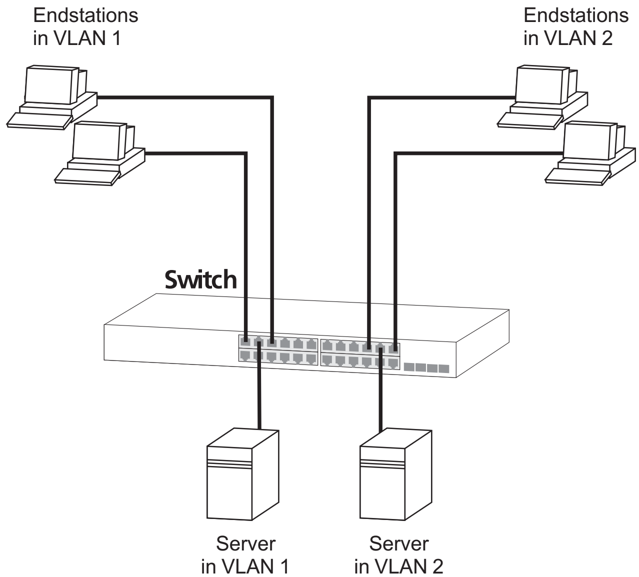
This section contains examples of VLAN configurations. It describes how to set up your Switch to support simple untagged and tagged connections.

Using Untagged Connections

The simplest VLAN operates on a small network using a single Switch. On 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 22 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 16, 17 and 18 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 22 VLAN Configuration Example: Using Untagged Connections



To set up the configuration shown in Figure 22:

1 **Configure the VLANs**
Define 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.

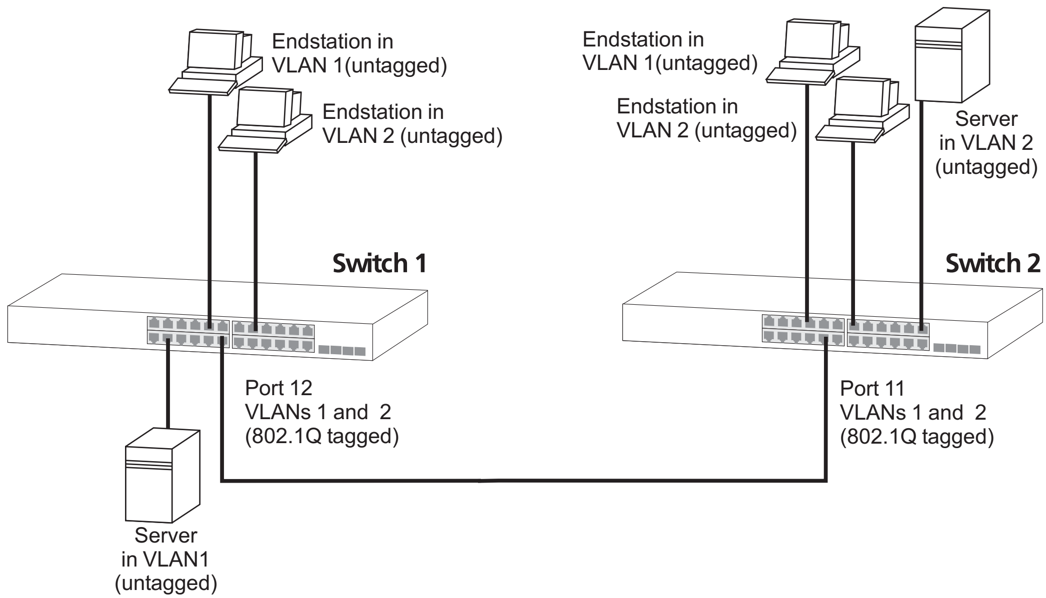
You can use the Switch's Web interface to change the VLAN configuration. VLAN configuration can be found at Bridge > VLAN.

Using 802.1Q Tagged Connections

On 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. 802.1Q tagging can only be used if the devices at both ends of a link support IEEE 802.1Q.

The example shown in Figure 23 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 23 VLAN Configuration Example: 802.1Q Tagged Connections



To set up the configuration shown in Figure 23:

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.

10 USING AUTOMATIC IP CONFIGURATION

This chapter explains more about IP addresses and how the automatic configuration option works. It covers the following topics:

- How Your Switch Obtains IP Information
- How Automatic IP Configuration Works
- Important Considerations

For detailed information on setting up your Switch for management, see 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, refer to the Management Interface Reference Guide supplied in HTML format on the CD-ROM that accompanies your Switch.

For background information on IP addressing, see *Appendix C: "IP Addressing".*

Automatic IP configuration only operates on the first IP interface of the Switch. Additional interfaces must be configured manually.

How Your Switch Obtains IP Information

Your Switch has two ways to obtain its IP address information:

- **Automatic IP Configuration** (default) — The Switch attempts to configure itself by communicating with a DHCP server on the network.
- **Manual IP Configuration** — You can manually input the IP information (IP address, subnet mask, and default gateway).

If you decide not to configure an IP interface (by selecting "None — No LAN Interface" in the configuration wizard), the Switch will not be accessible from a remote management workstation on the LAN. In addition, the Switch will not be able to respond to SNMP requests.

How Automatic IP Configuration Works

When the Switch is powered on for the first time the IP configuration setting is set to **`auto`** — this is the default setting.

If your Switch has been powered on before, whichever of the three options for IP configuration (`manual, auto, none`) was last configured is activated when the Switch powers on again.

You can switch to manual IP configuration at any time using a serial port connection to set up the IP information. For more information, see the Getting Started Guide that accompanies your Switch.

Automatic Process

To detect its IP information using the automatic configuration process, the Switch continually attempts to contact a DHCP server on the network to request an IP address.

If a DHCP server is on the network and working correctly, it responds to the client's request with an IP address (allocated from a pool of available addresses) and other parameters such as a subnet mask, default gateway, lease time, and any other options configured on the DHCP server.

The way a DHCP server responds is dependent on the DHCP server settings. Therefore the way your DHCP server responds may be different from the process outlined.

Important Considerations

This section contains some important points to note when using the automatic IP configuration feature.

If you want DHCP to be the method used for automatic configuration, make sure that your DHCP servers are operating normally before you power on the Switch.

The Switch has been tested to interoperate with DHCP servers that use the following operating systems:

- Microsoft Windows 2000 Server
- Microsoft Windows NT4 Server
- Sun Solaris v2.5.1

The dynamic nature of automatically configured IP information means that the Switch's IP address may be changed if it submits a new request to the DHCP server. Your DHCP server may allow you to reserve an IP address so that your Switch will always be allocated the same IP address.

11 SECURING YOUR NETWORK

This chapter explains the security features of the Switch and gives examples of how and why you would use them on your network. It covers the following topics:

For detailed descriptions of the Web interface operations and the Command Line Interface (CLI) commands that you require to manage the Switch, refer to the Management Interface Reference Guide supplied in HTML format on the CD-ROM that accompanies your Switch.

Securing Access to the Web Interface

The Switch 3870 supports Hypertext Transfer Protocol Secure (HTTPS), allowing secure access to the Web interface of the Switch.

If you administer your Switch remotely or over an insecure network, the Switch can encrypt all HTTP traffic to and from the Web interface using the Secure Sockets Layer (SSL) of HTTP. If your network traffic is intercepted, no passwords or configuration information will be visible in the data.

To use HTTPS, you need the following:

- A browser that supports SSL
- A digital certificate installed on the Switch

The Switch generates its own certificate the first time it is powered on. This is the default certificate for the Switch. As it has not been validated by a Certificate Authority (CA), your browser may warn you that certificate has not been certified.

Once you have obtained and installed a digital certificate, you will be able to securely browse your Switch by using HTTPS (HTTP over SSL). To access the Web interface securely, enter the following into your browser:

```
https://xxx.xxx.xxx.xxx/
```

where xxx.xxx.xxx.xxx is the IP address of your Switch.

Once you have set up your Switch to support HTTPS, you can optionally stop unencrypted administration by redirecting HTTP connections (port 80) to port 443 (the port used by HTTPS). The Switch can be configured to redirect all attempts to administer the Web interface.

Getting a Digital Certificate

Before accessing your Switch using HTTPS, you need a digital certificate that can be used to identify your Switch. The Switch uses certificates that adhere to the X.509 standard.

If you have the software to generate an X.509 certificate, you can self-certify your Switch. Administrators will be warned that the certificate has not been certified by a Certificate Authority (CA) but security will not be otherwise affected.

If you cannot generate an X.509 certificate yourself, you can buy one from one of the Certifying Authorities or your ISP. Each Switch will require its own X.509 certificate.

Securing Access to the Command Line Interface

The Switch 3870 supports Secure Shell (SSH), allowing secure access to the Command Line Interface of the Switch over a Telnet connection.

If you use SSH to administer your Switch and the network traffic is intercepted, no passwords or configuration information will be visible in the data. To securely administer the Switch using the Command Line Interface, you need an SSH client program. You do not need a digital certificate as your Switch can generate its own. However, you will need to download the SSH users' public keys generated by the SSH client program.

To administer your Switch using SSH, start your SSH client and enter the IP address of your Switch.

SSH users must be configured locally on the Switch before their public keys can be downloaded.

If your SSH application supports both encrypted and unencrypted modes, make sure that you have SSH encryption set.

At time of writing, the Telnet client supplied with Microsoft Windows does not support SSH.

Access Control Lists

Access Control Lists (ACLs) are layer 3 instructions that can be used to filter traffic on network ports. 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 network ports and determine the access limitations for packets received on a network port. When a packet is received on a network port, it is compared to an access list for this port. If a match is found, meaning the packet falls under the rule, it will be blocked or forwarded depending on the action.

A maximum of 256 access lists, with up to 32 rules per list, 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 network ports.

How Access Control List Rules Work

When a packet is received on a port, it is compared against the ACL bound to that port. The access list rules are applied to a range of IP addresses defined by the destination IP address and address 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 network port, 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.

Port Security

The Switch 3870 supports the following port security modes, which you can set for an individual port or a range of ports:

- **No Security**

  Port security is disabled and all network traffic is forwarded through the port without any restrictions.

- **Continuous Learning**

  MAC addresses are learned continuously by the port until the number of authorized addresses specified is reached. When this number is exceeded, the first address that was learned by the port is deleted, allowing a new address to be learned.

- **Automatic Learning**

  MAC addresses are learned continuously by the port until the number of authorized addresses specified is reached. When this number is exceeded, the port automatically stops learning addresses and Disconnect Unauthorized Device (DUD) is enabled on the port. For further information see "What is Disconnect Unauthorized Device (DUD)?" on page 105.

- **Learning Off**

  Only traffic received from an authorized address (either configured by management or learned while the port was previously operating in the "Automatic Learning" mode) is forwarded. While in this mode, the DUD operation is enabled. When a port in this mode has learned the maximum number of authorized addresses configured for the port, then it will transition to the "Learning Off" mode.

- **Network Login**

  When an 802.1X client has been successfully authorized, all network traffic is forwarded through the port without any restrictions. For further information, see "What is Network Login?" on page 99.

- **Network Login (Secure)**

  When an 802.1X client has been successfully authorized, only network traffic that is received from the authorized client device is forwarded through the port. The source MAC address in received packets is used to determine this; all traffic from other network devices is filtered. Disconnect Unauthorized Device (DUD) is enabled on the port.

- **Basic RADIUS Authenticated Device Access**

  Basic RADIUS Authenticated Device Access (RADA) provides a means of disabling access, and where necessary the VLAN assignment based on central authentication of an end station's MAC address. In practice, this can be used to provide RADIUS-based security for network administrators who do not have 802.1X clients installed. Another application would be required to isolate individual PCs that have been identified to contain viruses.

This mode should not be considered a totally secure mode, as it can be bypassed by MAC-address spoofing.

RADA can authenticate multiple MAC addresses on a single port, Network Login authentication is limited to a single device on each port.

