

Chapter 2

Creating Classifier Control Lists for Policies

This chapter provides information for configuring policy-based routing management on E-series routers. The chapter discusses the following topics:

- Classifier Control Lists Overview on page 10
- Creating or Modifying Classifier Control Lists for ATM Policy Lists on page 12
- Creating or Modifying Classifier Control Lists for Frame-Relay Policy Lists on page 12
- Creating or Modifying Classifier Control Lists for GRE Tunnel Policy Lists on page 12
- Creating or Modifying Classifier Control Lists for IP Policy Lists on page 13
- Creating or Modifying Classifier Control Lists for IPv6 Policy Lists on page 15
- Creating or Modifying Classifier Control Lists for L2TP Policy Lists on page 16
- Creating or Modifying Classifier Control Lists for MPLS Policy Lists on page 16
- Creating or Modifying Classifier Control Lists for VLAN Policy Lists on page 16

Classifier Control Lists Overview

Classifier control lists (CLACLs) specify the criteria by which the router defines a packet flow. Table 4 lists the criteria that you can use to create CLACLs for different types of traffic flows.

Table 4: CLACL Criteria

Type of CLACL	Criteria
ATM	<ul style="list-style-type: none"> ■ CLP ■ Color ■ Traffic class ■ User packet class
Frame Relay	<ul style="list-style-type: none"> ■ Color ■ Mark discard eligibility (DE) bit ■ Traffic class ■ User packet class
GRE	<ul style="list-style-type: none"> ■ Color ■ Traffic class ■ Type-of-service (ToS) byte ■ User packet class
IP	<ul style="list-style-type: none"> ■ Color ■ Destination IP address ■ Destination port ■ Destination route class ■ Internet Control Message Protocol (ICMP) ■ Internet Gateway Management Protocol (IGMP) ■ IP flags ■ IP fragmentation offset ■ Locally destined traffic ■ Protocol ■ Source IP address ■ Source port ■ Source route class ■ Transmission Control Protocol (TCP) ■ Traffic class ■ Type-of-service (ToS) byte ■ User Datagram Protocol (UDP) ■ User packet class

Table 4: CLACL Criteria (continued)

Type of CLACL	Criteria
IPv6	<ul style="list-style-type: none"> ■ Color ■ Destination IPv6 address ■ Destination port ■ Destination route class ■ Internet Control Message Protocol version 6 (ICMPv6) ■ IPv6 traffic class ■ Locally destined traffic ■ Multicast Listener Discovery (MLD) ■ Next header ■ Source IPv6 address ■ Source port ■ Source route class ■ Traffic class ■ Transmission Control Protocol (TCP) ■ User Datagram Protocol (UDP) ■ User packet class
L2TP	<ul style="list-style-type: none"> ■ Color ■ Traffic class ■ User packet class
MPLS	<ul style="list-style-type: none"> ■ Color ■ Mark experimental (EXP) bit ■ Traffic class ■ User packet class
VLAN	<ul style="list-style-type: none"> ■ Color ■ Traffic class ■ User packet class ■ User priority

You configure CLACLs with a name and then values to match in the IP datagram header. A CLACL does not include an action: actions take place when a match is included in a policy list.



NOTE: Do not use the asterisk (*) for the name of a classifier list. The asterisk is used as a wildcard for the **classifier-group** command.

NOTE: If you do not specify one of the **frame-relay**, **gre-tunnel**, **ip**, **ipv6**, **l2tp**, **mpls**, or **vlan** keywords, the router creates an IP classifier list. This version of the command has been deprecated and may be removed in a future release.

Related Topics

- For information about the hardware and software CLACLs that are supported for each interface type, see *Chapter 8, Policy Resources*.
- For information about monitoring Classifier Lists, see *Chapter 9, Monitoring Policy Management*.

Creating or Modifying Classifier Control Lists for ATM Policy Lists

You can create or modify a classifier control list that can be used only in ATM policy lists.

- Issue the **atm classifier-list** command:

```
host1(config)#atm classifier-list atmclassifier color red user-packet-class 10  
clp 1
```

Related Topics

- **atm classifier-list** command

Creating or Modifying Classifier Control Lists for Frame-Relay Policy Lists

You can create or modify a classifier control list that can be used only in Frame Relay policy lists.

- Issue the **frame-relay classifier-list** command.;

```
host1(config)#frame-relay classifier-list frclassifier color red user-packet-class 10  
de-bit 1
```

Related Topics

- **frame-relay classifier-list** command

Creating or Modifying Classifier Control Lists for GRE Tunnel Policy Lists

You can create or modify a classifier control list that can be used only in GRE tunnel policy lists.

