

Chapter 39

Generic Packet Classifier

| | |
|------------------------------------|-------|
| Introduction..... | 39-2 |
| Configuration of Classifiers | 39-2 |
| Command Reference | 39-3 |
| create classifier | 39-4 |
| destroy classifier | 39-17 |
| set classifier | 39-18 |
| show classifier | 39-28 |

Introduction

The classifier enables you to create packet matching rules—called *classifiers*—to sort packets into *data flows*. For example, you may want all packets with the same destination TCP/IP port to form a flow (e.g. all telnet or HTTP traffic). This chapter describes how to configure the classifier.

You can then configure the switch to process all packets in a data flow in a given manner. You have two choices for acting on classified flows:

- Quality of Service (QoS).

QoS prioritises packets and manages bandwidth. QoS is particularly useful for improving VoIP and video links, especially if your network is congested. Theory and configuration of QoS is described in [Chapter 41, Software Quality of Service \(QoS\)](#) and, for Rapier i Series switches, [Chapter 40, Quality of Service \(QoS\) on Switch Ports](#).

- Packet filters.

Filters forward or discard packets. They can also modify the packet's priority settings, send the packet to a mirror port, and do other advanced actions. Classifier-based filters are described in "[Classifier-Based Packet Filters](#)" on page 8-34 of [Chapter 8, Switching](#).

Configuration of Classifiers

Configuring the classifier involves creating a set of packet matching rules, called *classifiers*, using the command:

```
create classifier=1..9999 [options]
```

These classifiers can identify any single packet based upon many criteria. Available criteria depend on the type of interface you use the classifier on, and include:

- Physical (layer 1) and layer 2 port or interface

You can classify packets according to their ingress or egress port or ingress interface, and VLAN settings.

- Ethernet encapsulation type

You can classify packets depending on the specific protocol type of each frame. Different values indicate how the packet is formatted. For example, a value of 802.2 indicates the packet is formatted according to IEEE standards 802.2 and 802.3 with a Destination Service Access Point/Source Service Access Point (DSAP/SSAP) value not equal to AAAA in hexadecimal; SAP encapsulation. A value of ETHII indicates the packet is formatted according to RFC 894; Ethernet II encapsulation. For more details on values see the ETHFORMAT parameter in the [create classifier command on page 39-4](#).

- Source/Destination MAC address

You can classify frames from a specific source or destination MAC address. This classification can be used for users on remote networks. You can also specify MAC type to distinguish unicast packets from broadcast or multicast packets.

- Frame relay and PPP settings

You can classify according to DLCI, PPP index number or PPP protocol ID.

- Layer 3 protocols

You can classify frames based on any value for Layer 3 protocols. Layer 3 protocol and Ethernet encapsulation types are interrelated, e.g. IPX Ethernet II encapsulated packets are different to IPX NETWORKERAW encapsulated packets.

- DiffServ or IP TOS

You can classify packets according to the value of the DSCP bits in the DiffServ field of the header, or the TOS precedence bits in the Type of Service (TOS). These fields are alternatives, so are mutually exclusive.

- Source/destination IP or IPv6 address and other IP settings

You can classify packets based on an exact match of the source or destination IP address information within the IP or IPv6 header, and based on the presence of several other header fields.

- IPX settings

You can classify packets based on their destination IPX address, packet type and source or destination socket.

- Layer 4 protocol (TCP/UDP, ICMP etc.)

You can classify packets based on specific Layer 4 TCP or UDP destination and source port numbers contained within the IP or IPv6 header.

- Layer 4 source/destination port and other layer 4 settings

You can classify packets based on a specific port number or a range of port numbers, and based on TCP flags, ICMP code and ICMP type.

- Up to three 16-bit words inside the first 64 bytes of a packet

You can specify the bits to match, using the **match** parameter, and their position, using the **mask** and **offset** parameters.

Command Reference

This section describes the commands available to configure and manage the classifiers.

See [“Conventions” on page lxvi of About this Software Reference](#) 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.

create classifier

Classifier parameters are sorted approximately in order of the OSI model, with layer 1 (physical) parameters first.

Syntax:
hardware filters and
QoS on switch ports

For classifiers to use with QoS on switch ports (on Rapier i Series switches only) and hardware filters on switch ports:

```
CREate CLASSifier=1..9999 [EPort=port] [IPort=port]
[VLAN={vlan-name|1..4094|ANY}]
[ETHFormat={802.2|802.2-Tagged|802.2-Untagged|Ethii|
ETHII-Tagged|ETHII-Untagged|Netwareraw|
NETWARERAW-Tagged|NETWARERAW-Untagged|Snap|SNAP-Tagged|
SNAP-Untagged|ANY}]
[MACDaddr={macadd|ANY}] [MACSaddr={macadd|ANY}]
[PROTocol={protocol-type|IP|IPX|NONIpipx|ANY}]
[IPDAddr={ipadd[/0..32]|ANY}] [IPSAddr={ipadd[/
0..32]|ANY}]
[IPDScp={dscp-list|ANY}] [IPTOs={0..7|ANY}]
[IPPRotocol={TCP|UDP|ICMp|IGMp|NONTcpudp|
ip-protocol-num|ANY}]
[IPXDAddr={ipx-add|ANY}]
[IPXPacket={NLSp|RIP|SAP|SPX|NCP|NETbios|
ipx-packet-num|ANY}]
[TCPFlags={{Urg|Ack|Rst|Syn|Fin}|[,...]|ANY}]
[TCPPort={port-id|ANY}] [TCPSport={port-id|ANY}]
[UDPPort={port-id|ANY}] [UDPSport={port-id|ANY}]
[IPXDSocket={NCP|SAP|RIP|NNB|DIAG|NLSp|IPXwan|
ipx-socket-num|ANY}]
[IPXSsocket={NCP|SAP|RIP|NNB|DIAG|NLSp|IPXwan|
ipx-socket-num|ANY}] [MATCH1=hh MASK1=hh OFFSET1=0..62]
[MATCH2=hh MASK2=hh OFFSET2=0..62]
[MATCH3=hh MASK3=hh OFFSET3=0..62]
```

Syntax:
software QoS on
ingress

For classifiers to use with software QoS on ingress traffic over ETH ports, frame relay interfaces, and PPP interfaces:

```
CREate CLASSifier=1..9999
[IPDScp={dscp-list|ANY}] [IPTOs={0..7|ANY}]
[VLANPriority={priority-list|ANY}]
```

Syntax:
software QoS on egress

For classifiers to use with software QoS on egress traffic over ETH ports, frame relay interfaces, and PPP interfaces:

```
CREate CLASSifier=1..9999 [IINTERface={interface|NONE}]
[EPort={port|ANY}] [IPort={port|ANY}]
[SVlan={vlan-name|1..4094|ANY}]
[DVlan={vlan-name|1..4094|ANY}]
[VLANPriority={priority-list|ANY}]
[ETHFormat={802.2|802.2-Tagged|802.2-Untagged|Ethii|
ETHII-Tagged|ETHII-Untagged|Netwareraw|
NETWARERAW-Tagged|NETWARERAW-Untagged|Snap|SNAP-Tagged|
SNAP-Untagged|ANY}]
[MACDaddr={macadd|ANY}] [MACSaddr={macadd|ANY}]
[MACType={L2Ucast|L2BMcast|ANY}]
[DLCi={dlci-range|ANY}] [PPPIndex=0..1023]
[PPPProtocolid={ppp-protocol-id|IP|IPv6|ANY}]
```

```

[PROTOCOL={protocol-type|ARP|IP|IPV6|IPX|ANY}]
[IPDAddr={ipadd[/0..32]|ipv6add[/0..128]|ANY}]
[IPSAddr={ipadd[/0..32]|ipv6add[/0..128]|ANY}]
[IPDScp={dscp-list|ANY}] [IPTOS={0..7|ANY}]
[IPFRAG={YES|NO|ANY}] [IPOptions={YES|NO|ANY}]
[IPFLowlabel={0..1048575|ANY}]
[IPPRotocol={TCP|UDP|ICMp|IGMp|OSPF|NONTcpudp|ANY|
ip-protocol}]
[ICMptype={Any|ECHORply|Unreachable|Quench|Redirect|
ECHO|ADvertisement|Solicitation|TImeexceed|Parameter|
TSTAMP|TSTAMPRply|INFOREQ|INFOREP|ADDRREQ|ADDRREP|
NAMEREQ|NAMERply|icmp-type}]
[ICMPCode={Any|Filter|FRAGMent|FRAGReasm|HOSTComm|
HOSTIsolated|HOSTPrec|HOSTREdirect|HOSTRTos|HOSTTos|
HOSTUNKnown|HOSTUNReach|NETComm|NETREdirect|NETRTos|
NETTos|NETUNKnown|NETUNReach|NOptr|PORTunreach|
PREcedent|PROtunreach|PTRproblem|Sourceroute|Ttl|
icmp-code}]
[TCPFlags={{Urg|Ack|Rst|Syn|Fin}[,...]|ANY}]
[TCPDport={port-range|ANY}] [TCPSport={port-range|ANY}]
[UDPDport={port-range|ANY}] [UDPSport={port-range|ANY}]

```

Syntax: For classifiers to use with software QoS on GRE, IPsec and 6-to-4 tunnels:

software QoS on tunnels

```

CREate CLASSifier=1..9999 [IINTERface={interface|NONE}]
[IPDAddr={ipadd[/0..32]|ipv6add[/0..128]|ANY}]
[IPSAddr={ipadd[/0..32]|ipv6add[/0..128]|ANY}]
[IPDScp={dscp-list|ANY}] [IPTOs={0..7|ANY}]
[IPFRAG={YES|NO|ANY}] [IPOptions={YES|NO|ANY}]
[IPFLowlabel={flow-label-range|ANY}]
[IPPRotocol={TCP|UDP|ICMp|IGMp|OSPf|NONTcpudp|ANY|
ip-protocol}]
[ICmptype={Any|ECHORply|Unreachable|Quench|Redirect|
ECHO|ADvertisement|Solicitation|TImeexceed|Parameter|
TSTAMP|TSTAMPRply|INFOREQ|INFOREP|ADDRREQ|ADDRREP|
NAMEREq|NAMERply|icmp-type}]
[ICMPCode={Any|Filter|FRAGment|FRAGReassm|HOSTComm|
HOSTIsolated|HOSTPrec|HOSTREdirect|HOSTRTos|HOSTTos|
HOSTUNKnown|HOSTUNReach|NETComm|NETREdirect|NETRTos|
NETTos|NETUNKnown|NETUNReach|NOptr|Portunreach|
PREcedent|PROtunreach|PTRproblem|Sourceroute|Ttl|
icmp-code}]
[TCPFlags={{Urg|Ack|Rst|Syn|Fin}[,...]|ANY}]
[TCPDport={port-range|ANY}] [TCPSport={port-range|ANY}]
[UDPDport={port-range|ANY}] [UDPSport={port-range|ANY}]

```

Description This command creates a classifier, to sort traffic into flows. Classifiers are packet matching rules that identify particular data flows. The data flows may be specific in nature (e.g. IP packets with a particular TCP destination port from a particular source IP address) or general (e.g. all ICMP packets).

