match access-group through mls ip pbr

mac packet-classify

To classify Layer 3 packets as Layer 2 packets, use the **macpacket-classify** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

mac packet-classify [bpdu]

no mac packet-classify [bpdu]

Syntax Description

bpdu	(Optional) Specifies Layer 2 policy enforcement for BPDU packets.

Command Default

Layer 3 packets are not classified as Layer 2 packets.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	Added support for MAC ACLs on BPDU packets.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

You can configure these interface types for multilayer MAC access control list (ACL) quality of service (QoS) filtering:

- VLAN interfaces without Layer 3 addresses
- Physical LAN ports that are configured to support Ethernet over Multiprotocol Label Switching (EoMPLS)
- Logical LAN subinterfaces that are configured to support EoMPLS

The ingress traffic that is permitted or denied by a MAC ACL on an interface configured for multilayer MAC ACL QoS filtering is processed by egress interfaces as MAC-layer traffic. You cannot apply egress IP ACLs to traffic that was permitted or denied by a MAC ACL on an interface configured for multilayer MAC ACL QoS filtering.

Microflow policing does not work on interfaces that have the **macpacket-classify** command enabled.

The **macpacket-classify** command causes the Layer 3 packets to be classified as Layer 2 packets and disables IP classification.

Traffic is classified based on 802.1Q class of service (CoS), trunk VLAN, EtherType, and MAC addresses.

Examples

This example shows how to classify incoming and outgoing Layer 3 packets as Layer 2 packets:

```
Router(config-if)# mac packet-classify
Router(config-if)#
```

This example shows how to disable the classification of incoming and outgoing Layer 3 packets as Layer 2 packets:

```
Router(config-if)# no mac packet-classify
Router(config-if)#
```

This example shows how to enforce Layer 2 policies on BPDU packets:

```
Router(config-if)# mac packet-classify bpdu
Router(config-if)#
```

This example shows how to disable Layer 2 policies on BPDU packets:

```
Router(config-if)# no mac packet-classify bpdu
Router(config-if)#
```

Related Commands

Command	Description
mac packet-classify use vlan	Enables VLAN-based QoS filtering in the MAC ACLs.

mac packet-classify use vlan

To enable VLAN-based quality of service (QoS) filtering in the MAC access control lists (ACLs), use the **macpacket-classifyusevlan** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mac packet-classify use vlan

no mac packet-classify use vlan

Syntax Description

This command has no arguments or keywords.

Command Default

VLAN-based QoS filtering in the MAC ACLs is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported in PFC3BXL or PFC3B mode only.

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

You must use the **nomacpacket-classifyusevlan** command to disable the VLAN field in the Layer 2 key if you want to apply QoS to the Layer 2 Service Advertising Protocol (SAP)-encoded packets (for example, Intermediate System-to-Intermediate System [IS-IS] and Internet Packet Exchange [IPX]).

QoS does not allow policing of non-Advanced Research Protocol Agency (ARPA) Layer 2 packets (for example, IS-IS and IPX) if the VLAN field is enabled.

Examples

This example shows how to enable Layer 2 classification of IP packets:

```
Router(config)# mac packet-classify use vlan
Router(config)
```

This example shows how to disable Layer 2 classification of IP packets:

```
Router(config)# no mac packet-classify use vlan
Router(config)
```

Related Commands

Command	Description
mac packet-classify	Classifies Layer 3 packets as Layer 2 packets.

map ip

T o classify either all the IPv4 packets, or the IPv4 packets based on either differentiated service code point (DSCP) values or precedence values into high priority or low priority for POS, channelized, and clear-channel SPAs, use the following forms of the **mapip** command in ingress class-map mode. Use the **no** forms of this command listed here to remove the IPv4 settings.

Command to Classify all the IPv4 Packets

map ip all queue {**strict-priority**| **0**}

no map ip all queue {**strict-priority**| **0**}

Command to Classify IPv4 Packets Based on DSCP Values

map ip {**dscp-based**| **dscp** {*dscp-value*| *dscp-range*} **queue** {**strict-priority**| **0**}}

no map ip {**dscp-based**| **dscp** {*dscp-value*| *dscp-range*} **queue** {**strict-priority**| **0**}}

Command to Classify IPv4 Packets Based on Precedence Values

map ip {**precedence-based**| **precedence** {*precedence-value*| *precedence-range*} **queue strict-priority**| **0**}

no map ip {**precedence-based**| **precedence** {*precedence-value*| *precedence-range*} **queue strict-priority**| **0**}

Syntax Description

all queue	Implies the high priority or low priority configuration of all the IPv4 packets.
strict-priority	Classifies all the IPv4 packets as high priority (strict-priority).
0	Classifies all the IPv4 packets as low priority.
dscp-based	Enables classification based on DSCP value in IPv4.
dscp	Allows you to configure the DSCP value or range as high priority or low priority for IPv4 packets.
dscp-value	DSCP value for which the priority is to be configured as high or low.
dscp-range	Range of dscp-values for which the priority is to be configured as high or low.
queue	Enables the classification of an entire queue, DSCP values, or precedence values as high priority or low priority.
precedence-based	Enables the classification based on IPv4 precedence values.

precedence	Allows you to configure an IPv4 precedence value or range as high priority or low priority for IPv4 packets.
precedence-value	Precedence-value for which the priority is to be configured as high or low.
precedence-range	Range of precedence-values for which the priority is to be configured as high or low.

Command Default

If there is no configuration of IPv4 DSCP value or precedence values map to high priority specified, the system treats packets with DSCP range EF as high priority and precedence range 6-7 as high priority.

Command Modes

Ingress-class-map configuration mode

Command History

Release	Modification
3.1S	This command was introduced to classify either all the IPv4 packets, or the IPv4 packets based on either DSCP value or precedence values as high or low for POS, channelized, and clear-channel SPAs.

Usage Guidelines

To classify all IPv4 packets as high or low for POS, channelized, or clear-channel SPA, use the **mapipallqueue**command,

To classify IPv4 packets with specific DSCP values, enable the DSCP classification using the **mapipdscp-based**command. To classify IPV4 packets with specific DSCP values as high or low, use the **mapipdscp** {{*dscp-value* | *dscp-range*} **queue** {**strict-priority** | **0**}} command.

To classify IPv4 packets with specific precedence values, enable the precedence classification using the **mapipprecedence-based**command. To classify IPv4 packets with specific precedence values as high or low, use the **mapipprecedence** {{*precedence-value* | *precedence-range*} **queue** {**strict-priority** | **0**}} command.

Examples

The following example shows how to classify all the IPv4 Packets as high priority using the **mapipallqueuestrict-priority**command:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ip all queue strict-priority
```

The following example shows how to classify IPv4 Packets with DSCP value of cs1 as high priority:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ip dscp-based
Router(config-ing-class-map)# map ip dscp cs1 queue strict-priority
```

The following example shows how to classify IPv4 Packets with a precedence value 3 and 5 as high priority:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ip precedence-based
Router(config-ing-class-map)# map ip precedence 3 5 queue strict-priority
```

Related Commands

Command	Description
plim qos input class-map	Attaches the classification template to an interface.

map ipv6

T o classify either all the IPv6 packets, or IPv6 packets based on specific traffic class (TC) values as high priority or low priority in the context of POS, channelized, and clear-channel SPAs use the following forms of **mapipv6** commands in ingress class-map mode. Use the **no** forms of this command listed here to remove the IPv6 settings.

Command to Classify all the IPv6 Packets

map ipv6 all queue {**strict-priority**| **0**}

no map ipv6 all queue {**strict-priority**| **0**}

Command to Classify IPv6 Traffic-Class values as High Priority or Low Priority

map ipv6 tc {*tc-value*| *tc-range*} **queue** {**strict-priority**| **0**}

no map ipv6 tc {*tc-value*| *tc-range*} **queue** {**strict-priority**| **0**}

Syntax Description

all queue	Implies the high priority or low priority configuration of all the IPv6 packets.
strict-priority	Classifies all the IPv6 packets as high priority (strict-priority).
0	Classifies all the IPv6 Packets as low priority.
tc	Allows you to configure the traffic class value or range as high priority or low priority for IPv6 packets.
tc-value	Specific traffic-class value for which the priority is to be configured as either high or low(0).
tc-range	Range of traffic-class values for which the priority is to be configured as either high or low(0).
queue	Enables classification of the entire queue, traffic-class values, or range of traffic-class values as either high priority or low priority.

Command Default

If a user does not configure which IPv6 traffic class values map to high priority, the system treats packets the packets with traffic class EF as high priority.

Command Modes

Ingress-class-map configuration mode

Command History

Release	Modification
3.1S	This command was introduced to classify, all the IPv6 packets or the IPv6 packets based on traffic class values as high priority or low priority for POS, channelized, and clear-channel SPAs.

Usage Guidelines

To classify all the IPv6 packets as high priority or low priority in the context of POS, channelized, or clear-channel SPAs, use the **mapipv6allqueue**command.

To classify the IPv6 packets with specific traffic class values, use the **mapipv6tccs2queuestrict-priority**command.

Examples

The following example shows how to classify all the IPv6 packets as high priority using the **mapipv6allqueuestrict-priority** command:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ipv6 all queue strict-priority
```

The following example shows how to classify the IPv6 packets with traffic-class values cs2 as high priority:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ip tc cs2 queue strict-priority
```

Related Commands

Command	Description
plim qos input class-map	Attaches the classification template to an interface.

map mpls

T o classify either all the Multiprotocol Label Switching (MPLS) packets or MPLS packets with specified EXP values or range as high priority or low priority for POS, channelized, and clear-channel SPAs the following forms of the **mapmpls** command are used in ingress class-map mode. Use the **no** forms of this command listed here to remove the MPLS settings.

Command to Classify all the MPLS EXP Values as High Priority or Low Priority

map mpls all queue {**strict-priority**| **0**}

no map mpls all queue

Command to Classify the MPLS EXP Values as High Priority or Low Priority

map mpls exp {*exp-value*| *exp-range*} **queue** {**strict-priority**| **0**}

no map mpls exp {*exp-value*| *exp-range*} **queue** {**strict-priority**| **0**}

Syntax Description

all queue	Implies the high priority or low priority configuration of all the MPLS Packets.
strict-priority	Classifies either all the MPLS packets or the MPLS packets with specific EXP values as high priority (strict priority).
0	Classifies MPLS packets as low priority.
exp	Allows you to configure an EXP value or a range of EXP values as high priority or low priority for MPLS packets. The valid range for EXP values is 0 to 7.
exp-value	A specific EXP value for which the priority is to be configured as high or low(0).
exp-range	A range of EXP values for which the priority is to be configured as high or low(0). The valid range for EXP values is 0 to 7.
queue	Enables the classification priority of an entire queue, EXP values, or range of EXP values as high priority or low priority.

Command Default

If a user does not configure which MPLS EXP values map to high priority, the system treats packets with an EXP value of 6-7 as high priority.

Command Modes

Ingress-class-map configuration mode

Command History

Release	Modification
3.1S	This command was introduced to classify either all the MPLS packets or MPLS packets based on EXP values as high priority or low priority for POS, channelized, and clear-channel SPAs.

Usage Guidelines

To classify all the MPLS packets as high priority or low priority for POS, channelized, or clear-channel SPA, use the **mapmplsallqueue**command.

To classify the MPLS packets with specific EXP values, use the **mapmplsexp{exp-value|exp-range}queue{strict-priority|0}** command.

Examples

The following example shows how to classify all the MPLS packets as high priority using the **mapmplsallqueuestrict-priority** command:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map mpls all queue strict-priority
```

The following example shows how to classify the MPLS packets with EXP value of 4 as high priority:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map mpls exp 4 queue strict-priority
```

Related Commands

Command	Description
plim qos input class-map	Attaches the classification template to an interface.

match access-group

To configure the match criteria for a class map on the basis of the specified access control list (ACL), use the **match access-group** command in QoS class-map configuration or policy inline configuration mode. To remove the ACL match criteria from a class map, use the **no** form of this command.

match access-group {*access-group*| **name** *access-group-name*}

no match {*access-group*| **name** *access-group-name*}

Syntax Description

access-group	A numbered ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to the same class. The range is from 1 to 2699.
name *access-group-name*	Specifies a named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to the same class. The name can be up to 40 alphanumeric characters.

Command Default

No match criteria are configured.

Command Modes

QoS class-map configuration (config-cmap)

Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.0(17)SL	This command was modified. This command was enhanced to include matching of access lists on the Cisco 10000 series routers.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.4(6)T	This command was modified. This command was enhanced to support the zone-based policy firewall.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Release	Modification
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

Usage Guidelines

The **match access-group** command specifies a numbered or named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

A traffic rate is generated for packets that match an access group. In zone-based policy firewalls, only the first packet that creates a session matches the configured policy. Subsequent packets in the flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the inspect action.

Zone-based policy firewalls support only the **match access-group**, **match class-map**, and **match protocol** commands. If you specify more than one **match** command in a class map, only the last command that you specified will be applied to the class map. The last **match** command overrides the previously entered **match** commands.

The **match access-group** command specifies the numbered access list against whose contents packets are checked to determine if they match the criteria specified in the class map. Access lists configured with the **log** keyword of the **access-list** command are not supported when you configure the match criteria. For more information about the **access-list** command, refer to the *Cisco IOS IP Application Services Command Reference*.

When this command is configured in Cisco IOS Release 15.0(1)M and later releases, the firewall inspects only Layer 4 policy maps. In releases prior to Cisco IOS Release 15.0(1)M, the firewall inspects both Layer 4 and Layer 7 policy maps.

For class-based weighted fair queueing (CBWFQ), you can define traffic classes based on the match criteria that include ACLs, experimental (EXP) field values, input interfaces, protocols, and quality of service (QoS) labels. Packets that satisfy the match criteria for a class constitute the traffic for that class.

Note In zone-based policy firewalls, this command is not applicable for CBWFQ.

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration modes in which you can issue this command.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

To use the **match access-group** command, you must configure the **service-policy type performance-monitor inline** command.

Supported Platforms Other than Cisco 10000 Series Routers

To use the **match access-group** command, you must configure the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**
- **match protocol**

Cisco 10000 Series Routers

To use the **match access-group** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

Note The **match access-group** command specifies the numbered access list against whose contents packets are checked to determine if they match the criteria specified in the class map. Access lists configured with the **log** keyword of the **access-list** command are not supported when you configure the match criteria.

Cisco ASR 1000 Series Aggregation Services Routers

Cisco ASR 1000 Series Routers do not support more than 16 match statements per class map. An interface with more than 16 match statements rejects the service policy.

Examples

The following example shows how to specify a class map named acl144 and to configure the ACL numbered 144 to be used as the match criterion for that class:

```
Device(config)# class-map acl144
Device(config-cmap)# match access-group 144
```

The following example shows how to define a class map named c1 and configure the ACL numbered 144 to be used as the match criterion for that class:

```
Device(config)# class-map type inspect match-all c1
Device(config-cmap)# match access-group 144
```

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

The following example shows how to configure a service policy for the Performance Monitor in policy inline configuration mode. The policy specifies that packets traversing Ethernet interface 0/0 must match ACL144.

```
Device(config)# interface ethernet 0/0
Device(config-if)# service-policy type performance-monitor inline input
Device(config-if-spolicy-inline)# match access-group name ACL144
Device(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.