- **RADA or Network Login (Mixed Secure Network Login and RADA-based Network Access)**

  This mode provides for both 802.1X and RADA authentication to operate in parallel. It provides a migration path where a single port may be used by a number of devices at different times, only some of which support 802.1X. It also allows a single port configuration to be used throughout a Switch, regardless of the type of device that is to be connected. For example, this mode could be used in education, where a large and varied range of "student" PCs and devices can use RADA authentication, but permanent staff require a secure login to enhanced services.

  This mode can only be considered totally secure if the RADA-based authentication is configured to deny access to secure network resources, and where 802.1X Network Login does not share a port (that is, not via a hub).

- **RADA else Network Login (Secure Network Login with RADA Override)**

  This mode provides the secure login capability of 802.1X, and offers an override capability based on MAC address. This mode is intended for use where 802.1X Network Login is the normal access mechanism, but a means of isolating hosts is still required – for example client virus isolation.

  This mode is intended to compliment 802.1X network login, and can be used to authorize host access to any network resource. It can only be considered secure if the MAC-based authentication is configured to deny access to all secure network resources. It is intended to prevent access to secure network resources if a particular edge device is authorized by RADA (for example, if a PC is known to be infected by a virus) and placed on a separate 'safe' VLAN.

Important Considerations

This section contains some important considerations when using Port Security on the Switch 3870.

- Port security and the analyzer port used by roving analysis are mutually exclusive, that is, only the "No Security" option can be used for a port configured as an analyzer port.

What is Network Login?

Network Login controls user access at the network edge by blocking or unblocking access on a per-port basis.

When a client device attempts to connect to a Switch port, the user is challenged to provide their identity and authentication credentials in the form of a user name and password. The user information is then sent to a remote RADIUS server on the network for authentication. This information must be successfully authenticated and authorized before the client device is granted access to the network.

For further information about RADIUS, see "What is RADIUS?" on page 109.

The client device must be directly connected to the Switch port (no intervening switch or hub) as the Switch uses the link status to determine if an authorized client device is connected. Network Login will not operate correctly if there is a "bridge" device between the client device and the Switch port, or if there are multiple client devices attached via a hub to the Switch port.

In addition to providing protection against unauthorized network access, Network Login allows the user of a port to be identified. This user identification information can be used for service accounting or billing, or to help network administrators resolve problems.

Network Login is a feature that is particularly relevant in publicly accessible networks, such as education campuses or conference facilities, which often have limited control over physical access to areas with live network connections.

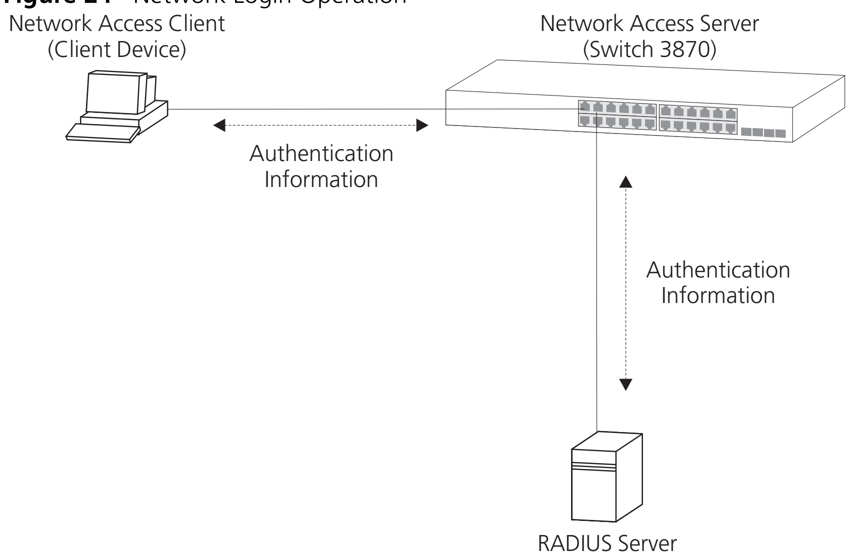
Network Login is based on the IEEE Std 802.1X-2001, which defines a mechanism for user authentication for port-based network access control.

For further information about Network Login, see "Auto VLAN Assignment" on page 103.

How Network Login Works

When Network Login is enabled, the Switch acts as a relay agent between the client device that is requesting access to the network and the RADIUS server. The authentication information that is exchanged between the client device and the RADIUS server is received and transmitted by the Switch, as shown in Figure 24. The Switch does not interpret or store this information.

Figure 24 Network Login Operation



When the client device and RADIUS server have exchanged authentication information, the Switch receives either an authentication succeeded or failed message from the server, and then configures the port to forward or filter traffic as appropriate. If access is granted, the Spanning Tree Protocol places the port into the forwarding state and the client device can obtain an IP address.

If possible, when a port is configured for Network Login, it should also be configured to enable Spanning Tree Protocol (STP) Fast Start. This minimizes the delay before STP places the port into the forwarding state.

For Network Login, the Switch uses EAP (Extensible Authentication Protocol).

For further information about RADIUS, see *"What is RADIUS?" on page 109*.

Important Considerations

This section contains some important considerations when using Network Login on the Switch 3870.

- Before you enable Network Login you must ensure that:
  - RADIUS has been configured on the Switch.
  - The RADIUS server on your network is operational.
- If the RADIUS server fails or is unavailable, client devices will be unable to access the network.
- Network Login is not supported on ports configured to operate as members of an aggregated link.
- Some client devices that are connected to the Switch port may not support the authentication service (for example, printers). You should configure the Switch port to operate in Automatic Learning mode, so that network traffic that does not match the MAC address for the client device is filtered.
- You should enable Network Login on all relevant Switch ports. Failure to enable authentication on a single port could compromise the security of the entire network.

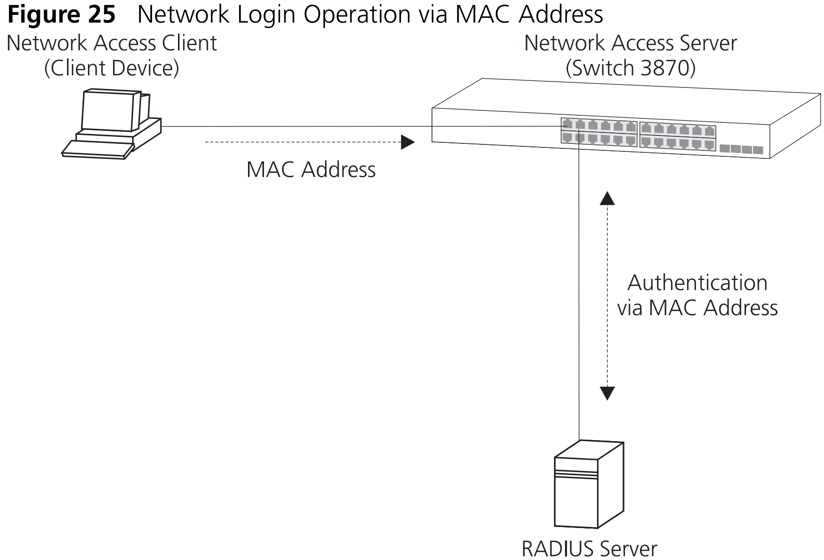
What is RADA?

RADIUS Authenticated Device Access feature compliments the existing 802.1X support of the Switch. Instead of needing an 802.1X client on every end station, the Switch can use the MAC address of the end station to query the RADIUS server.

How RADA Works

The RADA feature controls the network access of a host based on authenticating its MAC address. A host is allowed access to the entire network, to a restricted network or no access at all. The Switch obtains the network access authorization from a centrally located RADIUS server by supplying the MAC address of the host as shown in Figure 25

Figure 25 Network Login Operation via MAC Address



For RADA, the Switch uses PAP (Password Authentication Protocol).

RADA has an ‘Unauthorized Device action’ of allowDefaultAccess or blockMacAddress, which controls the action on authentication refusal.

- allowDefaultAccess grants a device access based on the ports configured VLAN parameters.
- blockMacAddress blocks (filters) any traffic to or from the device.

RADA is a type of port security mode and it supports Allow Default Access and Block MAC Address for DUD actions. The two DUD actions supported under RADA mode affect a single device. The other DUD actions supported by other port security modes (including No Action, Permanently Disable, and Temporarily Disable) affect a single port.

RADA can also be used in conjunction with the existing 802.1X Secure Network Login to provide the capability to support a variety of host and network configurations.

RADIUS Server Settings for RADA

When setting up RADA on a RADIUS server, the following attributes should be taken into consideration.

- Users must be set up on the RADIUS server for each device that is to be authenticated, using the MAC address for user name and the same MAC address for the password.
- The user name should be set as the MAC address of the device. This must be of the form of hexadecimal digits separated by hyphens, for example '08-05-54-AB-CD-EF'.

Table 7 Setting RADA Attributes

Attribute	Value
Framed-Protocol	PPP
Service-Type	Framed

Auto VLAN Assignment

Auto VLAN assignment complements the basic Network Login and RADA features. It allows appropriate VLAN configuration to be obtained from a RADIUS server when a user or device authenticates on a port. The configuration obtained will be specific to the user or device authenticated on the port.

The RADIUS server may be configured with VLAN parameters for each user or device. One or more VLANs may be configured for each user to allow multiple VLANs to be communicated to the device requesting the user authentication.

Important Considerations

This section contains some important considerations when using Network Login or RADA on the Switch.

- Before you enable Network Login or RADA you must ensure that:
  - RADIUS has been configured on the Switch.
  - The RADIUS server on your network is operational.

- If the RADIUS server fails or is unavailable, client devices will be unable to access the network or be restricted to the default access.
- Network Login and RADA are not supported on ports configured to operate as members of an aggregated link.
- Some client devices that are connected to the Switch port may not support network login (for example, printers). You should configure the Switch port to operate in Automatic Learning mode, so that network traffic that does not match the MAC address for the client device is filtered, or use the basic RADA mode.
- You should enable Network Login or RADA on all relevant Switch ports. Failure to enable authentication on a single port could compromise the security of the entire network.
- When a single port is set up for Auto VLAN mode, administration changes are not allowed to either static or dynamic VLANs as the result of Auto VLAN operation.
- A corresponding VLAN must be created on the device that the RADIUS server will assign ports to for the Auto VLAN setting.

RADIUS Server Settings for Auto VLAN

When setting up Auto VLAN on a RADIUS server, the following attributes must be set to supply VLAN data to the Switch.

Table 8 Setting Auto VLAN attributes

Attribute	Value
Tunnel-Type	VLAN
Tunnel-Medium-Type	802
Tunnel-Private-Group-ID	<VLAN ID to be assigned>

The Tunnel-Private-Group-ID attribute specifies the VLAN to be assigned. This can take various forms to indicate if the port is untagged or tagged member. For example, ‘2u 3t' means that the port is an untagged member of VLAN 2 and a tagged member of VLAN 3.

The Switch will assign the first VLAN number with no suffix, or with a ‘U’ or ‘u’ suffix, as an untagged VLAN for the port. Any further VLAN numbers with no suffix, or with the ‘U’ or ‘u’ suffix, will be assigned as a tagged VLAN on the same port. For example, all the following strings are identical after processing: “23 7T 88T”, “7T 88t 23u”, “88T 23 7t “,”23 7 88”, “7T 23u 88u”.

It is possible to check if the VLANs assigned to a port are those supplied by the RADIUS server by using the `bridge port detail` CLI command. The display will show 'dynamic' against the VLAN details if the RADIUS server supplied the assignments.

What is Disconnect Unauthorized Device (DUD)?

The port security feature Disconnect Unauthorized Device (DUD) disables a port if an unauthorized client device transmits data on it.

DUD is automatically enabled when a port is set to one of the following port security modes:

- Automatic Learning
- Network Login (Secure)
- RADA
- RADA or Network Login
- RADA else Network Login

How DUD Works

DUD protects the network by checking the source MAC address of each packet received on a port against the authorized addresses for that port.

You can configure DUD to perform one of the following actions if an unauthorized client device transmits data on the port:

- **Permanently disable the port**

  The port is disabled and data from the unauthorized client device is not transmitted.

- **Temporarily disable the port**

  The port is disabled for 20 seconds. When the time period has expired, the port is re-enabled; if the port is set to one of the Network Login security modes, the client device is authenticated again.