For software QoS, you can use up to 64 classifiers per policy. Both static classifiers and the dynamic classifiers created by DAR objects count towards this limit.

The syntax above and [Table 39-4 on page 39-15](#) both show whether parameters are valid in classifiers for switch ports or software QoS.

If a packet with an unknown destination port is to be transmitted, the packet is flooded to all ports in the VLAN. For such a packet, no hardware filters or switch port QoS will be applied to the packet. This also applies to any broadcast or multicast IP or IPX packet.

| Parameter | Description |
|------------|--|
| CLASSifier | <p>The ID number of the new classifier. An integer in the range 1 to 9999. For classifiers for hardware filters and switch port QoS, the ID number only uniquely identifies the rule, it does not imply an ordering between rules. For software QoS, the traffic class ID number and classifier ID number together determine the rule matching order. Classifiers within each traffic class are checked in ascending order of ID number (lowest first).</p> <p>Default: no default</p> |

| Parameter (cont.) | Description (cont.) | | | | | | |
|------------------------------------|--|------------------|---|---------|--|-----|--|
| Layer 1 parameters | | | | | | | |
| EPort | <p>The egress port—the Ethernet switch port through which the frame is destined to leave the switch. An integer in the range 1 to n, where n is the highest switch port.</p> <p>You can use classifiers that contain eport in software QoS policies on egress interfaces, or hardware filters, or switch port QoS policies. If you use the classifier for switch port QoS on a 48-port switch, you can only apply the policy to a port in the same port block as the eport (port blocks are ports 1-24 and ports 25-48).</p> <p>Default: any (ignores egress port)</p> | | | | | | |
| IPOrt | <p>The ingress port—the Ethernet switch port through which the frame arrives at the switch. An integer in the range 1 to n, where n is the highest switch port. Iport and iinterface are mutually exclusive.</p> <p>Default: any (ignores ingress port)</p> | | | | | | |
| IInterface | <p>The ingress interface—the interface through which the frame arrives at the switch. Valid entries are</p> <p>Layer 1 and 2 interfaces:</p> <ul style="list-style-type: none"> ● frame relay (e.g. fr0) ● DS3 ● PPP (such as ppp0) <p>To see a list of current valid Layer 1 and 2 interfaces, use the show interface command on page 11-87 of Chapter 11, Interfaces.</p> <p>Iport and iinterface are mutually exclusive. iinterface is only valid in classifiers for software QoS on egress interfaces or tunnels.</p> <p>Default: none (ignores ingress interface)</p> | | | | | | |
| Layer 2 Ethernet parameters | | | | | | | |
| SVlan | <p>The source VLAN—the VLAN associated with the frame when it arrives at the switch. Only valid in classifiers for software QoS on egress interfaces.</p> <p>Default: any</p> <table> <tr> <td><i>vlan-name</i></td><td>The name of the source VLAN. To see a list of current VLANs, use the show vlan command on page 8-146 of Chapter 8, Switching.</td></tr> <tr> <td>1..4094</td><td>The VLAN Identifier (VID) of the source VLAN.</td></tr> <tr> <td>ANY</td><td>The classifier ignores the source VLAN.</td></tr> </table> | <i>vlan-name</i> | The name of the source VLAN. To see a list of current VLANs, use the show vlan command on page 8-146 of Chapter 8, Switching. | 1..4094 | The VLAN Identifier (VID) of the source VLAN. | ANY | The classifier ignores the source VLAN. |
| <i>vlan-name</i> | The name of the source VLAN. To see a list of current VLANs, use the show vlan command on page 8-146 of Chapter 8, Switching. | | | | | | |
| 1..4094 | The VLAN Identifier (VID) of the source VLAN. | | | | | | |
| ANY | The classifier ignores the source VLAN. | | | | | | |
| DVlan | <p>The destination VLAN—the VLAN that the frame will be transmitted to. Only valid in classifiers for software QoS on egress interfaces.</p> <p>Default: any</p> <table> <tr> <td><i>vlan-name</i></td><td>The name of the destination VLAN. To see a list of current VLANs, use the show vlan command on page 8-146 of Chapter 8, Switching.</td></tr> <tr> <td>1..4094</td><td>The VLAN Identifier (VID) of the destination VLAN.</td></tr> <tr> <td>ANY</td><td>The classifier ignores the destination VLAN.</td></tr> </table> | <i>vlan-name</i> | The name of the destination VLAN. To see a list of current VLANs, use the show vlan command on page 8-146 of Chapter 8, Switching. | 1..4094 | The VLAN Identifier (VID) of the destination VLAN. | ANY | The classifier ignores the destination VLAN. |
| <i>vlan-name</i> | The name of the destination VLAN. To see a list of current VLANs, use the show vlan command on page 8-146 of Chapter 8, Switching. | | | | | | |
| 1..4094 | The VLAN Identifier (VID) of the destination VLAN. | | | | | | |
| ANY | The classifier ignores the destination VLAN. | | | | | | |

Layer 2 Ethernet parameters (cont.)

| | |
|---------------------|--|
| VLAN | <p>The destination VLAN—the VLAN that the frame will be transmitted to. Only valid in classifiers for hardware filters and QoS on switch ports.</p> <p>Default: any</p> |
| <i>vlan-name</i> | The name of the destination VLAN. To see a list of current VLANs, use the show vlan command on page 8-146 of Chapter 8, Switching . |
| 1..4094 | The VLAN Identifier (VID) of the destination VLAN. |
| ANY | The classifier ignores the destination VLAN. |
| VLANPriority | <p>The 802.1p VLAN priority value in the frame. An integer in the range 0 to 7; a range of integers separated by hyphens; or a comma separated list of integers and/or ranges (for example 0,2,4-6). Only valid in classifiers for software QoS on ingress and egress interfaces.</p> <p>Default: any (ignores VLAN priority)</p> |
| ETHFormat | <p>The Ethernet encapsulation type of the frame.</p> <p>The ethformat and protocol must match. Table 39-1 on page 39-13 shows possible combinations and whether they are valid.</p> <p>You can distinguish between frames that are tagged and untagged at ingress.</p> <p>Default: any</p> |
| 802.2 | Formatted according to IEEE Standards 802.2 and 802.3 with a DSAP/SSAP value not equal to hexadecimal AAAA. |
| 802.2-Tagged | Encapsulation: SAP |
| 802.2-Untagged | |
| EthII | Formatted according to RFC 894, <i>Standard for the transmission of IP datagrams over Ethernet networks</i> . |
| ETHII-Tagged | Encapsulation: Ethernet II |
| ETHII-Untagged | |
| NetwareRaw | Formatted as an IPX packet according to IEEE Standard 802.3. |
| NETWARERAW-Tagged | Encapsulation: NetWare Raw or Novell |
| NETWARERAW-Untagged | |
| Snap | Formatted according to IEEE Standards 802.2 and 802.3 and RFC 1042, <i>Standard for the transmission of IP datagrams over IEEE 802 networks</i> . |
| SNAP-Tagged | Encapsulation: SNAP |
| SNAP-Untagged | |
| ANY | The classifier ignores the Ethernet encapsulation. |
| MACDaddr | <p>The destination MAC address of the frame. An Ethernet six-octet MAC address, expressed as six pairs of hexadecimal digits delimited by hyphens.</p> <p>For classifiers attached to switch ports, it may not be possible to specify Layer 2 MAC address-based packet matching rules in conjunction with Layer 3 packet matching rules. If so, macdaddr and macsaddr will not be available.</p> <p>Default: any (ignores destination MAC address).</p> |
| MACSaddr | <p>The source MAC address of the frame. An Ethernet six-octet MAC address, expressed as six pairs of hexadecimal digits delimited by hyphens.</p> <p>For classifiers attached to switch ports, it may not be possible to specify Layer 2 MAC address-based packet matching rules in conjunction with Layer 3 packet matching rules. If so, macdaddr and macsaddr will not be available.</p> <p>Default: any (ignores source MAC address).</p> |

Layer 2 Ethernet parameters (cont.)

| | |
|----------------------|--|
| MACType | <p>The type of destination MAC address on the frame. Only valid in classifiers for software QoS on egress interfaces.</p> <p>Default: any</p> |
| L2Ucast | Layer 2 unicast addresses. |
| L2BMcast | Layer 2 broadcast or multicast addresses. |
| ANY | The classifier ignores the MAC address type. |
| PROTOCOL | <p>The protocol, determined from the value of the following Ethernet field:</p> <ul style="list-style-type: none"> ● for 802.2 (SAP encapsulation): the DSAP field, 1 byte hexadecimal ● for ETHII encapsulation: the ETYPE field, 2 bytes hexadecimal ● for NETWARERAW encapsulation: the IPX checksum field, 2 bytes hexadecimal with value FFFF ● for SNAP encapsulation: the ETYPE field, 5 bytes hexadecimal. The classifier matches on the last 2 bytes. <p>The encapsulation type (ethformat parameter) and protocol must match. Table 39-1 on page 39-13 shows possible combinations and whether they are valid.</p> <p>Default: any, unless you also specify a TCP or UDP parameter (for example, tcpSPORT). Then the default is IP.</p> |
| <i>protocol-type</i> | The protocol number or the predefined protocol name. Table 39-2 on page 39-14 shows predefined protocols, their numbers, and their encapsulations. |
| IP | Internet Protocol version 4. Valid with ethformat of ethii or snap . |
| IPV6 | Internet Protocol version 6. Valid with ethformat of ethii . Only valid in classifiers for software QoS. |
| ARP | Address Resolution Protocol. Valid with ethformat of ethii or snap . Only valid in classifiers for software QoS. |
| IPX | IPX. Valid with ethformat of 802.2 , ethii , netwareraw or snap . |
| NONIPIX | All protocols except for IP and IPX. Valid with ethformat of 802.2 , ethii or snap . Only valid in classifiers for hardware filters and switch port QoS. |
| ANY | The classifier ignores the protocol. |

Layer 2 parameters (frame relay and PPP)

| | |
|----------|--|
| DLCI | <p>The identification number of a Frame Relay Data Link Connection (DLC). An integer in the range 0 to 1023, or a range of integers separated by a hyphen (for example 0-3). Only valid in classifiers for software QoS on egress interfaces.</p> <p>Default: any (ignores DLCI).</p> |
| PPPIndex | The PPP interface number. For example, for ppp2, pppindex=2 . |

Layer 2 parameters (frame relay and PPP) (cont.)