Command	Description
access-list (IP standard)	Defines a standard IP access list.
class-map	Creates a class map to be used for matching packets to a specified class.
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
match class-map	Uses a traffic class as a classification policy.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match mpls experimental	Configures a class map to use the specified EXP field value as a match criterion.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.

match application (class-map)

To use the metadata application as a match criterion for control plane classification, use the **match application** command in QoS class-map configuration mode. To remove a previously configured metadata application from being used as a match criterion for control plane classification, use the **no** form of this command.

match application {**application-group** *application-group-name* | **attribute** {**category** {**business-and-productivity-tools**| **voice-and-video**}| **device-class** *device-class-type* | **media-type** *media-type*| **sub-category** {**remote-access-terminal**| **voice-video-chat-collaboration**}}| *application-name* [**source** {**msp** | **nbar** | **rsvp**}| **vendor** *vendor-name* **version** *version-number*]}

no match application {**application-group** *application-group-name* | **attribute** {**category** {**business-and-productivity-tools**| **voice-and-video**}| **device-class** *device-class-type* | **media-type** *media-type*| **sub-category** {**remote-access-terminal**| **voice-video-chat-collaboration**}}| *application-name* [**source** {**msp** | **nbar** | **rsvp**}| **vendor** *vendor-name* **version** *version-number*]}

Syntax Description

application-group *application-group-name*	Specifies the application group that the control plane classification engine must match. Use one of the following values to specify the relevant application group: **telepresence-group**, **vmware-group**, **webex-group**.
attribute	Specifies the relevant attribute to match.
category	Specifies the category type that the control plane classification engine must match.
business-and-productivity-tools	Specifies the business and productivity tools.
voice-and-video	Specifies the voice and video category.
device-class *device-class-type*	Specifies the device class to match. Use one of the following values to specify the relevant device class: **desktop-conferencing**, **desktop-virtualisation**, **physical-phone**, **room-conferencing**, **software-phone**, **surveillance**.
media-type *media-type*	Specifies the type of media to match. Use one of the following values to specify the relevant media type: **audio**, **audio-video control**, **data**, and**video**.
sub-category	Specifies the subcategory to match.
remote-access-terminal	Specifies the remote access terminal subcategory.
voice-video-chat-collaboration	Specifies the voice, video, and collaboration subcategory.

application-name	Name of the application that the control plane classification engine must match. The following applications are supported: **cisco-phone**, **citrix**, **h323**, **jabber**, **rtp**, **rtsp**, **sip**, **telepresence-control**, **telepresence-data**, **telepresence-media**, **vmware-view**, **webex-data**, **webex-meeting**, **webex-streaming**, **webex-video**, **webex-voice**, **wyze-zero-client**.
source	(Optional) Specifies the source of the application.
msp	Specifies the application source as Media-Proxy Services (MSP).
nbar	Specifies the application source as Network Based Application Recognition (NBAR).
rsvp	Specifies the application source as the Resource Reservation Protocol (RSVP).
vendor *vendor-name*	(Optional) Specifies the name of the vendor. Enter ? after the **vendor** keyword to get a list of supported vendors for the respective application name.
version *version-number*	(Optional) Specifies the version number.

Command Default

Metadata-based control plane classification is disabled.

Command Modes

QoS class-map configuration (config-cmap)

Command History

Release	Modification
15.2(1)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.3(1)T	This command was modified. The **source**, **msp**, **nbar**, and **rsvp** keywords were added.

Usage Guidelines

Enabling metadata-based control plane classification on a per-platform, per-line card basis for Quality of Service (QoS) policies involves the following key steps:

- Creating a class map with metadata-based filters.
- Creating a policy map that uses classes.

- Attaching a policy map to the target.

You can use the **match application** command to enable metadata-based filters that can be applied to a class map. Specifying the required application name ensures that the respective policies can be applied only to those flows that match the application name. The classification engine makes its first match.

You can use the **match application** command in conjunction with the any other **match** commands for specifying match criteria for classes. For example, you can use the **match dscp** command along with the **match application** command as the classification criteria for flows.

You can use the **show metadata flow classification table** command to check the metadata-based classification information.

You can use the **debug metadata flow all** command to check if a particular classification has been successfully created.

Note With CSCub24690, the **webex-data**, **webex-streaming**, **webex-video**, and **webex-voice** keywords are not supported in the **match application** *application-name* command.

Examples

The following example shows how to configure a class map c1 and specify metadata application webex-meeting as the matching criterion, thus achieving control plane classification. Only those flows that match the metadata application webex-meeting will be considered for the appropriate action.

```
Device(config)# class-map c1
Device(config-cmap)# match application webex-meeting
```

The following configuration is provided for the completeness of the example.

A policy map p1 that uses the previously configured class c1 is created. The requirement in this example is to provide a guaranteed bandwidth of 1 Mb/s to all the flows that match the criterion defined for class c1:

```
Device(config)# policy-map p1
Device(config-pmap)# class c1
Device(config-pmap-c)# priority 1
```

The following configuration example shows how to attach a policy to a target interface:

```
Device(config)# interface gigabitethernet 0/0
Device(config-if)# service-policy output p1
```

Related Commands

Command	Description
class (policy-map)	Specifies the name of the class whose policy you want to create or change.
class-map	Creates a class map to be used for matching packets to a specified class.
debug metadata	Enables debugging for metadata flow.
metadata application-params	Enters metadata application entry configuration mode and creates new metadata application parameters.

Command	Description
policy-map	Enters policy-map configuration mode and creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
priority	Gives priority to a class of traffic belonging to a policy map.
service-policy	Attaches a policy map to an input interface, a VC, an output interface, or a VC that will be used as the service policy for the interface or VC.
show metadata flow	Displays metadata flow information.

match any

To configure the match criteria for a class map to be successful match criteria for all packets, use the **matchany** command in class-map configuration or policy inline configuration mode. To remove all criteria as successful match criteria, use the **no** form of this command.

match any

no match any

Syntax Description

This command has no arguments or keywords.

Command Default

No match criteria are specified.

Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

Examples

In the following configuration, all packets traversing Ethernet interface 1/1 will be policed based on the parameters specified in policy-map class configuration mode:

```
Router(config)# class-map matchany
Router(config-cmap)# match any
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
set-qos-transmit 4
Router(config-pmap-c)# exit
Router(config)# interface ethernet1/1
Router(config-if)# service-policy output policy1
```

Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that all packets traversing Ethernet interface 0/0 will be matched and monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match any
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.

match atm-clp

To enable packet matching on the basis of the ATM cell loss priority (CLP), use the **matchatm-clp**command in class-map configuration mode. To disable packet matching on the basis of the ATM CLP, use the **no** form of this command.

match atm-clp

no match atm-clp

Syntax Description

This command has no arguments or keywords.

Command Default

Packets are not matched on the basis of the ATM CLP.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SRC	Support for the Cisco 7600 series router was added.
12.4(15)T2	This command was integrated into Cisco IOS Release 12.4(15)T2.
12.2(33)SB	Support for the Cisco 7300 series router was added.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

This command is supported on policy maps that are attached to ATM main interfaces, ATM subinterfaces, or ATM permanent virtual circuits (PVCs). However, policy maps (containing the **matchatm-clp** command) that are attached to these types of ATM interfaces can be *input* policy maps *only* .

This command is supported on the PA-A3 adapter *only* .

Examples

In the following example, a class called “class-c1” has been created using the **class-map** command, and the **matchatm-clp** command has been configured inside that class. Therefore, packets are matched on the basis of the ATM CLP and are placed into this class.

```
Router> enable
Router# configure terminal
```

```
Router(config)# class-map class-c1

Router(config-cmap)# match atm-clp
Router(config-cmap)# end
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
show atm pvc	Displays all ATM PVCs and traffic information.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

match atm oam

To enable the control traffic classification on an ATM interface, use the **matchatmoam**command in class-map configuration mode. To disable the control traffic classification, use the **no** form of this command.

match atm oam

no match atm oam

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.

Usage Guidelines

Use this command for policy maps attached to ATM interfaces or ATM permanent virtual circuits (PVCs). Policy maps containing the **matchatmoam** command attached to ATM interfaces or ATM PVCs can be input policy maps only.

Examples

The following example shows the control traffic classification being configured as the match criterion in a class map. The policy map containing this class map is then applied to the ATM interface.

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# class-map class-oam

Router(config-cmap)# match atm oam

Router(config-cmap)# exit
```

Related Commands

Command	Description
show class-map	Displays all class maps and their matching criteria.
show policy-map	Displays all policy maps.

Command	Description
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified ATM interface or on a specific PVC on the interface.

match atm-vci

To enable packet matching on the basis of the ATM virtual circuit interface (VCI), use the **matchatm-vci**command in class map configuration mode. To disable packet matching on the basis of the ATM VCI, use the**no**form of this command.

match atm-vci *vc-id* [*-vc-id*]

no match atm-vci

Syntax Description

vc-id	The VC number assigned to the virtual circuit between two provider edge routers. You can specify one VC or a range of VCs.
- *vc-id*	(Optional) The second VC number, separated from the first by a hyphen. If two VC numbers are specified, the range is 32 to 65535.

Command Default

No match criteria are configured.

Command Modes

Class map configuration (config-cmap)

Command History

Release	Modification
Cisco IOS XE Release 2.3	This command was introduced.
12.2(33)SRE	This command was modified. This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

When you configure the **matchatm-vci**command in class map configuration mode, you can add this class map to a policy map that can be attached only to an ATM permanent virtual path (PVP).

Note On the Cisco 7600 series router, the **matchatm-vci**command is supported only in the ingress direction on an ATM VP.

You can use the **matchnot** command to match any VC except those you specify in the command.

Examples

The following example enables matching on VC ID 50:

```
Router(config)# class-map map1
Router(config-cmap)# match atm-vci 50
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match not	Specifies a single match criterion value to use as an unsuccessful match criterion.

match class-map

To use a traffic class as a classification policy, use the **match class-map** command in class-map or policy inline configuration mode. To remove a specific traffic class as a match criterion, use the **no** form of this command.

match class-map *class-map-nam e*

no match class-map *class-map-name*

Syntax Description

class-map-name	Name of the traffic class to use as a match criterion.

Command Default

No match criteria are specified.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.4(6)T	This command was enhanced to support Zone-Based Policy Firewall.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was implemented on the Cisco 10000 series.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

The only method of including both match-any and match-all characteristics in a single traffic class is to use the **match class-map** command. To combine match-any and match-all characteristics into a single class, do one of the following:

- Create a traffic class with the match-anyinstruction and use a class configured with the match-all instruction as a match criterion (using the **match class-map** command).

- Create a traffic class with the match-allinstruction and use a class configured with the match-any instruction as a match criterion (using the **match class-map** command).

You can also use the **match class-map** command to nest traffic classes within one another, saving users the overhead of re-creating a new traffic class when most of the information exists in a previously configured traffic class.

When packets are matched to a class map, a traffic rate is generated for these packets. In a zone-based firewall policy, only the first packet that creates a session matches the policy. Subsequent packets in this flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the 'inspect' action.

Examples

Examples

In the following example, the traffic class called class1 has the same characteristics as traffic class called class2, with the exception that traffic class class1 has added a destination address as a match criterion. Rather than configuring traffic class class1 line by line, you can enter the **match class-map class2** command. This command allows all of the characteristics in the traffic class called class2 to be included in the traffic class called class1, and you can simply add the new destination address match criterion without reconfiguring the entire traffic class.

```
Router(config)# class-map match-any class2
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 3
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# class-map match-all class1
Router(config-cmap)# match class-map class2
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# exit
```

The following example shows how to combine the characteristics of two traffic classes, one with match-any and one with match-all characteristics, into one traffic class with the **match class-map** command. The result of traffic class called class4 requires a packet to match one of the following three match criteria to be considered a member of traffic class called class 4: IP protocol *and* QoS group 4, destination MAC address 1.1.1, or access group 2. Match criteria IP protocol *and* QoS group 4 are required in the definition of the traffic class named class3 and included as a possible match in the definition of the traffic class named class4 with the **match class-map class3** command.

In this example, only the traffic class called class4 is used with the service policy called policy1.

```
Router(config)# class-map match-all class3
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 4
Router(config-cmap)# exit
Router(config)# class-map match-any class4
Router(config-cmap)# match class-map class3
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
set-qos-transmit 4
Router(config-pmap-c)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.

match cos

To match a packet on the basis of a Layer 2 class of service (CoS)/Inter-Switch Link (ISL) marking, use the **matchcos** command in class-map configuration or policy inline configuration mode. To remove a specific Layer 2 CoS/ISL marking as a match criterion, use the **no** form of this command.

match cos cos-value [**cos-value** [**cos-value [cos-value**]]]

no match cos cos-value [**cos-value** [**cos-value [cos-value**]]]

Syntax Description

Supported Platforms Other Than the Cisco 10000 Series Routers	
cos-value	Specific IEEE 802.1Q/ISL CoS value. The *cos-value* is from 0 to 7; up to four CoS values, separated by a space, can be specified in one **matchcos** statement.
Cisco 10000 Series Routers	
cos-value	Specific packet CoS bit value. Specifies that the packet CoS bit value must match the specified CoS value. The *cos-value* is from 0 to 7; up to four CoS values, separated by a space, can be specified in one **matchcos** statement.

Command Default

Packets are not matched on the basis of a Layer 2 CoS/ISL marking.

Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.0(25)S	This command was integrated into Cisco IOS Release 12.0(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC and support for the Cisco 7600 series routers was added.
12.4(15)T2	This command was integrated into Cisco IOS Release 12.4(15)T2.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB and support for the Cisco 7300 series router was added.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.
3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the **service-policytypeperformance-monitorinline**command.

Examples

In the following example, the CoS values of 1, 2, and 3 are successful match criteria for the interface that contains the classification policy named cos:

```
Router(config)# class-map cos
Router(config-cmap)# match cos 1 2 3
```

In the following example, classes named voice and video-n-data are created to classify traffic based on the CoS values. QoS treatment is then given to the appropriate packets in the CoS-based-treatment policy map (in this case, the QoS treatment is priority 64 and bandwidth 512). The service policy configured in this example is attached to all packets leaving Fast Ethernet interface 0/0.1. The service policy can be attached to any interface that supports service policies.

```
Router(config)# class-map voice
Router(config-cmap)# match cos 7
Router(config)# class-map video-n-data
Router(config-cmap)# match cos 5
Router(config)# policy-map cos-based-treatment
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 64
Router(config-pmap-c)# exit
Router(config-pmap)# class video-n-data
Router(config-pmap-c)# bandwidth 512
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet0/0.1
Router(config-if)# service-policy output cos-based-treatment
```

Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria of a CoS value of 2 will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match cos 2
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Examples

The following example shows how to match traffic classes for the 802.1p domain with packet CoS values:

```
Router> enable
Router# config terminal
Router(config)# class-map cos7
Router(config-cmap)# match cos 2
Router(config-cmap)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set cos	Sets the Layer 2 CoS value of an outgoing packet.
show class-map	Displays all class maps and their matching criteria.

match cos inner

To match the inner cos of QinQ packets on a Layer 2 class of service (CoS) marking, use the **matchcosinner**command in class-map configuration mode. To remove a specific Layer 2 CoS inner tag marking, use the **no** form of this command.

match cos cos-value

no match cos cos-value

Syntax Description

cos-value	Specific IEEE 802.1Q/ISL CoS value. The *cos-value* is from 0 to 7; up to four CoS values can be specified in one **matchcos** statement.

Command Default

No match criteria are specified.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Examples

In the following example, the inner CoS-values of 1, 2, and 3 are successful match criteria for the interface that contains the classification policy called cos:

```
Router(config)# class-map cos
```

```
Router(config-cmap)# match cos inner 1 2 3
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

Command	Description
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set cos	Sets the Layer 2 CoS value of an outgoing packet.
show class-map	Displays all class maps and their matching criteria.

match destination-address mac

To use the destination MAC address as a match criterion, use the **matchdestination-addressmac**command in class-map configuration or policy inline configuration mode. To remove a previously specified destination MAC address as a match criterion, use the **no**form of this command.

match destination-address mac *address*

no match destination-address mac *address*

Syntax Description

address	Destination MAC address to be used as a match criterion.

