Chapter 3

Switching on the AR440S, AR441S and AR450S

Introduction

This chapter gives an overview of Layer 1 (physical layer) and Layer 2 (data link layer) switching, describes the support for switching, and how to configure and operate the switch ports on the router.

The router can connect multiple Local Area Network (LAN) segments together to form an extended LAN. Stations connected to different LANs can be configured to communicate with one another as if they were on the same LAN.

The router can also divide one physical LAN into multiple Virtual LANs (VLANs). Stations connected to each other on the same extended LAN can be grouped in separate VLANs, so that a station in one VLAN can communicate directly with other stations in the same VLAN, but must go through higher layer routing protocols to communicate with stations in other VLANs. By default, all switch ports on the router are included in the same VLAN.

Access to the physical link may not always be instant, so the router must be capable of storing and forwarding frames. Since the router can store and forward frames, it can examine and discard or admit frames according to their VLAN tag fields. The router can also examine the address fields of frames and forward them based on knowledge of which network contains the station with an address matching the frame’s destination address. In this way, the router acts as an intelligent filtering device, redirecting or blocking the movement of frames between networks.

Because frames may be received faster than they can be forwarded, there are *Quality of Service* queues in which frames await transmission according to their priority.

The router can:

- Increase the physical extent and/or the maximum number of stations on a LAN.

  LANs are limited in their physical extent by the signal distortion and propagation delay characteristics of the media. The router overcomes this limitation by receiving a frame on one LAN and then retransmitting the frame on another LAN, using the normal access methods for each LAN. The physical characteristics of the LAN media also place a practical limit on the number of stations that can be connected to a single LAN segment. The router overcomes this limitation by joining LAN segments together to form an extended LAN capable of supporting more stations than either of the individual LANs.
- Connect LANs which have a common data link layer protocol but different physical media, for example, Ethernet 10BASET, 100BASET, and 10BASEF.
- Prioritise the transmission of data with high Quality of Service requirements.

By using Virtual LANs (VLANs), a single physical LAN can be separated into multiple Virtual LANs. VLANs can be used to:

- Further improve LAN performance, as broadcast traffic is limited to LAN segments serving members of the VLAN to which the sender belongs.
- Provide security, as frames are only forwarded to those stations belonging to the sender’s VLAN, and not to stations in other VLANs on the same physical LAN.

- Reduce the cost of moving or adding stations to function-based or security-based LANs, as this generally requires a change in the VLAN configuration.

Switch Ports

A switch port is one of the physical Ethernet interfaces on the base router unit. Each switch port is uniquely identified by a port number. The router supports a number of features at the physical level that allow it to be connected in a variety of physical networks. This physical layer (Layer 1) versatility includes:

- Enabling and disabling of Ethernet ports.
- Autonegotiation of port speed and duplex mode for all 10/100 Ethernet ports.
- Manual setting of port speed and duplex mode for all 10/100 Ethernet ports.
- Packet storm protection.
- Support for SNMP management.

Enabling and Disabling Switch Ports

A switch port that is enabled is available for packet reception and transmission. The administrative status of the switch port in the Interfaces MIB is UP. Conversely, a port that is disabled is not available for packet reception and transmission. The port does not send or receive packets and the administrative status in the Interfaces MIB is DOWN. Every switch port is enabled by default.

To enable or disable a switch port, use the commands:

```
enable switch port={port-list|all}

disable switch port={port-list|all}
```

To reset the switch module, which resets all switch ports, clear dynamic switch information and reset counters and timers to zero, use the command:

```
reset switch
```

To display information about switch ports, use the command:

```
show switch port[={port-list|all}]
```

Autonegotiation of Port Speed and Duplex Mode

Switch ports can operate at either 10 Mbps or 100 Mbps, in either full duplex or half duplex mode. In full duplex mode a port can transmit and receive data simultaneously. In half duplex mode a port can either transmit or receive data, but not at the same time. This versatility makes it possible to connect devices with different speeds and duplex modes to different switch ports. Such versatility also requires that each switch port knows which speed and mode to use.

Each switch port can be configured with a fixed speed and duplex mode. Or switch ports can be configured to autonegotiate speed and duplex mode with a device connected to it that determines a speed and mode for successful transmission. Switch port speed and duplex modes are shown in Table 3-1 on page 3-5. Setting the switch port to a fixed speed and duplex mode lets the port support equipment that cannot autonegotiate. Autonegotiation permits switch ports to adjust their speed and duplex mode to accommodate devices connected to them. An autonegotiating switch port adopts the speed and duplex mode required by devices connected to it. When another autonegotiating device connects to the switch port, they negotiate the highest possible common speed and duplex mode.

It is also possible to require a switch port to operate at a single speed without disabling autonegotiation by allowing the port to autonegotiate, but constrain the speed/duplex options to the desired combination. For example, if one end of a link is set to AUTO and other to 100MFULL then the AUTO end selects 100MHALF operation because without the other end autonegotiating the AUTO end has no way of knowing that the fixed end is full duplex capable. When a specific speed is required, it is usually better to fix the speed/duplex combination using one of the autonegotiating speed values. Therefore, using 100MFAUTO at one end of a link and allows the AUTO end to autonegotiate 100MFULL.

If autonegotiation is disabled, the switch port is forced to operate at the specified speed and duplex mode, regardless of whether the link partner is capable of working at that speed.

Table 3-1: Switch Port Speed values

Value	**Meaning**
10MHALF	10 Mbps, half duplex, fixed, auto MDI/MDI-X
10MFULL	10 Mbps, full duplex, fixed, auto MDI/MDI-X
10MHAUTO	10 Mbps, half duplex, autonegotiate, auto MDI/MDI-X
10MFAUTO	10 Mbps, full duplex, autonegotiate, auto MDI/MDI-X-
100MHALF	100 Mbps, half duplex, fixed, auto MDI/MDI-X
100MFULL	100 Mbps, full duplex, fixed, auto MDI/MDI-X
100MHAUTO	100 Mbps, half duplex, autonegotiate, auto MDI/MDI-X
100MFAUTO	100 Mbps, full duplex, autonegotiate, auto MDI/MDI-X

Switch ports autonegotiate by default when they connect to a new device. To change this setting, use the command:

```
set switch port={port-list|all} speed={autonegotiate|10mhalf|
    10mfull|10mhauto|10mfauto|100mhalf|100mfull|100mhauto|
    100mfauto} [other-options...]
```

To display the port speed and duplex mode settings, use the command:

```
show switch port[={port-list|all}]
```

Auto MDI/MDI-X (POLARITY parameter) is not affected by setting the port speed and duplex mode.

Packet Storm Protection

The packet storm protection feature allows the user to set limits on the reception rate of broadcast, multicast and destination lookup failure packets.

The software allows separate limits to be set for each port, beyond which each of the different packet types are discarded.

By default, packet storm protection is set to NONE, that is, disabled. Packet storm protection can be enabled, and each of the limits set, using the command:

```
set switch port=port-list [bclimit={none|limit}]
   [dlflimit={none|limit}] [mclimit={none|limit}] [other-
   options...]
```

Three sets of options are allowed for packet storm protection:

- broadcast limit (BCLIMIT)
- broadcast limit and multicast limit (BCLIMIT and MCLIMIT)
- broadcast limit, multicast limit, and destination lookup failure limit (BCLIMIT, MCLIMIT, and DLFLIMIT)

The limit specified for each option, i.e the number of kilobits per second (Kbps), must be the same for all modes of storm protection selected. The limit is set to the most recent limit specified. For example:

```
set swi port=1 bclimit=256 mclimit=256 dlflimit=256
```

Packet storm protection limits are set on a per port basis.

To display the packet storm protection settings, use the command:

```
show switch port[={port-list|all}]
```

Virtual Local Area Networks (VLANs)

A Virtual LAN (VLAN) is a logical, software-defined subnetwork. It allows similar devices on the network to be grouped together into one broadcast domain, irrespective of their physical position in the network. Multiple VLANs can be used to group workstations, servers, and other network equipment connected to the router, according to similar data and security requirements.

Decoupling logical broadcast domains from the physical wiring topology offers several advantages, including the ability to:

- Move devices and people with minimal, or no, reconfiguration
- Change a device’s broadcast domain and access to resources without physically moving the device, by software reconfiguration or by moving its cable from one switch port to another
- Isolate parts of the network from other parts, by placing them in different VLANs
- Share servers and other network resources without losing data isolation or security
- Direct broadcast traffic to only those devices that need to receive it in order to reduce traffic across the network
- Connect 802.1q-compatible devices together through one port on each device

Devices that are members of the same VLAN only exchange data with each other through the router’s switching capabilities. To exchange data between devices in separate VLANs, the router's routing capabilities are used. The router passes VLAN status information, indicating whether a VLAN is up or down, to the Internet Protocol (IP) module. IP uses this information to determine route availability.

The router has a maximum of 64 VLANs ranging from a VLAN identifier (VID) of 1 to 4094.

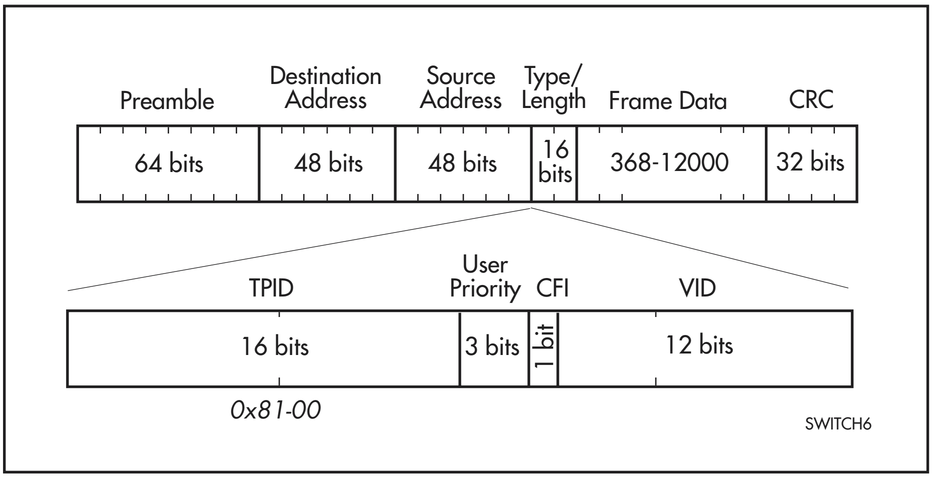
When the router is first powered up, a "default" VLAN is created and all ports are added to this VLAN. In this initial unconfigured state, the router broadcasts all packets it receives to the default VLAN. This VLAN has a VID of 1 and an interface name of *vlan1*. This VLAN cannot be deleted, and ports can only be removed from it when they also belong to at least one other VLAN. If all devices on a physical LAN are to belong to the same logical LAN; that is, in the same broadcast domain, then the default settings are acceptable and no additional VLAN configuration is necessary.

VLAN Tagging

An Ethernet packet can contain a VLAN tag, with fields that specify VLAN membership and user priority. The VLAN tag is described in IEEE 802.3ac, and is four octets that can be inserted between the Source Address and the Type/ Length fields in the Ethernet packet. To accommodate the tag, IEEE 802.3ac also increased the maximum allowable length for an Ethernet frame to 1522 octets (the minimum size is 64 octets). IEEE 802.1q specifies how the data in the VLAN tag is used to switch frames. VLAN-aware devices are able to add the VLAN tag to the packet header. VLAN-unaware devices cannot set or read the VLAN tag.