- **Do not disable the port**

  The port is not disabled and data from authorized client devices will continue to be transmitted, while data from unauthorized client devices will be filtered.

- **Allow Default Access**

  The port is not disabled and clients are assigned the default VLAN for the port.This allows you to segregate unauthorized devices on a different VLAN to authorized devices.

- **Block MAC Address**

  The port is not disabled but traffic from the client is blocked. If there are other clients on the port, they will be allowed to connect provided they are authorized.

What is Switch Management Login?

If you intend to manage the Switch using the Web interface or the Command Line Interface, you need to log in with a valid user name and password.

For further information on managing the Switch, see the "Setting Up For Management" chapter in the Getting Started Guide.

The user name and password information can be stored in either:

- **a RADIUS server** (recommended)

  If you enable RADIUS as the authentication mode of Switch Management Login, the user name and password information is stored on a database on a RADIUS server on the network. Subsequent login attempts to the Switch are remotely authenticated by the RADIUS server.

  or

- **the local Switch database** (default)

  If you enable Local as the authentication mode of Switch Management Login, the user name and password information is stored on the local database on the Switch. Subsequent login attempts to the Switch are authenticated by the local database.

Benefits of RADIUS Authentication

Day-to-day network maintenance can become a substantial overhead. For example, regularly changing the administrative password on a manageable network device is a commonplace security measure. If the local Switch database is enabled, the network administrator must have local access to each Switch to securely change user name and password information. This can be time consuming, tedious and often results in bad configurations and lapses in security.

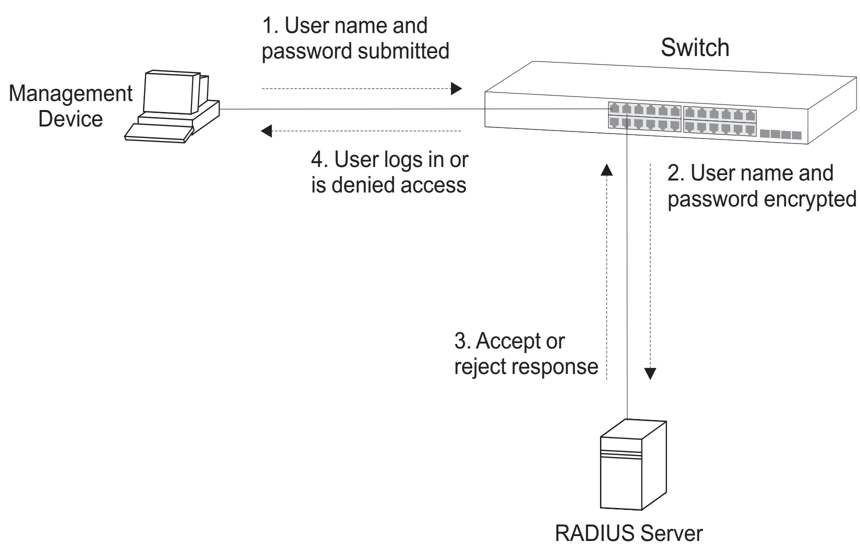
RADIUS authentication provides centralized, secure access and removes the need to physically visit each network device. Changes to user names and passwords require only a single action on the RADIUS database and are reflected immediately.

The Switch 3870 is fully compliant with the industry standard RADIUS protocol. For further information about RADIUS, see "What is RADIUS?" on page 109.

How RADIUS Authentication Works

When RADIUS authentication of Switch Management Login is enabled, the Switch obtains the user name and password and securely sends the information to the RADIUS server. The information is authenticated by the server and a valid user is allowed to log into the Switch. An invalid user receives a reject response and is not allowed to log into the Switch. This process is shown in Figure 26.

Figure 26 RADIUS Authentication Operation



RADIUS Server Settings for Switch Login

The user levels provided on the Switch are shown below:

- Monitor (1) — The user can view all manageable parameters, except special/security features,but cannot change any manageable parameters.
- Manager (2) — The user can access and change the operational parameters but not special/security features.
- Administrator (3) — The user can access and change all manageable parameters.

To create a user with Administrator privileges when using a RADIUS server for authentication, set the "Service-Type" attribute for the user to Administrative. You must configure the RADIUS server to send this attribute in the Access-Accept message to specify the access level required for each user account that requires Administrator access to the Switch.

For Switch Login, the Switch uses PAP (Password Authentication Protocol).

For further information about configuring the Switch for Switch Management Login and RADIUS authentication, refer to the Management Interface Reference Guide supplied in HTML format on the CD-ROM that accompanies your Switch.

Important Considerations

This section contains some important considerations when using RADIUS authentication of Switch Management Login on the Switch 3870.

- Before you enable RADIUS authentication, you must ensure that:
  - The Switch is configured with a static IP address.
  - RADIUS has been configured on the Switch.
  - The RADIUS server on your network is operational.
  - The RADIUS server has been configured with a "Service-Type" of Administrative for any users that require management access to the Switch.
- If the Switch is unable to contact the RADIUS server, the Command Line Interface automatically reverts to using the local Switch database for user authentication. This allows a user with "admin" access to log into the Switch via the console port and continue to manage it. The Web interface and Telnet do not revert to the local database, and the user will not be able to log into the Switch via the Web interface or Telnet.
- The user names and passwords stored on the local Switch database may not be the same as those stored on the RADIUS server. When a user account is created on a RADIUS server, an equivalent account is not automatically created on the local Switch database, and vice versa.

What is RADIUS?

Remote Authentication Dial-In User Service (RADIUS) is an industry standard protocol for carrying authentication, authorization and configuration information between a network device and a shared authentication server. Transactions between each network device and the server are authenticated by the use of a shared secret. Additional security is provided by encryption of passwords to prevent interception by a network snooper.

RADIUS is defined in the RFCs 2865 and 2866, "Remote Authentication Dial-in User Service (RADIUS)" and "RADIUS Accounting".

Network Login, a method of port-based access control, and Switch Management Login, used to control administrative access, both utilize the RADIUS protocol.

Trusted IP

Trusted IP enhances the security of your network by enabling you to define the IP host addresses and subnets trusted to access the management interfaces of the Switch. When Trusted IP is enabled, unauthorized IP host addresses will be prevented from connecting to the management interfaces of the Switch.

Trusted IP provides the following benefits:

- Restricts management access to authorized IP host addresses and subnets
- Increases password protection because the unauthorized user needs to be on the network to attempt access. Even if a password has been compromised it allows some protection because an unauthorized user still needs to access an authorized PC.
- Allows control of the type of access (SSH, SNMP, Telnet, or Web) per IP host address and subnet.

Configuring Trusted IP

Trusted IP can be configured to:

- Allow up to 16 authorized manager addresses with each entry specifying an IP host address, and subnet mask.
- Specify permit or block for each authorized manager on each management interface (SSH, Telnet, Web, and SNMP).
- Implement a configuration stack-wide.

Before enabling trusted IP, 3Com recommends that you add the IP address of your management station to the list of trusted IP addresses.

The trusted IP feature restricts network access to the management interfaces of the Switch. You will be able to access the management interface of the Switch using the console port, even if you have denied all access to the Switch using the trusted IP feature.

Trusted IP configuration is automatically saved when using the **`system backupConfig save`** *CLI command. For further information about saving and restoring configuration settings, see* *"Configuration Save and Restore" on page 141*.

For detailed descriptions of the Trusted IP Host Web interface operations and Command Line Interface (CLI) commands, refer to the Management Interface Reference Guide supplied in HTML format on the CD-ROM that accompanies your Switch.

Secure Shell (SSH)

The Switch 3870 supports Secure Shell, allowing secure access to the Command Line Interface via an encrypted path between the Switch and the management station.

If you use SSH to administer your Switch and the network traffic is intercepted, no passwords or configuration information will be visible in the data. SSH provides encrypted, authenticated transactions.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.

`http://www.openssl.org`

What is Secure Shell?

Secure Shell (SSH) is a program that provides secure network services over an insecure network. SSH can be used to replace other, less secure terminal applications (such as Telnet).

SSH uses a client/server architecture. An SSH server in the Switch accepts or rejects incoming connection attempts from an SSH client running on a management workstation.

There are two versions of the SSH protocol. The Switch 3870 uses SSHv2 (Secure Shell version 2) only, but can support either SSHv1 or SSHv2 clients.

How Secure Shell Works

SSH provides security by using Public-Key encryption to uniquely identify the Switch being managed (host authentication) and the user attempting to manage the Switch (user authentication). User authentication is performed using both the user Public-Key and password authentication.

Public-Key encryption allows you to freely distribute a public key without any security risk to your network, providing the private key is kept secret. Information encrypted using a public key cannot be decrypted without the corresponding private key.

SSH provides privacy by transparently encrypting all data transferred during a connection. The data itself is encrypted using a symmetric key. The symmetric key is a 'per session' key (shared secret). The symmetric key is exchanged at the start of a session using the Diffie-Hellman key exchange algorithm to prevent it being intercepted by a third party. The Switch supports the following data encryption ciphers:

- 3DES (168-bit)
- DES (56-bit)

The Switch 3870 software installed on units contains support for DES (56-bit) encryption. A software version with 3DES (168-bit) encryption is made available via the support site of www.3com.com for downloading where international trading regulations permit this.

Benefits of Secure Shell

The primary benefit of Secure Shell is that it allows you to exchange messages securely.

SSH helps protect against a number of common security attack techniques:

- Eavesdropping on a transmission, for example looking for user IDs, passwords or SNMP community strings.
- Hijacking, or taking over a communication in such a way that the attacker can inspect and modify any data being transmitted between the communicating parties.
- IP spoofing or faking network addresses to fool access control mechanisms based on them or to redirect connections to a fake server.

The SSH protocol includes the following features:

- Secure terminal sessions utilizing secure encryption.
- Multiple high security algorithms and strong authentication methods that prevent such security threats as identity spoofing.
- Multiple ciphers for encryption.
- Automatic and secure user and host authentication. Both the server and the client are authenticated to prevent identity spoofing, Trojan horses, etc.
- Secure user authentication by Public Key, and/or passwords.

Prerequisite for Using SSH

This section describes steps you must take before you configure your Switch for Command Line Interface management using SSH.

Before you can manage the Switch using SSH over a network, you must first check the following:

1. Ensure you have already set up the Switch with IP information as described in “Setting Up Overview” of the SuperStack 3 Switch 3870 Getting Started Guide.
2. Check that you have the TCP/IP correctly installed on your management workstation. You can check this by trying to browse the World Wide Web. If you can browse, TCP/IP is installed.

3 Check that you can communicate with the Switch by entering a ping command at the DOS prompt in the following format:

`c:\ ping xxx.xxx.xxx.xxx`

(where xxx.xxx.xxx.xxx is the IP address of the Switch)

If you get an error message, check that your IP information has been entered correctly and the Switch is powered on.

4 Ensure you have installed a publicly or commercially available SSH client application on the computer(s) you use for management access to the Switch. If you want user public-key authentication, then the client program must have the capability to generate public and private key pairs.

3Com recommends the following SSH clients: PuTTY, OpenSSH and SSH Communications Security Corp Secure Shell.

Generating and Configuring Switch Host Keys

This section describes how you can generate and configure the Switch's Host Public and Private Key Pair.

When the Switch is powered on for the first time, or after any reset to factory defaults, a host key pair will automatically be generated. Host key generation will take a few minutes, during which SSH connections to the Switch will be refused. During this time, management of the Switch may run more slowly than normal due to the increased processor overhead.

If you want to subsequently change the automatically generated host key, you can regenerate it through the CLI using the **`security device ssh serverAuth keyGen`** command.

3Com recommends that a new host key pair be generated for increased security.

For detailed descriptions of SSH CLI commands, refer to the Management Interface Reference Guide supplied in HTML format on the CD-ROM that accompanies your Switch.

Supplying the Switch's Host Public Key to Clients

When you begin an SSH session to the Switch for the first time, your SSH client will ask you to verify the validity of the Switch to which you are trying to connect, unless you have already copied the key to the client. Copying the Switch's key reduces the threat of an unauthorized device posing as your Switch and learning your passwords.