PPPProtocolid The network layer protocol of the PPP encapsulated packet. Note that network and link control packets are processed by the software QoS policy's system traffic class. Examples of control packets include NCP, LCP, IPCP and PAP.

Only valid in classifiers for software QoS on egress interfaces.

Default: **any**, unless you also specify a TCP or UDP parameter. Then the default is **IP**.

ppp-protocol-id A 4 byte hexadecimal protocol number. [Table 39-3 on page 39-15](#) shows valid protocols and numbers.

IP Internet Protocol.

IPV6 Internet Protocol version 6.

ANY The classifier ignores PPP protocol ID.

Layer 3 parameters

IPDAddr The destination IPv4 or IPv6 address of the packet.

Default: **any**

ipadd[/0..32] The destination IPv4 address, in dotted decimal notation. You can optionally specify a subnet by specifying a mask.

ipv6add[/0..128] The destination IPv6 address, specified as eight pairs of hexadecimal octets separated by colons. You can optionally specify a prefix length. Default prefix length is 128—a single address.

IPv6 addresses are only valid in classifiers for software QoS on egress or tunnel interfaces.

ANY The classifier ignores destination IP or IPv6 address.

IPSAAddr The source IPv4 or IPv6 address of the packet.

Default: **any**

ipadd[/0..32] The source IPv4 address, in dotted decimal notation. You can optionally specify a subnet by specifying a mask.

ipv6add[/0..128] The source IPv6 address, specified as eight pairs of hexadecimal octets separated by colons. You can optionally specify a prefix length. Default prefix length is 128—a single address.

IPv6 addresses are only valid in classifiers for software QoS on egress or tunnel interfaces.

ANY The classifier ignores source IPv4 or IPv6 address.

IPDScp The DSCP value—the Code Point bits of the DiffServ field of an IPv4 or IPv6 packet. An integer in the range 0 to 63; a range of integers separated by hyphens; or a comma separated list of integers and/or ranges (for example 0,2,4-6). You can also specify EF, AF1, AF2, AF3 or AF4.

Ipdsdp and **Iptos** are mutually exclusive.

Default: **any** (ignores DSCP).

IPTOs The TOS value—the value of the precedence field within the TOS byte of an IPv4 packet. An integer in the range 0 to 7. **Ipdsdp** and **Iptos** are mutually exclusive. **Iptos** is only valid for IPv4 packets.

Default: **any** (ignores TOS).

Layer 3 parameters (cont.)

| | | | | | | | | | | | | | | | | | |
|--------------------|---|--------------------|--|-----|--------------------------------|-----|-------------------------|-----------|--|------|------------------------------------|------|------------------------------------|------|--|-----|---|
| IPFRAG | Whether the IPv4 packet is fragmented. Only valid in classifiers for software QoS on egress or tunnel interfaces. Default: any (ignores whether the packet is fragmented). | | | | | | | | | | | | | | | | |
| IPOptions | Whether the packet includes the IPv4 header options field. Only valid in classifiers for software QoS on egress or tunnel interfaces. Default: any (ignores whether the header options field is present or not). | | | | | | | | | | | | | | | | |
| IPFLowlabel | The IPv6 flow label in an IPv6 packet, an integer in the range 0 to 1048575. Only valid for IPv6 packets in classifiers for software QoS on egress or tunnel interfaces. Default: any (ignores IPv6 flow label). | | | | | | | | | | | | | | | | |
| IPXAddr | The destination network address of an IPX packet, expressed as a 4 byte hexadecimal number. Only valid in classifiers for hardware filters and QoS on switch ports. Default: any (ignores destination IPX address). | | | | | | | | | | | | | | | | |
| IPXPacket | The value of the Packet Type field of an IPX packet. One of the options NLSp, RIP, SAP, SPX, NCP, or NETbios; or a 2 byte hexadecimal IPX packet number; or a recognised IPX packet type. Only valid in classifiers for hardware filters and QoS on switch ports. Default: any (ignores IPX packet type). | | | | | | | | | | | | | | | | |
| IPPRotocol | The Layer 4 IPv4 or IPv6 protocol of the packet. For IPv6 packets, ipprotocol matches against the Next Header field of the IPv6 packet header. You can use a total of 29 unique ipprotocol values, plus TCP and UDP, in total across all classifiers. Default: <ul style="list-style-type: none"> ● tcp if you also specify a TCP parameter (for example, tcpsport). ● udp if you also specify a UDP parameter (for example, udpsport). ● Otherwise, any (ignores IP protocol). <table> <tr> <td><i>ip-protocol</i></td><td>A 1 byte decimal IPv4 or IPv6 protocol number or a well-known protocol name.</td></tr> <tr> <td>TCP</td><td>Transmission Control Protocol.</td></tr> <tr> <td>UDP</td><td>User Datagram Protocol.</td></tr> <tr> <td>NOTtcpudp</td><td>Any IPv4 or IPv6 protocol except TCP or UDP.</td></tr> <tr> <td>ICMp</td><td>Internet Control Message Protocol.</td></tr> <tr> <td>IGMp</td><td>Internet Group Multicast Protocol.</td></tr> <tr> <td>OSPF</td><td>Open Shortest Path First. Only valid in classifiers for software QoS on egress or tunnel interfaces.</td></tr> <tr> <td>ANY</td><td>The classifier ignores the IP protocol value.</td></tr> </table> | <i>ip-protocol</i> | A 1 byte decimal IPv4 or IPv6 protocol number or a well-known protocol name. | TCP | Transmission Control Protocol. | UDP | User Datagram Protocol. | NOTtcpudp | Any IPv4 or IPv6 protocol except TCP or UDP. | ICMp | Internet Control Message Protocol. | IGMp | Internet Group Multicast Protocol. | OSPF | Open Shortest Path First. Only valid in classifiers for software QoS on egress or tunnel interfaces. | ANY | The classifier ignores the IP protocol value. |
| <i>ip-protocol</i> | A 1 byte decimal IPv4 or IPv6 protocol number or a well-known protocol name. | | | | | | | | | | | | | | | | |
| TCP | Transmission Control Protocol. | | | | | | | | | | | | | | | | |
| UDP | User Datagram Protocol. | | | | | | | | | | | | | | | | |
| NOTtcpudp | Any IPv4 or IPv6 protocol except TCP or UDP. | | | | | | | | | | | | | | | | |
| ICMp | Internet Control Message Protocol. | | | | | | | | | | | | | | | | |
| IGMp | Internet Group Multicast Protocol. | | | | | | | | | | | | | | | | |
| OSPF | Open Shortest Path First. Only valid in classifiers for software QoS on egress or tunnel interfaces. | | | | | | | | | | | | | | | | |
| ANY | The classifier ignores the IP protocol value. | | | | | | | | | | | | | | | | |

Layer 4 parameters

| | |
|----------|--|
| ICMptype | The ICMP message type to match against the ICMP type field in an ICMP packet header. One of the list of options, or a decimal value in the range 0 to 65535. Only valid if ipprotocol=icmp in classifiers for software QoS on egress or tunnel interfaces. Default: any (ignores ICMP type). |
| ICMPCode | The ICMP message reason code to match against the ICMP code field in an ICMP packet header. One of the list of options, or a decimal value in the range 0 to 65535. Only valid if ipprotocol=icmp in classifiers for software QoS on egress or tunnel interfaces. Default: any (ignores ICMP code). |

Layer 4 parameters (cont.)

| | |
|------------|--|
| TCPFlags | The TCP flags of the TCP/IP packet. One or a comma-separated list of the options URG, ACK, RST, SYN and FIN. Default: any (ignores TCP flag). |
| TCPDport | The destination TCP port—the value in the TCP destination port field of the packet. For classifiers for hardware filters or switch port QoS, a single port number. For classifiers for software QoS on egress or tunnel interfaces, a single port number or a range of port numbers separated by a hyphen. Default: any (ignores destination TCP port). |
| TCPSport | The source TCP port—the value in the TCP source port field of the packet. For classifiers for hardware filters or switch port QoS, a single port number. For classifiers for software QoS on egress or tunnel interfaces, a single port number or a range of port numbers separated by a hyphen. Default: any (ignores source TCP port). |
| UDPDport | The destination UDP port—the value in the UDP destination port field of the packet. For classifiers for hardware filters or switch port QoS, a single port number. For classifiers for software QoS on egress or tunnel interfaces, a single port number or a range of port numbers separated by a hyphen. Default: any (ignores destination UDP port). |
| UDPSport | The source UDP port—the value in the UDP source port field of the packet. For classifiers for hardware filters or switch port QoS, a single port number. For classifiers for software QoS on egress or tunnel interfaces, a single port number or a range of port numbers separated by a hyphen. Default: any (ignores source UDP port). |
| IPXDSocket | The destination IPX socket number of an IPX packet. One of the options NCP, SAP, RIP, NNB, DIAG, NLSp or IPXwan; or a 2 byte hexadecimal IPX socket number; or a recognised IPX socket type. You can use a total of 7 unique ipxdsocket values across all classifiers, including any of the options. Only valid in classifiers for hardware filters and QoS on switch ports. Default: any (ignores destination IPX socket). |
| IPXSsocket | The source IPX socket number of an IPX packet. One of the options NCP, SAP, RIP, NNB, DIAG, NLSp or IPXwan; or a 2 byte hexadecimal IPX socket number; or a recognised IPX socket type. You can use a total of 7 unique ipxssocket values across all classifiers, including any of the options. Only valid in classifiers for hardware filters and QoS on switch ports. Default: any (ignores source IPX socket). |