Command Default

No destination MAC address is specified.

Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

Examples

The following example specifies a class map named macaddress and specifies the destination MAC address to be used as the match criterion for this class:

```
Router(config)# class-map macaddress
Router(config-cmap)# match destination-address mac 00:00:00:00:00:00
```

Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the specified destination MAC address will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match
destination-address mac 00:00:00:00:00:00
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.

match discard-class

To specify a discard class as a match criterion, use the **matchdiscard-class** command in class-map configuration or policy inline configuration mode. To remove a previously specified discard class as a match criterion, use the **no** form of this command.

match discard-class *class-number*

no match discard-class *class-number*

Syntax Description

class-number	Number of the discard class being matched. Valid values are 0 to 7.

Command Default

Packets will not be classified as expected.

Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

A discard-class value has no mathematical significance. For example, the discard-class value 2 is not greater than 1. The value simply indicates that a packet marked with discard-class 2 should be treated differently than a packet marked with discard-class 1.

Packets that match the specified discard-class value are treated differently from packets marked with other discard-class values. The discard-class is a matching criterion only, used in defining per hop behavior (PHB) for dropping traffic.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

Examples

The following example shows that packets in discard class 2 are matched:

```
Router(config)# class-map d-class-2
Router(config-cmap)# match discard-class 2
```

Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria specified by discard-class 2 will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match
discard-class 2
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
set discard-class	Marks a packet with a discard-class value.

match dscp

To identify one or more differentiated service code point (DSCP), Assured Forwarding (AF), and Certificate Server (CS) values as a match criterion, use the **match dscp** command in class-map configuration or policy inline configuration mode. To remove a specific DSCP value from a class map, use the **no** form of this command.

match [ip] dscp *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value*]

no match [ip] dscp *dscp-value*

Syntax Description

ip	(Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets. **Note** For the Cisco 10000 series routers, the **ip** keyword is required.
dscp-value	The DSCP value used to identify a DSCP value. For valid values, see the “Usage Guidelines” section.

Command Default

No match criteria are configured.

Command Modes

class-map configuration (config-cmap) policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.2(13)T	This command was introduced. This command replaces the **match ip dscp** command.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S for support in IPv6.
12.0(17)SL	This command was integrated into Cisco IOS Release 12.0(17)SL and implemented on the Cisco 10000 series routers.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 Series Routers.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.

Release	Modification
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the **service-policy type performance-monitor inline** command.

DSCP Values

You must enter one or more differentiated service code point (DSCP) values. The command may include any combination of the following:

- Numbers (0 to 63) representing differentiated services code point values
- AF numbers (for example, af11) identifying specific AF DSCPs
- CS numbers (for example, cs1) identifying specific CS DSCPs
- **default—**Matches packets with the default DSCP.
- **ef—**Matches packets with EF DSCP.

For example, if you wanted the DCSP values of 0, 1, 2, 3, 4, 5, 6, or 7 (note that only one of the IP DSCP values must be a successful match criterion, not all of the specified DSCP values), enter the **match dscp 01234567** command.

This command is used by the class map to identify a specific DSCP value marking on a packet. In this context, *dscp-value* arguments are used as markings only and have no mathematical significance. For instance, the *dscp-value* of 2 is not greater than 1. The value simply indicates that a packet marked with the *dscp-value* of 2 is different than a packet marked with the *dscp-value* of 1. The treatment of these marked packets is defined by the user through the setting of Quality of Service (QoS) policies in policy-map class configuration mode.

Match Packets on DSCP Values

To match DSCP values for IPv6 packets only, the **match protocol ipv6** command must also be used. Without that command, the DSCP match defaults to match both IPv4 and IPv6 packets.

To match DSCP values for IPv4 packets only, use the **ip** keyword. Without the **ip** keyword the match occurs on both IPv4 and IPv6 packets. Alternatively, the **match protocol ip** command may be used with **match dscp** to classify only IPv4 packets.

After the DSCP bit is set, other QoS features can then operate on the bit settings.

The network can give priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain); data is then queued according to the precedence. Weighted fair queueing (WFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Random Early Detection (WRED) can ensure that high-precedence traffic has lower loss rates than other traffic during times of congestion.

Cisco 10000 Series Routers

The Cisco 10000 series routers support DSCP matching of IPv4 packets only. You must include the ip keyword when specifying the DSCP values to use as match criterion.

You cannot use the set ip dscp command with the set ip precedence command to mark the same packet. DSCP and precedence values are mutually exclusive. A packet can have one value or the other, but not both.

Examples

The following example shows how to set multiple match criteria. In this case, two IP DSCP values and one AF value.

```
Router(config)# class-map map1
Router(config-cmap)# match dscp 1 2 af11
```

Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criterion specified by DSCP value 2 will be monitored based on the parameters specified in the flow monitor configuration named fm-2:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match dscp 2
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# end
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match protocol ip	Matches DSCP values for packets.
match protocol ipv6	Matches DSCP values for IPv6 packets.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
set dscp	Marks the DSCP value for packets within a traffic class.
show class-map	Displays all class maps and their matching criteria.

match field

Note Effective with Cisco IOS Release 15.2(4)M, the **match field** command is not available in Cisco IOS software.

To configure the match criteria for a class map on the basis of the fields defined in the protocol header description files (PHDFs), use the **match field** command in class-map configuration mode. To remove the specified match criteria, use the **no** form of this command.

match field *protocol protocol-field* {**eq [mask]**| **neq [mask]**| **gt**| **lt**| **range** *range*| **regex** *string*} *value* [**next** *next-protocol*]

no match field *protocol protocol-field* {**eq [mask]**| **neq [mask]**| **gt**| **lt**| **range** *range*| **regex** *string*} *value* [**next** *next-protocol*]

Syntax Description

protocol	Name of protocol whose PHDF has been loaded onto a router.
protocol field	*Match criteria is based upon the specified f*ield *within the loaded protocol.*
eq	*Match criteria is met if the* packet is equal to the specified value or mask.
neq	*Match criteria is met if the* packet is not equal to the specified value or mask.
mask *mask*	(Optional) Can be used when the **eq** or the **neq** keywords are issued.
gt	*Match criteria is met if the* packet does not exceed the specified value.
lt	*Match criteria is met if the* packet is less than the specified value.
range *range*	Match criteria is based upon a lower and upper boundary protocol field range.
regex *string*	Match criteria is based upon a string that is to be matched.
value	Value for which the packet must be in accordance with.

next *next-protocol*	Specify the next protocol within the stack of protocols that is to be used as the match criteria.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).
Cisco IOS XE 2.2	This command was integrated into Cisco IOS XE Release 2.2.
15.2(4)M	This command was removed from the Cisco IOS software.

Usage Guidelines

Before issuing the **match-field** command, you must load a PHDF onto the router via the **load protocol** command. Thereafter, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

Match criteria are defined via a start point, offset, size, value to match, and mask. A match can be defined on a pattern with any protocol field.

Examples

The following example shows how to configure FPM for blaster packets. The class map contains the following match criteria: TCP port 135, 4444 or UDP port 69; and pattern 0x0030 at 3 bytes from start of IP header.

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf
class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp
class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp
class-map type access-control match-all blaster1
 match field tcp dest-port eq 135
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster3
 match field udp dest-port eq 69
 match start 13-start offset 3 size 2 eq 0x0030
policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
 drop
```

```
policy-map type access-control fpm-udp-policy
 class blaster3
 drop
policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
 service-policy fpm-udp-policy
interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
load protocol	Loads a PHDF onto a router.
match start	Configures the match criteria for a class map on the basis of the datagram header (Layer 2) or the network header (Layer 3).

match flow pdp

To specify a Packet Data Protocol (PDP) flow as a match criterion in a class map, use the **matchflowpdp** command in class-map configuration mode. To remove a PDP flow as a match criterion, use the **no** form of this command.

match flow pdp

no match flow pdp

Syntax Description

This command has no arguments or keywords.

Command Default

A PDP flow is not specified as a match criterion.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

The **matchflowpdp** command allows you to match and classify traffic on the basis of a PDP flow.

The **matchflowpdp** command is included with the Flow-Based QoS for GGSN feature available with Cisco IOS Release 12.4(9)T. The Flow-Based QoS for GGSN feature is designed specifically for the Gateway General Packet Radio Service (GPRS) Support Node (GGSN).

Per-PDP Policing

The Flow-Based QoS for GGSN feature includes per-PDP policing (session-based policing).

The **matchflowpdp** command (when used in conjunction with the **class-map** command, the **policy-map** command, the **policeratepdp** command, and the **service-policy** command) allows you to configure per-PDP policing (session-based policing) for downlink traffic on a GGSN.

Note the following points related to per-PDP policing:

- When using the **class-map** command to define a class map for PDP flow classification, do not use the **match-any**keyword.
- Per-PDP policing functionality requires that you configure Universal Mobile Telecommunications System (UMTS) quality of service (QoS). For information on configuring UMTS QoS, see the "Configuring QoS on the GGSN" section of the Cisco GGSN Release 6.0 Configuration Guide , Cisco IOS Release 12.4(2)XB.
- The policy map created to configure per-PDP policing cannot contain multiple classes within which only the **matchflowpdp** command has been specified. In other words, if there are multiple classes in the policy map, the **matchflowpdp**command must be used in conjunction with another match statement (for example, **matchprecedence**) in at least one class.

For More Information

For more information about the GGSN, along with the instructions for configuring the Flow-Based QoS for GGSN feature, see the Cisco GGSN Release 6.0 Configuration Guide , Cisco IOS Release 12.4(2)XB.

Note To configure the Flow-Based QoS for GGSN feature, follow the instructions in the section called " Configuring Per-PDP Policing ."

For more information about the GGSN-specific commands, see the Cisco GGSN Release 6.0 Command Reference , Cisco IOS Release 12.4(2)XB.

Examples

The following example specifies PDP flows as the match criterion in a class map named "class-pdp":

```
class-map class-pdp
 match flow pdp
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match precedence	Identifies IP precedence values as match criteria.
police rate pdp	Configures PDP traffic policing using the police rate.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an interface.

match fr-dlci

To specify the Frame Relay data-link connection identifier (DLCI) number as a match criterion in a class map, use the **matchfr-dlci**command in class-map configuration or policy inline configuration mode. To remove a previously specified DLCI number as a match criterion, use the **no** form of this command.

match fr-dlci *dlci-number*

no match fr-dlci *dlci-number*

Syntax Description

dlci-number	Number of the DLCI associated with the packet.

Command Default

No DLCI number is specified.

Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

This match criterion can be used in main interfaces and point-to-multipoint subinterfaces in Frame Relay networks, and it can also be used in hierarchical policy maps.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

Examples

In the following example a class map named “class1” has been created and the Frame Relay DLCI number of 500 has been specified as a match criterion. Packets matching this criterion are placed in class1.

```
Router(config)# class-map class1
Router(config-cmap)# match fr-dlci 500
```

Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the Frame Relay DLCI number of 500 will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match
fr-dlci 500
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
show class-map	Displays all class maps and their matching criteria.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

match input vlan

To configure a class map to match incoming packets that have a specific virtual local area network (VLAN) ID, use the **matchinputvlan**command in class map configuration mode. To remove the matching of VLAN IDs, use the **no** form of this command.

match input vlan *input-vlan-list*

no match input vlan *input-vlan-list*

Syntax Description

input-vlan-list	One or more VLAN IDs to be matched. The valid range for VLAN IDs is from 1 to 4094, and the list of VLAN IDs can include one or all of the following: • Single VLAN IDs, separated by spaces. For example: 100 200 300 • One or more ranges of VLAN IDs, separated by spaces. For example: 1-1024 2000-2499

Command Default

By default, no matching is done on VLAN IDs.

Command Modes

Class map configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced for Cisco Catalyst 6500 series switches and Cisco 7600 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **matchinputvlan** command allows you to create a class map that matches packets with one or more specific VLAN IDs, as they were received on the input (ingress) interface. This enables hierarchical Quality of Service (HQoS) for Ethernet over MPLS (EoMPLS) Virtual Circuits (VC), allowing parent and child relationships between QoS class maps and policy maps. This in turn enables service providers to easily classify and shape traffic for a particular EoMPLS network.

In EoMPLS applications, the parent class map typically specifies the maximum bandwidth for all of the VCs in a specific EoMPLS network. Then the child class maps perform other QoS operations, such as traffic shaping, on a subset of this traffic.

Do not confuse the **matchinputvlan** command with the **matchvlan** command, which is also a class-map configuration command.

- The **matchvlan** command matches the VLAN ID on packets for the particular interface at which the policy map is applied. Policy maps using the **matchvlan** command can be applied to either ingress or egress interfaces on the router, using the **service-policy** {**input** | **output**} command.
- The **matchinputvlan** command matches the VLAN ID that was on packets when they were received on the ingress interface on the router. Typically, policy maps using the **matchinputvlan** command are applied to egress interfaces on the router, using the **service-policyoutput** command.

The **matchinputvlan** command can also be confused with the **matchinput-interfacevlan** command, which matches packets being received on a logical VLAN interface that is used for inter-VLAN routing.

Tip Because class maps also support the **matchinput-interface** command, you cannot abbreviate the **input** keyword when giving the **matchinputvlan** command.

Note The **matchinputvlan** command cannot be used only on Layer 2 LAN ports on FlexWAN, Enhanced FlexWAN, and Optical Service Modules (OSM) line cards.

The following restrictions apply when using the **matchinputvlan** command:

- You cannot attach a policy with **matchinputvlan** to an interface if you have already attached a service policy to a VLAN interface (a logical interface that has been created with the **interfacevlan** command).
- Class maps that use the **matchinputvlan** command support only the **match-any** option. You cannot use the **match-all** option in class maps that use the **matchinputvlan** command.
- If the parent class contains a class map with a **matchinputvlan** command, you cannot use a **matchexp** command in a child class map.

Examples

The following example creates a class map and policy map that matches packets with a VLAN ID of 1000. The policy map shapes this traffic to a committed information rate (CIR) value of 10 Mbps (10,000,000 bps). The final lines then apply this policy map to a specific gigabit Ethernet WAN interface.