Configuring the Switch for User Authentication

It is possible to configure the Switch for user authentication in three ways:

- Password only authentication (default setting)
- User Public-Key authentication
- User Public-Key and password authentication

Configuring Password Only Authentication

When configured with this option, enter your user name and password to access CLI commands.

To configure your Switch for user password authentication:

1. Start an SSH session and access the Switch using the Switch's IP address and port number.
2. The Switch and the SSH client will authenticate each other and a secure connection will be established.
3. Enter your usual user name and password to access the CLI.

For increased security, change the default password when using SSH for the first time.

Configuring User Public-Key Authentication

This option uses a public key that must be stored on the Switch. Only a user with a private key that matches a stored public key can gain access to the Switch.

To configure your Switch for client public key authentication:

1. Generate a public/private key pair using an SSH key generator application provided with the SSH client.
2. Copy the client's public key into an ASCII file on a TFTP server accessible to the Switch.

3 Download the public key to the Switch and associate it with a CLI user name. For further information, see "Transferring Public Keys to the Switch" on page 115.

Figure 27 SSH2 Public Key in ASCII Format


```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: DSA Public Key for use with MyIsp

AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
---- END SSH2 PUBLIC KEY ----
```


4 Start an SSH session and access the Switch using the Switch's IP address and SSH port number. The Switch and SSH client will authenticate each other and a secure connection will be established.

5 Enter your user name and password to access the CLI.

Configuration Backup and Restore does not save SSH keys.

Transferring Public Keys to the Switch

When using user public-key authentication, it is necessary to transfer the user's public key to the Switch using the 3Com TFTP server.

The 3Com TFTP Server only runs on Microsoft® Windows®. If you are using another operating system (for example, Macintosh® or Unix®), you will require a different TFTP Server application. Please refer to the instructions that accompanied your system for further information.

Setting Up TFTP Server and Transferring Files to the Switch

These instructions apply to the 3Com TFTP Server, which is a Microsoft Windows NT only application.

1 Install the 3Com TFTP Server on your management workstation:

- From the CD-ROM that accompanies your Switch, or
- By downloading the 3Com TFTP Server from the 3Com Web site:

http://support.3com.com

2 Launch the 3Com TFTP Server.

3 Check that the 3Com TFTP Server is configured to point to where the client public key file is located. To do this:

   a Click the *Options* button on the 3Com TFTP Server menu bar. The Upload/Download directory file path should point to where the client public key (ASCII file) is located. (Refer to the documentation supplied with your client or key generator application for the exact location of the public key file).

   b Change the path to point to the directory containing the public key file.

   c Click the *OK* button to close the Setup window.

4 Access the Switch via Telnet.

5 Download the Public key to the Switch using the **`security device ssh userAuth userKey download`** CLI command.

The IP address of the 3Com TFTP Server is displayed on the title bar. You will need this to configure the Switch and TFTP Server with IP information.

Port Privacy

Port Privacy can be implemented where networks are used to supply services (for example, video streams, telephony, Internet access, etc.) to users in a public environment, such as apartment buildings or hotels. Port Privacy protects end users from any interference from other end users attached to the same network.

Port Privacy increases security by allowing individual ports (or port ranges) to be classified as "private" or "public". A "private" user port is prevented from communicating with other "private" ports, but is able to communicate with "public" ports on the same VLAN.

Limitations of Port Privacy

The following limitations must be considered when implementing Port Privacy:

- The following ports cannot be used in conjunction with the Port Privacy:
  - Ports that are members of Link Aggregations or LACP configured Link Aggregations.
  - Ports that are configured as the analyzer port used by the Roving Analysis feature.

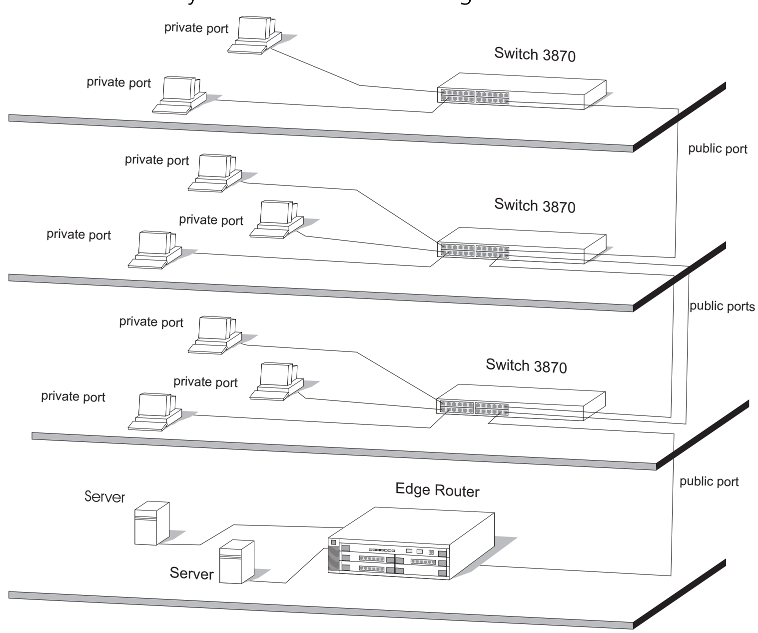
- Ports used as an uplink must remain “public”.

Implementing Port Privacy

- Port Privacy can be used to supply services (for example, video streams, telephony, Internet access, etc.) to users in a public environment, such as apartment buildings or hotels.
- Port Privacy can be used to implement security in a Visitor-Based Network (VBN) scenario. This also allows service providers to charge for additional services by controlling the connection of users at a higher layer on the network.

The space provided by the cable housing that runs between floors in a building is usually very narrow. Based on common installation practices, you may want to place a single Switch on each floor, and daisy-chain the Switches to provide a scalable solution. In this case, the Ethernet downlink from one Switch defined as a “public” port will be connected to an edge port of another Switch defined as a “private” port that is closer to the ISP. See Figure 28 for more details.

Figure 28 Port Privacy Scalable Network Configuration



Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) has been widely accepted as an industry standard way of ensuring the transmission of the management information between any two nodes. Using SNMP, network administrators can easily search and modify the information on any node on the network to locate faults, implement fault diagnosis, plan capacity and generate reports.

Designed as a centralized measure for network management, SNMPv1 (RFC 1157) is effective and easy to implement. SNMPv2c (RFC 1901-1907) was developed with new features and improved efficiency, but no security enhancements such as authentication and encryption. SNMPv3 (RFCs 3410-3418) addresses the shortfalls of SNMPv2c and provides secure access to devices by a combination of authenticating and encrypting packets over the network.

The optional security features provided in SNMPv3 are:

- Message integrity — Ensuring that a packet has not been tampered with in-transit.
- Authentication — Determining the message is from a valid source.
- Encryption — Scrambling the contents of a packet prevent it from being seen by an unauthorized source.

The Switch 3870 implements SNMPv1, SNMPv2c and SNMPv3.

Using SNMPv3, it is possible to implement security models and levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine which security mechanism is employed when an SNMP packet is handled. See Table 9 for a list of security levels available in SNMPv3.

Security Models and Levels for SNMPv1, v2c, v3

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- noAuthNoPriv — Security level that does not provide authentication or encryption.
- authNoPriv — Security level that provides authentication but does not provide encryption.

- authPriv — Security level that provides both authentication and encryption.

Three security models are available: SNMPv1, SNMPv2c, and SNMPv3. The security model combined with the security level determine the security mechanism applied when the SNMP message is processed.

Table 9 SNMP Security Models and Levels

Model	Level	Authentication	Encryption	Effect
v1	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	User name	No	Uses a user name match for authentication.
v3	authNoPriv	MD5 or SHA	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm, or the HMAC Secure Hash Algorithm (SHA).
v3	authPriv	MD5 or SHA	DES	Provides encryption based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

User-based Security Model (USM)

The User-based Security Model (USM) of SNMPv3 defines mechanisms for providing message-level security for SNMP implementations. USM is designed to protect against threats such as:

- Masquerade — An unauthorized user attempts to use the identity of an authorized user to perform management operations.
- Modification of information — Changing management information in transit between the SNMP manager and agent in order to achieve an unauthorized operation.
- Message stream modification — Reordering or replaying messages to achieve an unauthorized operation.

- Disclosure — An unauthorized user attempts to eavesdrop on an authorized management exchange.

USM uses two authentication protocols:

- HMAC-MD5-96 authentication protocol
- HMAC-SHA-96 authentication protocol

USM uses CBC-DES (DES-56) as the privacy protocol for message encryption.

View-based Access Control Model (VACM)

The SNMPv3 View-based Access Control Model (VACM) is designed to control access to management information based on a user's identity. VACM allows different access levels (read, write, notify) to be defined for different users and for each piece of MIB information.

The Switch 3870 includes fixed views that provide only restricted access to the MIB for the user access level of “monitor” (that is, read-only access to the entire MIB), partial access to the MIB for the user access level of “manager” (that is, read/write access to operational parameters but not special/security features), and full access to the MIB for the user access level of “security” (including read/write access to the entire MIB). Refer to the next section for information on how to configure user access levels.

Enabling SNMP

By default, SNMPv1, SNMPv2c and SNMPv3 are automatically enabled and a local engine ID is defined. The local engine ID may be a string specified by the user or a generated default string based on the MAC address of the device.

To configure SNMPv1 and SNMPv2c

1. Set the community string.
2. Configure your SNMP manager application to use the community string.

To configure SNMPv3

1. Set the desired access level (monitor, manager or security) when adding or modifying a user.
2. Ensure the user's access level is enabled for SNMPv3.

The access level is enabled by default.

3 Configure SNMPv3 security for the user, setting the authentication protocol, authentication password (if authentication is used), privacy protocol and privacy password (if privacy is used).

4 Configure your SNMP manager application to use the user name, with the same settings and passwords.

For detailed descriptions of SNMP CLI commands, refer to the Management Interface Reference Guide supplied in HTML format on the CD-ROM that accompanies your Switch.

For security reasons, authentication passwords are invalidated if the SNMPv3 engine ID is changed.

3Com recommends you use SNMPv3 with user authentication and privacy (authPriv) where possible for increased security.

Configuration Backup and Restore does not save SNMPv3 security information or the engine ID.

12 IP ROUTING

Routing is a method for distributing traffic throughout an IP 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
- Multiple IP Interfaces per VLAN
- Implementing IP Routing
- IP Routing Protocols
- User Datagram Protocol (UDP) Helper
- Advanced IP Routing Options

For detailed information on setting up your Switch for management, see 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, refer to the Management Interface Reference Guide supplied in HTML format on the CD-ROM supplied with your Switch or on the 3Com Web site.

What is Routing?