The format of VLAN data in an Ethernet frame is shown in Figure 3-1 on page 3-7. Twelve bits of the tag are the VLAN Identifier (VID), which indicate the VLAN to which the packet belongs.

Figure 3-1: Format of user priority and VLAN data in an Ethernet frame



The meaning and use of the fields in the Ethernet frame are listed in Table 3-2 on page 3-8.

Table 3-2: Fields in the Ethernet frame for QoS and VLAN switching

Field	Length	Meaning and use
TPID	2 octets	The Tag Protocol Identifier (TPID) is defined by IEEE Standard 802.1q as 0x81-00.
User Priority	3 bits	The User Priority field is the priority tag for the frame, which can be used by the router to determine the Quality of Service to apply to the frame. The three bit binary number represents eight priority levels, 0 to 7.
CFI	1 bit	The Canonical Format Indicator (CFI flag) is used to indicate whether all MAC address information that may be present in the MAC data carried by the frame is in canonical format.
VID	12 bits	The VLAN Identifier (VID) field uniquely identifies the VLAN to which the frame belongs.

The VLAN Identifier values that have specific meaning are listed in Table 3-3 on page 3-8.

Table 3-3: Reserved VID values

VID value (hexadecimal)	Meaning and use of reserved VID values
0	The null VLAN ID. Indicates that the tag header contains only user priority information; no VLAN Identifier is present in the frame. This VID value must not be configured in any Forwarding Database entry, or used in any management operation. Frames that contain the null VLAN ID are also known as priority-tagged frames.
1	The default VID value used for classifying frames on ingress through an untagged switch port.
FFF	Reserved for implementation use. This VID value must not be configured in any Forwarding Database entry, used in any management operation, or transmitted in a tag header.

Ethernet packets which contain a VLAN tag are referred to as tagged frames, and switch ports that transmit tagged frames are referred to as tagged ports. Ethernet packets which do not contain the VLAN tag are referred to as untagged frames, and switch ports that transmit untagged frames are referred to as untagged ports. VLANs can consist of simple logical groupings of untagged ports, in which the ports receive and transmit untagged packets. Alternatively, VLANs can contain only tagged ports, or a mixture of tagged and untagged ports.

Switch ports on the router are VLAN aware. They can accept VLAN tagged frames, and support the VLAN switching required by such tags. A network can contain a mixture of VLAN aware devices, for example, other 802.1q-compatible routers, and VLAN unaware devices, for example, workstations and legacy devices that do not support VLAN tagging. The router can be configured to send VLAN tagged or untagged frames on each switch port, depending on whether the devices connected to the port are VLAN aware. By assigning a port to two different VLANs, to one as an untagged port and to another as a tagged port, it is possible for the port to transmit both VLAN tagged and untagged frames.

A VID is associated with every frame admitted on a switch port. If a frame arrives on a tagged port, the associated VID is determined from the VLAN tag the frame had when it arrived. If a frame arrives on an untagged port, it is associated with the VID of the VLAN for which the incoming port is untagged. When the router forwards a frame over a tagged port, it adds a VLAN tag to the frame. When the router forwards the frame over an untagged port, it transmits the frame as a VLAN untagged frame, not including the VID in the frame.

The packet handling rules are that:

- If an untagged frame arrives at a port, a VID is assigned to the frame according to the ingress port's VLAN membership as an untagged port. The VID is then used when the packet is processed.
- If an untagged frame is switched to a tagged port the frame has a VLAN tag inserted into it before the frame is transmitted. The VID used in the tag is the VID assigned to the frame at the ingress port.
- If an untagged frame arrives at a tagged-only port the packet is dropped.
- If a tagged frame is switched to an untagged port the frame has the VLAN tag removed before it is transmitted.
- If a tagged frame arrives at a port which is not a member of the VLAN specified by the VID in the frame's VLAN tag the frame is accepted or dropped according to the port's Ingress Filtering rules.
- If a tagged frame arrives at a port with a VID that is unknown to the switch the frame is dropped.

Eth interfaces on the router can also apply a VLAN tag to frames that they transmit. For more information, see "VLAN Tagging on Eth Interfaces" on page 14-30 of Chapter 14, Internet Protocol (IP).

VLAN Membership using VLAN Tags

Switch ports can belong to many VLANs as tagged ports. Therefore, when the VLAN tag is used to determine which VLAN a packet belongs to, it is simple to:

- Share network resources, such as servers and printers, across several VLANs
- Configure VLANs that span several routers

For tagged ports, the router uses the VID of incoming frames, and the frame's destination field to switch traffic through a VLAN aware network. Frames are only transmitted on ports belonging to the required VLAN. Other vendors' VLAN aware devices on the network can be configured to accept traffic from one or more VLANs. A VLAN-aware server can be configured to accept traffic from many different VLANs, and then return data to each VLAN without mixing or leaking data into the wrong VLANs.

Figure 3-2 on page 3-10 shows a network configured with VLAN tagging. Table 3-4 on page 3-10 shows the VLAN membership. The server on port 2 on Router A belongs to both the *admin* and *marketing* VLANs. The two routers are connected through port 5 on Router A and port 3 on Router B, which belong to both the *marketing* VLAN and the *training* VLAN, so devices on both VLANs can use this link.

Figure 3-2: VLANs with tagged ports

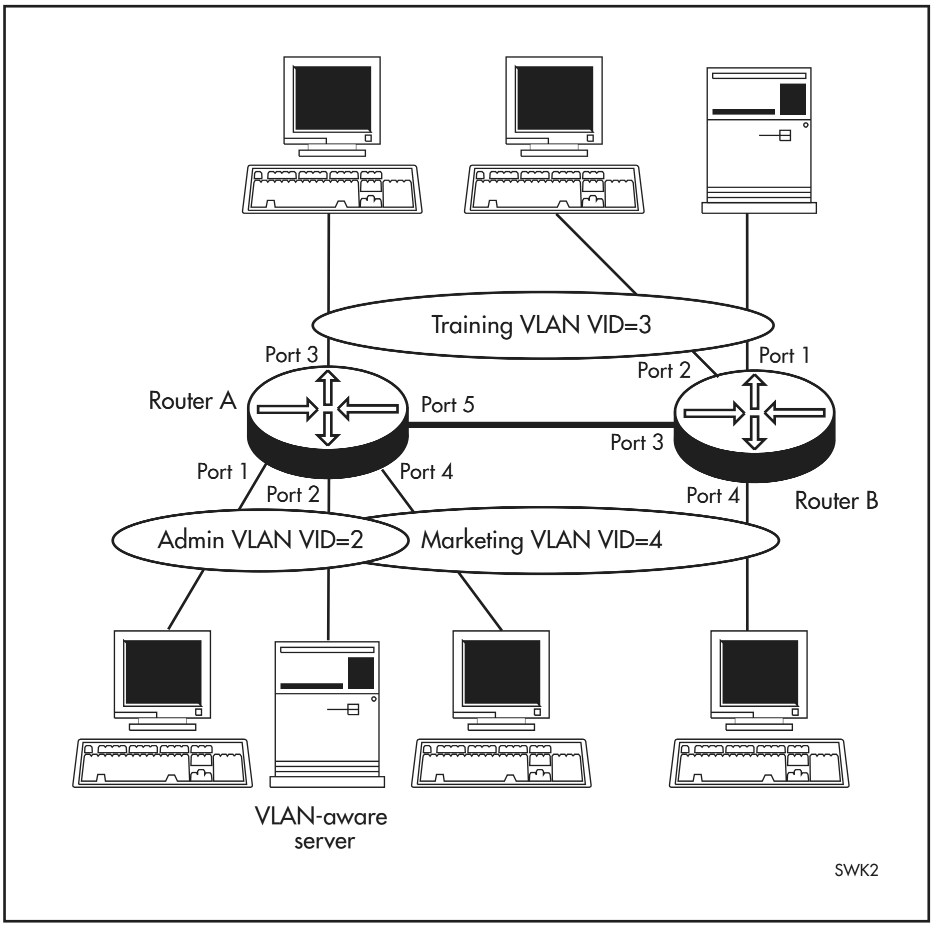


Table 3-4: VLAN membership of example of a network using tagged ports

VLAN	Member ports
Training	3, 5 on Router A 1, 2, 3 on Router B
Marketing	2, 4, 5 on Router A 3, 4 on Router B
Admin	1, 2 on Router A

VLAN Membership of Untagged Packets

A VLAN that does not send any VLAN tagged frames is a logical grouping of ports. All untagged traffic arriving at those ports belongs to that VLAN.

VLANs based on untagged ports are limited, because each port can only belong to one VLAN as an untagged port. Limitations include:

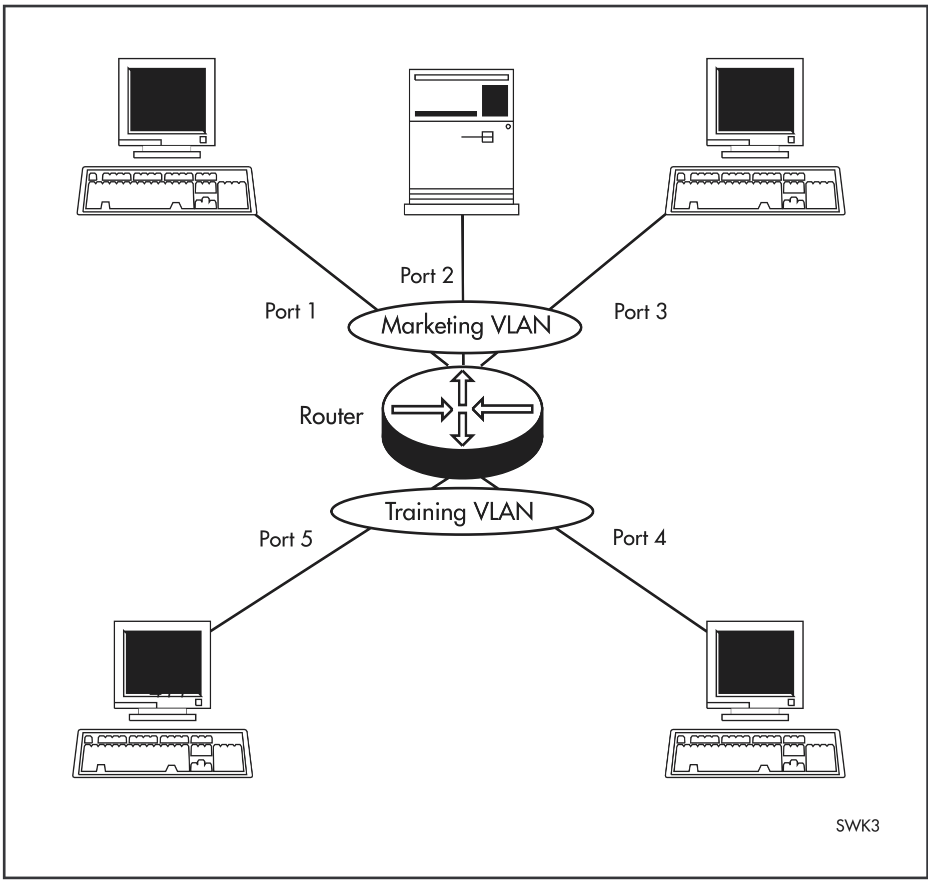
- It is difficult to share network resources, such as servers and printers, across several VLANs. The routing functions in the router must be configured to interconnect using untagged ports only.
- A VLAN that spans several devices requires a port on each device for the interconnection of the various parts of the VLAN. If there are several VLANs in the router that span more than one device, then many ports are

occupied with connecting the VLANs, and so are unavailable for other devices.