```
Router# configure terminal
Router(config)# class-map match-any vlan1000
Router(config-cmap)# match input vlan 1000
Router(config-cmap)# exit
Router(config)# policy-map policy1000
Router(config-pmap)# class vlan1000
Router(config-pmap-c)# exit
Router(config-pmap)# shape average 10000000
Router(config-pmap)# interface GE-WAN 3/0
Router(config-if)# service-policy output policy1000
Router(config-if)#
```

The following example shows a class map being configured to match VLAN IDs 100, 200, and 300:

```
Router# configure terminal

Router(config)# class-map match-any hundreds

Router(config-cmap)# match input vlan 100 200 300

Router(config-cmap)#
```

The following example shows a class map being configured to match all VLAN IDs from 2000 to 2999 inclusive:

```
Router# configure terminal

Router(config)# class-map match-any vlan2000s

Router(config-cmap)# match input vlan 2000-2999

Router(config-cmap)#
```

The following example shows a class map being configured to match both a range of VLAN IDs, as well as specific VLAN IDs:

```
Router# configure terminal

Router(config)# class-map match-any misc

Router(config-cmap)# match input vlan 1 5 10-99 2000-2499

Router(config-cmap)#
```

Related Commands

Command	Description
clear cef linecard	Clears Cisco Express Forwarding (CEF) information on one or more line cards, but does not clear the CEF information on the main route processor (RP). This forces the line cards to synchronize their CEF information with the information that is on the RP.
match qos-group	Identifies a specified QoS group value as a match criterion.
mls qos trust	Sets the trusted state of an interface, to determine which incoming QoS field on a packet, if any, should be preserved.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.

Command	Description
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.
show platform qos policy-map	Displays the type and number of policy maps that are configured on the router.

match input-interface

To configure a class map to use the specified input interface as a match criterion, use the **match input-interface** command in class-map configuration or policy inline configuration mode. To remove the input interface match criterion from a class map, use the **no** form of this command.

match input-interface *interface-name*

no match input-interface *interface-name*

Syntax Description

interface-name	Name of the input interface to be used as match criteria.

Command Default

No match criteria are specified.

Command Modes

Class-map configuration (config-cmap)

Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.0(17)SL	This command was enhanced to include matching on the input interface.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

Note With CSCtx62310, the minimum string you must enter to uniquely identify this command is **match input-**. The device no longer accepts **match input** as an abbreviated version of this command.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

To enter policy inline configuration mode, you must first enter the **service-policy type performance-monitor inline** command.

Supported Platforms Other Than Cisco 10000 Series Routers

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria including input interfaces, access control lists (ACLs), protocols, quality of service (QoS) labels, and experimental (EXP) field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match input-interface** command specifies the name of an input interface to be used as the match criterion against which packets are checked to determine if they belong to the class specified by the class map.

To use the **match input-interface** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**
- **match protocol**

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

Cisco 10000 Series Routers

For CBWFQ, you define traffic classes based on match criteria including input interfaces, ACLs, protocols, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

To use the **match input-interface** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

Examples

The following example specifies a class map named ethernet1 and configures the input interface named ethernet1 to be used as the match criterion for this class:

```
Router(config)# class-map ethernet1
Router(config-cmap)# match input-interface ethernet1
```

Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria of the input interface named ethernet1 will be monitored based on the parameters specified in the flow monitor configuration named fm-2:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match input-interface ethernet 1
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match access-group	Configures the match criteria for a class map based on the specified ACL.
match mpls experimental	Configures a class map to use the specified EXP field value as a match criterion.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.

match ip dscp

The **matchipdscp**command is replaced by the match dscpcommand. See the match dscpcommand for more information.

match ip precedence

The **matchipprecedence**command is replaced by the match precedencecommand. See the match precedencecommand for more information.

match ip rtp

To configure a class map to use the Real-Time Protocol (RTP) port as the match criterion, use the **matchiprtp**command in class-map configuration or policy inline configuration mode. To remove the RTP port match criterion, use the **no** form of this command.

match ip rtp *starting-port-number port-range*

no match ip rtp

Syntax Description

starting-port-number	The starting RTP port number. Values range from 2000 to 65535.
port-range	The RTP port number range. Values range from 0 to 16383.

Command Default

No match criteria are specified.

Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

This command is used to match IP RTP packets that fall within the specified port range. It matches packets destined to all even User Datagram Port (UDP) port numbers in the range from the *starting port number* argument to the *starting port number* plus the *port range* argument.

Use of an RTP port range as the match criterion is particularly effective for applications that use RTP, such as voice or video.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

Examples

The following example specifies a class map named ethernet1 and configures the RTP port number 2024 and range 1000 to be used as the match criteria for this class:

```
Router(config)# class-map ethernet1
Router(config-cmap)# match ip rtp 2024 1000
```

Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria of RTP port number 2024 and range 1000 will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match
ip rtp 2024 1000
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
ip rtp priority	Reserves a strict priority queue for a set of RTP packet flows belonging to a range of UDP destination ports.
match access-group	Configures the match criteria for a class map based on the specified ACL number.

match mpls experimental

To configure a class map to use the specified value or values of the experimental (EXP) field as a match criteria, use the **matchmplsexperimental**command in class-map configuration mode. To remove the EXP field match criteria from a class map, use the **no** form of this command.

match mpls experimental *number*

no match mpls experimental *number*

Syntax Description

number	EXP field value (any number from 0 through 7) to be used as a match criterion. You can specify multiple values, separated by a space (for example, 3 4 7).

Command Default

No match criteria are specified.

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(7)XE1	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco MGX 8850 switch and the MGX 8950 switch with a Cisco MGX RPM-PR card.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Supported Platforms Other Than the Cisco 10000 Series

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria such as input interfaces, access control lists (ACLs), protocols, quality of service (QoS) labels, and experimental (EXP) field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **matchmplsexperimental** command specifies the name of an EXP field value to be used as the match criterion against which packets are compared to determine if they belong to the class specified by the class map.

To use the **matchmplsexperimental** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**
- **match protocol**

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

Cisco 10000 Series

This command is available only on the ESR-PRE1 module.

For CBWFQ, you define traffic classes based on match criteria such as input interfaces, ACLs, protocols, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

To use the **matchmplsexperimental** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

Examples

The following example specifies a class map called ethernet1 and configures the Multiprotocol Label Switching (MPLS) experimental values of 1 and 2 to be used as the match criteria for this class:

```
Router(config)# class-map ethernet1
Router(config-cmap)# match mpls experimental 1 2
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match access-group	Configures the match criteria for a class map based on the specified ACL.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match mpls experimental topmost	Matches the EXP value in the topmost label.
match protocol	Matches traffic by a particular protocol.

Command	Description
match qos-group	Configures the match criteria for a class map based on the specified protocol.

match mpls experimental topmost

To match the experimental (EXP) value in the topmost label header, use the **matchmplsexperimentaltopmost**command in class-map configuration or policy inline configuration mode. To remove the EXP match criterion, use the no form of this command.

match mpls experimental topmost number

no match mpls experimental topmost number

Syntax Description

number	Multiprotocol Label Switching (MPLS) EXP field in the topmost label header. Valid values are 0 to 7.

Command Default

No EXP match criterion is configured for the topmost label header.

Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

You can enter this command on the input interfaces and the output interfaces. It will match only on MPLS packets.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the **service-policytypeperformance-monitorinline**command.

Examples

The following example shows that the EXP value 3 in the topmost label header is matched:

```
Router(config)# class-map mpls exp
Router(config-cmap)# match mpls experimental topmost 3
```

Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria of a EXP value of 3 in the topmost label header will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match mpls experimental topmost 3
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
set mpls experimental topmost	Sets the MPLS EXP field value in the topmost MPLS label header at the input or output interfaces.

match not

To specify the single match criterion value to use as an unsuccessful match criterion, use the **matchnot**command inclass-map configuration or policy inline configuration mode. To remove a previously specified source value to not use as a match criterion, use the **no**form of this command.

match not *match-criterion*

no match not *match-criterion*

Syntax Description

match-criterion	The match criterion value that is an unsuccessful match criterion. All other values of the specified match criterion will be considered successful match criteria.

Command Default

No unsuccessful match criterion is configured.

Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

The **matchnot**command is used to specify a quality of service (QoS) policy value that is not used as a match criterion. When the**matchnot** command is used, all other values of that QoS policy become successful match criteria.

For instance, if the **matchnotqos-group4** command is issued in QoS class-map configuration mode, the specified class will accept all QoS group values except 4 as successful match criteria.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

Examples

In the following traffic class, all protocols except IP are considered successful match criteria:

```
Router(config)# class-map noip
Router(config-cmap)# match not protocol ip
```

Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 for all protocols except IP will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match not protocol ip
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.

match packet length (class-map)

To specify the Layer 3 packet length in the IP header as a match criterion in a class map, use the **matchpacketlength** command in class-map configuration or policy inline configuration mode. To remove a previously specified Layer 3 packet length as a match criterion, use the **no** form of this command.

match packet length {**max** *maximum-length-value* [**min** *minimum-length-value*]| **min** *minimum-length-value* [**max** *maximum-length-value*]}

no match packet length {**max** *maximum-length-value* [**min** *minimum-length-value*]| **min** *minimum-length-value* [**max** *maximum-length-value*]}

Syntax Description

max	Indicates that a maximum value for the Layer 3 packet length is to be specified.
maximum-length-value	Maximum length value of the Layer 3 packet length, in bytes. The range is from 1 to 2000.
min	Indicates that a minimum value for the Layer 3 packet length is to be specified.
minimum-length-value	Minimum length value of the Layer 3 packet length, in bytes. The range is from 1 to 2000.

Command Default

The Layer 3 packet length in the IP header is not used as a match criterion.

Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2 and implemented on the Cisco ASR 1000 Series Routers.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.

Release	Modification
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

This command considers only the Layer 3 packet length in the IP header. It does not consider the Layer 2 packet length in the IP header.

When using this command, you must at least specify the maximum or minimum value. However, you do have the option of entering both values.

If only the minimum value is specified, a packet with a Layer 3 length greater than the minimum is viewed as matching the criterion.

If only the maximum value is specified, a packet with a Layer 3 length less than the maximum is viewed as matching the criterion.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

Examples

In the following example a class map named “class 1” has been created, and the Layer 3 packet length has been specified as a match criterion. In this example, packets with a minimum Layer 3 packet length of 100 bytes and a maximum Layer 3 packet length of 300 bytes are viewed as meeting the match criteria.

```
Router(config)# class-map match-all class1
Router(config-cmap)# match packet length min 100 max 300
```

Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria of a minimum Layer 3 packet length of 100 bytes and a maximum Layer 3 packet length of 300 bytes will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match packet length min 100 max 300
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
show class-map	Displays all class maps and their matching criteria.

Command	Description
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

match port-type

To match the access policy on the basis of the port for a class map, use the **matchport-type** command in class-map configuration mode. To delete the port type, use the **no** form of this command.

match port-type {**routed**| **switched**}

no match port-type {**routed**| **switched**}

Syntax Description

routed	Matches the routed interface. Use this keyword if the class map has to be associated with only a routed interface.
switched	Matches the switched interface. Use this keyword if the class map has to be associated with only a switched interface.

Command Default

Access policy is not matched.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used because, on the basis of the port on which a user is connecting, the access policies that are applied to it can be different.

Examples

The following example shows that an access policy has been matched on the basis of the port for a class map:

```
Router(config-cmap)# matchport-typerouted
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match tag (class-map)	Specifies the tag to be matched for a tag type of class map.

match precedence

To identify IP precedence values to use as the match criterion, use the **matchprecedence** command in class-map configuration or policy inline configuration mode. To remove IP precedence values from a class map, use the **no** form of this command.

match [ip] precedence {*precedence-criteria1*| *precedence-criteria2*| *precedence-criteria3*| *precedence-criteria4*}

no match [ip] precedence {*precedence-criteria1*| *precedence-criteria2*| *precedence-criteria3*| *precedence-criteria4*}

Syntax Description

ip	(Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets. **Note** For the Cisco 10000 series routers, the **ip** keyword is required.
precedence-criteria1 *precedence-criteria2* *precedence-criteria3* *precedence-criteria4*	Identifies the precedence value. You can enter up to four different values, separated by a space. See the "Usage Guidelines" section for valid values.

Command Default

No match criterion is configured.

Command Modes

class-map configuration (config-cmap) policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.2(13)T	This command was introduced. This command replaces the **matchipprecedence** command.
12.0(17)SL	This command was integrated into Cisco IOS Release 12.0(17)SL and implemented on the Cisco 10000 series routers.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S for IPv6.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.

Release	Modification
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.
Cisco IOS XE Release 3.6	This command was implemented on the Cisco ASR 903 Router.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

You can enter up to four matching criteria, a number abbreviation (0 to 7) or criteria names (critical, flash, and so on), in a single match statement. For example, if you wanted the precedence values of 0, 1, 2, or 3 (note that only one of the precedence values must be a successful match criterion, not all of the specified precedence values), enter the **matchipprecedence0123**command. The *precedence-criteria* numbers are not mathematically significant; that is, the *precedence-criteria* of 2 is not greater than 1. The way that these different packets are treated depends upon quality of service (QoS) policies, set in policy-map configuration mode.

You can configure a QoS policy to include IP precedence marking for packets entering the network. Devices within your network can then use the newly marked IP precedence values to determine how to treat the packets. For example, class-based weighted random early detection (WRED) uses IP precedence values to determine the probability that a packet is dropped. You can also mark voice packets with a particular precedence. You can then configure low-latency queueing (LLQ) to place all packets of that precedence into the priority queue.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the **service-policytypeperformance-monitorinline** command.

Matching Precedence for IPv6 and IPv4 Packets on the Cisco 7600 and 10000 and Series Routers

On the Cisco 7600 series and 10000 series routers, you set matching criteria based on precedence values for only IPv6 packets using the **matchprotocol**command with the **ipv6** keyword. Without that keyword, the precedence match defaults to match both IPv4 and IPv6 packets. You set matching criteria based on precedence values for IPv4 packets only using the **ip** keyword. Without the **ip** keyword the match occurs on both IPv4 and IPv6 packets.

Precedence Values and Names

The following table lists all criteria conditions by value, name, binary value, and recommended use. You may enter up to four criteria, each separated by a space. Only one of the precedence values must be a successful match criterion. The table below lists the IP precedence values.

Table 1: IP Precedence Values

Precedence Value	Precedence Name	Binary Value	Recommended Use
0	routine	000	Default marking value
1	priority	001	Data applications
2	immediate	010	Data applications
3	flash	011	Call signaling

Precedence Value	Precedence Name	Binary Value	Recommended Use
4	flash-override	100	Video conferencing and streaming video
5	critical	101	Voice
6	internet (control)	110	Network control traffic (such as routing, which is typically precedence 6)
7	network (control)	111	

Do not use IP precedence 6 or 7 to mark packets, unless you are marking control packets.

Examples

Examples

The following example shows how to configure the service policy named priority50 and attach service policy priority50 to an interface, matching for IPv4 traffic only. In a network where both IPv4 and IPv6 are running, you might find it necessary to distinguish between the protocols for matching and traffic segregation. In this example, the class map named ipprec5 will evaluate all IPv4 packets entering Fast Ethernet interface 1/0/0 for a precedence value of 5. If the incoming IPv4 packet has been marked with the precedence value of 5, the packet will be treated as priority traffic and will be allocated with bandwidth of 50 kbps.