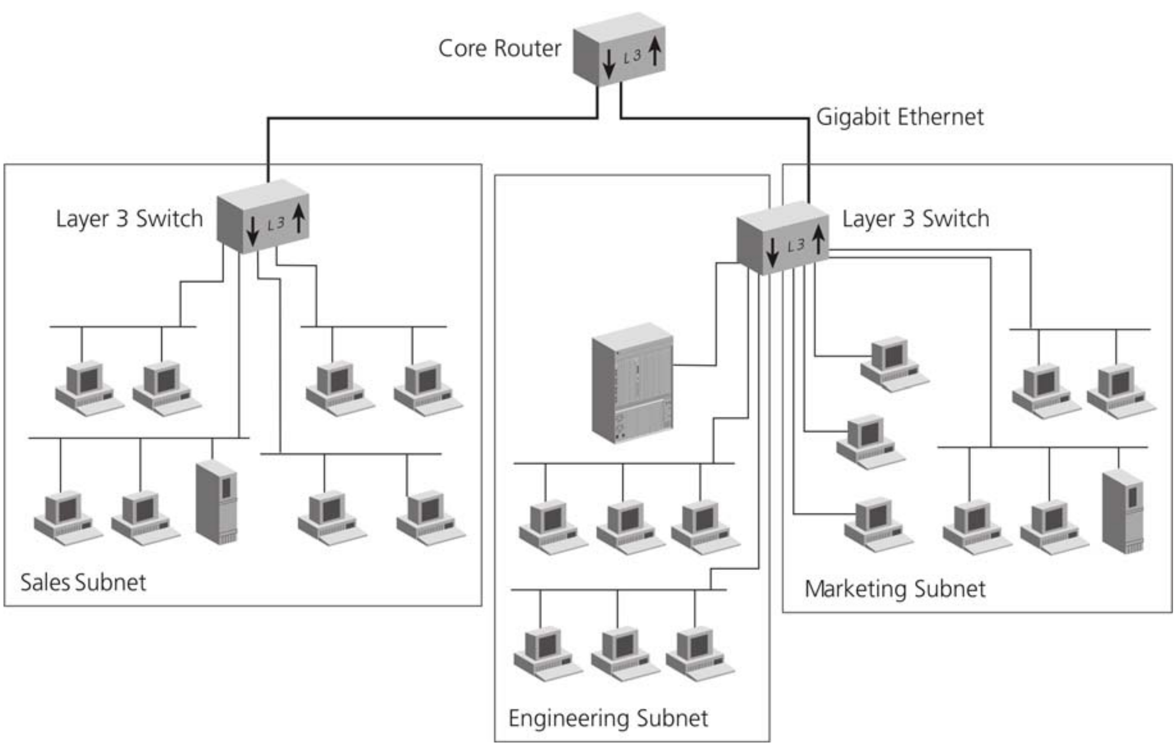
Routing distributes packets over potentially dissimilar networks. A router is the device that accomplishes this task. Your Switch, as a Layer 3 device, can act as a router. Routers typically:

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

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. In the example shown in Figure 29, one of the Layer 3 Switches is forwarding traffic between the Engineering and Marketing subnets, reducing the traffic that goes to the core router.

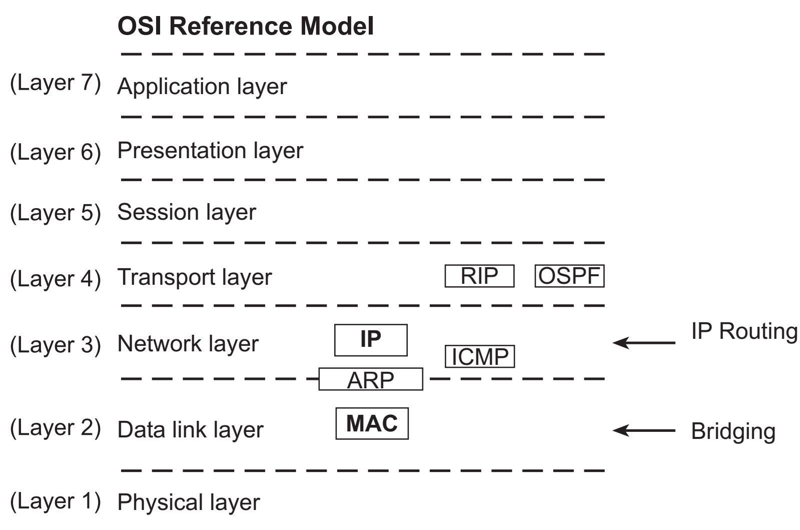
Figure 29 Subnetwork Routing Architecture



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 (at Layer 2) to perform forwarding. See Figure 30.

Figure 30 OSI Reference Model and IP Routing



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 on 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 on 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
- Layer 3 Switching
- Multiple IP Interfaces per VLAN

Router Interfaces

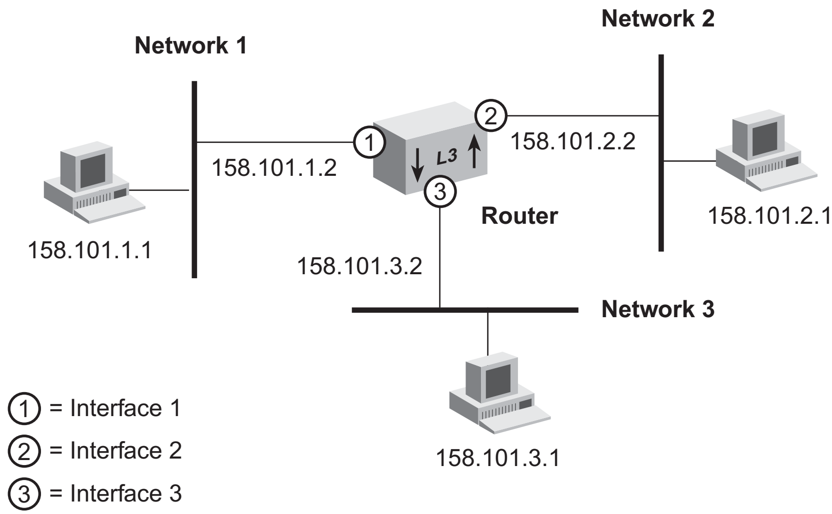
A router interface connects the router to a subnetwork. On your Switch, more than one port can connect to the same subnetwork.

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 three functions:

- Sends IP packets to or from the router.
- Defines the network and subnetwork numbers of the segment that is connected to that interface.
- Provides access to the Switch using TCP/IP or to manage the Switch using the Simple Network Management Protocol (SNMP)

Figure 31 shows an example of a router interface configuration.

Figure 31 Routing Interfaces



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 most 2000 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.

Routing table data is updated statically or dynamically:

- **Statically** — You manually enter static routes in the routing table. You can define up to 12 (maximum) static routes. 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.
- **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.

The Switch supports both RIPv1 and RIPv2.

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.

Layer 3 Switching

Layer 3 switching 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 router port on this Switch, the packet is routed (Layer 3).
- If the destination MAC address is not one of the router interfaces MAC addresses on this Switch, then the packet will be switched and is forwarded according to the IEEE 802.1D protocol.

This model allows the Switch to route the packet first, and then if the packet cannot be routed, give the packet to Layer 2 to be bridged by the VLAN. 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.

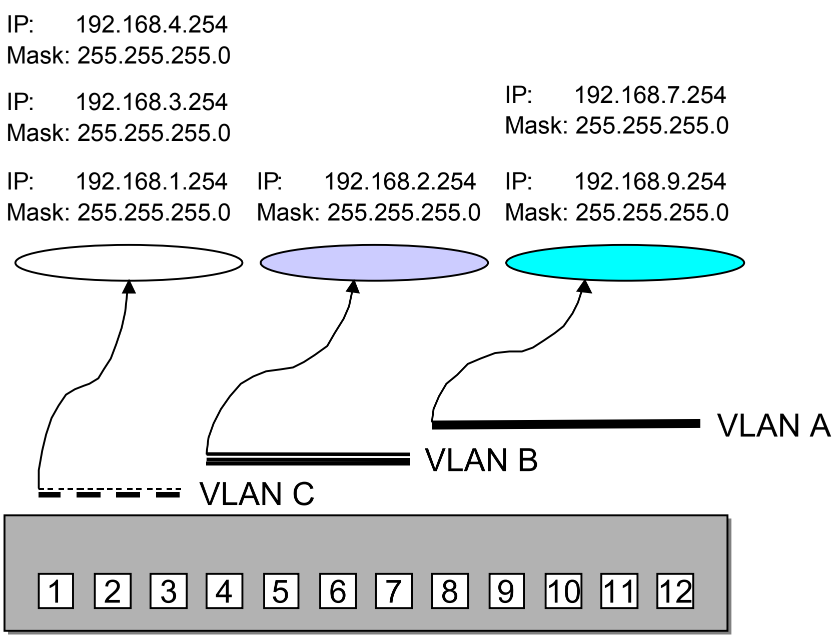
Typically, each VLAN will be allocated its own subnet with each subnet having its own IP interface on the Switch.

See Chapter 9: "Setting Up Virtual LANs" for more information on VLANs.

Multiple IP Interfaces per VLAN

You can overlap IP interfaces without configuring a separate VLAN for each subnet. This is called multinetting. 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 32.

Figure 32 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 VLANs.

2 Establish IP interfaces on those VLANS.

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 that are grouped according to the IP network address and mask.

See Chapter 9: "Setting Up Virtual LANs" for more information on 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`). This is not a user configurable parameter.
- **VLAN interface index** — 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.

Defining an IP Interface

After you decide the VLAN index, IP address, and subnet mask for each IP interface you want to create, you can define each interface using the Command Line Interface or the Web 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.

Remember that you must define a VLAN before you define the IP (routing) interface. See Chapter 9: "Setting Up Virtual LANs" for more information on VLANs.

Your Switch provides the following advanced IP features:

- Routing Information Protocol (RIP)
- User Datagram Protocol (UDP) Helper
- ARP Proxy
- Internet Control Message Protocol (ICMP)

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 `ICMP Network Unreachable` error.
- Before you can define static routes, you must define at least one IP interface. See "Defining an IP Interface" on page 131 for more information. Remember the following guidelines:
  - Static routes remain in the routing table until you remove them.
  - Static routes are removed during a system initialize.

- 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 to which networks must adhere in order to successfully operate. Protocols that are discussed in this section include:

- Routing Information Protocol (RIP)
- User Datagram Protocol (UDP) Helper
- Address Resolution Protocol (ARP)
- Internet Control Message Protocol (ICMP)

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 on 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
RIP Mode*	disabled
Cost†	1
Update Time*	30 seconds
Send Mode	RIPv1Compatible
Receive Mode	RIPv1OrRIPv2
Poison Reverse	disabled
Advertisement Address	limited broadcast address (224.0.0.9)

* These RIP parameters apply to the entire Switch. All other parameters are defined per interface.

† The Cost value cannot be altered, it is fixed at 1.

RIP 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.

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 will not broadcast (or advertise) RIP updates.
- doNotReceive – The Switch does not process (or passively learn) 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 directed broadcast address 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, it puts the route into the routing table with the subnet mask that was advertised.

Important Considerations

Note the following considerations 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 (Variable Length Subnet Mask).
- 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), Rapid Spanning Tree (RSTP) and Routing Information Protocol (RIP) all Switches must communicate with each other on the same VLAN.

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 (DHCP)**

  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. The Switch will inform your DHCP server of the subnet of each client that requests an address so that the client is issued an IP address in the correct subnet.

Implementing UDP Helper

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

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 33.

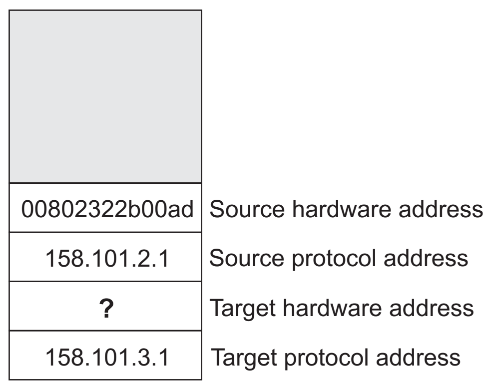
Figure 33 Example of an ARP Cache

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 34.

Figure 34 Example of an ARP Request Packet



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 35.

Figure 35 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.

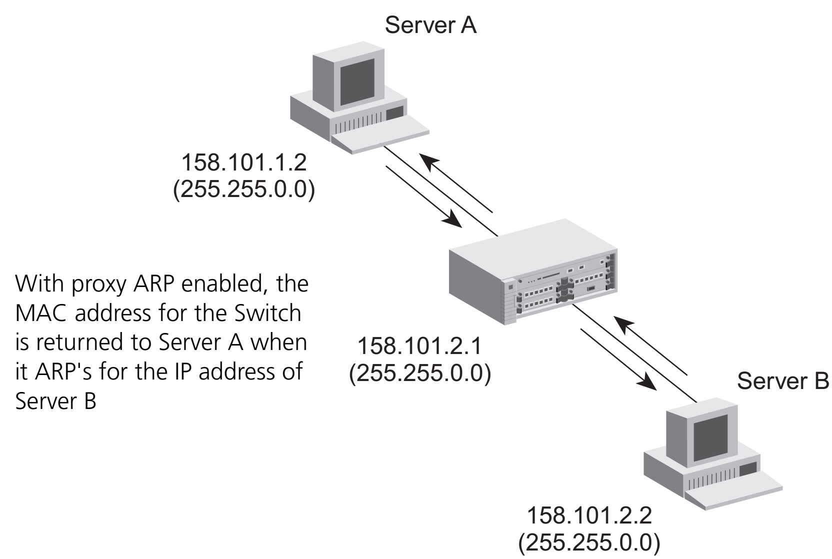
When ARP proxy is enabled and a workstation sends an ARP request for a remote network, the Switch determines if it has the best route and then answers the ARP request by sending its own MAC address to the workstation. The workstation then sends the frames for the remote destination to the Switch, which 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 36 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.