If the network includes VLANs that do not need to share network resources or span several routers, VLAN membership can usefully be based on untagged ports. Otherwise, VLAN membership should be determined by tagging (see "VLAN Tagging" on page 3-7).

Figure 3-3 on page 3-11 shows two port-based VLANs with untagged ports belonging to them. Ports 1, 2, and 3 belong to the *marketing* VLAN, and ports 4 and 5 belong to the *training* VLAN. The router acts as two separate bridges: one that forwards traffic between the ports belonging to the *marketing* VLAN, and a second one that forwards traffic between the ports belonging to the *training* VLAN. Devices in the *marketing* VLAN can only communicate with devices in the *training* VLAN by using the router's routing functions.

Figure 3-3: VLANS with untagged ports



Setting up VLANs

A summary of the process is:

1. Create the VLAN.
2. Add tagged ports to the VLAN, if required.
3. Add untagged ports to the VLAN, if required.

To create a VLAN, use the command:

```
create vlan=vlan-name vid=2..4094
```

Every port must belong to a VLAN. By default, all ports belong to the default VLAN as untagged ports.

To add tagged ports to a VLAN, use the command:

```
add vlan={vlan-name|1..4094} port={port-list|all}
    frame=tagged
```

A port can be tagged for any number of VLANs.

To add untagged ports to a VLAN, use the command:

```
add vlan={vlan-name|1..4094} port={port-list|all}
    [frame=untagged]
```

A port can be untagged for zero or one VLAN. A port can only be added to the default VLAN as an untagged port if it is not untagged for another VLAN. A port cannot transmit both tagged and untagged frames for the same VLAN (that is, it cannot be added to a VLAN as both a tagged and an untagged port).

To remove ports from a VLAN, use the command:

```
delete vlan={vlan-name|1..4094} port={port-list|all}
```

Removing an untagged port from a VLAN return it to the default VLAN, unless it is a tagged port for another static VLAN. An untagged port can only be deleted from the default VLAN when the port is a tagged port for another static VLAN.

Ports tagged for some VLANs and left in the default VLAN as untagged ports transmit broadcast traffic for the default VLAN. If this is not required, the unnecessary traffic in the router can be reduced by deleting those ports from the default VLAN.

To change the tagging status of a port in a VLAN, use the command:

```
set vlan={vlan-name|1..4094} port={port-list|all}
    frame=tagged
```

To destroy a VLAN, use the command:

```
destroy vlan={vlan-name|2..4094|all}
```

VLANs can only be destroyed if no ports belong to them.

To display the VLANs configured on the router, use the command:

```
show vlan[={vlan-name|1..4094|all}]
```

Information which may be useful for trouble-shooting a network is displayed with the VLAN debugging mode. This is disabled by default, and can be enabled for a specified time, disabled, and displayed using the commands:

```
enable vlan={vlan-name|1..4094|all} debug={pkt|all}
    [output=console] [timeout={1..4000000000|none}]

disable vlan={vlan-name|1..4094|all} debug={pkt|all}

show vlan debug
```

To view packet reception and transmission counters for a VLAN, use the command:

```
show interface=vlann counter
```

See the **show interface** command on page 7-66 of Chapter 7, Interfaces.

Summary of VLAN Tagging Rules

The following rules apply when designing a VLAN and adding ports to it.

- Each port must belong to at least one static VLAN. By default, a port is an untagged member of the default VLAN.
- A port can be untagged for zero or one VLAN. A port that is untagged for a VLAN transmits frames destined for that VLAN without a VLAN tag in the Ethernet frame.
- A port can be tagged for zero or more VLANs. A port that is tagged for a VLAN transmits frames destined for that VLAN with a VLAN tag, including the numerical VLAN Identifier of the VLAN.
- A port cannot be untagged and tagged for the same VLAN.

The Layer 2 Switching Process

The Layer 2 switching process comprises related but separate processes. The *Ingress Rules* admit or discard frames based on their VLAN tagging. The *Learning Process* learns the MAC addresses and VLAN membership of frames admitted on each port. The *Forwarding Process* determines which ports the frames are forwarded to, and the *Quality of Service* priority with which they are transmitted. Finally, the *Egress Rules* determine for each frame whether VLAN tags are included in the Ethernet frames that are transmitted. These processes assume that each station on the extended LAN has a unique data link layer address, and that all data link layer frames have a header which includes the source (sender's) MAC address and destination (recipient's) MAC address.

The Ingress Rules

When a frame first arrives at a port, the Ingress Rules for the port check the VLAN tagging in the frame to determine whether it should be discarded or forwarded to the Learning Process.

The first check depends on whether the Acceptable Frame Types parameter is set to Admit All Frames or to Admit Only VLAN Tagged Frames. A port that transmits only VLAN tagged frames, regardless of which VLAN the port belongs to, is automatically set to Admit Only VLAN Tagged Frames. The user cannot change this setting. Frames with a null numerical VLAN Identifier (VID) are VLAN untagged frames, or frames with priority tagging only.

Every frame the router receives must be associated with a VLAN. If a frame is admitted by the Acceptable Frame Types parameter, the second part of the Ingress Rules associates each untagged frame admitted with the VID of the VLAN for which the port is untagged.

Every port belongs to one or more VLANs, and therefore every incoming frame has a VID to show to which VLAN the frame belongs. The final part of the Ingress Rules depends on whether *Ingress Filtering* is enabled for the port. If Ingress Filtering is disabled, all frames are passed on to the Learning Process, regardless of which VLAN they belong to. If Ingress Filtering is enabled, frames are admitted only if they have the VID of a VLAN to which the port belongs. If they have the VID of a VLAN to which the port does not belong, they are discarded.

The default settings for the Ingress Rules are to Admit All Frames, and for Ingress Filtering to be OFF. This means that if no VLAN configuration has been done, all incoming frames pass on to the Learning Process, regardless of whether they are VLAN tagged. The parameters for each port's Ingress Rules can be configured using the command:

```
set switch port={port-list|all} [infiltering={on|off}]
   [other-options...]
```

The Learning Process

The Learning Process uses an adaptive learning algorithm, sometimes called *backward learning,* to discover the location of each station on the extended LAN.

All frames admitted by the Ingress Rules on any port are passed on to the Forwarding Process if they are for destinations within the same VLAN. Frames destined for other VLANs are passed to the layer three protocol, for instance IP. For every frame admitted, the frame's source MAC address is compared with entries in the Forwarding Database (also known as a MAC address table, or a forwarding table) maintained by the router. The Forwarding Database contains one entry for every unique station MAC address the router knows in each VLAN.

If the frame's source address is not in the Forwarding Database, the address is added and an ageing timer is started for it. If the frame's source address is already in the database, the ageing timer is restarted for it. By default, switch learning is enabled, and it can be disabled or enabled by using the commands:

```
disable switch learning
```

```
enable switch learning
```

If the ageing timer for an entry in the Forwarding Database expires before another frame with the same source address is received, the entry is removed from the Forwarding Database. This prevents the Forwarding Database from being filled up with information about stations that are inactive or have been disconnected from the network, while ensuring that entries for active stations are kept alive in the Forwarding Database. By default, the ageing timer is enabled.

To disable or enable the ageing timer, use the commands:

```
enable switch ageingtimer
```

```
disable switch ageingtimer
```

If switch learning is disabled and the ageing timer has aged out all dynamically learned filter entries, only statically entered MAC source addresses are used to decide which packets to forward or discard. If the router finds no matching entries in the Forwarding Database during the Forwarding Process, then all switch ports in the VLAN are flooded with the packet, except the port on which the packet was received.

The default of the ageing timer is 304 seconds (approximately 5 minutes). To modify the default, use the command:

```
set switch ageingtimer=16..4080
```

The Forwarding Database relates a station’s (source) address to a port on the router, and is used by the router to determine from which port (if any) to transmit frames with a destination MAC address matching the entry in the station map.

To display the contents of the Forwarding Database, use the command:

```
show switch fdb [address=macadd][port={port-list|all}]
    [status={static|dynamic}]
```

To display general router settings, including settings for switch learning and the ageing timer, use the command:

```
show switch
```

The Forwarding Process

The Forwarding Process forwards received frames that are to be relayed to other ports in the same VLAN.

The destination address is then looked up in the Forwarding Database for the VLAN. If the destination address is not found, the router floods the frame on all ports in the VLAN except the port on which the frame was received. If the destination address is found, the router discards the frame if the destination address is on the same port as the source address.

The Forwarding Process provides storage for queued frames to be transmitted over a particular port(s). More than one transmission queue may be provided for a given port. The user priority tag in the Ethernet frame and the Quality of Service mapping (see “Quality of Service” on page 3-15) determine the transmission queue where a frame is sent.

Quality of Service

The router hardware has a number of Quality of Service (QOS) *egress queues* that can be used to give priority to the transmission of some frames over other frames on the basis of their user priority tagging. The user priority field in an incoming frame (with value 0 to 7) determines which of the eight priority levels the frame is allocated. When a frame is forwarded, it is sent to a QOS egress queue on the port determined by the mapping of priority levels to QOS egress queues. All frames in the first QOS queue are sent before any frames in the second QOS egress queue, and so on, until frames in the last QOS egress queue, which are sent only when there are no frames waiting to be sent in any of the higher QOS egress queues.

The mapping between user priority and a QOS egress queue is configured using the command:

```
set switch qos=p0,p1,p2,p3,p4,p5,p6,p7
```

The router has four QOS egress queues. The router has a default mapping of priority levels to QOS egress queues as defined in IEEE 802.1q (see Table 3-5 on page 3-15).

Table 3-5: Default priority level to queue mapping for four QOS egress queues

Priority level	QOS Egress Queue
0	1

Table 3-5: Default priority level to queue mapping for four QOS egress queues

Priority level	**QOS Egress Queue**
1	0
2	0
3	1
4	2
5	2
6	3
7	3

To display the mapping of user priority to QOS egress queues, use the command:

```
show switch qos
```

The Egress Rules

After the Forwarding Process has determined the ports and transmission queues from which to forward a frame, the Egress Rules for each port determine whether the outgoing frame is VLAN tagged with its numerical VLAN Identifier (VID).

When a port is added to a VLAN, it is configured to transmit either untagged or VLAN tagged packets, using the command:

```
add vlan={vlan-name|1..4094} port={port-list|all}
    [frame={tagged|untagged}]
```

In the default configuration, no ports transmit VLAN tagged packets.

This setting can be changed for a port that is already part of a VLAN, using the command:

```
set vlan={vlan-name|1..4094} port={port-list|all}
    frame={untagged|tagged}
```

Triggers

The Trigger Facility can be used to automatically run specified command scripts when particular triggers are activated. When a trigger is activated by an event, global parameters and parameters specific to the event are passed to the script that is run. For a full description of the Trigger Facility, see Chapter 30, Trigger Facility.

The router can generate triggers to activate scripts when a switch port goes up or down.

The following section lists the events that may be specified for the Switching module for the EVENT parameter, the parameters that may be specified as *module-specific-parameters* for the Switching module, and the arguments passed to the script activated by the trigger.

Module	Layer 2 Switching module: MODULE=SWI

Event LINKDOWN

Description The port link specified by the PORT parameter has just gone down.

Parameters The following command parameter(s) must be specified in the CREATE/SET TRIGGER commands:

Parameter	Description
PORT=*port*	The port where the event activates the trigger.

Script Parameters The trigger passes the following parameter(s) to the script:

Argument	Description
%1	The port number of the port that has just gone down.