- Issue the **gre-tunnel classifier-list** command:

```
host1(config)#gre-tunnel classifier-list greClassifier50 color yellow  
user-packet-class 7 dsfield 40
```

Related Topics

- **gre-tunnel classifier-list** command

Creating or Modifying Classifier Control Lists for IP Policy Lists

You can create or modify a classifier control list that can be used only in IP policy lists. The behavior of multiple-element classifier-list classification is the logical OR of the elements in the CLACL.

- Issue the **ip classifier-list** command to match all packets that have a source IP address of 192.168.30.100 or have a destination IP address of 192.168.30.200:

```
host1(config)#ip classifier-list boston5 ip host 192.168.30.100 any
host1(config)#ip classifier-list boston5 ip any host 192.168.30.200
```

Related Topics

- **ip classifier-list** command

Setting Up an IP Classifier Control List to Accept Traffic from All Sources

You can set up a CLACL to accept IP traffic from all source addresses on the subnet.

- Issue the **ip classifier-list** command:

```
host1(config)#ip classifier-list XYZCorpPermit ip 192.168.0.0 0.0.255.255 any
```

Classifying IP Traffic Based on Source and Destination Addresses

You can classify traffic based on source and destination addresses. You can specify the address as a host address, a subnet, or a wildcard. If you specify the address as a subnet, the mask, in binary notation, must be a series of contiguous zeros, followed by a series of contiguous ones. The **any** keyword is the address wildcard, matching traffic for any address.

- Issue the **ip classifier-list** command to classify traffic on any source or destination address:

```
host1(config)#ip classifier-list YourListName ip any any
host1(config)#ip classifier-list YourListName ip host 10.10.10.10 any
host1(config)#ip classifier-list YourListName ip 10.10.0.0 0.0.255.255 host
10.10.10.2
```

Using IP Classifier Control Lists to Match Route Class Values

You can set up classifier control lists to match route-class values. In this example, svale20 matches the source address lookup route-class value of 1, svale30 matches the destination address lookup route-class value of 1 and a ToS byte value of 10, svale40 matches the source address lookup route-class value of 1 and the packets destined to a local interface, and west20 matches the source address lookup route-class value of 1 and packets that are not destined for a local interface (packets destined for remote interfaces).

- Issue the **ip classifier-list** command:

```
host1(config)#ip classifier-list svale20 source-route-class 1 ip any any
host1(config)#ip classifier-list svale30 destination-route-class 1 ip any any
tos 10
```

```
host1(config)#ip classifier-list sval40 source-route-class 1 local true ip
any any
host1(config)#ip classifier-list west25 source-route-class 1 local false ip any any
```

Creating IP Classifier Control Lists for TCP and UDP Ports

You can specify a single TCP or UDP port or a range of ports, where packets are matched with source address 198.168.30.100 and UDP source port numbers in the range 1–10.

- Issue the **ip classifier-list** command to create a CLACL on a UDP host:

```
host1(config)#ip classifier-list YourListName udp host 192.168.30.100 range 1
10 any
```

To create a CLACL that matches all traffic on UDP source ports greater than 100:

```
host1(config)#ip classifier-list XYZCorpUdp udp any gt 100 172.17.2.1
0.0.255.255
```

To match a non-TCP packet originating from IP address 172.28.100.52:

```
host1(config)#ip classifier-list YourListName not tcp host 172.28.100.52 any
```

To specify a single TCP or UDP port or range of ports, an ICMP code and optional type, or an IGMP type, which matches packets with source address 198.168.30.100 and ICMP type 2 and code 10:

```
host1(config)#ip classifier-list YourListName icmp host 192.168.30.100 any 2
10
```

Creating an IP Classifier Control List That Matches the ToS Byte

You can create an IP CLACL that matches the ToS byte in the IP header.

- Issue the **ip classifier-list** command using the **tos** keyword.

```
host1(config)#ip classifier-list tos128 ip any any tos 128
host1(config)#ip classifier-list low-drop-prec ip any any dsfield 10
host1(config)#ip classifier-list priority ip any any precedence 1
```

Creating an IP Classifier Control List That Filters ICMP Echo Requests

You can create a CLACL that filters all ICMP echo requests headed toward an access link under a denial-of-service attack.