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

13 USING SWITCH CONFIGURATION FEATURES

This chapter explains the configuration features supported by the Switch that aid ease of use and configuration of your network. It covers the following topics:

- Configuration Save and Restore
- Upgrading Management Software

For detailed descriptions of the Web interface operations and the command line interface (CLI) commands that you require to manage the Switch, refer to the Management Interface Reference Guide supplied in HTML format on the CD-ROM supplied with your Switch or on the 3Com Web site.

Configuration Save and Restore

The Configuration Save and Restore feature allows the configuration of your Switch to be saved as a file to a remote server, or to be restored onto the Switch from a remote file. The configuration information is stored in an editable ASCII text file as a set of Command Line Interface (CLI) commands.

All configuration information that can be set using the Switch's Command Line Interface is saved and restored. Sensitive information such as user passwords and the IP address configuration is not saved. You can edit the text file and add this information if you want before restoring the configuration.

If the Switch is part of a stack, it is the configuration of the stack that is saved and restored. You cannot restore the configuration of a single unit in the stack from the saved file; you must restore the configuration of the entire stack.

You must have the security management access level to save and restore the Switch configuration.

Important Considerations

- The Switch unit must be reset to its factory default settings before you can restore a configuration onto it. You can reset the Switch using the **`protocol control initialize`** CLI command or the *System* > *Control* > *Init* Web interface operation.
- The configuration can only be restored onto a device or stack that has the same physical connections and configuration, including expansion modules, as when the configuration was initially saved. The restore operation will be unsuccessful if the physical configuration of the device or stack is different.
- The configuration of the Switch must only be restored or saved by a single user at a time. The **`system summary`** CLI command displays the progress of restore and save operations to all other users.
- When using the Configuration Save and Restore feature, 3Com recommends that aggregated links are configured as either:
  - Manual aggregations with Link Aggregation Configuration Protocol (LACP) disabled on the ports that are to be manually placed in the aggregated link.

  or

  - LACP automatic aggregations — that is, LACP enabled on all ports and the aggregated links created automatically. The aggregated link should be enabled and Spanning Tree Protocol enabled.

  Parameters such as VLANs and Fast Start may be set up as required.

  Other combinations of port settings, however, are not recommended as Configuration Restore will only perform a "best effort" restore of the configuration. For example, LACP automatic aggregations with manually defined ports are restored as manual aggregations with manual ports. LACP automatic aggregations with automatic ports where the aggregated link is disabled and Spanning Tree Protocol is disabled are restored as manual aggregations with the aggregated link disabled.

For further information about LACP, see *Chapter 2: Optimizing Bandwidth*.

- When restoring a configuration onto a unit over an aggregated link, communication with that unit may be lost because the restore operation disables the aggregated link ports. Communication over the aggregated links is re-established when the restore operation has been completed.

- When RADIUS is set as the authentication system mode for the Switch and the configuration is saved, the shared secret (password) is not saved and the system mode is saved as local. You must either edit the saved configuration text file prior to restoring it, or reconfigure the values using the CLI or Web interface after the Configuration Restore has been completed.

For detailed descriptions of the Configuration Save and Restore Web interface operations and Command Line Interface (CLI) commands, refer to the Management Interface Reference Guide supplied in HTML format on the CD-ROM that accompanies your Switch.

Upgrading Management Software

Your Switch has an image of the Switching software residing in flash memory. During the software upgrade process, the loading software image will always overwrite the existing software image. In the event of a software upgrade failing, you must completely reinstall the image to avoid potential complications. You will not be able to run a corrupted or missing software image.

For a detailed description of how to upgrade the software on your Switch, refer to the Management Interface Reference Guide supplied in HTML format on the CD-ROM supplied with your Switch or on the 3Com Web site.

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

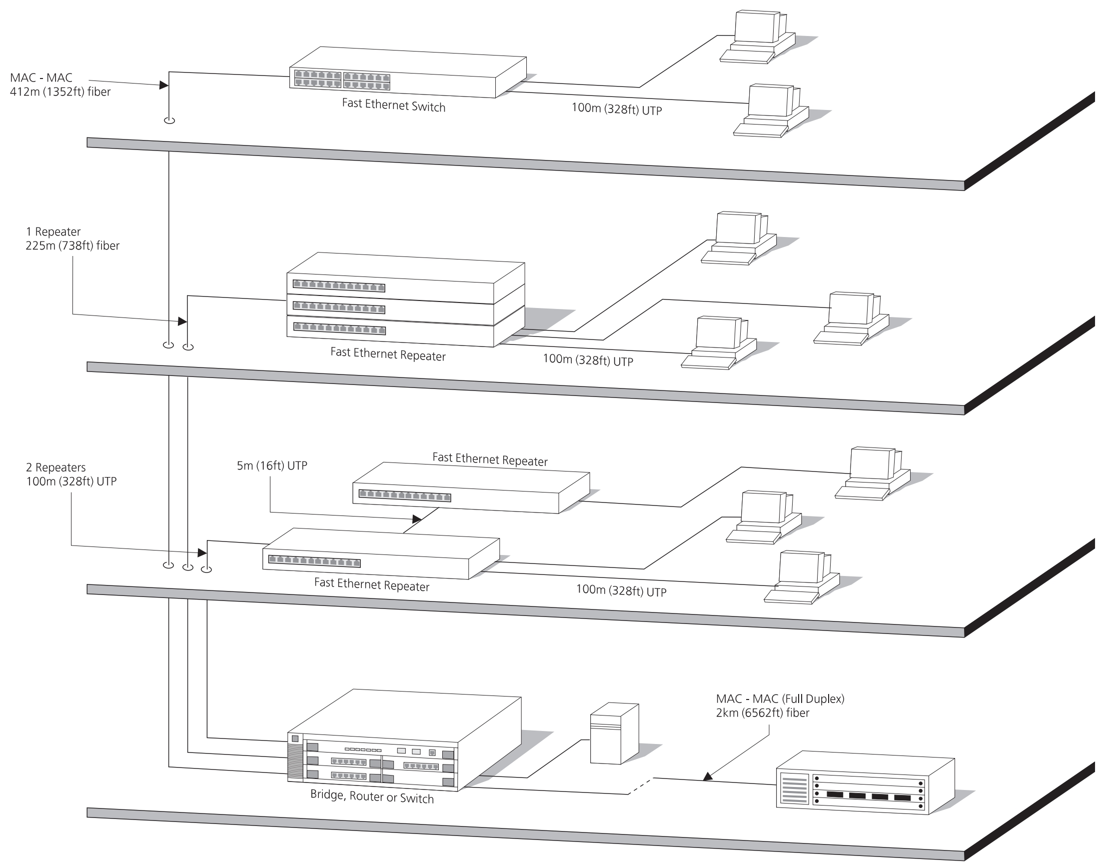
Gigabit Ethernet Transceivers	Fiber Type	Modal Bandwidth (MHz/km)	Lengths Supported Specified by IEEE (Meters)
1000BASE-LH70	10 μm SM	N/A	2-70000
1000BASE-LX	62.5 μm MM 50 μm MM 50 μm MM 10 μm SM	500 400 500 N/A	2–550 2–550 2–550 2–5000
1000BASE-SX	62.5 μm MM 62.5 μm MM 50 μm MM 50 μm MM	160 120 400 500	2–220 2–275 2–500 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 37 illustrates the key topology rules and provides examples of how they allow for large-scale Fast Ethernet networks.

Figure 37 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 RJ-45 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 appendix contains the following sections:

- Simple Network Configuration Examples
  - Collapsed Backbone Switch Example
  - Desktop Switch Example
- Advanced Network Configuration Examples
  - Edge Switch Example

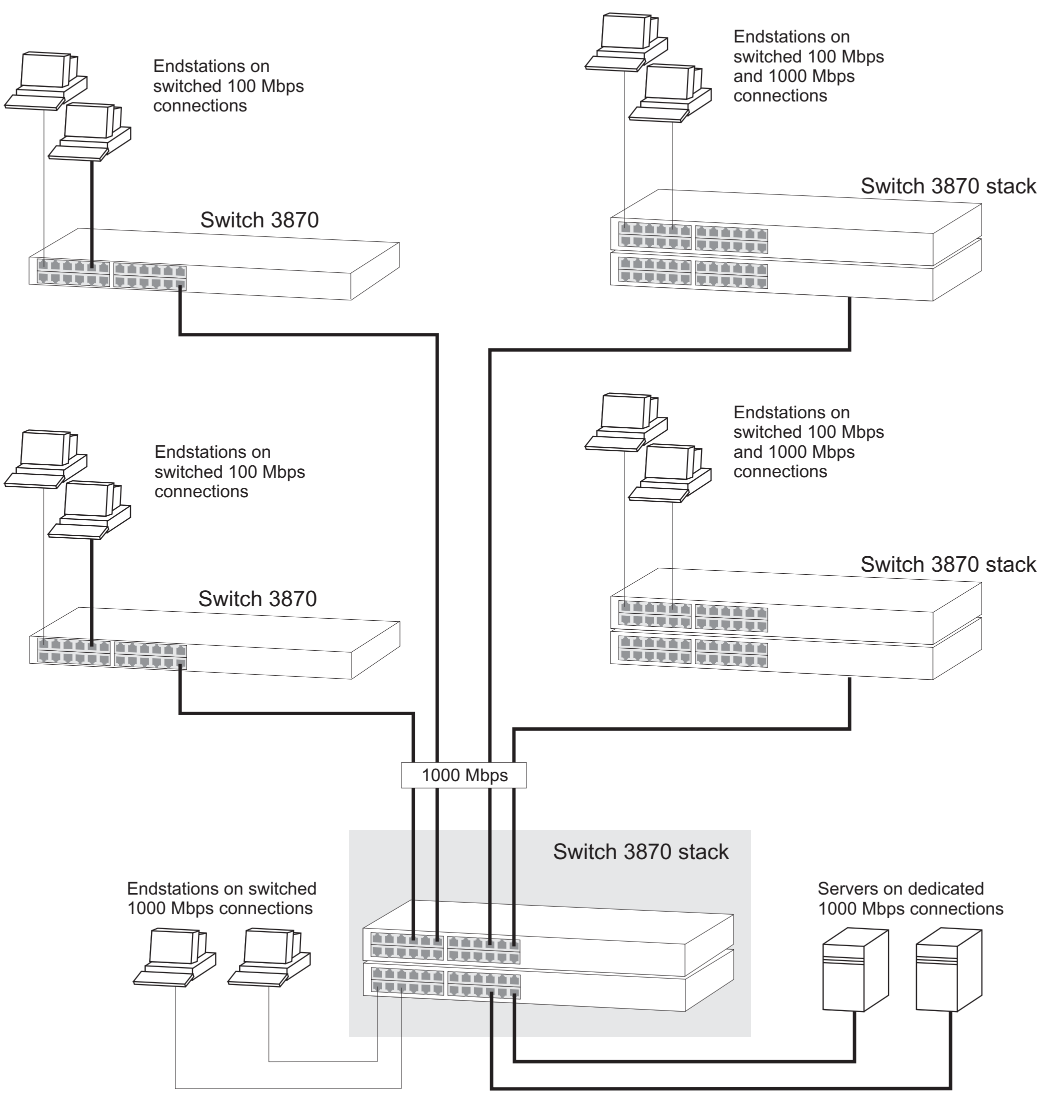
Simple Network Configuration Examples

The following illustrations show some simple examples of how the Switch 3870 can be used on your network.