```
Router(config)# class-map ipprec5
Router(config-cmap)# match ip precedence 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipprec5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority50
```

Examples

The following example shows the same service policy matching on precedence for IPv6 traffic only. Notice that the **match protocol** command with the **ipv6** keyword precedes the **match precedence** command. The **match protocol** command is required to perform matches on IPv6 traffic alone.

```
Router(config)# class-map ipprec5
Router(config-cmap)# match protocol ipv6
Router(config-cmap)# match precedence 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipprec5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority50
```

Examples

The following example shows how to use policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criterion of a match precedence of 4 will be monitored based on the parameters specified in the flow monitor configuration named fm-2:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match precedence 4
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# end
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match protocol	Configures the match criteria for a class map on the basis of a specified protocol.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
set ip precedence	Sets the precedence value in the IP header.
show class-map	Displays all class maps and their matching criteria, or a specified class map and its matching criteria.

match protocol

To configure the match criterion for a class map on the basis of a specified protocol, use the **matchprotocol** command in class-map configuration or policy inline configuration mode. To remove the protocol-based match criterion from the class map, use the **no** form of this command.

match protocol *protocol-name*

no match protocol *protocol-name*

Syntax Description

protocol-name	Name of the protocol (for example, bgp) used as a matching criterion. See the "Usage Guidelines" for a list of protocols supported by most routers.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(13)E	This command was integrated into Cisco IOS Release 12.1(13)E and implemented on Catalyst 6000 family switches without FlexWAN modules.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(13)T	This command was modified to remove **apollo**, **vines**, and **xns** from the list of protocols used as matching criteria. These protocols were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems (XNS) were removed in this release. The IPv6 protocol was added to support matching on IPv6 packets.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S for IPv6.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.

Release	Modification
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE and implemented on the Supervisor Engine 720.
12.4(6)T	This command was modified. The Napster protocol was removed because it is no longer supported.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2 and implemented on the Cisco 10000 series routers.
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY. This command was modified to enhance Network-Based Application Recognition (NBAR) functionality on the Catalyst 6500 series switch that is equipped with the Supervisor 32/programmable intelligent services accelerator (PISA) engine.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T and implemented on the Cisco 1700, Cisco 1800, Cisco 2600, Cisco 2800, Cisco 3700, Cisco 3800, Cisco 7200, and Cisco 7300 series routers.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2 and implemented on the Cisco ASR 1000 Series Routers.
Cisco IOS XE Release 3.1S	This command was modified. Support for more protocols was added.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

Supported Platforms Other Than Cisco 7600 Routers and Cisco 10000 Series Routers

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria protocols, access control lists (ACLs), input interfaces, quality of service (QoS) labels, and Experimental (EXP) field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **matchprotocol** command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

The **matchprotocolipx** command matches packets in the output direction only.

To use the **matchprotocol** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

To configure NBAR to match protocol types that are supported by NBAR traffic, use the **matchprotocol(NBAR)**command.

Cisco 7600 Series Routers

The **matchprotocol** command in QoS class-map configuration configures NBAR and sends all traffic on the port, both ingress and egress, to be processed in the software on the Multilayer Switch Feature Card 2 (MSFC2).

For CBWFQ, you define traffic classes based on match criteria like protocols, ACLs, input interfaces, QoS labels, and Multiprotocol Label Switching (MPLS) EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **matchprotocol**command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

If you want to use the **matchprotocol**command, you must first enter the **class-map** command to specify the name of the class to which you want to establish the match criteria.

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

This command can be used to match protocols that are known to the NBAR feature. For a list of protocols supported by NBAR, see the "Classification" part of the *Cisco IOS Quality of Service Solutions Configuration Guid*e.

Cisco 10000 Series Routers

For CBWFQ, you define traffic classes based on match criteria including protocols, ACLs, input interfaces, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **matchprotocol** command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

The **matchprotocolipx** command matches packets in the output direction only.

To use the **matchprotocol** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

If you are matching NBAR protocols, use the **matchprotocol**(NBAR) command.

Match Protocol Command Restrictions (Catalyst 6500 Series Switches Only)

Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) on the basis of a protocol type or application. You can create as many traffic classes as needed.

Cisco IOS Release 12.2(18)ZY includes software intended for use on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine. For this release and platform, note the following restrictions for using policy maps and **matchprotocol** commands:

- A single traffic class can be configured to match a maximum of 8 protocols or applications.
- Multiple traffic classes can be configured to match a cumulative maximum of 95 protocols or applications.

Supported Protocols

The table below lists the protocols supported by most routers. Some routers support a few additional protocols. For example, the Cisco 7600 router supports the AARP and DECnet protocols, while the Cisco 7200 router supports the directconnect and PPPOE protocols. For a complete list of supported protocols, see the online help for the **matchprotocol** command on the router that you are using.

Table 2: Supported Protocols

Protocol Name	Description
802-11-iapp	IEEE 802.11 Wireless Local Area Networks Working Group Internet Access Point Protocol
ace-svr	ACE Server/Propagation
aol	America-Online Instant Messenger
appleqtc	Apple QuickTime
arp *	IP Address Resolution Protocol (ARP)
bgp	Border Gateway Protocol
biff	Biff mail notification
bootpc	Bootstrap Protocol Client
bootps	Bootstrap Protocol Server
bridge *	bridging
cddbp	CD Database Protocol
cdp *	Cisco Discovery Protocol
cifs	CIFS
cisco-fna	Cisco FNATIVE
cisco-net-mgmt	cisco-net-mgmt
cisco-svcs	Cisco license/perf/GDP/X.25/ident svcs

Protocol Name	Description
cisco-sys	Cisco SYSMAINT
cisco-tdp	cisco-tdp
cisco-tna	Cisco TNATIVE
citrix	Citrix Systems Metaframe
citriximaclient	Citrix IMA Client
clns *	ISO Connectionless Network Service
clns_es *	ISO CLNS End System
clns_is *	ISO CLNS Intermediate System
clp	Cisco Line Protocol
cmns *	ISO Connection-Mode Network Service
cmp	Cluster Membership Protocol
compressedtcp *	Compressed TCP
creativepartnr	Creative Partner
creativeserver	Creative Server
cuseeme	CU-SeeMe desktop video conference
daytime	Daytime (RFC 867)
dbase	dBASE Unix
dbcontrol_agent	Oracle Database Control Agent
ddns-v3	Dynamic DNS Version 3
dhcp	Dynamic Host Configuration
dhcp-failover	DHCP Failover
directconnect	Direct Connect
discard	Discard port
dns	Domain Name Server lookup

Protocol Name	Description
dnsix	DNSIX Security Attribute Token Map
echo	Echo port
edonkey	eDonkey
egp	Exterior Gateway Protocol
eigrp	Enhanced Interior Gateway Routing Protocol
entrust-svc-handler	Entrust KM/Admin Service Handler
entrust-svcs	Entrust sps/aaas/aams
exec	Remote Process Execution
exchange	Microsoft RPC for Exchange
fasttrack	FastTrack Traffic (KaZaA, Morpheus, Grokster, and so on)
fcip-port	FCIP
finger	Finger
ftp	File Transfer Protocol
ftps	FTP over TLS/SSL
gdoi	Group Domain of Interpretation
giop	Oracle GIOP/SSL
gnutella	Gnutella Version 2 Traffic (BearShare, Shareeza, Morpheus, and so on)
gopher	Gopher
gre	Generic Routing Encapsulation
gtpv0	GPRS Tunneling Protocol Version 0
gtpv1	GPRS Tunneling Protocol Version 1
h225ras	H225 RAS over Unicast
h323	H323 Protocol

Protocol Name	Description
h323callsigalt	H323 Call Signal Alternate
hp-alarm-mgr	HP Performance data alarm manager
hp-collector	HP Performance data collector
hp-managed-node	HP Performance data managed node
hsrp	Hot Standby Router Protocol
http	Hypertext Transfer Protocol
https	Secure Hypertext Transfer Protocol
ica	ica (Citrix)
icabrowser	icabrowser (Citrix)
icmp	Internet Control Message Protocol
ident	Authentication Service
igmpv3lite	IGMP over UDP for SSM
imap	Internet Message Access Protocol
imap3	Interactive Mail Access Protocol 3
imaps	IMAP over TLS/SSL
ip *	IP (version 4)
ipass	IPASS
ipinip	IP in IP (encapsulation)
ipsec	IP Security Protocol (ESP/AH)
ipsec-msft	Microsoft IPsec NAT-T
ipv6 *	IP (version 6)
ipx	IPX
irc	Internet Relay Chat
irc-serv	IRC-SERV

Protocol Name	Description
ircs	IRC over TLS/SSL
ircu	IRCU
isakmp	ISAKMP
iscsi	iSCSI
iscsi-target	iSCSI port
kazaa2	Kazaa Version 2
kerberos	Kerberos
l2tp	Layer 2 Tunnel Protocol
ldap	Lightweight Directory Access Protocol
ldap-admin	LDAP admin server port
ldaps	LDAP over TLS/SSL
llc2 *	llc2
login	Remote login
lotusmtap	Lotus Mail Tracking Agent Protocol
lotusnote	Lotus Notes
mgcp	Media Gateway Control Protocol
microsoft-ds	Microsoft-DS
msexch-routing	Microsoft Exchange Routing
msnmsgr	MSN Instant Messenger
msrpc	Microsoft Remote Procedure Call
msrpc-smb-netbios	MSRPC over TCP port 445
ms-cluster-net	MS Cluster Net
ms-dotnetster	Microsoft .NETster Port
ms-sna	Microsoft SNA Server/Base

Protocol Name	Description
ms-sql	Microsoft SQL
ms-sql-m	Microsoft SQL Monitor
mysql	MySQL
n2h2server	N2H2 Filter Service Port
ncp	NCP (Novell)
net8-cman	Oracle Net8 Cman/Admin
netbios	Network Basic Input/Output System
netbios-dgm	NETBIOS Datagram Service
netbios-ns	NETBIOS Name Service
netbios-ssn	NETBIOS Session Service
netshow	Microsoft Netshow
netstat	Variant of systat
nfs	Network File System
nntp	Network News Transfer Protocol
novadigm	Novadigm Enterprise Desktop Manager (EDM)
ntp	Network Time Protocol
oem-agent	OEM Agent (Oracle)
oracle	Oracle
oracle-em-vp	Oracle EM/VP
oraclenames	Oracle Names
orasrv	Oracle SQL*Net v1/v2
ospf	Open Shortest Path First
pad *	Packet assembler/disassembler (PAD) links
pcanywhere	Symantec pcANYWHERE

Protocol Name	Description
pcanywheredata	pcANYWHEREdata
pcanywherestat	pcANYWHEREstat
pop3	Post Office Protocol
pop3s	POP3 over TLS/SSL
pppoe	Point-to-Point Protocol over Ethernet
pptp	Point-to-Point Tunneling Protocol
printer	Print spooler/ldp
pwdgen	Password Generator Protocol
qmtp	Quick Mail Transfer Protocol
radius	RADIUS & Accounting
rcmd	Berkeley Software Distribution (BSD) r-commands (rsh, rlogin, rexec)
rdb-dbs-disp	Oracle RDB
realmedia	RealNetwork's Realmedia Protocol
realsecure	ISS Real Secure Console Service Port
rip	Routing Information Protocol
router	Local Routing Process
rsrb *	Remote Source-Route Bridging
rsvd	RSVD
rsvp	Resource Reservation Protocol
rsvp-encap	RSVP ENCAPSULATION-1/2
rsvp_tunnel	RSVP Tunnel
rtc-pm-port	Oracle RTC-PM port
rtelnet	Remote Telnet Service
rtp	Real-Time Protocol

Protocol Name	Description
rtsp	Real-Time Streaming Protocol
r-winsock	remote-winsock
secure-ftp	FTP over Transport Layer Security/Secure Sockets Layer (TLS/SSL)
secure-http	Secured HTTP
secure-imap	Internet Message Access Protocol over TLS/SSL
secure-irc	Internet Relay Chat over TLS/SSL
secure-ldap	Lightweight Directory Access Protocol over TLS/SSL
secure-nntp	Network News Transfer Protocol over TLS/SSL
secure-pop3	Post Office Protocol over TLS/SSL
secure-telnet	Telnet over TLS/SSL
send	SEND
shell	Remote command
sip	Session Initiation Protocol
sip-tls	Session Initiation Protocol-Transport Layer Security
skinny	Skinny Client Control Protocol
sms	SMS RCINFO/XFER/CHAT
smtp	Simple Mail Transfer Protocol
snapshot	Snapshot routing support
snmp	Simple Network Protocol
snmptrap	SNMP Trap
socks	Sockets network proxy protocol (SOCKS)
sqlnet	Structured Query Language (SQL)*NET for Oracle
sqlserv	SQL Services
sqlsrv	SQL Service

Protocol Name	Description
sqlserver	Microsoft SQL Server
ssh	Secure shell
sshell	SSLshell
ssp	State Sync Protocol
streamwork	Xing Technology StreamWorks player
stun	cisco Serial Tunnel
sunrpc	Sun remote-procedure call (RPC)
syslog	System Logging Utility
syslog-conn	Reliable Syslog Service
tacacs	Login Host Protocol (TACACS)
tacacs-ds	TACACS-Database Service
tarantella	Tarantella
tcp	Transport Control Protocol
telnet	Telnet
telnets	Telnet over TLS/SSL
tftp	Trivial File Transfer Protocol
time	Time
timed	Time server
tr-rsrb	cisco RSRB
tto	Oracle TTC/SSL
udp	User Datagram Protocol
uucp	UUCPD/UUCP-RLOGIN
vdolive	VDOLive streaming video
vofr *	Voice over Frame Relay

Protocol Name	Description
vqp	VLAN Query Protocol
webster	Network Dictionary
who	Who’s service
wins	Microsoft WINS
x11	X Window System
xdmcp	XDM Control Protocol
xwindows *	X-Windows remote access
ymsgr	Yahoo! Instant Messenger

* This protocol is not supported on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine.

Examples

The following example specifies a class map named ftp and configures the FTP protocol as a match criterion:

```
Router(config)# class-map ftp
Router(config-cmap)
#
 match protocol ftp
```

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 for the IP protocol will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match protocol ip
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
match access-group	Configures the match criteria for a class map based on the specified ACL.

Command	Description
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match mpls experimental	Configures a class map to use the specified value of the experimental field as a match criterion.
match precedence	Identifies IP precedence values as match criteria.
match protocol (NBAR)	Configures NBAR to match traffic by a protocol type known to NBAR.
match qos-group	Configures a class map to use the specified EXP field value as a match criterion.

match protocol attribute application-group

To configure the match criterion for a class map based on the specified application group, use the **match protocol attribute application-group** command in class-map configuration mode. To remove the application-group match criterion from the class map, use the **no** form of this command.

match protocol attribute application-group *application-group* [*application-name*]

no match protocol attribute application-group *application-group*

Syntax Description

application-group	Name of the application group as a matching criterion. See the "Usage Guidelines" section for a list of application groups supported by most routers.
application-name	(Optional) Name of the application. When the application name is specified, the application is configured as the match criterion instead of the application group.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) based on an application group. Multiple traffic classes can be created. The following table lists the supported application groups.

Table 3: Supported Application Groups

Application Group	Description
apple-talk-group	AppleTalk-related applications.
banyan-group	Banyan-related applications.
bittorrent-group	Bittorrent-related applications.

Application Group	Description
corba-group	Corba-related applications.
edonkey-emule-group	edonkey-emule-related applications.
fasttrack-group	Fasttrack-related applications.
flash-group	Flash-related applications.
fring-group	Fring-related applications.
ftp-group	FTP-related applications.
gnutella-group	Gnutella-related applications.
icq-group	I Seek You (ICQ)-related applications.
imap-group	Internet Message Access Protocol (IMAP)-related applications.
irc-group	Internet Relay Chap (IRC)-related applications.
kerberos-group	Kerberos-related applications.
ldap-group	Lightweight Directory Access Protocol (LDAP)-related applications.
my-jabber-group	My-jabber-related applications.
netbios-group	NetBIOS-related applications.
nntp-group	Network News Transfer Protocol (NNTP)-related applications.
npmp-group	Network Peripheral Management Protocol (NPMP)-group related objectives.
other	Other applications.
pop3-group	Post Office Protocol 3 (pop3)-related applications.
prm-group	Performance Report Message (PRM)-related applications.
skinny-group	Skinny-related applications.
skype-group	Skype-related applications.

Application Group	Description
smtp-group	Simple Mail Transfer Protocol (SMTP)-related applications.
snmp-group	Simple Network Management Protocol (SNMP)-related applications.
sqlsvr-group	Structured Query Language (SQL)-server-related applications.
telepresence-group	Telepresence-related applications.
tftp-group	TFTP-related applications.
wap-group	Wireless Application Protocol (WAP)-related applications.
webex-group	Webex-related applications.
windows-live-messenger-group	Windows-live-messenger-related applications.
xns-xerox-group	Xerox Network Services (XNS)-xerox related applications.
yahoo-messenger-group	Yahoo Messenger-related applications.

Examples

The following example shows how to configure an application group as a match criterion:

```
Router(config)# class-map apps
Router(config-cmap)# match protocol attribute application-group skype-group
```

Related Commands

Command	Description
match protocol (NBAR)	Configures NBAR to match traffic by a protocol type known to NBAR.

match protocol attribute category

To configure the match criterion for a class map based on the specified application category, use the **match protocol attribute category** command in class-map configuration mode. To remove the application category match criterion from the class map, use the **no** form of this command.

match protocol attribute category *application-category* [*application-name*]

no match protocol attribute category *application-category*

Syntax Description

application-category	Name of the application category used as a matching criterion. See the "Usage Guidelines" section for a list of application categories supported by most routers.
application-name	(Optional) Name of the application. When the application name is specified, the application is configured as the match criterion instead of the application category.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) based on an application category. You can create as many traffic classes as needed.

The following table lists the supported application categories.

Table 4: Supported Application Categories

Category Name	Description
browsing	Browsing-related applications.
business-and-productivity-tools	Business and productivity tools-related applications.

Category Name	Description
email	Email-related applications.
file-sharing	File-sharing related applications.
gaming	Gaming-related applications.
industrial-protocols	Industrial protocols-related applications.
instant-messaging	Instant messaging-related applications.
internet-privacy	Internet privacy-related applications.
layer2-non-ip	Layer2 non-ip-related applications.
layer3-over-ip	Layer3-over-IP-related applications.
location-based-services	Location-based services-related applications.
net-admin	Net-admin-related applications.
newsgroup	Newsgroup-related applications.
obsolete	Obsolete applications.
other	Other applications.
trojan	Trojan-related applications.
voice-and-video	Voice and video-related applications.

Examples

The following example shows how to configure email-related applications as a match criterion:

```
Router(config)# class-map mygroup
Router(config-cmap)# match protocol attribute category email
```

Related Commands

Command	Description
match protocol attribute sub-category	Configures the match criterion for a specified application subcategory.

match protocol attribute encrypted

To configure the match criterion for a class map based on encryption, use the **match protocol attribute encrypted** command in class-map configuration mode. To remove the encryption match criterion from the class map, use the **no** form of this command.

match protocol attribute encrypted {**encrypted-no**| **encrypted-unassigned**| **encrypted-yes**} [*application-name*]

no match protocol attribute encrypted {**encrypted-no**| **encrypted-unassigned**| **encrypted-yes**}

Syntax Description

encrypted-no	Specifies applications without encryption.
encrypted-unassigned	Specifies applications without an encrypted networking protocol application tag.
encrypted-yes	Specifies encrypted applications.
application-name	(Optional) Name of the application. When the application name is specified, the application within the specified encrypted status is configured as the match criterion instead of all the applications within the group.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) based on encryption. Multiple traffic classes can be created.

Examples

The following examples show how to specify a class map with encryption as a match criterion:

```
Router(config)# class-map my-class
Router(config-cmap)# match protocol attribute encrypted encrypted-no ayiya-ipv6-tunneled

Router(config)# class-map my-class
Router(config-cmap)# match protocol attribute encrypted encrypted-unassigned aurora-cmgr
Router(config)# class-map my-class
Router(config-cmap)# match protocol attribute encrypted encrypted-yes citrix
```

Related Commands

Command	Description
match protocol (NBAR)	Configures NBAR to match traffic by a protocol type known to NBAR.

match protocol attribute sub-category

To configure the match criterion for a class map based on the specified application subcategory, use the **match protocol attribute sub-category** command in class-map configuration mode. To remove the application subcategory match criterion from the class map, use the **no** form of this command.

match protocol attribute sub-category *sub-category-name* [*aplication-name*]

no match protocol attribute sub-category *sub-category-name*

Syntax Description

sub-category-name	Name of the application subcategory used as a matching criterion. See the "Usage Guidelines" section for a list of application subcategories supported by most routers.
application-name	(Optional) Name of the application. When the application name is specified, the application is configured as the match criterion instead of the subcategory.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) based on an application subcategory. You can create as many traffic classes as needed.

lists the supported application subcategories.

Table 5: Supported Application Subcategories

Sub-Category Name	Description
authentication-services	Authentication services-related applications.
backup-systems	Backup systems-related applications.

Sub-Category Name	Description
client-server	Client-server-related applications.
commercial-media-distribution	Commercial media distribution-related applications.
control-and-signaling	Control and signaling-related applications.
database	Database-related applications.
epayement	Epayement-related applications.
inter-process-rpc	Inter-process remote procedure call-related applications.
license-manager	License manager-related applications.
naming-services	Naming services-related applications.
network-management	Network management-related applications
network-protocol	Network protocol-related applications.
other	Other related applications.
p2p-file-transfer	Peer-to-peer file transfer-related applications.
p2p-networking	Peer-to-peer networking-related applications.
remote-access-terminal	Remote access terminal-related applications.
rich-media-http-content	Rich media HTTP content-related applications.
routing-protocol	Routing protocol-related applications.
storage	Storage-related applications.
streaming	Streaming-related applications.
terminal	Terminal-related applications.
tunneling-protocols	Tunneling protocols-related applications.
voice-video-chat-collaboration	Voice-video chat collaboration-related applications.

Examples

The following example shows how to configure client-server applications as a match criterion:

```
Router(config)# class-map newmap
Router(config-cmap)# match protocol attribute sub-category client-server
```

Related Commands

Command	Description
match protocol attribute category	Configures the match criterion for a specified application category.

match protocol attribute tunnel

To configure the match criterion for a class map based on tunneling, use the **match protocol attribute tunnel** command in class-map configuration mode. To remove the tunneling match criterion from the class map, use the **no** form of this command.

match protocol attribute tunnel {**tunnel-no| tunnel-unassigned| tunnel-yes**} [*application-name*]

no match protocol attribute tunnel {**tunnel-no| tunnel-unassigned| tunnel-yes**} [*application-name*]

Syntax Description

tunnel-no	Specifies the applications without tunneling.
tunnel-unassigned	Specifies the unassigned tunneled applications.
tunnel-yes	Specifies tunneled applications.
application-name	(Optional) Name of the application. When the application name is specified, the application within the specified tunneling status is configured as the match criterion instead of all the applications within the tunneling group.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) based on tunneling. Multiple traffic classes can be created.

Examples

The following examples show how to specify a class map with tunneling as a match criterion:

```
Router(config)# class-map mygroup
Router(config-cmap)# match protocol attribute tunnel tunnel-no agentx

Router(config)# class-map mygroup
Router(config-cmap)# match protocol attribute tunnel tunnel-unassigned aris