Event LINKUP

Description The port link specified by the PORT parameter has just come up.

Parameters The following command parameter(s) must be specified in the CREATE/SET TRIGGER commands:

Parameter	Description
PORT=*port*	The port where the event activates the trigger.

Script Parameters The trigger passes the following parameter(s) to the script:

Argument	Description
%1	The port number of the port that has just come up.

To create or modify a switch trigger, use the commands:

```
create trigger=trigger-id module=switch event={linkdown|
    linkup} port=port [after=hh:mm] [before=hh:mm] [date=date|
    days=day-list] [name=name] [repeat={yes|no|once|forever|
    count}] [script=filename...] [state={enabled|disabled}]
    [test={yes|no|on|off|true|false}]
```

```
set trigger=trigger-id [port=port] [after=hh:mm]
    [before=hh:mm] [date=date|days=day-list] [name=name]
    [repeat={yes|no|once|forever|count}] [test={yes|no|on|
    off|true|false}]
```

Configuration Examples

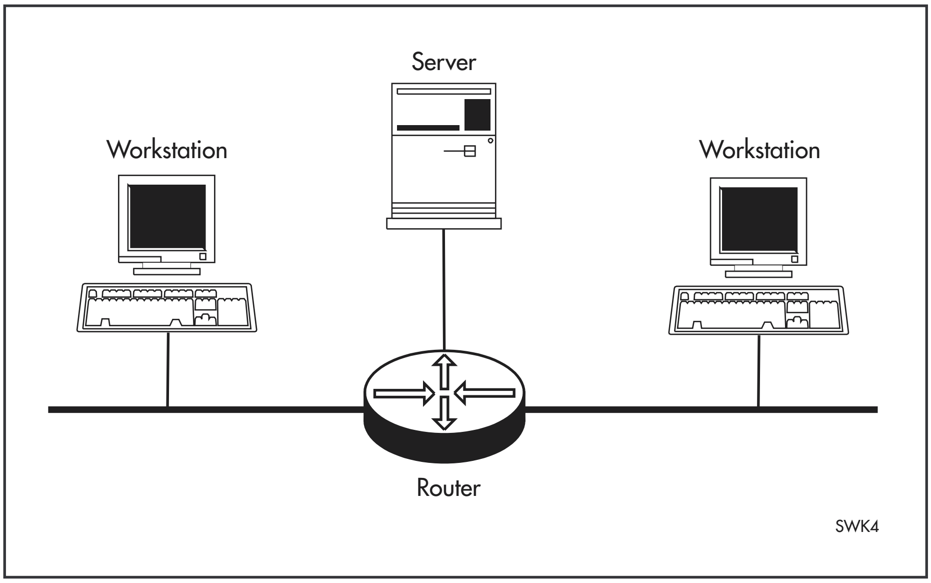
This section shows examples of configuring the switch functions on the router. All examples assume that the switch configuration begins from factory default settings.

Note that routing, required for communication between the VLANs, is not shown in these examples.

Example Using One Router to Extend a Local LAN

The example in Figure 3-4 on page 3-18 uses a single router to connect two (or more) physical LANs and a server. All devices connected to the router belong to the same broadcast domain, and separate collision domains. The Learning and Forwarding Processes in the router give this topology better performance than a single LAN would give, and allow more devices to be attached than would a single physical LAN.

Figure 3-4: Example of router with default configuration



No software configuration is required. The default switching settings allow the router to learn source addresses and forward frames to the correct ports as soon as the router is physically connected and powered up.

VLAN Example Using Untagged Ports

The example in Figure 3-5 on page 3-19 has two VLANs using untagged ports. Ports 1, 2, and 3 belong to one broadcast domain, the *marketing* VLAN, and ports 4 and 5 belong to another broadcast domain, the *training* VLAN. The router acts as two separate bridges: one that forwards between the ports belonging to the *marketing* VLAN, and a second one that forwards between the ports belonging to the *training* VLAN.

Figure 3-5: VLANS with untagged ports

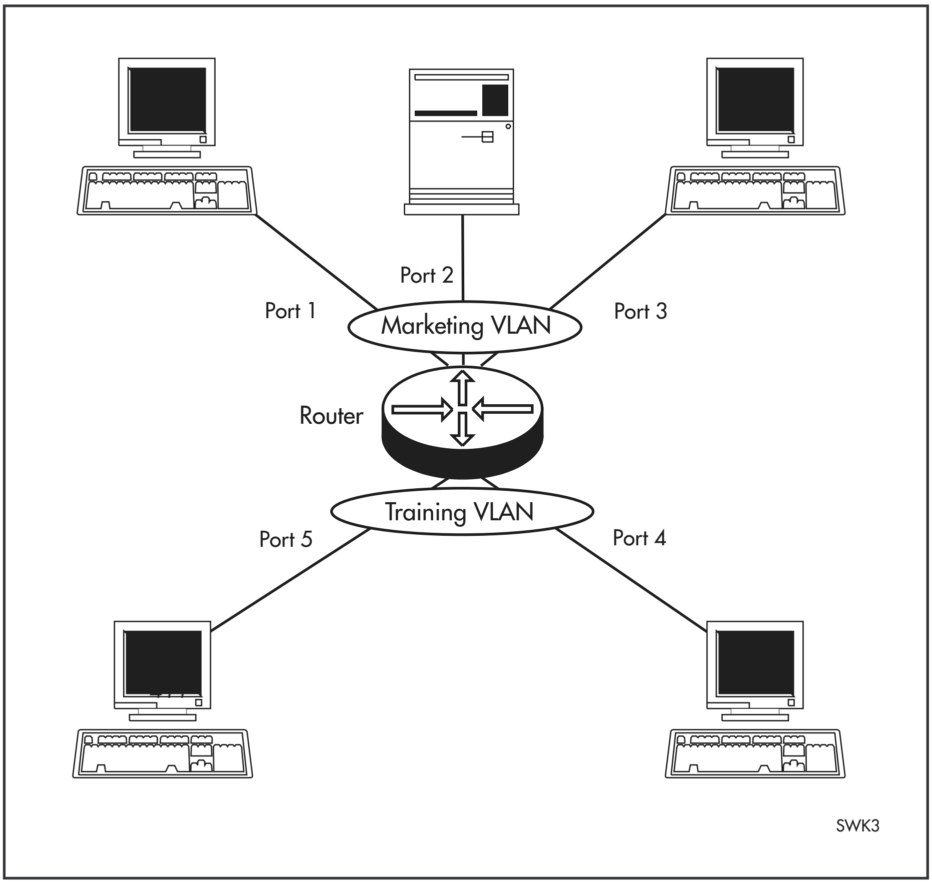


Table 3-6 on page 3-19 shows the parameters used to configure this example. This example assumes that the router has factory default settings.

Table 3-6: Parameters for port-based VLAN example

VLAN name	VLAN ID	Ports
Marketing	VID=2	PORT 1-3
Training	VID=3	PORT 4, 5

Configure the router

1. **Create VLANs**

   Create the two VLANs using the following commands on the router:

   ```
   create vlan=marketing vid=2
   create vlan=training vid=3
   ```

2. **Add ports to VLANs**

   Add the ports to these VLANs on the router by using the following commands:

   ```
   add vlan=marketing port=1-3
   add vlan=training port=4,5
   ```

   Check the VLAN configuration by using the command:

   ```
   show vlan
   ```

Check

Check that the router is switching across the ports. Traffic on the router is monitored using the command:

```
show switch port=1-5 counter
```

VLAN Example Using Tagged Ports

Figure 3-6 on page 3-20 shows a network that must be configured with VLAN tagging, since the VLAN aware server on port 2 on Router A belongs to both the *admin* VLAN and the *marketing* VLAN. Using VLAN tags, port 5 on Router A and port 3 on Router B belong to both the *marketing* VLAN and the *training* VLAN, so that devices on both VLANs can use this link to communicate with other devices in the same VLAN on the other router.

Figure 3-6: VLANs with tagged ports

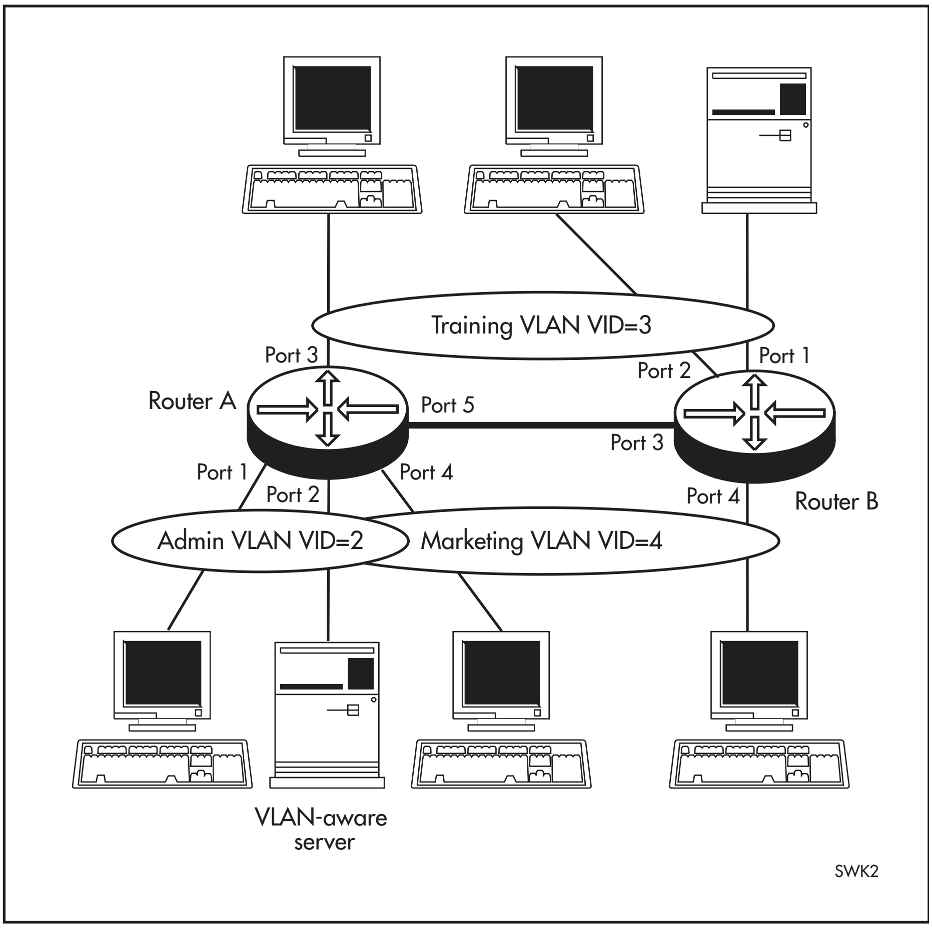


Table 3-7 on page 3-20 shows the parameters used to configure this example.