- Issue the **ip classifier-list** command:

```
host1(config)#ip classifier-list XYZCorplcmpEchoReqs icmp any any 8 0

host1(config)#ip classifier-list XYZCorplgmpType1 igmp any any 1
```

Creating IP Classifier Control Lists That Use TCP or IP Flags

You can create CLACLs that use TCP or IP flags. For both IP flags and TCP flags, if you specify only a single flag, the logical equation does not require quotation marks.

- Issue the **ip classifier-list** command with the **tcp-flags** keyword and a logical equation (a quotation-enclosed string using ! for NOT, & for AND) to match one or more of the **ack**, **fin**, **psh**, **rst**, **syn**, or **urg** TCP flags:

```
host1(config)#ip classifier-list telnetConnects tcp 192.168.10.0 0.0.0.255 host
10.10.10.10 eq 23 tcp-flags "syn & !ack"
```

- Issue the **ip classifier-list** command with the **ip-flags** keyword and a logical equation (a quotation-enclosed string using ! for NOT, & for AND) to match one or more of the **dont-fragment**, **more-fragments**, or **reserved** IP flags:

```
host1(config)#ip classifier-list dontFragment ip any any ip-flags "dont-fragment"
```

Creating IP Classifier Control Lists That Match the IP Fragmentation Offset

You can create CLACLs that match the IP fragmentation offset.

- Issue the **ip classifier-list** command with the **ip-frag-offset** keyword and the **eq** or **gt** operator to match an IP fragmentation offset equal to 0, 1, or greater than 1:

```
host1(config)#ip classifier-list fragOffsetAttack ip any host 10.10.10.10
ip-frag-offset eq 1
host1(config)#ip policy-list dosProtect
host1(config-policy-list)#filter classifier-group fragOffsetAttack
host1(config-policy-list)#forward
```

Creating or Modifying Classifier Control Lists for IPv6 Policy Lists

You can create or modify a classifier control list that can be used only in IPv6 policy lists.

- Issue the **ipv6 classifier-list** command:

```
host1(config)#ipv6 classifier-list ipv6classifier color red user-packet-class 5
tcfield 10
```

```
host1(config)#ipv6 classifier-list YourListName udp destination-port eq 75
```

```
host1(config)#ipv6 classifier-list telnetConnects tcp destination-port eq 23
tcp-flags "syn & !ack"
```

```
host1(config)#ipv6 classifier-list listname icmpv6 icmp-type 3 icmp-code 6
```

```
host1(config)#ipv6 classifier-list sval20 source-route-class 1
host1(config)#ipv6 classifier-list sval30 destination-route-class 1 tcfield 10
host1(config)#ipv6 classifier-list sval40 source-route-class 1 local true
host1(config)#ipv6 classifier-list west25 source-route-class 1 local false
```

```
host1(config)#ipv6 classifier-list YourClacList source-host 2001:db8:1::8001
destination-address 2001:db8:3::/48
```

Related Topics

- `ipv6 classifier-list` command

Creating or Modifying Classifier Control Lists for L2TP Policy Lists

You can create or modify a classifier control list that can be used only in L2TP policy lists.

- Issue the `l2tp classifier-list` command:
`host1(config)#l2tp classifier-list l2tpclassifier color red user-packet-class 7`

Related Topics

- `l2tp classifier-list` command

Creating or Modifying Classifier Control Lists for MPLS Policy Lists

You can create or modify a classifier control list that can be used only in MPLS policy lists.

- Issue the `mpls classifier-list` command:
`host1(config)#mpls classifier-list mplsClass user-packet-class 10 exp-bits 3 exp-mask 5`

Related Topics

- `mpls classifier-list` command

Creating or Modifying Classifier Control Lists for VLAN Policy Lists

You can create or modify a classifier control list that can be used only in VLAN policy lists.

- Issue the `vlan classifier-list` command:
`host1(config)#vlan classifier-list lowLatencyLowDrop user-priority 7`
`host1(config)#vlan classifier-list lowLatencyLowDrop user-priority 6`
`host1(config)#vlan classifier-list lowLatency user-priority 5`
`host1(config)#vlan classifier-list excellentEffort user-priority 4`
`host1(config)#vlan classifier-list bestEffort user-priority 3`
`host1(config)#vlan classifier-list bestEffort user-priority 2`
`host1(config)#vlan classifier-list bestEffort user-priority 1`
`host1(config)#vlan classifier-list bestEffort user-priority 0`

Related Topics

- `vlan classifier-list` command