Collapsed Backbone Switch Example

The example in Figure 38 shows how a Switch 3870 stack can act as a backbone for switched network segments.

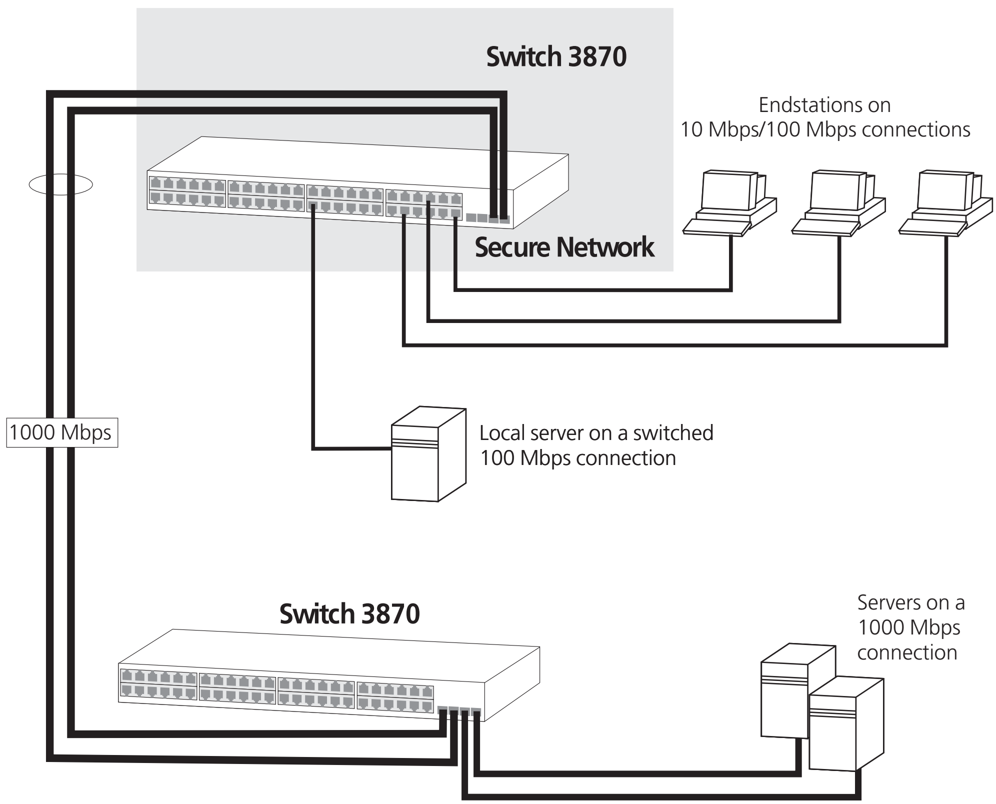
Figure 38 Using the Switch 3870 As a Collapsed Backbone



Desktop Switch Example

The example in Figure 39 shows how a Switch 3870 can be used for a group of users that require dedicated 10 Mbps, 100 Mbps, or 1000 Mbps connections to the desktop. It also illustrates the use of an aggregated link to increase the bandwidth on key links in your network.

Figure 39 Using the Switch 3870 in a Desktop Environment



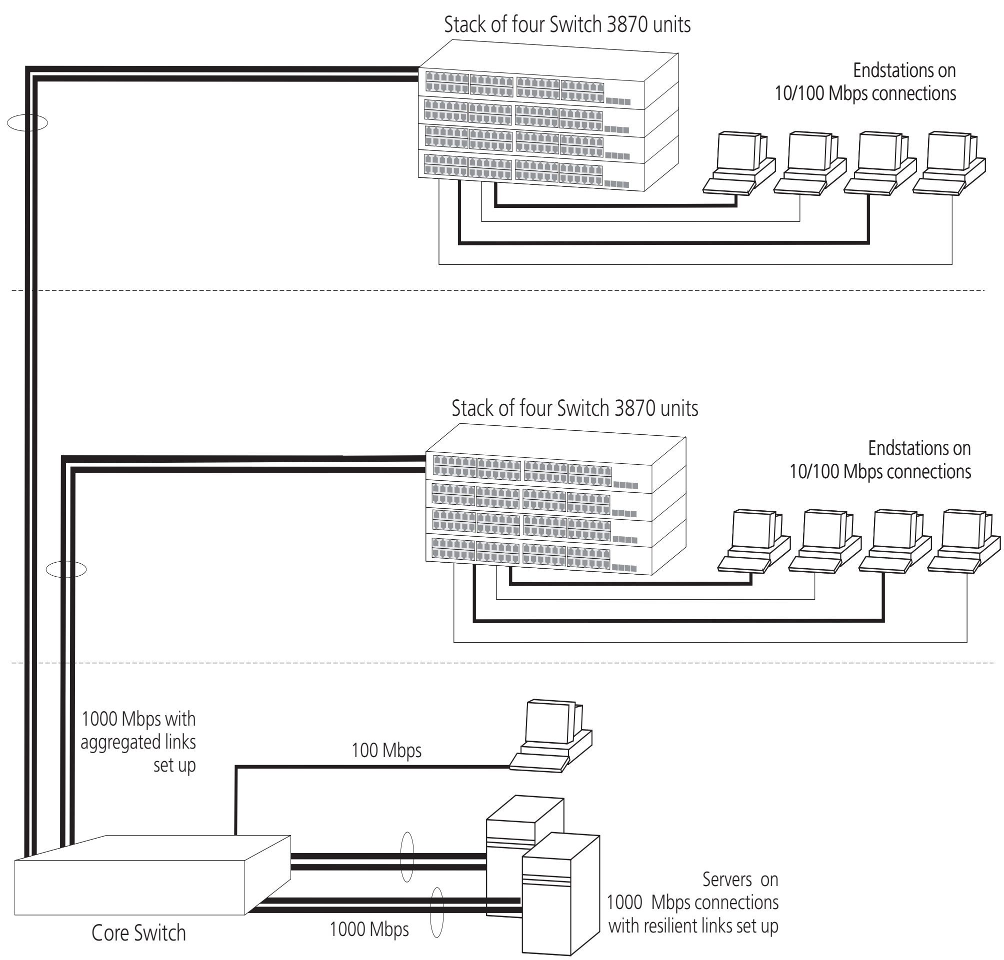
Advanced Network Configuration Examples

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.

Edge Switch Example

The example in Figure 40 shows how you can use a Switch 3870 as an edge switch on a large network. It shows how you can use aggregated links to increase bandwidth and provide extra resilience to your core network. In this network, end-to-end security can be implemented using a VLAN architecture and core traffic reduced by using Layer 3 switching at the edge

Figure 40 Network Set Up to Provide Resilience



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

IP addressing is a vast topic and there are white papers on the World Wide Web and publications available if you want 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.

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

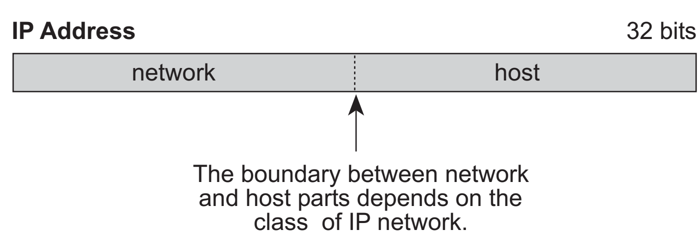
InterNIC Registration Services is the organization responsible for supplying registered IP addresses. The following contact information is correct at time of publication:

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 41 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 42 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 43.

Figure 43 Subnet Masking

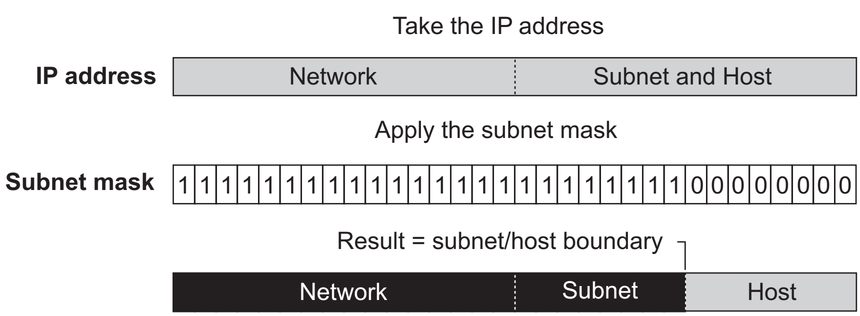


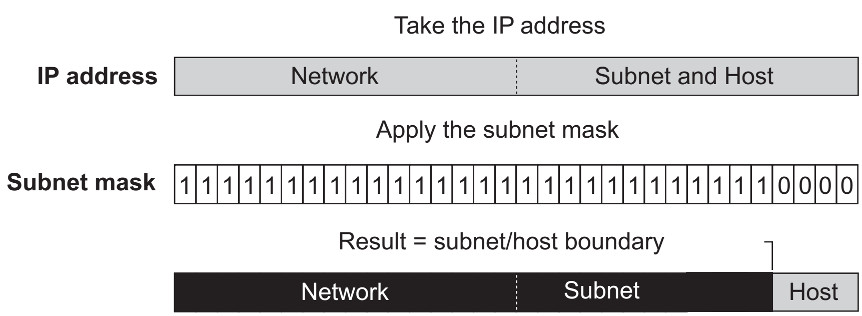
Figure 44 shows an example of an IP address that includes network, subnetwork, and host parts. Suppose the IP address is *158.101.230.52* with a subnet mask of *255.255.255.0*. Since this is a Class B address, this address is divided as follows:

- *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 44.

Figure 44 Extending the Network Prefix



Using the Class B IP address from Figure 43 (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 that 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.

D ADVANCED IP ROUTING CONCEPTS

This appendix 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 the Switch on 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.

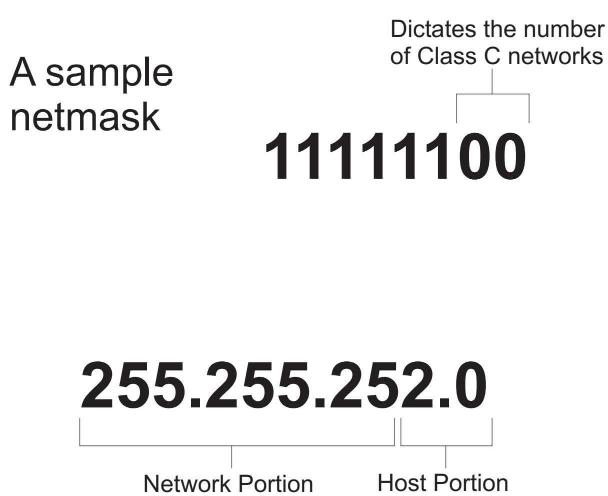
Since supernet addressing is a fairly complex mechanism, the easiest way to understand it is to step through the setup process.

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 45.

Figure 45 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.

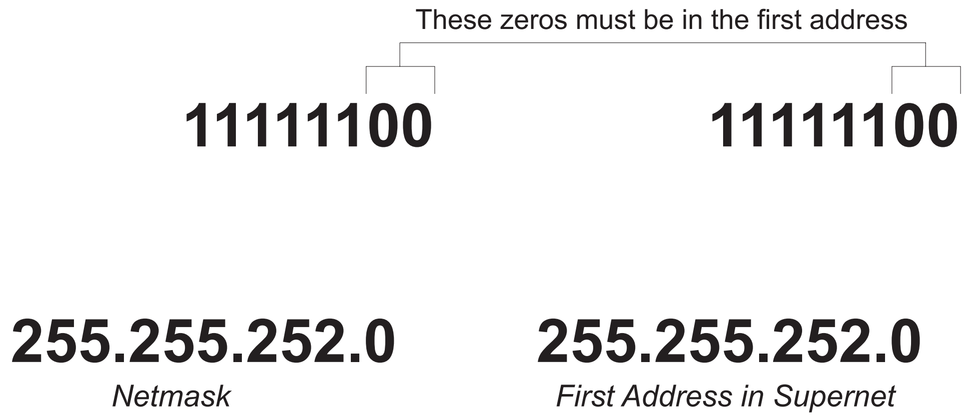
This allows a smaller supernet to share the address space of a larger supernet. If, for example, you had a supernet of size 6 and a supernet of size 2, you could assign the larger supernet an 8 network address space and assign the smaller supernet the portion of that address space that the larger supernet 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 46.