Table 3-7: Configuration example parameters for VLANs with tagged ports

		Router A		Router B	
VLAN name	**VID**	**Tagged ports**	**Untagged ports**	**Tagged ports**	**Untagged ports**
Admin	VID=2	PORT 2	PORT 1		
Training	VID=3	PORT 5	PORT 3	PORT 3	PORT 1,2
Marketing	VID=4	PORT 2,5	PORT 4	PORT 3	PORT 4

Configure Router A

1. **Create VLANs**

   Create the three VLANs using the following commands on the router:

   ```
   create vlan=admin vid=2
   
   create vlan=training vid=3
   
   create vlan=marketing vid=4
   ```

2. **Add ports to VLANs**

   Add the ports to these VLANs on the router by using the following commands:

   ```
   add vlan=admin port=2 frame=tagged
   
   add vlan=admin port=1
   
   add vlan=training port=5 frame=tagged
   
   add vlan=training port=3
   
   add vlan=marketing port=2,5 frame=tagged
   
   add vlan=marketing port=4
   ```

   Check the VLAN configuration by using the command:

   ```
   show vlan
   ```

Configure Router B

1. **Create VLANs**

   Create the two VLANs using the following commands on the router:

   ```
   create vlan=training vid=3
   
   create vlan=marketing vid=4
   ```

2. **Add ports to VLANs**

   Add the ports to these VLANs on the router by using the following commands:

   ```
   add vlan=training port=3 frame=tagged
   
   add vlan=training port=1,2
   
   add vlan=marketing port=3 frame=tagged
   
   add vlan=marketing port=4
   ```

   Check the VLAN configuration by using the command:

   ```
   show vlan
   ```

Check

Check that the router is switching across the ports. Traffic on Router A can be monitored using the command:

```
show switch port=1-5 counter
```

Traffic on Router B can be monitored using the command:

```
show switch port=1-4 counter
```

Command Reference

This section describes the commands available to configure and manage the switching functions on the router.

See “Conventions” on page xcv of Preface in the front of this manual for details of the conventions used to describe command syntax. See Appendix A, Messages for a complete list of messages and their meanings.

add vlan port

Syntax

```
ADD VLAN={vlan-name|1..4094} POrt={port-list|ALL}
   [FRAme={TAGged|UNTAGged}]
```

where:

- *vlan-name is* a unique name from 1 to 32 characters. Valid characters are uppercase and lowercase letters, digits (0-9), the underscore character ("_"), and the hyphen (-). The *vlan-name* cannot be a number or ALL.
- *port-list* is a port number, range (specified as *n-m*), or comma-separated list of numbers and/or ranges. Port numbers start at 1 and end at *m*, where *m* is the highest numbered Ethernet port.

Description This command adds ports to the specified VLAN.

The **vlan** parameter specifies the name or numerical VLAN Identifier (VID) of the VLAN. The name is not case sensitive although the case is preserved for display purposes. The VLAN must already exist. By default, all ports belong to the default VLAN, with a VID of 1.

The **port** parameter specifies the ports. All the ports in a trunk group must have the same VLAN configuration. If the command would succeed on a subset of the ports specified, but cause an error on the others, then the command as a whole fails and has no effect.

The **frame** parameter specifies whether a VLAN tag header is included in each frame transmitted on the specified ports. If **tagged** is specified, a VLAN tag is added to frames prior to transmission. The port is then called a *tagged* port for this VLAN.

If **untagged** is specified, the frame is transmitted without a VLAN tag. The port is then called an *untagged* port for this VLAN. A port can be untagged for one and only one of the VLANs to which it belongs, or for none of the VLANs to which it belongs. A port can have the **frame** parameter set to TAGGED for zero or more VLANs to which it belongs. It is not possible to add an untagged port to a VLAN when the port is already present in another port-based VLAN, except the default VLAN.

When the port is an untagged member of the default VLAN and you add it as an untagged port to another VLAN, it is deleted from the default VLAN. The default is **untagged**.

Examples To add port 4 to the port-based *marketing* VLAN, use the command:

```
add vlan=marketing port=4
```

To add port 2 to the *training* VLAN as a tagged port, use the command:

```
add vlan=training port=2 frame=tagged
```

Related Commands **delete vlan port**
show vlan

create vlan

Syntax

```
CREate VLAN=vlan-name VID=2..4094
```

vlan-name is a unique name from 1 to 32 characters. Valid characters are uppercase and lowercase letters, digits (0-9), the underscore character ("_"), and the hyphen (-). The *vlan-name* cannot be a number or ALL.

Description

This command creates a VLAN with a unique name and VLAN Identifier (VID). To change the VID of an existing VLAN, that VLAN must be destroyed and created again with the modified VID. A maximum of 64 VLANs, including the default VLAN, can be created with any VID from 2 to 4094.

The **vlan** parameter specifies a unique name for the VLAN. This name can be more meaningful than the VID, to make administration easier. The VLAN name is used internally; it is not transmitted to other VLAN-aware devices, or used in the Forwarding Process or stored in the Forwarding Database. If the VLAN name begins with "vlan" and ends with a number, for instance "vlan1" or "vlan234", then the number must be the same as the VID specified. This avoids confusion when identifying to which VLAN subsequent commands refer.

The **vid** parameter specifies a unique VLAN Identifier for the VLAN. If tagged ports are added to this VLAN, the specified VID is used in the VID field of the tag in outgoing frames. If untagged ports are added to this VLAN, the specified VID acts as an identifier for the VLAN in the Forwarding Database. The default port based VLAN has a VID of 1.

Examples

To create a VLAN named *marketing* with a VLAN Identifier of 2, use the command:

```
create vlan=marketing vid=2
```

To create a VLAN named *vlan42*, which must have a VID of 42, use the command:

```
create vlan=vlan42 vid=42
```

Related Commands

destroy vlan
show vlan

delete vlan port

Syntax

```
DELete VLAN={vlan-name|1..4094} POrt={port-list|ALL}
```

where:

- *vlan-name is* a unique name from 1 to 32 characters. Valid characters are uppercase and lowercase letters, digits (0-9), the underscore character (“_”), and the hyphen (-). The *vlan-name* cannot be a number or ALL.
- *port-list* is a port number, range (specified as *n-m*), or comma-separated list of numbers and/or ranges. Port numbers start at 1 and end at *m*, where *m* is the highest numbered Ethernet port.

Description

This command deletes ports from the specified VLAN. An untagged port can be deleted from a VLAN if the port is still a member of a VLAN after the deletion has occurred. If the port does not belong to any VLAN as a tagged port then the port is implicitly added to the default VLAN as an untagged port. It is not possible to delete a port that belongs only to the default VLAN as an untagged port.

A tagged port can be deleted from a VLAN if the port is still a member of a VLAN afterwards.

The **vlan** parameter specifies the name or numerical VLAN Identifier of the VLAN. The name is not case sensitive. The VLAN must already exist.

The **port** parameter specifies the ports to be deleted from the VLAN. If ALL is specified, then all ports belonging to the VLAN are deleted. If the command would succeed on a subset of the ports specified, but cause an error on the others, then the command as a whole fails and has no effect.

Example

To delete port 3 from the *marketing* VLAN, use the command:

```
delete vlan=marketing port=3
```

Related Commands

add vlan port
show vlan

destroy vlan

Syntax `DESTroy VLAN={vlan-name|2..4094|ALL}`

where *vlan-name is* a unique name from 1 to 32 characters. Valid characters are uppercase and lowercase letters, digits (0-9), the underscore character ("_"), and the hyphen (-). The *vlan-name* cannot be a number or ALL or DEFAULT.

Description This command destroys the specified static VLAN or all static VLANs in the router. The default VLAN, with a VID of 1, cannot be destroyed. If ALL is specified then all VLANs except the default VLAN are destroyed. A VLAN cannot be destroyed if ports still belong to it, or if other modules are attached to it.

Examples To destroy the VLAN with the VID of 1234, use the command:

```
destroy vlan=1234
```

To remove all user created VLANs from the router, none of which have any member ports, use the command:

```
destroy vlan=all
```

Related Commands create vlan
show vlan

disable switch ageing timer

Syntax `DISable SWItch AGEingtimer`

Description This command disables the ageing timer from ageing out dynamically learned entries in the Forwarding Database. The default setting for the ageing timer is enabled.

Example To disable the ageing out of learned MAC addresses, use the command:

```
disable switch ageingtimer
```

Related Commands enable switch ageing timer
show switch

disable switch debug

Syntax

```
DISable SWItch DEBug={ARL|DMA|M6|PHY|ALL}
```

Description This command disables the specified switch debug mode or all switch debugging. The **debug** parameter specifies the switch debug mode to be disabled (see Table 1-17 on page 1-53).

Table 3-8: Switch debugging options.

Debug Options	Description
ARL	Operations related to the Forwarding Database.
DMA	Operations related to Direct Memory Access requests.
M6	Operations related to the switch chip.
PHY	Operations related to the PHY port interfaces.
ALL	All debug options

Example To disable all switch debugging, use the command:

```
disable switch debug=all
```

Related Commands enable switch debug
show switch

disable switch learning

Syntax

```
DISable SWItch LEarning
```

Description This command disables the dynamic learning and updating of the Forwarding Database. The default setting for the learning function is enabled.

If switch learning is disabled, and the ageing timer has aged out all dynamically learned filter entries, statically entered MAC source addresses are used to decide which packets to forward or discard. If no matching entries in the Forwarding Database are found during the Forwarding Process, then all switch ports in the VLAN are flooded with the packet except the port where packet was received.

Example To disable the switch learning function, use the command:

```
disable switch learning
```

Related Commands enable switch learning
show switch

disable switch port

Syntax

```
DISable SWItch POrt={port-list|ALL} [AUTOMDI]
```

```
DISable SWItch POrt={port-list|ALL} [FLOW]
```

where *port-list* is a port number, range (specified as *n-m*), or comma-separated list of numbers and/or ranges. Port numbers start at 1 and end at *m*, where *m* is the highest numbered Ethernet port.

Description

This command disables a switch port or group of switch ports, or disables the auto MDI/MDI-X, or disables the flow control mechanism. If the port is disabled, it no longer sends or receives packets. Switch ports are enabled by default.

The **port** parameter specifies the port(s) to be disabled or which are to have flow control methods disabled.

The **automdi** parameter disables auto MDI/MDI-X.

The **flow** parameter specifies that flow control is disabled for the port. The type of flow control is full-duplex flow control or half-duplex backpressure.

Example

To disable ports 2, 3, and 4, use the command:

```
disable switch port=2-4
```

Related Commands

enable switch port
set switch port
show switch port

disable vlan debug

Syntax

```
DISable VLAN={vlan-name|1..4094|ALL} DEBug={PKT|ALL}
```

where *vlan-name is* a unique name from 1 to 32 characters. Valid characters are uppercase and lowercase letters, digits (0-9), the underscore character (“_”), and the hyphen (-). The *vlan-name* cannot be a number or ALL.

Description

This command disables packet debugging or all debugging for the specified VLAN or all VLANs. The default is for all VLAN debugging to be disabled.

The **debug** parameter specifies the VLAN debugging mode to be disabled. If PKT is specified, the packet debug mode (displaying raw ASCII packets) is disabled. If ALL is specified, all debugging is disabled.

Example

To disable packet debugging on the *default* VLAN, use the command:

```
disable vlan=default debug=pkt
```

Related Commands

enable vlan debug
show vlan debug

enable switch ageing timer

Syntax `ENAble SWItch AGEingtimer`

router**Description** This command enables the ageing timer to age out dynamically learned entries in the Forwarding Database after 304 seconds (approximately 5 minutes). The default setting for the ageing timer is enabled.

Example To enable the ageing out of learned MAC addresses, use the command:

```
enable switch ageingtimer
```

Related Commands **disable switch ageing timer**
show switch

enable switch debug

Syntax

```
ENAble SWItch DEBug={ARL|DMA|M6|PHY|ALL} [OUTPUT=CONSOLE]
    [TIMEOUT={1..4000000000|NONE}]
```

Description

This command enables the specified switch debug mode or all switch debugging. Be aware that enabling debug could flood the receiving Telnet session or asynchronous port with raw data.