Bit matching parameters

| | |
|--------|---|
| MATCH1 | A general 16-bit word to match inside a packet, specified as a 2 byte hexadecimal number. Match specifies the actual data to match. You must specify all three of matchx , maskx and offsetx together, where x is 1, 2 or 3. Only valid in classifiers for hardware filters and QoS on switch ports on Rapier i Series switches. Default: no default |
| MATCH2 | |
| MATCH3 | |
| MASK1 | Whether the corresponding bit in match is “on” for a match or “don't care” for a match, specified as a 2 byte hexadecimal number. If the mask bit is set (on), the bit in match must be the same as the corresponding bit in the actual packet (so place binary “ones” in bit positions you want to match). If the mask bit is clear (don't care), the same bit in match will not be checked with the corresponding bit in the actual packet. Only valid in classifiers for hardware filters and QoS on switch ports on Rapier i Series switches. Default: no default |
| MASK2 | |
| MASK3 | |

Bit matching parameters (cont.)

| | |
|---------|---|
| OFFSET1 | The offset from the start of the packet, specified as an integer in the range 0 to 62. You must specify offsets in order (e.g. offset1 before offset2). Only valid in classifiers for hardware filters and QoS on switch ports on Rapier i Series switches. Default: no default |
| OFFSET2 | |
| OFFSET3 | |

Table 39-1: Possible **ethformat** and **protocol** parameter combinations

| ethformat | protocol | validity |
|------------------|----------------------|--|
| ETHII | [not specified] | OK |
| | ANY | OK |
| | ARP | OK |
| | IP | OK (equivalent to protocol=0800) |
| | IPV6 | OK |
| | IPX | OK (equivalent to protocol=8137) |
| | NONIIPX | OK |
| | <i>protocol-type</i> | OK (see Table 39-2 for valid combinations) |
| NETWARERAW | [not specified] | OK (equivalent to protocol="IPX 802.3") |
| | ANY | OK (equivalent to protocol="IPX 802.3") |
| | ARP | Error |
| | IP | Error |
| | IPV6 | Error |
| | IPX | OK (equivalent to protocol="IPX 802.3") |
| | "IPX 802.3" | OK |
| | NONIIPX | Error |
| | <i>protocol-type</i> | Error |
| SNAP | [not specified] | OK |
| | ANY | OK |
| | ARP | OK |
| | IP | OK |
| | IPV6 | Error |
| | IPX | OK |
| | NONIIPX | OK |
| | <i>protocol-type</i> | OK (see Table 39-2 for valid combinations) |
| 802.2 | [not specified] | OK |
| | ANY | OK |
| | ARP | Error |
| | IP | Error |
| | IPV6 | Error |
| | IPX | OK |
| | NONIIPX | OK |
| | <i>protocol-type</i> | OK (see Table 39-2 for valid combinations) |

Table 39-2: Predefined protocol types for use in the **protocol** parameter

| Protocol Name | Protocol Number | Encapsulation | Min. characters to enter |
|------------------|-----------------|-------------------|--------------------------|
| SNA Path Control | 04 | SAP | 3 |
| PROWAY-LAN | 0E | SAP | 7 |
| EIA-RS | 4E | SAP | 3 |
| PROWAY | 8E | SAP | 3 |
| IPX 802.2 | E0 | SAP | 9 |
| NetBEUI | F0 | SAP | 3 |
| ISO CLNS IS | FE | SAP | 5 |
| IP ETHII | 0800 | EthII | 8 |
| X.75 Internet | 0801 | EthII | 4 |
| NBS Internet | 0802 | EthII | 3 |
| ECMA Internet | 0803 | EthII | 4 |
| Chaosnet | 0804 | EthII | 4 |
| X.25 Level 3 | 0805 | EthII | 4 |
| ARP | 0806 | EthII | 3 |
| XNS Compat | 0807 | EthII | 3 |
| Banyan Systems | 0BAD | EthII | 3 |
| BBN Simnet | 5208 | EthII | 3 |
| DEC MOP Dump/Ld | 6001 | EthII | 9 |
| DEC MOP Rem Cons | 6002 | EthII | 9 |
| DEC DECNET | 6003 | EthII | 7 |
| DEC LAT | 6004 | EthII | 7 |
| DEC Diagnostic | 6005 | EthII | 7 |
| DEC Customer | 6006 | EthII | 7 |
| DEC LAVC | 6007 | EthII | 7 |
| RARP | 8035 | EthII | 4 |
| DEC LANBridge | 8038 | EthII | 7 |
| DEC Encryption | 803D | EthII | 7 |
| AppleTalk | 809B | EthII | 3 |
| IBM SNA | 80D5 | EthII | 7 |
| IPX EthII | 8137 | EthII | 9 |
| AppleTalk AARP | 80F3 | EthII | 11 |
| SNMP | 814C | EthII | 4 |
| IPv6 ETHII | 86DD | EthII | 10 |
| IPX 802.3 | FFFF | NetWare 802.3 Raw | 9 |
| ETHERTALK 2 | 080007809B | SNAP | 11 |
| ETHERTALK 2 AARP | 0000080F3 | SNAP | 13 |
| IPX SNAP | 000008137 | SNAP | 8 |

Note: When you enter a protocol name that contains spaces, you must surround the name with double quotation marks. You can use lowercase or uppercase letters. For example, to specify ETHERTALK 2 AARP, enter **protocol="ethertalk 2 aarp"** or **protocol="ethertalk 2 a"**.

Table 39-3: PPP Network Layer protocol ID values for use in the **pppprotocolid** parameter

| PPP Protocol | Number | Long Name |
|--------------|--------|--------------------------------------|
| IP | 0021 | Internet Protocol |
| OSI | 0023 | OSI Network Layer |
| DEC | 0027 | Decnet Phase IV |
| APP | 0029 | Appletalk |
| IPX | 002B | IPX |
| VJC | 002D | Van Jacobson Compressed TCP/IP |
| VJU | 002F | Van Jacobson Uncompressed TCP/IP |
| BRI | 0031 | Bridging PDU |
| MP | 003D | Multilink Protocol |
| IP6HC | 004F | IP6 Header Compression |
| ENC | 0053 | Encryption |
| IPV6 | 0057 | Internet Protocol version 6 |
| SINGLE | 00FB | Single Link Compression in Multilink |
| Compressed | 00FD | Compressed Datagram |

Table 39-4: The classifier parameters that are valid for hardware filters and QoS on switch ports, and software QoS on ingress interfaces, egress interfaces, and tunnels

| Parameter | Hardware filters and switch ports | Software QoS egress | Software QoS tunnels | Software QoS ingress |
|-------------|-----------------------------------|---------------------|----------------------|----------------------|
| dlci | | ✓ | | |
| dvlan | | ✓ | | |
| eport | ✓ | ✓ | | |
| ethformat | ✓ | ✓ | | |
| icmpcode | | ✓ | ✓ | |
| icmptype | | ✓ | ✓ | |
| iinterface | | ✓ | ✓ | |
| ipdaddr | ✓ (IPv4 only) | ✓ (IPv4, IPv6) | ✓ (IPv4, IPv6) | |
| ipdscp | ✓ | ✓ | ✓ | ✓ |
| ipflowlabel | | ✓ | ✓ | |
| ipfrag | | ✓ | ✓ | |
| ipoptions | | ✓ | ✓ | |
| ipport | ✓ | ✓ | ✓ | |
| ipprotocol | ✓ | ✓ | ✓ | |
| ipsaddr | ✓ (IPv4 only) | ✓ (IPv4, IPv6) | ✓ (IPv4, IPv6) | |
| iptos | ✓ | ✓ | ✓ | ✓ |
| ipxdaddr | ✓ | | | |
| ipxdsocket | ✓ | | | |

Table 39-4: The classifier parameters that are valid for hardware filters and QoS on switch ports, and software QoS on ingress interfaces, egress interfaces, and tunnels (cont.)

| Parameter | Hardware filters and switch ports | Software QoS egress | Software QoS tunnels | Software QoS ingress |
|---------------|-----------------------------------|---------------------|----------------------|----------------------|
| ipxpacket | ✓ | | | |
| ipxssocket | ✓ | | | |
| macdaddr | ✓ | ✓ | | |
| macsaddr | ✓ | ✓ | | |
| mactype | | ✓ | | |
| maskx | ✓ (Rapier i) | | | |
| matchx | ✓ (Rapier i) | | | |
| offsetx | ✓ (Rapier i) | | | |
| pppindex | | ✓ | | |
| pppprotocolid | | ✓ | | |
| protocol | ✓ | ✓ | | |
| svlan | | ✓ | | |
| tcpdport | ✓ (single value) | ✓ (range) | ✓ (range) | |
| tcpflags | ✓ (Rapier i) | ✓ | ✓ | |
| tcpsport | ✓ (single value) | ✓ (range) | ✓ (range) | |
| udpport | ✓ (single value) | ✓ (range) | ✓ (range) | |
| udpsport | ✓ (single value) | ✓ (range) | ✓ (range) | |
| vlan | ✓ | | | |
| vlanpriority | | ✓ | | ✓ |

Examples To create packet matching rule 1 so that it matches all IP packets from the IP subnet 192.168.100.2 (mask=255.255.255.0), with a destination TCP port of 23, use one of the commands:

```
cre class=1 ipsaddr=192.168.100.2/24 tcpdport=23
cre class=1 protocol=ip ipsaddr=192.168.100.2/24 tcpdport=23
```

To create packet matching rules to separate PPPoE interfaces 1 and 2 on an Ethernet interface, use the commands:

```
cre class=1 pppi=1
cre class=2 pppi=2
```

Related Commands [destroy classifier](#)
[set classifier](#)
[show classifier](#)

destroy classifier

Syntax DESTroy CLASSifier={*rule-list*|ALL}

Description This command destroys one or more packet matching rules. You cannot destroy a classifier that is being used by a hardware filter or QoS.