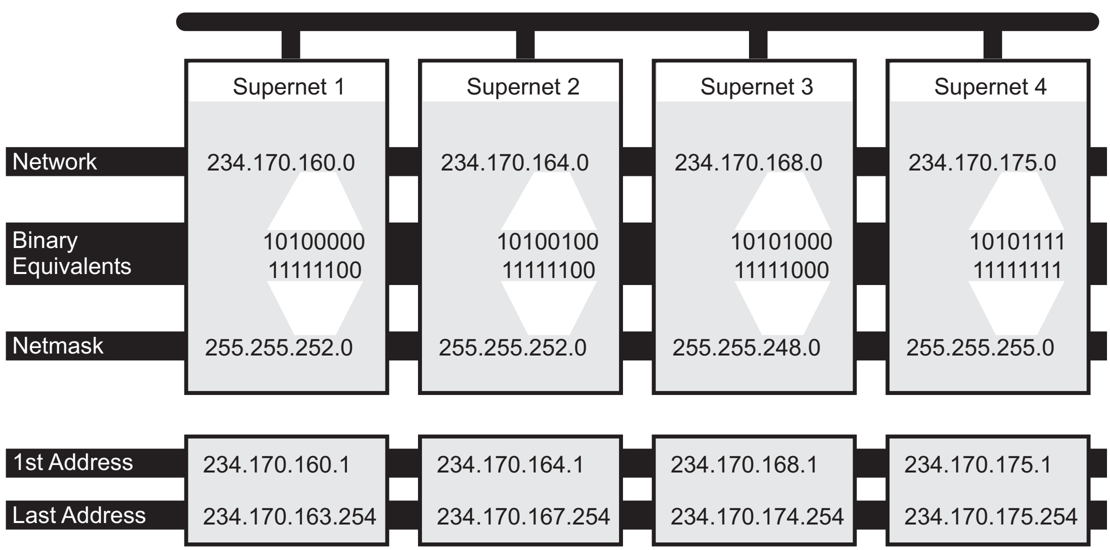
Figure 46 Selecting a Range of Addresses



Supernet Example

The four networks in Figure 47 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 47 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 is not 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 it's 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

3Com Network Supervisor The 3Com network management application used to manage 3Com's networking solutions.

3DES (Triple-DES) An encrypting algorithm that operates by applying DES encryption three times on the same data with three different keys.

10BASE-T The IEEE specification for 10 Mbps Ethernet over Category 3, 4 or 5 twisted pair cable.

100BASE-FX The IEEE specification for 100 Mbps Fast Ethernet over fiber-optic cable.

100BASE-TX The IEEE specification for 100 Mbps Fast Ethernet over Category 5 twisted-pair cable.

1000BASE-LH The specification for long-haul 1000 Mbps Gigabit Ethernet over fiber-optic cable.

1000BASE-T The IEEE specification for 1000 Mbps Gigabit Ethernet over four-pair Category 5 twisted-pair cable.

1000BASE-SX The IEEE specification for 1000 Mbps Gigabit Ethernet over fiber-optic cable.

Access Control List (ACL) A permission system used to restrict access to a resource. An ACL comprises a list of authorized IP addresses or address groups.

aggregated links 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.

aging The automatic removal of dynamic entries from the Switch Database that have timed-out and are no longer valid.

Asymmetric keys A separate but integrated user key-pair, comprised of one public key and one private key. Each key is one way, meaning that a key used to encrypt information cannot be used to decrypt the same data.

auto-negotiation 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.

auto-VLAN Automatic VLAN. Auto-VLAN is the automatic insertion of an endstation into a particular VLAN based on its MAC address. The relationship between a MAC address and a VLAN is stored on a RADIUS server.

backbone The part of a network used as a primary path for transporting traffic between network segments.

bandwidth 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*.

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.

CA See *Certificate Authority*.

cache Stores copies of frequently accessed objects locally to users and serves them to users when requested.

Certificate Authority An organization that issues Digital Certificates.

cipher A cipher is a method for encrypting data concealing its readability and meaning.

Classless InterDomain Routing (CIDR) Routing between two subnets where the size of the subnet is explicitly stated using a Variable Length Subnet Mask (VLSM) rather than being implied by the class of the IP address.

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.

CoS Class of Service. A network prioritization scheme that sorts packets into queues based on tagging or traffic type.

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.

DES Data Encryption Standard is a 64-bit block symmetric cipher algorithm. It is also known as Data Encryption Algorithm (DEA) and DEA-1 by the International Organization for Standardization (ISO) and as FIPS 46 by the US National Institute for Standards of Technology (NIST).

DHCP Dynamic Host Control Protocol. A protocol that lets you centrally manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network.

Digital Certificate Digital Certificates are blocks of data that are used to identify users and systems and encrypt their data. Digital Certificates used by SSL adhere to the X.509 standard.

Distance Vector Algorithm (DVA) Routing protocol algorithm that calculates routes for transmitting packets through networks with multiple paths to a destination.

DNS Domain Name System. This system maps a numerical Internet Protocol (IP) address to a more meaningful and easy-to-remember name. When you need to access another device on your network, you enter the name of the device, instead of its IP address.

DUD Disconnect Unauthorized Device. DUD is a port security feature that disables a port if an unauthorized device transmits data on it.

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.

FTP File Transfer Protocol. A protocol based on TCP/IP for reliable file transfer.

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.

gateway See *router*.

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 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.

HTTP Hypertext Transfer Protocol. This is a set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

HTTPS Hypertext Transfer Protocol over SSL. The term is used to describe HTTP transfers that are encrypted using the SSL protocol.

IEEE Institute of Electrical and Electronics Engineers. This American organization was founded in 1963 and sets standards for computers and communications.

IEEE Std 802.1D, 1998 Edition A standard that defines the behavior of bridges in an Ethernet network.

IEEE Std 802.1p A standard that defines traffic prioritization. 802.1p is now incorporated into the relevant sections of the IEEE Std 802.1D, 1998 Edition.

IEEE Std 802.1s A standard that defines Multiple Spanning Tree Protocol (MSTP) behavior.

IEEE Std 802.1w-2001 A standard that defines Rapid Spanning Tree Protocol (RSTP) behavior.

IEEE Std 802.1X-2001 A standard that defines port-based network access control behavior.

IEEE Std 802.1Q-1998 A standard that defines VLAN tagging.

IEEE Std 802.3ad A standard that defines link aggregation. 802.3ad is now incorporated into the relevant sections of the IEEE Std 802.3-2002.

IEEE Std 802.3x A standard that defines a system of flow control for ports that operate in full-duplex. 802.3x is now incorporated into the relevant sections of the IEEE Std 802.3-2002.

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.

IGMP snooping A mechanism performed by an intermediate device, such as a Layer 2 Switch, that optimizes the flow of multicast traffic. The device listens for IGMP messages and build mapping tables and associated forwarding filters, in addition to reducing the IGMP protocol traffic.

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.

intranet An intranet is an organization wide network using Internet protocols such as Web services, TCP/IP, HTTP and HTML. An intranet is normally used for internal communication and information, and is not accessible to computers on the wider Internet.

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.

IST Internal Spanning Tree. The IST is a special Multiple Spanning Tree Instance used by the MSTP master to control the Region.

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

key A means of gaining or preventing access, possession, or control represented by any one of a large number of values.

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).

latency The delay between the time a device receives a packet and the time the packet is forwarded out of the destination port.

line speed See *baud*.

loop 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.

MAC Media Access Control. A protocol specified by the IEEE for determining which devices have access to a network at any one time.

MAC address 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.

MDI Medium Dependent Interface. An Ethernet port connection where the transmitter of one device is connected to the receiver of another device.

MDI-X Medium Dependent Interface Cross-over. An Ethernet port connection where the internal transmit and receive lines are crossed.

MIB 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.

multicast A packet sent to a specific group of endstations on a network.

multicast filtering 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.

multiple spanning tree See *MSTP*.

MSTP Multiple Spanning Tree Protocol. An enhanced version of the Spanning Tree Protocol that is VLAN aware and supports multiple links between devices provided that the are on separate VLANs.

MSTI Multiple Spanning Tree Instance. An MSTI is one of the spanning trees supported by an MSTP network. Typically each VLAN will be associated with an MSTI.

network login Network login is a port security feature that controls user access at the network edge by blocking or allowing access on a port by port basis.

NIC Network Interface Card. A circuit board installed in an endstation that allows it to be connected to a network.

OSPF Open Shortest Path First. A hierarchical Interior Gateway Protocol (IGP) routing algorithm.

port privacy Port Privacy protects end users from any interference from other end users attached to the same network.

POST Power On Self Test. An internal test that a Switch carries out when it is powered-up.

private key A private key is the privately held component of an integrated asymmetric key pair. It is also known as the decryption key.

protocol A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

public key A public key is the publicly available component of an integrated asymmetric key pair. It is also known as the encryption key.

QoS Quality of Service. A network prioritization scheme that monitors traffic passing through the network and weights each packet according to the type of data it carries and its progress though the network.

RADA RADIUS Authenticated Device Access. RADA uses an endstation's MAC address to authenticate with a RADIUS server.

RADIUS RADIUS Authentication Dial-In User Service. An industry standard protocol for carrying authentication, authorization and configuration information between a network device and a shared authentication server.

Rapid Spanning Tree Protocol An enhanced version of the Spanning Tree Protocol that allows faster determination of Spanning Tree topology throughout the bridged network.

rate limiting The restriction of traffic on a network connection to below its maximum capacity. Typically rate limiting is used with *traffic prioritization* to ensure that the most important traffic is passed over the link.

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.

RIP Routing Information Protocol. An Interior Gateway Protocol for TCP/IP networks. RIP uses distance-vector algorithms (DVA) to calculate least-hops routes to a destination.

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 router is a device on your network which is used to forward IP packets to a remote destination. An alternative name for a router is a gateway.

Roving Analysis Port (RAP) RAP is a system that allows you to copy the traffic from one port on a switch to another port on a switch. Roving analysis is used to monitor the physical characteristics of a LAN segment without changing the characteristics by attaching a monitoring device.

RPS Redundant Power System. An RPS is a device that provides a backup source of power when connected to a switch.

RSTP See *Rapid Spanning Tree Protocol*.

Secure Shell See *SSH*.

Secure Sockets Layer See *SSL*.

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.

session key A session key is an encryption key used to encrypt data for a single communication session. When the session is over the key is discarded.

SMTP Simple Mail Transfer Protocol. An IETF standard protocol used for transferring mail across a network reliably and efficiently (as defined in RFC 821).

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.

SSH Secure Shell. A protocol which allows secure access to the Command Line Interface of the Switch.

SSL Secure Sockets Layer. A protocol used for encrypting network traffic. It is commonly used to encrypt HTTP traffic between and browser and a Web server.

stack A group of network devices that are integrated to form a single logical device.

STP See *Spanning Tree Protocol (STP)*.

subnet mask A subnet mask is used to divide the device part of the IP address into two further parts. The first part identifies the subnet number. The second part identifies the device on that subnet.

supernetting Creating several IP networks that share the same routing entry. See RFC 1519.

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.

symmetric algorithm Symmetric algorithm also known as conventional, secret key, and single key algorithms; the encryption and decryption key are either the same or can be calculated from one another.

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. TFTP allows you to transfer files from a TFTP server to a client. It is typically used to upgrade the software of a switch using an external TFTP server.

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.

Triple-DES See *3DES*.

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

Variable Length Subnet Mask (VLSM) A suffix to an IP address that indicates the size of the subnet that contains it. Taking the address 192.168.1.1/24 as an example, the VLSM is */24* and indicates that the first 24 bits of the address form the network part of the address.

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.

X.509 A standard for Digital Certificates as used by SSL.

INDEX