The **debug** parameter specifies the switch debug mode to be disabled (see Table 3-9 on page 3-30). If ALL is specified, all switch debugging modes are enabled.

Table 3-9: Switch debugging options

Debug Options	Description
ARL	Operations related to the Forwarding Database.
DMA	Operations related to Direct Memory Access requests.
M6	Operation related to the switch chip.
PHY	Operations related t the PHY port interfaces.
ALL	All debug options.

The **output** parameter set to CONSOLE specifies that the debugging information produced is sent to the console. The debugging data is by default sent to the port where it received the ENABLE SWITCH DEBUG command. Use this option if the command is in a script since a script is not received on a port.

The **timeout** parameter specifies the time in seconds for which any switch debugging is enabled. This reduces the risk of overloading the router and the display with too much debugging information. The value set by the **timeout** parameter overrides any previous switch debugging timeout values, even if they were specified for other debugging modes. If TIMEOUT is not specified, the time out is the most recent one from a previous ENABLE VLAN DEBUG command or NONE if it had not been set.

Example

To enable the ARL switch debugging mode, use the command:

```
enable switch debug=arl
```

Related Commands

enable switch debug
show switch

enable switch learning

Syntax

```
ENAble SWItch LEarning
```

Description

This command enables the dynamic learning and updating of the Forwarding Database. The default setting for the learning function is enabled.

Example

To enable the switch learning function, use the command:

```
enable switch learning
```

Related Commands

disable switch learning
show switch

enable switch port

Syntax

```
ENAble SWItch POrt={port-list|ALL} [AUTOmdi]

ENAble SWItch POrt={port-list|ALL} [FLOw]
```

where *port-list* is a single port number or a group as either a comma-separated list, a range (specified as *n-m*), or a combination of the two. Port numbers start at 1 and end at m, where m is the highest numbered Ethernet port.

Description

This command enables a switch port or group of ports on the router, or enables auto MDI/MDI-X, or enables the flow control mechanism. Switch ports are enabled by default.

To enable a port that has been disabled by the Port Security function, use the **show switch port** command on page 3-44 rather than this command.

The **port** parameter specifies the port(s) to be enabled or which are to have flow control methods enabled.

The **automdi** parameter enables auto MDI/MDI-X. Auto MDI/MDI-X overrides the setting of the **polarity** parameter for the switch port.

The **flow** parameter specifies that flow control is enabled for the port. The type of flow control is full-duplex flow control or half-duplex backpressure.

Example

To enable ports 2, 4, use the command:

```
enable switch port=2,4
```

Related Commands

disable switch port
set switch port
show switch port

enable vlan debug

Syntax

```
ENAble VLAN={vlan-name|1..4094|ALL} DEBug={PKT|ALL}
   [OUTput=CONSOLE] [TIMEOut={1..4000000000|NONE}]
```

where *vlan-name is* a unique name from 1 to 32 characters. Valid characters are uppercase and lowercase letters, digits (0-9), the underscore character ("_"), and the hyphen (-). The *vlan-name* cannot be a number or ALL.

Description

This command enables debugging options for the specified VLAN or all VLANs. The default is for all VLAN debugging to be disabled. Be aware that enabling debug could flood the receiving Telnet session or asynchronous port with raw data.

The **debug** parameter specifies the debugging mode that is enabled. If PKT is specified, packet debug mode (displaying raw ASCII packets) is enabled. If ALL is specified, all debugging is enabled.

The **output** parameter set to CONSOLE specifies that the debugging information is to be sent to the console. By default the debugging data is sent to the port that received the ENABLE VLAN DEBUG command. Use this option if the command is in a script since a script is not received on a port.

The **timeout** parameter specifies the time in seconds when debugging is to be enabled on the specified VLAN. This reduces the risk of the router and the display being overloaded with too much debugging information. This value overrides previous VLAN debugging timeout values for the VLAN, even if they were specified for other debugging modes. If **timeout** is not specified, the time out is the most recent one used in an ENABLE VLAN DEBUG command or NONE if it had not been previously set.

Example

To enable all debugging on the *default* VLAN, use the command:

```
enable vlan=default debug=all
```

Related Commands

disable vlan debug
show vlan debug

reset switch

Syntax

```
RESET SWItch
```

Description

This command resets the switch module. All dynamic switch information is cleared. All ports are reset. All counters and timers are reset to zero.

Example

To reset the switch module, use the command:

```
reset switch
```

Related Commands

show switch

set switch ageingtimer

Syntax

```
SET SWItch AGEingtimer=16..4080
```

Description This command sets the threshold value, in increments of 16 seconds, of the ageing timer, after which a dynamic entry in the Layer 2 Forwarding Database is automatically removed. The default is 304 seconds (approximately 5 minutes).

Example To set the ageing timer to 80 seconds, use the command:

```
set switch ageingtimer=80
```

Related Commands

disable switch ageing timer
enable switch ageing timer
show switch

set switch port

Syntax

```
SET SWItch POrt={port-list|ALL} [POLarity={MDI|MDIX}]
    [BCLimit={NONE|limit}] [DESCription=description]
    [DLFLimit={NONE|limit}] [INFILTering=OFF|ON]
    [MCLimit={NONE|limit}] [SPeed={AUTOnegotiate|10MHALf|
    10MFUll|10MHAUto|10MFAuto|100MHALf|100MFUll|100MHAuto|
    100MFAuto}]
```

where:

- *port-list* is a port number, range (specified as *n-m*), or comma-separated list of numbers and/or ranges. Port numbers start at 1 and end at *m*, where *m* is the highest numbered switch port.
- *limit* is a decimal number, from 0 to the maximum value of the limit variable based on the particular switch hardware.
- *description* is a string 1 to 47 characters long. Valid characters are any printable characters.

Description

This command modifies the value of parameters for switch ports.

The **port** parameter specifies the ports for which parameters are modified. If the command would succeed on a subset of the ports specified, but cause an error on the others, then the command as a whole fails and has no effect.

While you may specify **set switch port** commands using groups of ports, the **create config** command on page 1-70 of Chapter 1, Operation generates a separate **set switch port** command for each port.

The **polarity** parameter specifies MDI mode (the transmit and receive pairs are not crossed), or MDI-X mode (the transmit and receive pairs are crossed) for the port. For the **polarity** parameter to take effect, auto MDI/MDI-X mode must be disabled using the **disable switch port** command on page 3-28. If auto MDI/MDI-X mode has not been disabled, the port remains in auto MDI/MDI-X mode and this polarity setting is remembered. When the auto MDI/MDI-X mode is disabled, the polarity setting for the port takes effect.

The **bclimit** parameter specifies a limit on the rate of reception of broadcast packets for the port(s). The value of this parameter represents a per second rate of packet reception, above which broadcast packets are discarded. If the value NONE or 0 is specified, then packet rate limiting for broadcast packets is turned off. If any other value is specified, the reception of broadcast packets is limited to that number of kilobits per second (Kbps). Whenever packet rate limits are set, the latest parameter values supersede earlier values. The default is NONE.

The three sets of options used for packet storm protection are: broadcast limit (**bclimit**) only; broadcast limit and multicast limit (**bclimit** and **mclimit**); broadcast limit, multicast limit, and destination lookup failure limit (**bclimit**, **mclimit**, and **dlflimit**). The limit specified for each option, i.e the number of kilobits per second (Kbps), must be the same for all modes of storm protection selected. The limit is set to the most recent limit specified.

The **description** parameter can be used to describe the port. It is displayed by the **show switch port** command, but does not affect the operation of the router in any way. The default is no description.

The **dlflimit** parameter specifies a limit on the rate of reception of destination lookup failure packets for the port. The value of this parameter represents a per second rate of packet reception, above which destination lookup failure packets are discarded. If the value NONE or 0 is specified, then packet rate limiting for destination lookup failure packets is turned off. If any other value is specified, the reception of destination lookup failure packets is limited to that number of kilobits per second (Kbps). Whenever packet rate limits are set, the latest parameter values supersede earlier values. The default is NONE.

The **infiltering** parameter enables or disables Ingress Filtering of packets admitted according to the IEEE 802.1Q Mode set on the specified ports. Each switch port belongs to one or more VLANs. If **infiltering** is set to ON, Ingress Filtering is enabled and packets received on a specified port are admitted if the port belongs to the VLAN with which the packets are associated. Conversely, packets received on the port are discarded if the port does not belong to the VLAN with which the packets are associated. Untagged packets are admitted when the port is not a tagged-only port, since the packets have the numerical VLAN Identifier (VID) of the VLAN that the port is an untagged member of. If **off** is specified, Ingress Filtering is disabled, and no packet are discarded by this part of the Ingress Rules. The default is **off**.

The **mclimit** parameter specifies a limit on the rate of reception of multicast packets for the port. The value of this parameter represents a per second rate of packet reception above which multicast packets are discarded. If the value NONE or 0 is specified, then packet rate limiting for multicast packets is turned off. If any other value is specified, the reception of multicast packets is limited to that number of kilobits per second (Kbps). Whenever packet rate limits are set, the latest parameter values supersede earlier values. The default is NONE.

The **speed** parameter specifies the configured line speed and duplex mode of the port(s) (see Table 3-10 on page 3-35). If **autonegotiate** is specified, the port(s) autonegotiate the highest mutually possible line speed and duplex mode with the link partner. If one of **10mfauto**, **10mhauto**, **100mfauto**, or **100mhauto** is specified, the port autonegotiates with the link partner but only accepts operation at the specified speed and duplex mode. If one of **10mhalf**, **10mfull**, **100mhalf**, or **100mfull** is specified, then autonegotiation is disabled and the interface is forced to operate at the specified speed and duplex mode, regardless of whether the link partner is capable of working at that speed. The default is **autonegotiate**.

Table 3-10: Switch port speed values

Value	Meaning
10MHALF	10 Mbps, half duplex, fixed, auto MDI/MDI-X
10MFULL	10 Mbps, full duplex, fixed, auto MDI/MDI-X
10MHAUTO	10 Mbps, half duplex, autonegotiate, auto MDI/MDI-X
10MFAUTO	10 Mbps, full duplex, autonegotiate, auto MDI/MDI-X
100MHALF	100 Mbps, half duplex, fixed, auto MDI/MDI-X
100MFULL	100 Mbps, full duplex, fixed, auto MDI/MDI-X
100MHAUTO	100 Mbps, half duplex, autonegotiate, auto MDI/MDI-X
100MFAUTO	100 Mbps, full duplex, autonegotiate, auto MDI/MDI-X

Example To set the speed of port 2 to 10Mbps, half duplex, use the command:

```
set switch port=2 speed=10mhalf
```

Related Commands

disable switch port
enable switch port
show switch port

set switch qos

Syntax

```
SET SWItch QOS=P0,P1,P2,P3,P4,P5,P6,P7
```

where *P0-P7* are each numbers from 0-n, where n+1 is the number of Quality of Service egress queues supported

Description

This command maps user priority levels to Quality of Service egress queues.

The **qos** parameter specifies a comma-separated list of eight values, all of which must be present. The first value, P0, represents the QOS queue for priority level 0. The last value, P7, represents the QOS queue for priority level 7. Similarly, values P1 to P6 represent the QOS queue for the corresponding priority level.

The router has four QOS egress queues. The default QOS values are 1,0,0,1,2,2,3,3 as shown in Table 3-11 on page 3-37.

Packets that originate on the router, or are routed by the router's software, have been assigned a Quality of Service priority of 7. To ensure that these packets are transmitted promptly, do not assign priority 7 to a low-numbered egress queue.