The **classifier** parameter specifies the classifiers to destroy, and is the rule ID of an existing classifier, a comma-separated list of rule IDs, a range of rule IDs separated by a hyphen, or a combination (for example, 3,5,9-12). If you specify **all**, then all classifiers are destroyed.

Examples To destroy the packet matching rules with rule-ids 3, 5 and 9 to 12, use the command:

```
dest class=3,5,9-12
```

To destroy all packet matching rules, use the command:

```
dest class=all
```

Related Commands [create classifier](#)
[set classifier](#)
[show classifier](#)

set classifier

Classifier parameters are sorted approximately in order of the OSI model, with layer 1 (physical) parameters first.

Syntax:
hardware filters and
QoS on switch ports

For classifiers to use with QoS on switch ports (on Rapier i Series switches only) and hardware filters on switch ports:

```
SET CLASSifier=1..9999 [EPort=port] [IPort=port]
[VLAN={vlan-name|1..4094|ANY}]
[ETHFormat={802.2|802.2-Tagged|802.2-Untagged|Ethii|
ETHII-Tagged|ETHII-Untagged|Netwareraw|
NETWARERAW-Tagged|NETWARERAW-Untagged|Snap|SNAP-Tagged|
SNAP-Untagged|ANY}]
[MACDaddr={macadd|ANY}] [MACSaddr={macadd|ANY}]
[PROTocol={protocol-type|IP|IPX|NONIpipx|ANY}]
[IPDAddr={ipadd[/0..32]|ANY}] [IPSAddr={ipadd[/
0..32]|ANY}]
[IPDScp={dscp-list|ANY}] [IPTOs={0..7|ANY}]
[IPProtocol={TCP|UDP|ICMP|IGMP|NONTcpudp|
ip-protocol-num|ANY}]
[IPXDAddr={ipx-add|ANY}]
[IPXPacket={NLSp|RIP|SAP|SPX|NCP|NETbios|
ipx-packet-num|ANY}]
[TCPFlags={{Urg|Ack|Rst|Syn|Fin}|[,...]|ANY}]
[TCPPort={port-id|ANY}] [TCPSport={port-id|ANY}]
[UDPPort={port-id|ANY}] [UDPSport={port-id|ANY}]
[IPXDSocket={NCP|SAP|RIP|NNB|DIAG|NLSp|IPXwan|
ipx-socket-num|ANY}]
[IPXSSocket={NCP|SAP|RIP|NNB|DIAG|NLSp|IPXwan|
ipx-socket-num|ANY}] [MATCH1=hh MASK1=hh OFFSET1=0..62]
[MATCH2=hh MASK2=hh OFFSET2=0..62]
[MATCH3=hh MASK3=hh OFFSET3=0..62]
```

Syntax:
software QoS on
ingress

For classifiers to use with software QoS on ingress traffic over ETH ports, frame relay interfaces, and PPP interfaces:

```
SET CLASSifier=1..9999
[IPDScp={dscp-list|ANY}] [IPTOs={0..7|ANY}]
[VLANPriority={priority-list|ANY}]
```

Syntax:
software QoS on egress

For classifiers to use with software QoS on egress traffic over ETH ports, frame relay interfaces, and PPP interfaces:

```
SET CLASSifier=1..9999 [IINTERface={interface|NONE}]
[EPort={port|ANY}] [IPort={port|ANY}]
[SVlan={vlan-name|1..4094|ANY}]
[DVlan={vlan-name|1..4094|ANY}]
[VLANPriority={priority-list|ANY}]
[ETHFormat={802.2|802.2-Tagged|802.2-Untagged|Ethii|
ETHII-Tagged|ETHII-Untagged|Netwareraw|
NETWARERAW-Tagged|NETWARERAW-Untagged|Snap|SNAP-Tagged|
SNAP-Untagged|ANY}]
[MACDaddr={macadd|ANY}] [MACSaddr={macadd|ANY}]
[MACType={L2Ucast|L2BMcast|ANY}]
[DLCi={dlci-range|ANY}] [PPPIndex=0..1023]
[PPPProtocolid={ppp-protocol-id|IP|IPv6|ANY}]
```

```

[PROTOCOL={protocol-type|ARP|IP|IPV6|IPX|ANY}]
[IPDAddr={ipadd[/0..32]|ipv6add[/0..128]|ANY}]
[IPSAddr={ipadd[/0..32]|ipv6add[/0..128]|ANY}]
[IPDScp={dscp-list|ANY}] [IPTOS={0..7|ANY}]
[IPFRAG={YES|NO|ANY}] [IPOptions={YES|NO|ANY}]
[IPFLowlabel={0..1048575|ANY}]
[IPPRotocol={TCP|UDP|ICMp|IGMp|OSPF|NONTcpudp|ANY|
ip-protocol}]
[ICMptype={Any|ECHORply|Unreachable|Quench|Redirect|
ECHO|ADvertisement|Solicitation|TImeexceed|Parameter|
TSTAMP|TSTAMPRply|INFOREQ|INFOREP|ADDRREQ|ADDRREP|
NAMEREQ|NAMERPLY|icmp-type}]
[ICMPCode={Any|Filter|FRAGMent|FRAGReasm|HOSTComm|
HOSTIsolated|HOSTPrec|HOSTREdirect|HOSTRTos|HOSTTos|
HOSTUNKnown|HOSTUNReach|NETComm|NETREdirect|NETRTos|
NETTos|NETUNKnown|NETUNReach|NOptr|PORTunreach|
PREcedent|PROtunreach|PTRproblem|Sourceroute|Ttl|
icmp-code}]
[TCPFlags={{Urg|Ack|Rst|Syn|Fin}[,...]|ANY}]
[TCPDport={port-range|ANY}] [TCPSport={port-range|ANY}]
[UDPDport={port-range|ANY}] [UDPSport={port-range|ANY}]

```

Syntax: For classifiers to use with software QoS on GRE, IPsec and 6-to-4 tunnels:

software QoS on tunnels

```
SET CLASSifier=1..9999 [IINTERface={ interface | NONE } ]
[IPDAddr={ ipadd [/0..32] | ipv6add [/0..128] | ANY } ]
[IPSAddr={ ipadd [/0..32] | ipv6add [/0..128] | ANY } ]
[IPDScp={ dscp-list | ANY } ] [IPTOs={ 0..7 | ANY } ]
[IPFRAg={ YES | NO | ANY } ] [IPOptions={ YES | NO | ANY } ]
[IPFLowlabel={ flow-label-range | ANY } ]
[IPPRotocol={ TCP | UDP | ICMP | IGMP | OSPf | NONTcpudp | ANY |
ip-protocol } ]
[ICMptype={ Any | ECHORply | Unreachable | Quench | Redirect |
ECHO | ADvertisement | Solicitation | TImeexceed | Parameter |
TSTAMP | TSTAMPReply | INFOREQ | INFOREP | ADDRREQ | ADDRREP |
NAMEReq | NAMERply | icmp-type } ]
[ICMPCode={ Any | Filter | FRAGment | FRAGReasm | HOSTComm |
HOSTIsolated | HOSTPrec | HOSTREdirect | HOSTRTos | HOSTTos |
HOSTUNKnown | HOSTUNReach | NETComm | NETREdirect | NETRTos |
NETTos | NETUNKnown | NETUNReach | NOptr | Portunreach |
PREcedent | PROtunreach | PTRproblem | Sourceroute | Ttl |
icmp-code } ]
[TCPFlags={ { Urg | Ack | Rst | Syn | Fin } [, ... ] | ANY } ]
[TCPDport={ port-range | ANY } ] [TCPSport={ port-range | ANY } ]
[UDPDport={ port-range | ANY } ] [UDPSport={ port-range | ANY } ]
```

Description This command modifies a classifier. Classifiers are packet matching rules that identify particular data flows. The data flows may be specific in nature (e.g. IP packets with a particular TCP destination port from a particular source IP address) or general (e.g. all ICMP packets).

The syntax above and [Table 39-4 on page 39-15](#) both show whether parameters are valid in classifiers for switch ports or software QoS.

| Parameter | Description |
|---------------------------|---|
| CLASSifier | The ID number of the classifier. For classifiers for hardware filters and switch port QoS, the ID number only uniquely identifies the rule, it does not imply an ordering between rules. For classifiers for software QoS, the ID number determines the rule matching order. Within each traffic class, the classifiers are checked in ascending order of ID number (lowest first). Default: no default |
| Layer 1 parameters | |
| EPort | The egress port—the Ethernet switch port through which the frame is destined to leave the switch. An integer in the range 1 to <i>n</i> , where <i>n</i> is the highest switch port. You can use classifiers that contain eport in software QoS policies on egress interfaces, or hardware filters, or switch port QoS policies. If you use the classifier for switch port QoS on a 48-port switch, you can only apply the policy to a port in the same port block as the eport (port blocks are ports 1-24 and ports 25-48). Default: any (ignores egress port) |
| IPort | The ingress port—the Ethernet switch port through which the frame arrives at the switch. An integer in the range 1 to <i>n</i> , where <i>n</i> is the highest switch port. Iport and iinterface are mutually exclusive. Default: any (ignores ingress port) |

| Parameter (cont.) | Description (cont.) |
|-------------------|--|
| IInterface | <p>The ingress interface—the interface through which the frame arrives at the switch. Valid entries are</p> <p>Layer 1 and 2 interfaces:</p> <ul style="list-style-type: none"> ● frame relay (e.g. fr0) ● DS3 ● PPP (such as ppp0) <p>To see a list of current valid Layer 1 and 2 interfaces, use the show interface command in the Interfaces chapter.</p> <p>Iport and iinterface are mutually exclusive. iinterface is only valid in classifiers for software QoS on egress interfaces or tunnels.</p> <p>Default: none (ignores ingress interface)</p> |