Router(config)# class-map mygroup
Router(config-cmap)# match protocol attribute tunnel tunnel-yes rsvp_tunnel
```

Related Commands

Command	Description
match protocol (NBAR)	Configures NBAR to match traffic by a protocol type known to NBAR.

match protocol (NBAR)

To configure Network-Based Application Recognition (NBAR) to match traffic by a protocol type that is known to NBAR, use the **matchprotocol**commandinclass map configuration mode. To disable NBAR from matching traffic by a known protocol type, use the **no** form of this command.

match protocol *protocol-name* [*variable-field-name value*]

no match protocol *protocol-name* [*variable-field-name value*]

Syntax Description

protocol-name	Particular protocol type that is known to NBAR. These known protocol types can be used to match traffic. For a list of protocol types that are known to NBAR, see the table below in “Usage Guidelines.”
variable-field-name	(Optional and usable only with custom protocols) Predefined variable that was created when you created a custom protocol. The value for the *variable-field-name*argument will match the *field-name* variable entered when you created the custom protocol using the**ip nbar custom**command.
value	(Optional and usable only with custom protocols) Specific value in the custom payload to match. A value can be entered along with a value for the *variable-field-name*argument only. The value can be expressed in decimal or hexadecimal format.

Command Default

Traffic is not matched by a protocol type that is known to NBAR.

Command Modes

Class map configuration (config-cmap)

Command History

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E, and the *variable-field-namevalue*argument was added.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(13)T	This command was implemented on Catalyst 6000 family switches without FlexWAN modules.

Release	Modification
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
12.4(2)T	This command was modified to include support for additional protocols, such as the BitTorrent protocol.
12.4(4)T	This command was modified to include support for additional protocols, such as the Skype and DirectConnect protocols.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY. This command was modified to enhance NBAR functionality on the Catalyst 6500 series switch that is equipped with the Supervisor 32/programmable intelligent services accelerator (PISA) engine.
12.2(18)ZYA	This command was modified to integrate NBAR and Firewall Service Module (FWSM) functionality on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine and to recognize additional protocols as noted in the table below in "Usage Guidelines."
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(18)ZYA1	This command was modified to recognize additional protocols as noted in the table below in "Usage Guidelines."
Cisco IOS XE Release 2.3	This command was modified to recognize additional protocols as noted in the table below in "Usage Guidelines."
12.2(18)ZYA2	This command was modified to recognize additional protocols, such as the TelePresence protocol.
Cisco IOS XE Release 2.5	This command was modified to recognize additional protocols as noted in the table below in "Usage Guidelines."
12.2XN	This command was modified to recognize additional protocols as noted in the table below in "Usage Guidelines."
12.4(24)T	This command was modified to recognize additional protocols as noted in the table below in "Usage Guidelines."
12.4(24)MDA	This command was modified to recognize additional protocols as noted in the table below in "Usage Guidelines."
Cisco IOS XE Release 3.4S	This command was modified to recognize additional protocols as noted in the table below in "Usage Guidelines."

Release	Modification
15.1(3)S	This command was modified. Support was removed from Cisco 7200 series routers.

Usage Guidelines

Use the **matchprotocol**(NBAR) command to match protocol types that are known to NBAR. NBAR is capable of classifying the following types of protocols:

- Non-UDP and non-TCP IP protocols
- TCP and UDP protocols that use statically assigned port numbers
- TCP and UDP protocols that use statically assigned port numbers but still require stateful inspection
- TCP and UDP protocols that dynamically assign port numbers and therefore require stateful inspection

The table below lists the NBAR-supported protocols available in Cisco IOS software, sorted by category. The table also provides information about the protocol type, the well-known port numbers (if applicable), and the syntax for entering the protocol in NBAR. The table is modified as new protocols are added or supported by different releases.

Note The table below includes the NBAR-supported protocols available with the 12.2(18)ZY and 12.2(18)ZYA releases. Protocols included in the 12.2(18)ZY and 12.2(18)ZYA releases are supported on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine.

Table 6: NBAR-Supported Protocols

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Enterprise Applications	Novadigm	TCP/ UDP	3460-3465	Novadigm Enterprise Desktop Manager (EDM)	novadigm	Cisco IOS XE Release 2.3
	Citrix (ICA, CGP, IMA, SB)	TCP/ UDP	TCP: 1494, 2512, 2513, 2598 UDP: 1604	Citrix ICA traffic	citrix citrix app citrix ica-tag	12.1(2)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.5
	Oracle	TCP	1525	Oracle	ora-srv	Cisco IOS XE Release 2.3
	PCAnywhere	TCP/UDP	TCP: 5631, 65301 UDP: 22, 5632	Symantic PCAnywhere	pcanywhere	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	SAP	TCP	3300-3315 3200-3215 3600-3615	Application server to application server traffic (sap-pgm.pdlm) Client to application server traffic (sap-app.pdlm) Client to message server traffic (sap-msg.pdlm)	sap	12.1E 12.2T 12.3 12.3T 12.2(18)ZYA1 Cisco IOS XE Release 2.5
	Exchange [1]	TCP	135	MS-RPC for Exchange	exchange	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
						12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZY 12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.5
Routing Protocols	BGP	TCP/ UDP	179	Border Gateway Protocol	bgp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	EGP	IP	8	Exterior Gateway Protocol	egp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	EIGRP	IP	88	Enhanced Interior Gateway Routing Protocol	eigrp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	OSPF	IP	89	Open Shortest Path First	ospf	12.3(8)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	RIP	UDP	520	Routing Information Protocol	rip	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Database	CIFS	TCP	139, 445	Common Internet File System	cifs	12.2(18)ZYA 12.2(18)ZYA1
	MS-SQLServer	TCP	1433	Microsoft SQL Server Desktop Videoconferencing	sqlserver	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1
	SQL-exec	TCP/UDP	9088	SQL Exec	sqlexec	Cisco IOS XE Release 2.3
	SQL*NET	TCP/ UDP	1521	SQL*NET for Oracle	sqlnet	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.5
Financial	FIX	TCP	Heuristic	Financial Information Exchange	fix	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.5
Security and Tunneling	GRE	IP	47	Generic Routing Encapsulation	gre	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
IPINIP	IP	4	IP in IP	ipinip	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
IPsec	IP/TCP	50, 51 TCP-Heuristic	IP Encapsulating Security Payload/ Authentication-Header	ipsec	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3	
L2TP	UDP	1701	L2F/L2TP Tunnel	l2tp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3	
PPTP	TCP	1723	Point-to-Point Tunneling Protocol for VPN	pptp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3	
SFTP	TCP	990	Secure FTP	secure-ftp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3	
SHTTP	TCP	443	Secure HTTP	secure-http	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.3	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
STELNET	TCP	992	Secure Telnet	secure-telnet	Cisco IOS XE Release 2.3	
	SIMAP	TCP/ UDP	585, 993	Secure Internet Message Access Protocol	secure-imap	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	SIRC	TCP/ UDP	994	Secure Internet Relay Chat	secure-irc	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	SLDAP	TCP/ UDP	636	Secure Lightweight Directory Access Protocol	secure-ldap	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	SNNTP	TCP/ UDP	563	Secure Network News Transfer Protocol	secure-nntp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	SOCKS	TCP	1080	Firewall Security Protocol	socks	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
	SPOP3	TCP/ UDP	995	Secure POP3	secure-pop3	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	SSH	TCP	22	Secured Shell	ssh	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	STELNET	TCP	992	Secure Telnet	secure-telnet	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
Network Management	ICMP	IP	1	Internet Control Message Protocol	icmp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	SNMP	TCP/ UDP	161, 162	Simple Network Management Protocol	snmp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	Syslog	UDP	514	System Logging Utility	syslog	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Network Mail Services	IMAP	TCP/ UDP	143, 220	Internet Message Access Protocol	imap	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	Notes	TCP/ UDP	1352	Lotus Notes	notes	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	POP3	TCP/ UDP	110, Heuristic	Post Office Protocol	pop3	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.3
	SMTP	TCP	25, Heuristic	Simple Mail Transfer Protocol	smtp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Directory	DHCP/ BOOTP	UDP	67, 68	Dynamic Host Configuration Protocol/Bootstrap Protocol	dhcp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1
	DNS	TCP/ UDP	53	Domain Name System	dns	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1
	Finger	TCP	79	Finger User Information Protocol	finger	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	Kerberos	TCP/ UDP	88, 749	Kerberos Network Authentication Service	kerberos	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	LDAP	TCP/ UDP	389	Lightweight Directory Access Protocol	ldap	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Internet	FTP	TCP	21, 21000, Heuristic	File Transfer Protocol	ftp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1
	Gopher	TCP/ UDP	70	Internet Gopher Protocol	gopher	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	HTTP	TCP	80[2], Heuristic	Hypertext Transfer Protocol	http	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.5
	IRC	TCP/ UDP	194	Internet Relay Chat	irc	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	NNTP	TCP/ UDP	119, Heuristic	Network News Transfer Protocol	nntp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	Telnet	TCP	23	Telnet Protocol	telnet	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
						12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1
	TFTP	UDP	69	Trivial File Transfer Protocol	tftp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.5
Signaling	AppleQTC	TCP/UDP	458	Apple Quick Time	appleqtc	12.2(18)ZYA 12.2(18)ZYA1Cisco IOS XE Release 2.3
Chargen	TCP/UDP	19	Character Generator	chargen	12.2(18)ZYA 12.2(18)ZYA1Cisco IOS XE Release 2.3	
ClearCase	TCP/UDP	371	Clear Case Protocol Software Informer	clearcase	12.2(18)ZYA 12.2(18)ZYA1Cisco IOS XE Release 2.3	
Corba	TCP/UDP	683, 684	Corba Internet Inter-Orb Protocol (IIOP)	corba-iiop	12.2(18)ZYA 12.2(18)ZYA1Cisco IOS XE Release 2.3	
Daytime	TCP/UDP	13	Daytime Protocol	daytime	12.2(18)ZYA 12.2(18)ZYA1Cisco IOS XE Release 2.3	
Doom	TCP/UDP	666	Doom	doom	12.2(18)ZYA 12.2(18)ZYA1Cisco IOS XE Release 2.3	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Echo	TCP/UDP	7	Echo Protocol	echo	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3	
IBM DB2	TCP/UDP	523	IBM Information Management	ibm-db2	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3	
IPX	TCP/UDP	213	Internet Packet Exchange	server-ipx	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3	
ISAKMP	TCP/UDP	500	Internet Security Association and Key Management Protocol	isakmp	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3	
ISI-GL	TCP/UDP	55	Interoperable Self Installation Graphics Language	isi-gl	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release		
			KLogin	TCP	543	KLogin	klogin	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
KShell	TCP		544	KShell	kshell	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3		
LockD	TCP/UDP		4045	LockD	lockd	12.2(18)ZYA Cisco IOS XE Release 2.3		
MSSQL	TCP		1433	Microsoft Structured Query Language (SQL) Server	mssql	Cisco IOS XE Release 2.3		
RSVP	IP/ UDP		IP: 46 UDP: 1698, 1699	Resource Reservation Protocol	rsvp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3		

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
RPC	AOL-messenger	TCP	5190, 443	AOL Instant Messenger Chat Messages	aol-messenger	12.2(18)ZYA 12.2(18)ZYA1
	NFS	TCP/UDP	2049	Network File System	nfs	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	Sunrpc	TCP/ UDP	111, Heuristic	Sun Remote Procedure Call	sunrpc	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.5
Non-IP and LAN/ Legacy	NetBIOS	TCP/ UDP	TCP-137, 138 UDP-137,139	NetBIOS over IP (MS Windows)	netbios	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	Nickname	TCP/UDP	43	Nickname	nicname	12.2(18)ZYA 12.2(18)ZYA1Cisco IOS XE Release 2.3
	NPP	TCP/UDP	92	Network Payment Protocol	npp	12.2(18)ZY 12.2(18)ZYA1 Cisco IOS XE Release 2.3

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Voice	Google Talk VoIP	TCP/UDP	Dynamically assigned	Google Talk VoIP Protocol	gtalk-voip	12.2XN 12.4(24)MDA
	H.323	TCP	Heuristic	H.323 Teleconferencing Protocol	h323	Cisco IOS XE Release 2.1
	MSN VoIP	UDP	Dynamically assigned	MSN Messenger Protocol	msn-voip	12.4(24)MDA 12.4(24)T
	RTCP	TCP/ UDP	Dynamically assigned	Real-Time Control Protocol	rtcp	12.1E 12.2T 12.2(18)ZYA1 12.3 12.3T
	RTP	TCP/ UDP	Dynamically assigned	Real-Time Transport Protocol Payload Classification	rtp	12.2(8)T 12.2(18)ZYA1 Cisco IOS XE Release 2.5
	SIP	TCP/UPD	5060	Session Initiation Protocol	sip	12.3(7)T Cisco IOS XE Release 2.1 12.2(18)ZYA1 Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.3
	STUN	UDP	Dynamically assigned	Simple Traversal of UDP through NAT (STUN)	stun-nat	12.4(24)MDA 12.4(24)T
	Skype[3]	TCP/UDP	TCP-80, Heuristic	VoIP Client Software	skype	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.5

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
	Yahoo VoIP	TCP/UDP	Dynamically assigned	Yahoo Messenger VoIP Protocol	yahoo-voip	12.4(24)MDA 12.4(24)T
Desktop Media	CUSeeMe	TCP/UDP	TCP: 7648, 7649 UDP: 24032	CU-SeeMe Desktop Video Conference	cuseeme	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1
Streaming Media	RealAudio	TCP/ UDP	Dynamically assigned	RealAudio Streaming Protocol	realaudio	12.0(5)XE2 12.1(1)E 12.1(5)T
	RTSP	TCP	554, 8554	Real-Time Streaming Protocol	rtsp	12.2(18)ZYA1 12.3(11)T Cisco IOS XE Release 2.1
	StreamWorks	UDP	Dynamically assigned	Xing Technology Stream Works Audio and Video	streamwork	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1
	VDOLive	TCP/ UDP	Static (7000) with inspection	VDOLive Streaming Video	vdolive	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1
	YouTube[4]	TCP	Both static (80) and dynamically assigned	Online Video-Sharing Website	youtube	12.2(18)ZYA 12.2(18)ZYA1