Table 3-11: Default priority level to queue mapping for four QOS egress queues

Priority level	Queue
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

Example

To set the mapping shown in Table 3-12 on page 3-37, use the command:

```
set switch qos=0,0,0,1,1,2,2,3
```

Table 3-12: Example priority level to QOS egress queue mapping

Priority level	Queue
0	0
1	0
2	0
3	1
4	1
5	2
6	2
7	3

Related Commands show switch qos

set vlan port

Syntax

```
SET VLAN={vlan-name|1..4094} POrt={port-list|ALL}
    FRAme={UNTAGged|TAGged}
```

where:

- *vlan-name is* a unique name from 1 to 32 characters. Valid characters are uppercase and lowercase letters, digits (0-9), the underscore character ("_"), and the hyphen (-). The *vlan-name* cannot be a number or ALL.
- *port-list* is a port number, range (specified as *n-m),* or comma-separated list of numbers and/or ranges. Port numbers start at 1 and end at *m*, where *m* is the highest numbered Ethernet port.

Description This command changes the status of ports in a VLAN from tagged to untagged or vice-versa.

The **vlan** parameter specifies the name of the VLAN or the numerical VLAN Identifier of the VLAN. The name is not case sensitive although the case is preserved for display purposes. The VLAN specified must exist.

The **port** parameter specifies the port(s) to be changed. The ports must belong to the specified VLAN. If the command would succeed on a subset of the ports specified, but cause an error on the others, then the command as a whole fails and has no effect. If ALL is specified, then all ports in the VLAN change.

The **frame** parameter specifies whether packets transmitted from a port for the specified VLAN include a VLAN tag header. If **frame** is set to UNTAGGED, the port becomes an untagged port for the specified VLAN. **frame** must be set to UNTAGGED if the port was previously tagged in the same VLAN, and is not an UNTAGGED port of another VLAN. If **frame** is set to TAGGED, then the port becomes a tagged port for the specified VLAN. **frame** may be set to TAGGED only if the ports were previously untagged ports in the same VLAN.

Example To change the status of port 1 of the default VLAN from untagged to tagged, use the command:

```
set vlan=default port=1 frame=tagged
```

Related Commands add vlan port
delete vlan port
show vlan

show switch

Syntax `SHow SWItch`

Description This command displays configuration information for the switch functions (Figure 3-7 on page 3-39, Table 3-13 on page 3-39).

Figure 3-7: Example output from the **show switch** command

```
Switch Configuration
-----------------------------------------------------------
Switch Address ............. 00-00-cd-00-7a-47
Number of Fixed Ports ...... 5
Learning .................. ON
Ageing Timer ............... ON
Ageing Time ................ 304
UpTime ..................... 00:10:32
------------------------------------------------------------
```

Table 3-13: Parameters in the output of the **show switch** command

Parameter	Meaning
Switch Address	MAC address of the router.
Number Of Fixed Ports	Number of fixed Ethernet switch ports.
Learning	Whether the router’s dynamic learning and updating of the Forwarding Database is enabled.
Ageing Timer	Whether the ageing timer is enabled. The time that a MAC address entry remains in the address lookup cannot be altered.
Ageing Time	Value in seconds of the ageing timer after which a dynamic entry is removed from the Forwarding Database.
UpTime	Time in hours:minutes:seconds since the router was last powered up, rebooted, or restarted. Uptime is the same as the value of the MIB object sysUpTime.

Example To display the configuration of the switch module, use the command:

```
show switch
```

Related Commands reset switch

show switch debug

Syntax `SHow SWItch DEBug`

Description This command displays debugging information for switching (Figure 3-8 on page 3-40, Table 3-14 on page 3-40).

Figure 3-8: Example output from the **show switch debug** command

```
Enabled Switch Debug Modes    Output     Timeout
----------------------------------------------------------
DMA                           16         12345
----------------------------------------------------------
```

Table 3-14: Parameters in the output of the **show switch debug** command

Parameter	Meaning
Enabled Switch Debug Modes	Whether the debugging option for the router is ARL, DMA, M6, PHY, or None.
Output	Output device for the router; shown when a debug mode is enabled.
Timeout	Time in seconds that the debugging options for the router are enabled; shown when a debug mode is enabled.

Example To display debugging information, use the command:

```
show switch debug
```

Related Commands **disable switch debug**
enable switch debug

show switch counter

Syntax `SHow SWItch COUnter`

Description This command displays counters associated with the router (Figure 3-9 on page 3-41, Table 3-15 on page 3-41).

Figure 3-9: Example output from the **show switch counter** command

```
Switch Counters
----------------------------------------------------------
Switch instance:        0

Packet DMA counters:
 Receive:                        Transmit:
  Octets                  486     Octets                 482
  Packets                   6     Packets                  6
  Discards                  0     Discards                 0
  TooFewBuffers             0     Aborts                   0
  NonOctetAlignedFrames     0     DescriptorAreaFilleds    0
  FIFOOverruns              0     FIFOUnderruns            0
  FrameTooLongs             0     QueueLength              0
  FrameTooShorts            0
  CRCErrors                 0
  QueueLength               0

General counters:
  Resets                    1
-----------------------------------------------------------
```

Table 3-15: Parameters in the output of the **show switch counter** command

Parameters	Meaning
Packet Dma counters	
Receive	Counters for packets received.
Octets	Number of octets received by the CPU from the switch chip.
Packets	Number of packets received by the CPU from the switch chip.
Discards	Number of packets received from the switch chip that were discarded because either the receive queue was too long, or because the free buffers in the router were below BufferLevel3, or because there were no data bytes in the packet.
TooFewBuffers	Number of packets received from the switch chip that were discarded because the free buffers in the router were below BufferLevel3.
NonOctetAlignedFrames	Number of received frames with alignment and CRC errors.
FIFOOverruns	Number of times reception of a packet failed because of a FIFO overrun.
FrameTooLongs	Number of received packets that exceeded the maximum permitted frame size.
FrameTooShorts	Number of received packets that their lengths were less than the minimum permitted frame size.
CRCErrors	Number of received frames with CRC but not alignment errors.

Table 3-15: Parameters in the output of the **show switch counter** command

Parameters	**Meaning**
QueueLength	Number of packets received from the switch chip waiting to be processed by the CPU.
Transmit	Counters for packets transmitted.
Octets	Number of octets transferred from the CPU to the switch chip, including framing.
Packets	Number of packets transferred from the CPU to the switch chip.
Discards	Number of packets waiting for transmission that were discarded when the DMA process was reset due to an error.
Aborts	Number of times the transmission of a packet was aborted due to it taking excessive time for the transmission to complete.
DescriptorAreaFilleds	Number of times the transmit descriptors are filled due to a high rate of transfer of packets from the CPU to the switch chip.
FIFOUnderruns	Number of times transmission of a packet failed because of a FIFO underrun.
QueueLength	Number of packets currently queued for transmission, or that have been transmitted and are waiting to be purged from the transmit queue.
General Counters	
Resets	Number of times the switch chip has been reset due to a router configuration change.

Example To display the switching counters, use the command:

```
show switch counter
```

Related Commands reset switch
show switch

show switch fdb

Syntax SHow SWItch FDB [ADDRESS=*macadd*] [POrt={*port-list*|ALL}] [STAtus={STAtic|DYnamic}]

where:

- *macadd* is an Ethernet six-octet MAC address, expressed as six pairs of hexadecimal digits delimited by hyphens.
- *port-list* is a port number, range (specified as *n-m*), or comma-separated list of numbers and/or ranges. Port numbers start at 1 and end at *m*, where *m* is the highest numbered Ethernet port.

Description This command displays the contents of the Forwarding Database (Figure 3-10 on page 3-43, Table 3-16 on page 3-43).

- The **address** parameter specifies the MAC address of the device that the Forwarding Database is to display.
- The **port** parameter specifies entries to be displayed in the Forwarding Database that were learned from the specified port.
- The **status** parameter specifies whether to display static filter entries or dynamically learned filter entries.

Figure 3-10: Example output from the **show switch fdb** command

```
Switch Forwarding Database
---------------------------------------------------
MAC Address                Port           Status
---------------------------------------------------
00-00-c0-1d-2c-f8          1              dynamic
00-00-c0-71-e0-e4          1              dynamic
00-00-cd-00-45-c7          CPU            static
00-00-cd-00-a4-d6          1              dynamic
00-00-cd-00-ab-dc          1              dynamic
00-60-b0-ac-18-51          1              dynamic
00-90-27-23-a4-e9          1              dynamic
00-90-27-32-ad-61          1              dynamic
00-90-27-76-8a-55          1              dynamic
00-90-27-76-9a-99          1              dynamic
00-90-27-87-a5-22          1              dynamic
00-90-27-bd-c8-93          1              dynamic
00-90-27-bd-c9-7f          1              dynamic
00-90-27-d0-ae-c2          1              dynamic
---------------------------------------------------
```

Table 3-16: Parameters in the output of the **show switch fdb** command

Parameter	Meaning
Mac Address	MAC address as learned from the source address field of a frame, or entered as part of a static filter entry.
Port	Port where the MAC address was learned.
Status	Whether the entry was a static filter entry or dynamically learned.

Example To display the contents of the Forwarding Database, use the command:

```
show switch fdb
```

Related Commands show switch

show switch port

Syntax `SHow SWItch POrt[={port-list|ALL}]`

where *port-list* is a port number, range (specified as *n-m*), or comma-separated list of numbers and/or ranges. Port numbers start at 1 and end at *m*, where *m* is the highest numbered Ethernet port.

Description This command displays general information about the specified switch ports or all switch ports (Figure 3-11 on page 3-44, Table 3-17 on page 3-45).

Figure 3-11: Example output from the **show switch port** command

```
Switch Port Information
-----------------------------------------------------------
 Port ............................ 1
   Description ................... To intranet hub, port 4
   Status ........................ ENABLED
   Link State .................... Up
   UpTime ........................ 00:10:49
   Configured speed/duplex ....... Autonegotiate
   Actual speed/duplex ........... 100 Mbps, full duplex
   Automatic MDI/MDI-X ........... Enabled
   Configured MDI/MDI-X........... MDI-X
   Actual MDI/MDI-X............... MDI
   Broadcast rate limit .......... 128Kbps
   Multicast rate limit .......... -
   DLF rate limit ................ -
   Flow control(s) ............... Disabled
   Send tagged pkts for VLAN(s) .. vlan2 (2)
                                   vlan3 (3)
   Port-based VLAN ............... accounting (4)
   Ingress Filtering ............. OFF
----------------------------------------------------------
```

Table 3-17: Parameters in the output of the **show switch port** command

Parameter	Meaning
Port	Number of the switch port.
Description	Description of the port.
Status	Whether the port is enabled.
Link State	Whether the link of the port is up.
UpTime	Count in hours:minutes:seconds of the elapsed time since the port was last reset or initialised.
Configured speed/duplex	Port speed mode configured for this port. One of "Autonegotiate" or a combination of a speed (one of "10 Mbps" or "100 Mbps") and a duplex mode (one of "half duplex" or "full duplex") and optionally "(by autonegotiation)".
Actual speed/duplex	Port speed and duplex mode at which this port is running. A combination of a speed (one of "10 Mbps" or "100 Mbps") and a duplex mode (one of "half duplex" or "full duplex").
Automatic MDI/MDI-X	Whether the automatic MDI/MDI-X command is enabled.
Configured MDI/MDI-X	Whether the configured polarity of the port is MDI or MDI-X.
Actual MDI/MDI-X	Whether the actual polarity of the port is MDI or MDI-X.
Broadcast rate limit	Limit in Kbps of the rate of reception of broadcast frames for this port.
Multicast rate limit	Limit in Kbps of the rate of reception of multicast frames for this port.
DLF rate limit	Limit in Kbps of the rate of reception of DLF (destination lookup failure) frames for this port.
Flow control(s)	Whether flow control parameters are set for the port. If implemented, then flow control is applied to the port.
Send tagged pkts for VLAN(s)	Name and VLAN Identifier (VID) of tagged VLANs to which the port belongs.
Port-based VLAN	Name and VLAN Identifier (VID) of the port-based VLAN to which the port belongs.
Ingress Filtering	Whether ingress filtering is on.