Layer 2 Ethernet parameters

| | |
|------------------|--|
| SVlan | <p>The source VLAN—the VLAN associated with the frame when it arrives at the switch. Only valid in classifiers for software QoS on egress interfaces.</p> <p>Default: any</p> |
| <i>vlan-name</i> | The name of the source VLAN. To see a list of current VLANs, use the show vlan command on page 8-146 of Chapter 8, Switching. |
| 1..4094 | The VLAN Identifier (VID) of the source VLAN. |
| ANY | The classifier ignores the source VLAN. |
| DVlan | <p>The destination VLAN—the VLAN that the frame will be transmitted to. Only valid in classifiers for software QoS on egress interfaces.</p> <p>Default: any</p> |
| <i>vlan-name</i> | The name of the destination VLAN. To see a list of current VLANs, use the show vlan command on page 8-146 of Chapter 8, Switching. |
| 1..4094 | The VLAN Identifier (VID) of the destination VLAN. |
| ANY | The classifier ignores the destination VLAN. |
| VLAN | <p>The destination VLAN—the VLAN that the frame will be transmitted to. Only valid in classifiers for hardware filters and QoS on switch ports.</p> <p>Default: any</p> |
| <i>vlan-name</i> | The name of the destination VLAN. To see a list of current VLANs, use the show vlan command on page 8-146 of Chapter 8, Switching. |
| 1..4094 | The VLAN Identifier (VID) of the destination VLAN. |
| ANY | The classifier ignores the destination VLAN. |
| VLANPriority | <p>The 802.1p VLAN priority value in the frame. An integer in the range 0 to 7; a range of integers separated by hyphens; or a comma separated list of integers and/or ranges (for example 0,2,4-6). Only valid in classifiers for software QoS on ingress and egress interfaces.</p> <p>Default: any (ignores VLAN priority)</p> |

Layer 2 Ethernet parameters (cont.)

| | | |
|-----------|---|---|
| ETHFormat | The Ethernet encapsulation type of the frame. The ethformat and protocol must match. Table 39-1 on page 39-13 shows possible combinations and whether they are valid. You can distinguish between frames that are tagged and untagged at ingress. Default: any | |
| | 802.2 | Formatted according to IEEE Standards 802.2 and 802.3 |
| | 802.2-Tagged | with a DSAP/SSAP value not equal to hexadecimal AAAA. |
| | 802.2-Untagged | Encapsulation: SAP |
| | EthII | Formatted according to RFC 894, <i>Standard for the transmission of IP datagrams over Ethernet networks</i> . |
| | ETHII-Tagged | Encapsulation: Ethernet II |
| | ETHII-Untagged | |
| | NetwareRaw | Formatted as an IPX packet according to IEEE Standard 802.3. |
| | NETWARERAW-Tagged | Encapsulation: NetWare Raw or Novell |
| | NETWARERAW-Untagged | |
| Snap | Snap | Formatted according to IEEE Standards 802.2 and 802.3 |
| | SNAP-Tagged | and RFC 1042, <i>Standard for the transmission of IP datagrams over IEEE 802 networks</i> . |
| | SNAP-Untagged | Encapsulation: SNAP |
| | ANY | The classifier ignores the Ethernet encapsulation. |
| | | |
| MACDaddr | The destination MAC address of the frame. An Ethernet six-octet MAC address, expressed as six pairs of hexadecimal digits delimited by hyphens. For classifiers attached to switch ports, it may not be possible to specify Layer 2 MAC address-based packet matching rules in conjunction with Layer 3 packet matching rules. If so, macdaddr and macsaddr will not be available. Default: any (ignores destination MAC address). | |
| MACSaddr | The source MAC address of the frame. An Ethernet six-octet MAC address, expressed as six pairs of hexadecimal digits delimited by hyphens. For classifiers attached to switch ports, it may not be possible to specify Layer 2 MAC address-based packet matching rules in conjunction with Layer 3 packet matching rules. If so, macdaddr and macsaddr will not be available. Default: any (ignores source MAC address). | |
| MACType | The type of destination MAC address on the frame. Only valid in classifiers for software QoS on egress interfaces. Default: any | |
| | L2Ucast | Layer 2 unicast addresses. |
| | L2BMcast | Layer 2 broadcast or multicast addresses. |
| | ANY | The classifier ignores the MAC address type. |

Layer 2 Ethernet parameters (cont.)

| | |
|----------------------|--|
| PROToCol | <p>The protocol, determined from the value of the following Ethernet field:</p> <ul style="list-style-type: none"> ● for 802.2 (SAP encapsulation): the DSAP field, 1 byte hexadecimal ● for ETHII encapsulation: the ETYPE field, 2 bytes hexadecimal ● for NETWARERAW encapsulation: the IPX checksum field, 2 bytes hexadecimal with value FFFF ● for SNAP encapsulation: the ETYPE field, 5 bytes hexadecimal. The classifier matches on the last 2 bytes. <p>The encapsulation type (ethformat parameter) and protocol must match. Table 39-1 on page 39-13 shows possible combinations and whether they are valid.</p> <p>Default: any, unless you also specify a TCP or UDP parameter (for example, tcpsport). Then the default is IP.</p> |
| <i>protocol-type</i> | The protocol number or the predefined protocol name. Table 39-2 on page 39-14 shows predefined protocols, their numbers, and their encapsulations. |
| IP | Internet Protocol version 4. Valid with ethformat of ethii or snap . |
| IPV6 | Internet Protocol version 6. Valid with ethformat of ethii . Only valid in classifiers for software QoS. |
| ARP | Address Resolution Protocol. Valid with ethformat of ethii or snap . Only valid in classifiers for software QoS. |
| IPX | IPX. Valid with ethformat of 802.2 , ethii , netwareraw or snap . |
| NONIPIX | All protocols except for IP and IPX. Valid with ethformat of 802.2 , ethii or snap . Only valid in classifiers for hardware filters and switch port QoS. |
| ANY | The classifier ignores the protocol. |

Layer 2 parameters (frame relay and PPP)

| | |
|-------------------------|--|
| DLCi | <p>The identification number of a Frame Relay Data Link Connection (DLC). An integer in the range 0 to 1023, or a range of integers separated by a hyphen (for example 0-3). Only valid in classifiers for software QoS on egress interfaces.</p> <p>Default: any (ignores DLCI).</p> |
| PPPIIndex | The PPP interface number. For example, for ppp2, pppindex=2 . |
| PPPProtocolid | <p>The network layer protocol of the PPP encapsulated packet. Note that network and link control packets are processed by the software QoS policy's system traffic class. Examples of control packets include NCP, LCP, IPCP and PAP.</p> <p>Only valid in classifiers for software QoS on egress interfaces.</p> <p>Default: any, unless you also specify a TCP or UDP parameter. Then the default is IP.</p> |
| <i>ppp-protocol-id </i> | A 4 byte hexadecimal protocol number. Table 39-3 on page 39-15 shows valid protocols and numbers. |
| IP | Internet Protocol. |
| IPV6 | Internet Protocol version 6. |
| ANY | The classifier ignores PPP protocol ID. |

Layer 3 parameters

| | | |
|-------------|--|---|
| IPDAddr | The destination IPv4 or IPv6 address of the packet. Default: any | |
| | <i>ipadd</i> [/0..32] | The destination IPv4 address, in dotted decimal notation. You can optionally specify a subnet by specifying a mask. |
| | <i>ipv6add</i> [/0..128] | The destination IPv6 address, specified as eight pairs of hexadecimal octets separated by colons. You can optionally specify a prefix length. Default prefix length is 128—a single address. IPv6 addresses are only valid in classifiers for software QoS on egress or tunnel interfaces. |
| | ANY | The classifier ignores destination IP or IPv6 address. |
| IPSAddr | The source IPv4 or IPv6 address of the packet. Default: any | |
| | <i>ipadd</i> [/0..32] | The source IPv4 address, in dotted decimal notation. You can optionally specify a subnet by specifying a mask. |
| | <i>ipv6add</i> [/0..128] | The source IPv6 address, specified as eight pairs of hexadecimal octets separated by colons. You can optionally specify a prefix length. Default prefix length is 128—a single address. IPv6 addresses are only valid in classifiers for software QoS on egress or tunnel interfaces. |
| | ANY | The classifier ignores source IPv4 or IPv6 address. |
| IPDScp | The DSCP value—the Code Point bits of the DiffServ field of an IPv4 or IPv6 packet. An integer in the range 0 to 63; a range of integers separated by hyphens; or a comma separated list of integers and/or ranges (for example 0,2,4-6). You can also specify EF, AF1, AF2, AF3 or AF4. lpsdscp and lptos are mutually exclusive. Default: any (ignores DSCP). | |
| IPTOs | The TOS value—the value of the precedence field within the TOS byte of an IPv4 packet. An integer in the range 0 to 7. lpsdscp and lptos are mutually exclusive. lptos is only valid for IPv4 packets. Default: any (ignores TOS). | |
| IPFRAG | Whether the IPv4 packet is fragmented. Only valid in classifiers for software QoS on egress or tunnel interfaces. Default: any (ignores whether the packet is fragmented). | |
| IPOptions | Whether the packet includes the IPv4 header options field. Only valid in classifiers for software QoS on egress or tunnel interfaces. Default: any (ignores whether the header options field is present or not). | |
| IPFLowlabel | The IPv6 flow label in an IPv6 packet, an integer in the range 0 to 1048575. Only valid for IPv6 packets in classifiers for software QoS on egress or tunnel interfaces. Default: any (ignores IPv6 flow label). | |
| IPXDAddr | The destination network address of an IPX packet, expressed as a 4 byte hexadecimal number. Only valid in classifiers for hardware filters and QoS on switch ports. Default: any (ignores destination IPX address). | |

Layer 3 parameters (cont.)

| | |
|--------------------|---|
| IPXPacket | The value of the Packet Type field of an IPX packet. One of the options NLSp, RIP, SAP, SPX, NCP, or NETbios; or a 2 byte hexadecimal IPX packet number; or a recognised IPX packet type. Only valid in classifiers for hardware filters and QoS on switch ports. Default: any (ignores IPX packet type). |
| IPProtocol | The Layer 4 IPv4 or IPv6 protocol of the packet. For IPv6 packets, ipprotocol matches against the Next Header field of the IPv6 packet header. You can use a total of 29 unique ipprotocol values, plus TCP and UDP, in total across all classifiers. Default: <ul style="list-style-type: none"> ● tcp if you also specify a TCP parameter (for example, tcpsport). ● udp if you also specify a UDP parameter (for example, udpsport). ● Otherwise, any (ignores IP protocol). |
| <i>ip-protocol</i> | A 1 byte decimal IPv4 or IPv6 protocol number or a well-known protocol name. |
| TCP | Transmission Control Protocol. |
| UDP | User Datagram Protocol. |
| NOTtcpudp | Any IPv4 or IPv6 protocol except TCP or UDP. |
| ICMP | Internet Control Message Protocol. |
| IGMP | Internet Group Multicast Protocol. |
| OSPF | Open Shortest Path First. Only valid in classifiers for software QoS on egress or tunnel interfaces. |
| ANY | The classifier ignores the IP protocol value. |

Layer 4 parameters

| | |
|----------|---|
| ICMptype | The ICMP message type to match against the ICMP type field in an ICMP packet header. One of the list of options, or a decimal value in the range 0 to 65535. Only valid if ipprotocol=icmp in classifiers for software QoS on egress or tunnel interfaces. Default: any (ignores ICMP type). |
| ICMPCode | The ICMP message reason code to match against the ICMP code field in an ICMP packet header. One of the list of options, or a decimal value in the range 0 to 65535. Only valid if ipprotocol=icmp in classifiers for software QoS on egress or tunnel interfaces. Default: any (ignores ICMP code). |
| TCPFlags | The TCP flags of the TCP/IP packet. One or a comma-separated list of the options URG, ACK, RST, SYN and FIN. Default: any (ignores TCP flag). |
| TCPDport | The destination TCP port—the value in the TCP destination port field of the packet. For classifiers for hardware filters or switch port QoS, a single port number. For classifiers for software QoS on egress or tunnel interfaces, a single port number or a range of port numbers separated by a hyphen. Default: any (ignores destination TCP port). |
| TCPSport | The source TCP port—the value in the TCP source port field of the packet. For classifiers for hardware filters or switch port QoS, a single port number. For classifiers for software QoS on egress or tunnel interfaces, a single port number or a range of port numbers separated by a hyphen. Default: any (ignores source TCP port). |

Layer 4 parameters (cont.)

| | |
|------------|--|
| UDPDport | The destination UDP port—the value in the UDP destination port field of the packet. For classifiers for hardware filters or switch port QoS, a single port number. For classifiers for software QoS on egress or tunnel interfaces, a single port number or a range of port numbers separated by a hyphen. Default: any (ignores destination UDP port). |
| UDPSport | The source UDP port—the value in the UDP source port field of the packet. For classifiers for hardware filters or switch port QoS, a single port number. For classifiers for software QoS on egress or tunnel interfaces, a single port number or a range of port numbers separated by a hyphen. Default: any (ignores source UDP port). |
| IPXDSocket | The destination IPX socket number of an IPX packet. One of the options NCP, SAP, RIP, NNB, DIAG, NLSp or IPXwan; or a 2 byte hexadecimal IPX socket number; or a recognised IPX socket type. You can use a total of 7 unique ipxdsocket values across all classifiers, including any of the options. Only valid in classifiers for hardware filters and QoS on switch ports. Default: any (ignores destination IPX socket). |
| IPXSsocket | The source IPX socket number of an IPX packet. One of the options NCP, SAP, RIP, NNB, DIAG, NLSp or IPXwan; or a 2 byte hexadecimal IPX socket number; or a recognised IPX socket type. You can use a total of 7 unique ipxssocket values across all classifiers, including any of the options. Only valid in classifiers for hardware filters and QoS on switch ports. Default: any (ignores source IPX socket). |

Bit matching parameters

| | |
|-------------------------------|---|
| MATCH1 MATCH2 MATCH3 | A general 16-bit word to match inside a packet, specified as a 2 byte hexadecimal number. Match specifies the actual data to match. You must specify all three of matchx , maskx and offsetx together, where x is 1, 2 or 3. Only valid in classifiers for hardware filters and QoS on switch ports on Rapier i Series switches. Default: no default |
| MASK1 MASK2 MASK3 | Whether the corresponding bit in match is “on” for a match or “don't care” for a match, specified as a 2 byte hexadecimal number. If the mask bit is set (on), the bit in match must be the same as the corresponding bit in the actual packet (so place binary “ones” in bit positions you want to match). If the mask bit is clear (don't care), the same bit in match will not be checked with the corresponding bit in the actual packet. Only valid in classifiers for hardware filters and QoS on switch ports on Rapier i Series switches. Default: no default |
| OFFSET1 OFFSET2 OFFSET3 | The offset from the start of the packet, specified as an integer in the range 0 to 62. You must specify offsets in order (e.g. offset1 before offset2). Only valid in classifiers for hardware filters and QoS on switch ports on Rapier i Series switches. Default: no default |

Examples To set packet matching rule 1 so that it matches all IP packets from the IP subnet 192.168.100.2 (mask=255.255.255.0), with a destination TCP port of 23, use one of the commands:

```
set class=1 ipsa=192.168.100.2/24 tcpd=23
set class=1 prot=ip ipsa=192.168.100.2/24 tcpd=23
```

To change packet matching rule 2 so that it matches traffic over ppp3, use the command:

```
set class=2 ppi=3
```

Related Commands [create classifier](#)
[destroy classifier](#)
[show classifier](#)

show classifier

Syntax `SHoW CLASSifier[={id-list | ALL | DYnamic}]`

Description This command displays information about the classifiers configured.

If you specify **classifier** with no value, then a summary of all classifiers is displayed (Figure 39-1 and Table 39-5).

If you specify **classifier=all**, then details of all classifiers are displayed.

If you specify **classifier=id-list**, then details of the specified classifiers are displayed.

If you specify **classifier=dynamic**, then details of classifiers created by the DAR objects are displayed.

Figure 39-1: Example summary output from the **show classifier** command

| Classifier General Info | | |
|------------------------------|-----------|------------------------------|
| ----- | | |
| Total number of rules 6 | | |
| Rule | Type | Related Module(s) |
| ----- | | |
| 1 | L2 | L3 switch |
| 2 | L2 | L3 switch, QoS |
| 100 | L4,L3,L2 | QoS, Software QoS |
| 200 | L3,L2 | L3 switch, QoS, Software QoS |
| 700 | L3 | None |
| 9999 | Match all | None |
| ----- | | |

Table 39-5: Parameters in the summary output of the **show classifier** command

| Parameter | Meaning |
|-------------------|--|
| Rule | The identifier number for the classifier. |
| Type | A list of OSI layers at which parameters with non-default values in the rule operate, items in the list include L5, L4, L3, L2 and L1. |
| Related module(s) | The name of the module(s) that are currently using the classifier. |

Figure 39-2: Example summary output from the **show classifier=all** command

| Classifier Rules | |
|--------------------|-------------|
| ----- | |
| Rule | 1 |
| VLAN | default (1) |
| Rule | 2 |
| VLAN | v2 (2) |
| Rule | 100 |
| Protocol | IP |
| D-IP Address | 10.0.0.1/32 |
| IP Protocol | TCP |
| D-TCP Port | 23 |
| Rule | 200 |
| Protocol | IP |
| D-IP Address | 10.0.0.1/32 |
| Rule | 700 |
| MATCH1 | 1111 |
| MASK1 | 2222 |
| OFFSET1 | 1 |
| Rule | 9999 |
| Match all frames | |
| ----- | |

Table 39-6: Parameters in the summary output of the **show classifier= all** command

| Parameter | Meaning |
|--------------|---|
| Rule | The identifier number for the classifier. |
| VLAN | The name of a VLAN with only the first 10 characters shown. The VLAN Identifier appears in brackets. If the packet is Layer 3 switched, this VLAN is the destination VLAN. If the packet is Layer 3 routed by the CPU, this VLAN is the source VLAN. If the packet is Layer 2 switched, its source and destination VLAN are the same. |
| Protocol | The hexadecimal value of the protocol. If the protocol is not for the general family of IP and IPX protocols, and the commonly known name for the protocol is known to the Classifier, then this commonly known name will be printed in brackets after the hexadecimal number. |
| D-IP Address | The destination IP address field of a packet. |
| IP Protocol | The Layer 4 IP protocol field of a packet. |
| D-TCP Port | The destination TCP/IP port field of a packet. |
| MATCH1 | A 16-bit word to match inside a packet. |
| MASK1 | A 16-bit word used as a mask for the MATCH1 parameter value. |
| OFFSET1 | The offset from the start of the packet. |

Figure 39-3: Example detailed output from the **show classifier=2,3** command for classifiers that can be applied to software QoS

```
Classifier Rules
-----
Rule ..... 2
  Ingress Port ..... 1

Rule ..... 3
  Protocol ..... IP
  DSCP ..... 10,12,14 (AF1)
-----
```

Figure 39-4: Example output from the **show classifier=dynamic** command

```
Classifier Rules
-----
Rule ..... 10001
  Protocol ..... IPv4/IPv6
  IP Protocol ..... UDP
  D-UDP Port ..... 42768
-----
```