Example To display the configuration for switch port 1, use the command:

```
show switch port=1
```

Related Commands set switch port

show switch port counter

Syntax SHow SWItch POrt[={*port-list*|ALL}] COUnter

where *port-list* is a port number, range (specified as *n-m*), or comma-separated list of numbers and/or ranges. Port numbers start at 1 and end at *m*, where *m* is the highest numbered Ethernet port.

Description This command displays counters for the specified switch ports or all switch ports (Figure 3-12 on page 3-46, Table 3-18 on page 3-46).

Figure 3-12: Example output from the **show switch port counter** command

```
Port 1. Statistics counters:

Receive/Transmit Packet by size (octets) counters:
   Receive                  Transmit
    64                 2    64                      0
    65 - 127           0    65 - 127                0
    128 - 255          0    128 - 255               0
    256 - 511          0    256 - 511               0
    512 - 1023         0    512 - 1023              0
    1024 - 1522        0    1024 - 1522             0

General Counters:
   Receive                  Transmit
   Octets            128    Octets                  0
   Pkts                2    Pkts                    0
   UnicastPkts         0    UnicastPkts             0
   BroadcastPkts       0    BroadcastPkts           0
   PauseFramess        0    PauseFrames             0
   MulticastPkts       0    MulticastPkts           0
   Discards            0    Discards                0
   AlignmentErrors     0
   BadOctets           0
   UndersizePkts       0
   Fragments           0
   Jabber              0
   OversizePkts        0
   Filtered            0
                            CollisionFrames         0
                            LateCollisions          0
                            ExcessiveCollisions     0
                            MultCollsnFrames        0
                            SingleCollisionFrames   0
                            Deferred                0
```

Table 3-18: Parameters in output from **show switch port counter** command

Parameter	Description
Receive	Counters for traffic received.
64	Total frames received with a length of exactly 64 octets, including those with errors.
65 – 127	Total frames received with a length of between 65 and 127 octets inclusive, including those with errors.
128 – 255	Total frames received with a length of between 128 and 255 octets inclusive, including those with errors.

Table 3-18: Parameters in output from **show switch port counter** command

Parameter	Description
256 – 511	Total frames received with a length of between 256 and 511 octets inclusive, including those with errors.
512 – 1023	Total frames received with a length of between 512 and 1023 octets inclusive, including those with errors.
1024 - 1522	Total frames received with a length of between 1024 and 1522 octets inclusive, including those with errors. The maximum packet size is 1518 for non-tagged frames, 1522 for tagged frames.
Octets	Total data octets received in frames with a valid FCS. Undersize and Oversize frames are included. The count includes the FCS but not the preamble.
Pkts	The number of packets.
UnicastPkts	Total valid frames received with a unicast Destination Address.
BroadcastPkts	Total valid frames received with a Destination Address equal to FF:FF:FF:FF:FF:FF.
PauseFrames	Total valid pause frames received.
Multicastpkts	Total valid frames received with a multicast Destination Address that are not counted in BroadcastPkts or PauseFrms.
Discards	Total valid frames received that are discarded due to a lack of buffer space. This includes frames discarded at ingress as well as those dropped due to priority and congestion considerations at the output queues. Frames dropped at egress due to excessive collisions are not included but are counted in the Excessive counter.
AlignmentErrors	Total frames received with a valid length (between 64 octets and MaxPktSz octets inclusive) that have an invalid FCS and a non-integral number of octets.
BadOctets	Total data octets received in frames with an invalid FCS. Fragments and Jabbers are included. The count includes the FCS but not the preamble.
UndersizePkts	Total frames received with a length of less than 64 octets but with a valid FCS.
Fragments	Total frames received with a length of less than 64 octets and an invalid FCS.
Jabber	Total frames received with a length of more than MaxPktSz octets but with an invalid FCS.
OversizePkts	Total frames received with a length of more than MaxPktSz octets but with a valid FCS.
Filtered	I*f Ingress Filtering is disabled on this port:* Total valid frames received that are not forwarded to a destination port. These are frames for which the destination port vector is 0 or are not forwarded due to the state of the PortState bits. Valid frames discarded due to a lack of buffer space are not included. *If Ingress Filtering is enabled on this port:* Total valid frames received (tagged or untagged) that were discarded due to an unknown VID (i.e., the frame’s VID was not in the VTU).
Transmit	Counters for traffic transmitted.
64	Total frames transmitted with a length of exactly 64 octets, including those with errors.

Table 3-18: Parameters in output from **show switch port counter** command

Parameter	Description
65 - 127	Total frames transmitted with a length of between 65 and 127 octets inclusive, including those with errors.
128 - 255	Total frames transmitted with a length of between 128 and 255 octets inclusive, including those with errors.
256 - 511	Total frames transmitted with a length of between 256 and 511 octets inclusive, including those with errors.
512 - 1023	Total frames transmitted with a length of between 512 and 1023 octets inclusive, including those with errors.
1024 - 1522	Total frames transmitted with a length of between 1024 and 1522 octets inclusive, including those with errors. The maximum packet size is 1518 for non-tagged frames, 1522 for tagged frames.
Octets	Total data octets transmitted from frames counted in Group 5 above. The count includes the FCS but not the preamble.
Pkts	The number of packets.
UnicastPkts	Total frames transmitted with a unicast Destination Address.
BroadcastPkts	Total frames transmitted with a Destination Address equal to FF-FF-FF-FF-FF-FF.
PauseFrames	Total pause frames transmitted.
MulticastPkts	Total frames transmitted with a multicast Destination Address that are not counted in OutBroadcasts or OutPause.
Discards	Total valid frames discarded that were not transmitted due to a lack of buffer space. Always 0 in this device since all discards occur at Ingress and are counted in InDiscards.
CollisionFrames	Total number of collisions during frame transmission.
LateCollisions	Total number of times a collision is detected later than 512 bit-times into the transmission of a frame.
ExcessiveCollisions	Total number of frames not transmitted because the frame experienced 16 transmission attempts and it was discarded. The discard occurs when DiscardExcessive is set to a 1 (in Global Control).
MultCollsnFrames	Total number of successfully transmitted frames that experienced more than one collision.
SingleCollisionFrames	Total number of successfully transmitted frames that experienced exactly one collision.
Deferred	Total number of successfully transmitted frames that are delayed because the medium is busy during the first attempt.

Example To display counters for switch port 1, use the command:

```
show switch port=1 counter
```

Related Commands

set switch port
show switch counter
show switch port

show switch qos

Syntax

`SHow SWItch QOS`

Description

This command displays the current mapping of user priority level to QOS egress queue for the switch ports (Figure 3-13 on page 3-49, Table 3-19 on page 3-49).

Packets that originate on the router, or are routed by the router's software, have been assigned a Quality of Service priority of 7. To ensure that these packets are transmitted promptly do not assign priority 7 to a low-numbered egress queue.

Figure 3-13: Example output from the SHOW SWITCH QOS command

```
Priority Level       QOS egress queue
-------------------------------------
0 .................. 1
1 .................. 0
2 .................. 0
3 .................. 1
4 .................. 2
5 .................. 2
6 .................. 3
7 .................. 3
```

Table 3-19: Parameters in the output of the **show switch qos** command

Parameter	Meaning
Priority Level	Priority level of the received frame.
Qos egress queue	Quality Of Service egress queue that frames with this priority level join.

Example

To display the current configuration of the priority level to QOS egress queue mappings, use the command:

```
show switch qos
```

Related Commands

set switch qos

show vlan

Syntax `SHow VLAN[={vlan-name|1..4094|ALL}]`

where *vlan-name is* a unique name from 1 to 32 characters. Valid characters are uppercase and lowercase letters, digits (0-9), the underscore character (“_”), and the hyphen (-). The *vlan-name* cannot be a number or ALL.

Description This command displays information about the specified VLAN. If no VLAN or ALL is specified, then all VLANs are displayed (Figure 3-14 on page 3-50, Table 3-20 on page 3-50).

Figure 3-14: Example output from the **show vlan** command

```
VLAN Information
---------------------------------------------------------------------------
 Name ............... default
 Identifier ......... 1
 Status ............. static
 Untagged ports ..... 1-2,4-5
 Tagged ports ....... None
 Attachments:
 Module           Protocol         Format    Discrim     MAC address
 -------------------------------------------------------------------
 IP               IP               Ethernet  0800           -
 IP               ARP              Ethernet  0806           -
 -------------------------------------------------------------------

 Name ............... vlan2
 Identifier ......... 2
 Status ............. static
 Untagged ports ..... 3
 Tagged ports ....... None
 Attachments:
 Module           Protocol         Format    Discrim     MAC address
 -------------------------------------------------------------------
   -                -                -         -            -
 -------------------------------------------------------------------
```

Table 3-20: Parameters in the output of the **show vlan** command

Parameter	Meaning
Name	Name of the VLAN.
Identifier	Numerical VLAN identifier (VID) of the VLAN.
Status	Whether the VLAN is dynamic or static.
Untagged ports	List of untagged ports that belong to the VLAN.
Tagged ports	List of tagged ports that belong to the VLAN.
Attachments – information about attachments to the VLAN made by other modules in the router	
Module	Name of the software module attached to the VLAN.
Protocol	Name of the protocol, which is determined from the format and identification number.
Format	Encapsulation format specified by the module.

Table 3-20: Parameters in the output of the **show vlan** command (continued)

Parameter	Meaning
Discrim	Discriminator specified by the module to identify which packets of the given format should be received.
MAC address	Media Access Control source address for which the module wants to receive packets. This is commonly known as the Ethernet address.

Examples To display information on the default VLAN, use the command:

```
show vlan=default
```

Related Commands **create vlan**
destroy vlan

show vlan debug

Syntax `SHow VLAN DEBug`

Description This command displays debug information for all VLANs (Figure 3-15 on page 3-52, Table 3-21 on page 3-52).

Figure 3-15: Example output from the **show vlan debug** command

```
Vlan      Enabled Debug Modes       Output     Timeout
-------------------------------------------------------------
Vlan1     PKT                       16         NONE
-------------------------------------------------------------

Vlan      Enabled Debug Modes       Output     Timeout
-------------------------------------------------------------
Vlan4094  None
-------------------------------------------------------------
```

Table 3-21: Parameters in the output of the **show vlan debug** command

Parameter	Meaning
Vlan	String comprising the constant “Vlan” and the VLAN Identifier of the VLAN.
Enabled Debug Modes	Whether the debugging option for the VLAN is PKT or None.
Output	Output device for the VLAN; shown when a debug mode is enabled.
Timeout	Time in seconds that the debugging options for the VLAN are enabled; shown when a debug mode is enabled. If a timeout value is not set, “None” is shown.

Examples To display debugging information for all VLANs, use the command:

```
show vlan debug
```

Related Commands **disable vlan debug**
enable vlan debug