Table 39-7: Parameters in the detailed output of the **show classifier** command for classifiers that can be applied to software QoS

| Parameter | Meaning |
|-------------------|---|
| Rule | The ID number of the classifier. For classifiers for hardware filters and switch port QoS, the ID number only uniquely identifies the rule, it does not imply an ordering between rules. For software QoS, the traffic class ID number and classifier ID number together determine the rule matching order. Classifiers within each traffic class are checked in ascending order of ID number (lowest first). |
| Egress Port | The Ethernet switch port through which the frame is destined to leave the switch. |
| Ingress Port | The Ethernet switch port through which the frame arrives at the switch. |
| Ingress Interface | The interface through which the frame arrives at the switch. |
| D-MAC Address | The destination MAC address of the frame. |
| S-MAC Address | The source MAC address of the frame. |
| M-Type | The type of destination MAC address on the frame; one of L2Ucast (Layer 2 unicast addresses), L2Mcast (Layer 2 multicast addresses), L2Bcast (Layer 2 broadcast addresses) L2BMcast (Layer 2 broadcast or multicast addresses) or ANY. |
| S-VLAN | The source VLAN—the VLAN associated with the frame when it arrives at the switch. |
| D-VLAN | The destination VLAN—the VLAN that the frame will be transmitted to. |
| E-Format | The Ethernet encapsulation type of the frame. |
| Protocol | The protocol, determined from the value of the following Ethernet field: <ul style="list-style-type: none"> ● for 802.2 (SAP encapsulation): the DSAP field, 1 byte hexadecimal ● for ETHII encapsulation: the ETYPE field, 2 bytes hexadecimal ● for NETWARERAW encapsulation: the IPX checksum field, 2 bytes hexadecimal with value FFFF ● for SNAP encapsulation: the ETYPE field, 5 bytes hexadecimal. The classifier matches on the last 2 bytes. |
| VLAN Priority | The 802.1p VLAN priority value in the frame. |
| DLCI | The identification number of a Frame Relay Data Link Connection (DLC). |
| PPP Index | The PPP interface number. For example, for ppp2, PPP Index is 2. |
| PPP Protocol ID | The network layer protocol of the PPP encapsulated packet. Table 39-3 on page 39-15 shows valid protocols and numbers. Note that network and link control packets are processed by the software QoS policy's system traffic class. Examples of control packets include NCP, LCP, IPCP and PAP. |
| S-IP Address | The source IPv4 or IPv6 address of the packet. |
| D-IP Address | The destination IPv4 or IPv6 address of the packet. |
| IP flow label | The IPv6 flow label in an IPv6 packet. |
| IP Protocol | The Layer 4 IPv4 or IPv6 protocol of the packet. For IPv6 packets, IP protocol matches against the Next Header field of the IPv6 packet header. |

Table 39-7: Parameters in the detailed output of the **show classifier** command for classifiers that can be applied to software QoS (cont.)

| Parameter | Meaning |
|------------|--|
| DSCP | The DSCP value—the Code Point bits of the DiffServ field of an IPv4 or IPv6 packet. |
| TOS | The TOS value—the value of the precedence field within the TOS byte of an IPv4 packet. |
| IPOPTIONS | Whether the packet includes the IPv4 header options field. |
| IPFRAG | Whether the IPv4 packet is fragmented. |
| ICMP Code | The ICMP message reason code to match against the ICMP code field in an ICMP packet header. |
| ICMP Type | The ICMP message type to match against the ICMP type field in an ICMP packet header. |
| S-TCP Port | The source TCP port—the value in the TCP source port field of the packet. |
| D-TCP Port | The destination TCP port—the value in the TCP destination port field of the packet. |
| TCP Flags | The TCP flags of the TCP/IP packet. One or a comma-separated list of the options URG, ACK, RST, SYN and FIN. |
| S-UDP Port | The source UDP port—the value in the UDP source port field of the packet. |
| D-UDP Port | The destination UDP port—the value in the UDP destination port field of the packet. |

Figure 39-5: Example detailed output from the **show classifier** command for a classifier that can be applied to a hardware filter or switch port, for a TCP/IP data flow

| Classifier Rules | |
|---------------------|--------------------|
| ----- | |
| Rule | 1 |
| Ingress Port | 1 |
| Egress Port | 24 |
| D-MAC Address | 00-00-cd-00-01-e4 |
| S-MAC Address | 00-00-cd-00-03-48 |
| M-Type | L2UCAST |
| S-VLAN | vlan1234 (1234) |
| E-Format | ETHII |
| Protocol | 0800 (IP EthII) |
| S-IP Address | 192.168.123.123/32 |
| D-IP Address | 192.168.123.123/32 |
| IP Protocol | TCP |
| S-TCP Port | 23 |
| D-TCP Port | 23 |
| ----- | |

Figure 39-6: Example detailed output from the **show classifier** command for a classifier that can be applied to a hardware filter or switch port, for a UDP/IP data flow

| Classifier Rules | |
|---------------------|--------------------|
| ----- | |
| Rule | 21 |
| Ingress Port | 1 |
| Egress Port | 24 |
| D-MAC Address | 00-00-cd-00-01-e4 |
| S-MAC Address | 00-00-cd-00-03-48 |
| M-Type | L2UCAST |
| S-VLAN | vlan1234 (1234) |
| E-Format | ETHII |
| Protocol | 0800 (IP EthII) |
| S-IP Address | 192.168.123.123/32 |
| D-IP Address | 192.168.123.123/32 |
| IP Protocol | UDP |
| S-UDP Port | 23 |
| D-UDP Port | 23 |
| ----- | |

Table 39-8: Parameters in detailed output from the **show classifier** command for a classifier that can be applied to a hardware filter or switch port, for a TCP or UDP/IP data flows

| Parameter | Meaning |
|---------------|---|
| Rule | The rule identifier for the packet matching rule/classifier. |
| Ingress Port | The number of the ingress switch port associated with the rule. |
| Egress Port | The number of the egress switch port associated with the rule. |
| D-MAC Address | The destination MAC address field of a packet. |
| S-MAC Address | The source MAC address field of a packet. |
| M-Type | The type of destination MAC address on the frame; one of L2Ucast (Layer 2 unicast addresses), L2Mcast (Layer 2 multicast addresses), L2Bcast (Layer 2 broadcast addresses) L2BMcast (Layer 2 broadcast or multicast addresses) or ANY. |
| S-VLAN | The name of a VLAN with only the first 10 characters shown. The VLAN Identifier appears in brackets. If the packet is Layer 3 switched, this VLAN is the destination VLAN. If the packet is Layer 3 routed by the CPU, this VLAN is the source VLAN. If the packet is Layer 2 switched, its source and destination VLAN are the same. |
| E-Format | The Ethernet encapsulation format for the packet, suffixed with "-TAGGED" or "-UNTAGGED" if this has been specified in the rule. |
| Protocol | The hexadecimal value of the protocol. If the protocol is not for the general family of IP and IPX protocols, and the commonly known name for the protocol is known to the Classifier, then this commonly known name will be printed in brackets after the hexadecimal number. |
| S-IP Address | The source IP address field of a packet. |
| D-IP Address | The destination IP address field of a packet. |
| IP Protocol | The Layer 4 IP protocol field of a packet. |
| TOS/DSCP | The IP TOS or DiffServ Code Point field of a packet. |
| S-TCP Port | The source TCP/IP port field of a packet. |
| D-TCP Port | The destination TCP/IP port field of a packet. |
| S-UDP Port | The source UDP/IP port field of a packet. |

Table 39-8: Parameters in detailed output from the **show classifier** command for a classifier that can be applied to a hardware filter or switch port, for a TCP or UDP/IP data flows (cont.)

| Parameter | Meaning |
|------------|---|
| D-UDP Port | The destination UDP/IP port field of a packet. |
| TCP Flags | A series of letters representing the TCP/IP flag field, one of URG, ACK, RST, SYN or FIN. |

Figure 39-7: Example detailed output from the **show classifier** command for a MAC-address-based classifier that can be applied to a hardware filter or switch port

| | |
|---------------------|-------------------|
| Classifier Rules | |
| ----- | |
| Rule | 2222 |
| D-MAC Address | aa-bb-cc-dd-ee-ff |
| S-MAC Address | aa-bb-cc-dd-ee-ff |
| M-Type | L2UCAST |
| S-VLAN | vlan1234 (1234) |
| E-Format | SNAP |
| Protocol | 1234567890 (-) |
| ----- | |

Table 39-9: Parameters in the detailed output from the **show classifier** command for a MAC-address-based classifier that can be applied to a hardware filter or switch port

| Parameter | Meaning |
|---------------|---|
| Rule | The rule identifier for the packet matching rule/classifier. |
| D-MAC Address | The destination MAC address field of a packet. |
| S-MAC Address | The source MAC address field of a packet. |
| M-Type | The type of destination MAC address on the frame; one of L2Ucast (Layer 2 unicast addresses), L2Mcast (Layer 2 multicast addresses), L2Bcast (Layer 2 broadcast addresses) L2BMcast (Layer 2 broadcast or multicast addresses) or ANY. |
| S-VLAN | The name of a VLAN with only the first 10 characters shown. The VLAN Identifier appears in brackets. If the packet is Layer 3 switched, this VLAN is the destination VLAN. If the packet is Layer 3 routed by the CPU, this VLAN is the source VLAN. If the packet is Layer 2 switched, its source and destination VLAN are the same. |
| E-Format | The Ethernet encapsulation format for the packet, suffixed with "-TAGGED" or "-UNTAGGED" if this has been specified in the rule. |
| Protocol | The hexadecimal value of the protocol. If the protocol is not for the general family of IP and IPX protocols, and the commonly known name for the protocol is known to the Classifier, then this commonly known name will be printed in brackets after the hexadecimal number. |

Figure 39-8: Example detailed output from the **show classifier** command for a classifier that can be applied to a hardware filter or switch port, for an IPX data flow

| Classifier Rules | |
|--------------------|-----|
| ----- | |
| Rule | 31 |
| Protocol | IPX |
| D-IPX Socket | RIP |
| ----- | |

Table 39-10: Parameters in the detailed output from the **show classifier** command for a classifier that can be applied to a hardware filter or switch port, for an IPX data flow

| Parameter | Meaning |
|---------------|---|
| Rule | The rule identifier for the packet matching rule. |
| VLAN | The name of a VLAN with only the first 10 characters shown. The VLAN Identifier appears in brackets. If the packet is Layer 3 switched, this VLAN is the destination VLAN. If the packet is Layer 3 routed by the CPU, this VLAN is the source VLAN. If the packet is Layer 2 switched, its source and destination VLAN are the same. |
| E-Format | The Ethernet encapsulation format for the packet, suffixed with "-TAGGED" or "-UNTAGGED" if this has been specified in the rule. |
| Protocol | The hexadecimal value of the protocol, its common name, or both. |
| D-IPX Address | The destination IPX network address field of a packet. |
| D-IPX Socket | The destination IPX socket field of a packet. |
| S-IPX Socket | The source IPX socket field of a packet. |

Examples To display the number of each of the classifiers and which module is using each classifier, use the command:

```
sh class
```

To display what each classifier matches against, use the command:

```
sh class=all
```

Related Commands [create classifier](#)
[destroy classifier](#)
[set classifier](#)