Peer-to-Peer File-Sharing Applications	BitTorrent[5]	TCP	Heuristic, or 6881-6889	BitTorrent File Transfer Traffic	bittorrent	12.2(18)ZYA1 12.4(2)T Cisco IOS XE Release 2.5

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
DirectConnect	TCP	80, 411-413, Heuristic	Direct Connect File Transfer Traffic	directconnect	Cisco IOS XE Release 2.5	
eDonkey/eMule[6]	TCP	80, 4662, Heuristic	eDonkey File-Sharing Application eMule traffic is also classified as eDonkey traffic in NBAR.	edonkey	12.2(18)ZYA1 12.3(11)T Cisco IOS XE Release 2.5	
Encrypted Emule	TCP	Heuristic	P2P file sharing encrypted protocol	encrypted-emule	Cisco IOS XE Release 3.4S	
FastTrack	—	Heuristic	FastTrack traffic	fasttrack	12.1(12c)E 12.2(18)ZYA1 Cisco IOS XE Release 2.5	
FastTrack Static	—	Heuristic	FastTrack Static	fasttrack-static	Cisco IOS XE Release 3.3S	
Gnutella	TCP/UDP	Heuristic, or TCP-80, 6346-6349, 6355,5634	Gnutella traffic	gnutella	Cisco IOS XE Release 2.5	
Gnutella Networking	TCP/UDP	Heuristic, or UDP-6346-6348	Gnutella Networking traffic	networking-gnutella	Cisco IOS XE Release 3.4S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
KaZaA	TCP/ UPD	Heuristic	KaZaA Note that earlier KaZaA version 1 traffic can be classified using FastTrack.	kazaa2	12.2(8)T 12.2(18)ZYA1 Cisco IOS XE Release 2.5	
WinMX	TCP	6699	WinMX Peer-to-Peer File-Sharing	winmx	12.2(18)ZYA1 12.3(7)T Cisco IOS XE Release 2.5	
Miscellaneous	3Com AMP3	TCP/UDP	629	3Com AMP3	3com-amp3	Cisco IOS XE Release 3.1S
	3Com TSMUX	TCP/UDP	106	3Com TSMUX	3com-tsmux	Cisco IOS XE Release 3.1S
3PC	TCP/UDP	34	Third Party Connect Protocol	3pc	Cisco IOS XE Release 3.1S	
914 C/G	TCP/UDP	211	Texas Instruments 914 Terminal	914c/g	Cisco IOS XE Release 3.1S	
9PFS	TCP/UDP	564	Plan 9 file service	9pfs	Cisco IOS XE Release 3.1S	
ACAP	TCP/UDP	674	ACAP	acap	Cisco IOS XE Release 3.1S	
ACAS	TCP/UDP	62	ACA Services	acas	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
AccessBuilder	TCP/UDP	888	Access Builder	accessbuilder	Cisco IOS XE Release 3.1S	
AccessNetwork	TCP/UDP	699	Access Network	accessnetwork	Cisco IOS XE Release 3.1S	
ACP	TCP/UDP	599	Aeolon Core Protocol	acp	Cisco IOS XE Release 3.1S	
ACR-NEMA	TCP/UDP	104	ACR-NEMA Digital Img	acr-nema	Cisco IOS XE Release 3.1S	
AED-512	TCP/UDP	149	AED 512 Emulation service	aed-512	Cisco IOS XE Release 3.1S	
Agentx	TCP/UDP	705	AgentX	agentx	Cisco IOS XE Release 3.1S	
Alpes	TCP/UDP	463	Alpes	alpes	Cisco IOS XE Release 3.1S	
AMInet	TCP/UDP	2639	AMInet	aminet	Cisco IOS XE Release 3.1S	
AN	TCP/UDP	107	Active Networks	an	Cisco IOS XE Release 3.1S	
ANET	TCP/UDP	212	ATEXSSTR	anet	Cisco IOS XE Release 3.1S	
ANSANotify	TCP/UDP	116	ANSA REX Notify	ansanotify	Cisco IOS XE Release 3.1S	
ANSATrader	TCP/UDP	124	ansatrader	ansatrader	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
AODV	TCP/UDP	654	AODV	aodv	Cisco IOS XE Release 3.1S	
	Apertus-LDP	TCP/UDP	539	Apertus Tech Load Distribution	apertus-ldp	Cisco IOS XE Release 3.1S
	AppleQTC	TCP/UDP	458	apple quick time	appleqtc	Cisco IOS XE Release 3.1S
AppleQTSRVR	TCP/UDP	545	appleqtcsrvr	appleqtcsrvr	Cisco IOS XE Release 3.1S	
Applix	TCP/UDP	999	Applix ac	applix	Cisco IOS XE Release 3.1S	
ARCISDMS	TCP/UDP	262	arcisdms	arcisdms	Cisco IOS XE Release 3.1S	
ARGUS	TCP/UDP	13	ARGUS	argus	Cisco IOS XE Release 3.1S	
Ariel1	TCP/UDP	419	Ariel1	ariel1	Cisco IOS XE Release 3.1S	
Ariel2	TCP/UDP	421	Ariel2	ariel2	Cisco IOS XE Release 3.1S	
Ariel3	TCP/UDP	422	Ariel3	ariel3	Cisco IOS XE Release 3.1S	
ARIS	TCP/UDP	104	ARIS	aris	Cisco IOS XE Release 3.1S	
ARNS	TCP/UDP	384	A remote network server system	arns	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
ASA	TCP/UDP	386	ASA Message router object def	asa	Cisco IOS XE Release 3.1S	
ASA-Appl-Proto	TCP/UDP	502	asa-appl-proto	asa-appl-proto	Cisco IOS XE Release 3.1S	
ASIPRegistry	TCP/UDP	687	asipregistry	asipregistry	Cisco IOS XE Release 3.1S	
ASIP-Webadmin	TCP/UDP	311	AppleShare IP WebAdmin	asip-webadmin	Cisco IOS XE Release 3.1S	
AS-Servermap	TCP/UDP	449	AS Server Mapper	as-servermap	Cisco IOS XE Release 3.1S	
AT-3	TCP/UDP	203	AppleTalk Unused	at-3	Cisco IOS XE Release 3.1S	
AT-5	TCP/UDP	205	AppleTalk Unused	at-5	Cisco IOS XE Release 3.1S	
AT-7	TCP/UDP	207	AppleTalk Unused	at-7	Cisco IOS XE Release 3.1S	
AT-8	TCP/UDP	208	AppleTalk Unused	at-8	Cisco IOS XE Release 3.1S	
	AT-Echo	TCP/UDP	204	AppleTalk Echo	at-echo	Cisco IOS XE Release 3.1S
AT-NBP	TCP/UDP	202	AppleTalk Name Binding	at-nbp	Cisco IOS XE Release 3.1S	
AT-RTMP	TCP/UDP	201	AppleTalk Routing Maintenance	at-rtmp	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
AT-ZIS	TCP/UDP	206	AppleTalk Zone Information	at-zis	Cisco IOS XE Release 3.1S	
Audit	TCP/UDP	182	Unisys Audit SITP	audit	Cisco IOS XE Release 3.1S	
Auditd	TCP/UDP	48	Digital Audit daemon	auditd	Cisco IOS XE Release 3.1S	
Aurora-CMGR	TCP/UDP	364	Aurora CMGR	aurora-cmgr	Cisco IOS XE Release 3.1S	
AURP	TCP/UDP	387	Appletalk Update-Based Routing Protocol	aurp	Cisco IOS XE Release 3.1S	
AUTH	TCP/UDP	113	Authentication Service	auth	Cisco IOS XE Release 3.1S	
Avian	TCP/UDP	486	avian	avian	Cisco IOS XE Release 3.1S	
AX25	TCP/UDP	93	AX.25 Frames	ax25	Cisco IOS XE Release 3.1S	
Banyan-RPC	TCP/UDP	567	Banyan-RPC	banyan-rpc	Cisco IOS XE Release 3.1S	
Banyan-VIP	TCP/UDP	573	Banyan-VIP	banyan-vip	Cisco IOS XE Release 3.1S	
BBNRCCMON	TCP/UDP	10	BBN RCC Monitoring	bbnrccmon	Cisco IOS XE Release 3.1S	
BDP	TCP/UDP	581	Bundle Discovery protocol	bdp	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
BFTP	TCP/UDP	152	Background File Transfer Program	bftp	Cisco IOS XE Release 3.1S	
BGMP	TCP/UDP	264	Border Gateway Multicast Protocol	bgmp	Cisco IOS XE Release 3.1S	
BGP	TCP/UDP	179	Border Gateway Protocol	bgp	Cisco IOS XE Release 3.1S	
BGS-NSI	TCP/UDP	482	BGS-NSI	bgs-nsi	Cisco IOS XE Release 3.1S	
	Bhevent	TCP/UDP	357	Bhevent	bhevent	Cisco IOS XE Release 3.1S
	BHFHS	TCP/UDP	248	BHFHS	bhfhs	Cisco IOS XE Release 3.1S
BHMDS	TCP/UDP	310	BHMDS	bhmds	Cisco IOS XE Release 3.1S	
BL-IDM	TCP/UDP	142	Britton Lee IDM	bl-idm	Cisco IOS XE Release 3.1S	
BMPP	TCP/UDP	632	BMPP	bmpp	Cisco IOS XE Release 3.1S	
BNA	TCP/UDP	49	BNA	bna	Cisco IOS XE Release 3.1S	
Bnet	TCP/UDP	415	BNET	bnet	Cisco IOS XE Release 3.1S	
Borland-DSJ	TCP/UDP	707	Borland-dsj	borland-dsj	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
BR-SAT-Mon	TCP/UDP	76	Backroom SATNET Monitoring	br-sat-mon	Cisco IOS XE Release 3.1S	
Cableport-AX	TCP/UDP	282	Cable Port A/X	cableport-ax	Cisco IOS XE Release 3.1S	
Cab-Protocol	TCP/UDP	595	CAB Protocol	cab-protocol	Cisco IOS XE Release 3.1S	
Cadlock	TCP/UDP	770	Cadlock	cadlock	Cisco IOS XE Release 3.1S	
CAIlic	TCP/UDP	216	Computer Associates Intl License Server	CAIlic	Cisco IOS XE Release 3.1S	
CBT	TCP/UDP	7	CBT	cbt	Cisco IOS XE Release 3.1S	
CDC	TCP/UDP	223	Certificate Distribution Center	cdc	Cisco IOS XE Release 3.1S	
CFDPTKT	TCP/UDP	120	cfdptkt	cfdptkt	Cisco IOS XE Release 3.1S	
CFTP	TCP/UDP	62	CFTP	cftp	Cisco IOS XE Release 3.1S	
CHAOS	TCP/UDP	16	Chaos	chaos	Cisco IOS XE Release 3.1S	
CharGen	TCP/UDP	19	Character Generator	chargen	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
	ChShell	TCP/UDP	562	chcmd	chshell	Cisco IOS XE Release 3.1S
	Cimplex	TCP/UDP	673	Cimplex	cimplex	Cisco IOS XE Release 3.1S
Cisco-FNA	TCP/UDP	130	Cisco FNATIVE	cisco-fna	Cisco IOS XE Release 3.1S	
Cisco-phone[7]	UDP	5060	Cisco IP Phones and PC-Based Unified Communicators	cisco-phone	12.2(18)ZYA 12.2(18)ZYA1	
Cisco-SYS	TCP/UDP	132	Cisco SYSMAINT	cisco-sys	Cisco IOS XE Release 3.1S	
Cisco-TDP	TCP/UDP	711	Cisco TDP	cisco-tdp	Cisco IOS XE Release 3.1S	
Cisco-TNA	TCP/UDP	131	Cisco TNATIVE	cisco-tna	Cisco IOS XE Release 3.1S	
Clearcase	TCP/UDP	371	Clearcase	clearcase	Cisco IOS XE Release 3.1S	
Cloanto-Net-1	TCP/UDP	356	Cloanto-net-1	cloanto-net-1	Cisco IOS XE Release 3.1S	
CMIP-Agent	TCP/UDP	164	CMIP/TCP Agent	cmip-agent	Cisco IOS XE Release 3.1S	
CMIP-Man	TCP/UDP	163	CMIP/TCP Manager	cmip-man	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Coauthor	TCP/UDP	1529	Oracle	coauthor	Cisco IOS XE Release 3.1S	
Codaauth2	TCP/UDP	370	Codaauth2	codaauth2	Cisco IOS XE Release 3.1S	
Collaborator	TCP/UDP	622	Collaborator	collaborator	Cisco IOS XE Release 3.1S	
Commerce	TCP/UDP	542	Commerce	commerce	Cisco IOS XE Release 3.1S	
Compaq-Peer	TCP/UDP	110	Compaq Peer Protocol	compaq-peer	Cisco IOS XE Release 3.1S	
Compressnet	TCP/UDP	2	Management Utility	compressnet	Cisco IOS XE Release 3.1S	
COMSCM	TCP/UDP	437	COMSCM	comscm	Cisco IOS XE Release 3.1S	
CON	TCP/UDP	759	Con	con	Cisco IOS XE Release 3.1S	
Conference	TCP/UDP	531	Chat	conference	Cisco IOS XE Release 3.1S	
	Connendp	TCP/UDP	693	Almanid Connection Endpoint	connendp	Cisco IOS XE Release 3.1S
	ContentServer	TCP/UDP	3365	Contentserver	contentserver	Cisco IOS XE Release 3.1S
CoreRJD	TCP/UDP	284	Corerjd	corerjd	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Courier	TCP/UDP	530	RPC	courier	Cisco IOS XE Release 3.1S	
Covia	TCP/UDP	64	Communications Integrator	covia	Cisco IOS XE Release 3.1S	
CPHB	TCP/UDP	73	Computer Protocol Heart Beat	cphb	Cisco IOS XE Release 3.1S	
CPNX	TCP/UDP	72	Computer Protocol Network Executive	cpnx	Cisco IOS XE Release 3.1S	
Creativepartnr	TCP/UDP	455	Creativepartnr	creativepartnr	Cisco IOS XE Release 3.1S	
Creativeserver	TCP/UDP	453	Creativeserver	creativeserver	Cisco IOS XE Release 3.1S	
CRS	TCP/UDP	507	CRS	crs	Cisco IOS XE Release 3.1S	
CRTP	TCP/UDP	126	Combat Radio Transport Protocol	crtp	Cisco IOS XE Release 3.1S	
CRUDP	TCP/UDP	127	Combat Radio User Datagram	crudp	Cisco IOS XE Release 3.1S	
CryptoAdmin	TCP/UDP	624	Crypto Admin	cryptoadmin	Cisco IOS XE Release 3.1S	
CSI-SGWP	TCP/UDP	348	Cabletron Management Protocol	csi-sgwp	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
CSNET-NS	TCP/UDP	105	Mailbox Name Nameserver	csnet-ns	Cisco IOS XE Release 3.1S	
CTF	TCP/UDP	84	Common Trace Facility	ctf	Cisco IOS XE Release 3.1S	
CUSTIX	TCP/UDP	528	Customer Ixchange	custix	Cisco IOS XE Release 3.1S	
CVC_Hostd	TCP/UDP	442	CVC_Hostd	cvc_hostd	Cisco IOS XE Release 3.1S	
Cybercash	TCP/UDP	551	Cybercash	cybercash	Cisco IOS XE Release 3.1S	
Cycleserv	TCP/UDP	763	Cycleserv	cycleserv	Cisco IOS XE Release 3.1S	
	Cycleserv2	TCP/UDP	772	Cycleserv2	cycleserv2	Cisco IOS XE Release 3.1S
Dantz	TCP/UDP	497	Dantz	dantz	Cisco IOS XE Release 3.1S	
DASP	TCP/UDP	439	Dasp	dasp	Cisco IOS XE Release 3.1S	
DataSurfSRV	TCP/UDP	461	DataRamp Svr	datasurfsrv	Cisco IOS XE Release 3.1S	
DataSurfSRVSec	TCP/UDP	462	DataRamp Svr svs	datasurfsrvsec	Cisco IOS XE Release 3.1S	
Datex-ASN	TCP/UDP	355	datex-asn	datex-asn	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Daytime	TCP/UDP	13	Daytime (RFC 867)	daytime	Cisco IOS XE Release 3.1S	
Dbase	TCP/UDP	217	dBASE Unix	dbase	Cisco IOS XE Release 3.1S	
DCCP	TCP/UDP	33	Datagram Congestion Control Protocol	dccp	Cisco IOS XE Release 3.1S	
DCN-Meas	TCP/UDP	19	DCN Measurement Subsystems	dcn-meas	Cisco IOS XE Release 3.1S	
DCP	TCP/UDP	93	Device Control Protocol	dcp	Cisco IOS XE Release 3.1S	
DCTP	TCP/UDP	675	DCTP	dctp	Cisco IOS XE Release 3.1S	
DDM-DFM	TCP/UDP	447	DDM Distributed File management	ddm-dfm	Cisco IOS XE Release 3.1S	
DDM-RDB	TCP/UDP	446	DDM-Remote Relational Database Access	ddm-rdb	Cisco IOS XE Release 3.1S	
DDM-SSL	TCP/UDP	448	DDM-Remote DB Access Using Secure Sockets	ddm-ssl	Cisco IOS XE Release 3.1S	
DDP	TCP/UDP	37	Datagram Delivery Protocol	ddp	Cisco IOS XE Release 3.1S	
DDX	TCP/UDP	116	D-II Data Exchange	ddx	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
DEC_DLM	TCP/UDP	625	dec_dlm	dec_dlm	Cisco IOS XE Release 3.1S	
Decap	TCP/UDP	403	Decap	decap	Cisco IOS XE Release 3.1S	
	Decauth	TCP/UDP	316	Decauth	decauth	Cisco IOS XE Release 3.1S
Decbsrv	TCP/UDP	579	Decbsrv	decbsrv	Cisco IOS XE Release 3.1S	
Decladebug	TCP/UDP	410	DECLadebug Remote Debug Protocol	decladebug	Cisco IOS XE Release 3.1S	
Decvms-sysmgt	TCP/UDP	441	Decvms-sysmgt	decvms-sysmgt	Cisco IOS XE Release 3.1S	
DEI-ICDA	TCP/UDP	618	dei-icda	dei-icda	Cisco IOS XE Release 3.1S	
DEOS	TCP/UDP	76	Distributed External Object Store	deos	Cisco IOS XE Release 3.1S	
Device	TCP/UDP	801	Device	device	Cisco IOS XE Release 3.1S	
DGP	TCP/UDP	86	Dissimilar Gateway Protocol	dgp	Cisco IOS XE Release 3.1S	
DHCP-Failover	TCP/UDP	647	DHCP Failover	dhcp-failover	Cisco IOS XE Release 3.1S	
DHCP-Failover2	TCP/UDP	847	dhcp-failover2	dhcp-failover2	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
DHCPv6-client	TCP/UDP	546	DHCPv6 Client	dhcpv6-client	Cisco IOS XE Release 3.1S	
DHCPv6-server	TCP/UDP	547	DHCPv6 Server	dhcpv6-server	Cisco IOS XE Release 3.1S	
Dicom	TCP/UDP	Heuristic	Digital Imaging and Communications in Medicine	dicom	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.3S	
Digital-VRC	TCP/UDP	466	digital-vrc	digital-vrc	Cisco IOS XE Release 3.1S	
Directplay	TCP/UDP	2234	DirectPlay	directplay	Cisco IOS XE Release 3.1S	
Directplay8	TCP/UDP	6073	DirectPlay8	directplay8	Cisco IOS XE Release 3.1S	
Directv-Catlg	TCP/UDP	3337	Direct TV Data Catalog	directv-catlg	Cisco IOS XE Release 3.1S	
Directv-Soft	TCP/UDP	3335	Direct TV Software Updates	directv-soft	Cisco IOS XE Release 3.1S	
	Directv-Tick	TCP/UDP	3336	Direct TV Tickers	directv-tick	Cisco IOS XE Release 3.1S
	Directv-Web	TCP/UDP	3334	Direct TV Webcasting	directv-web	Cisco IOS XE Release 3.1S
Discard	TCP/UDP	9	Discard	discard	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Disclose	TCP/UDP	667	campaign contribution disclosures	disclose	Cisco IOS XE Release 3.1S	
Dixie	TCP/UDP	96	DIXIE Protocol Specification	dixie	Cisco IOS XE Release 3.1S	
DLS	TCP/UDP	197	Directory Location Service	dls	Cisco IOS XE Release 3.1S	
DLS-Mon	TCP/UDP	198	Directory Location Service Monitor	dls-mon	Cisco IOS XE Release 3.1S	
DN6-NLM-AUD	TCP/UDP	195	DNSIX Network Level Module Audit	dn6-nlm-aud	Cisco IOS XE Release 3.1S	
DNA-CML	TCP/UDP	436	DNA-CML	dna-cml	Cisco IOS XE Release 3.1S	
DNS	TCP/UDP	53	Domain Name Server lookup	dns	Cisco IOS XE Release 3.1S	
DNSIX	TCP/UDP	90	DNSIX Security Attribute Token Map	dnsix	Cisco IOS XE Release 3.1S	
DOOM	TCP/UDP	666	Doom Id Software	doom	Cisco IOS XE Release 3.1S	
DPSI	TCP/UDP	315	DPSI	dpsi	Cisco IOS XE Release 3.1S	
DSFGW	TCP/UDP	438	DSFGW	dsfgw	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
DSP	TCP/UDP	33	Display Support Protocol	dsp	Cisco IOS XE Release 3.1S	
DSP3270	TCP/UDP	246	Display Systems Protocol	dsp3270	Cisco IOS XE Release 3.1S	
DSR	TCP/UDP	48	Dynamic Source Routing Protocol	dsr	Cisco IOS XE Release 3.1S	
DTAG-DTE-SB	TCP/UDP	352	DTAG	dtag-ste-sb	Cisco IOS XE Release 3.1S	
DTK	TCP/UDP	365	DTK	dtk	Cisco IOS XE Release 3.1S	
	DWR	TCP/UDP	644	DWR	dwr	Cisco IOS XE Release 3.1S
Echo	TCP/UDP	7	Echo	echo	Cisco IOS XE Release 3.1S	
EGP	TCP/UDP	8	Exterior Gateway Protocol	egp	Cisco IOS XE Release 3.1S	
EIGRP	TCP/UDP	88	Enhanced Interior Gateway Routing Protocol	eigrp	Cisco IOS XE Release 3.1S	
ELCSD	TCP/UDP	704	errlog copy/server daemon	elcsd	Cisco IOS XE Release 3.1S	
EMBL-NDT	TCP/UDP	394	EMBL Nucleic Data Transfer	embl-ndt	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
EMCON	TCP/UDP	14	EMCON	emcon	Cisco IOS XE Release 3.1S	
EMFIS-CNTLl	TCP/UDP	141	EMFIS Control Service	emfis-cntl	Cisco IOS XE Release 3.1S	
EMFIS-Data	TCP/UDP	140	EMFIS Data Service	emfis-data	Cisco IOS XE Release 3.1S	
Encap	TCP/UDP	98	Encapsulation Header	encap	Cisco IOS XE Release 3.1S	
Encrypted Bittorrent	TCP	Heuristic	Encrypted Bittorrent	encrypted-bittorrent	Cisco IOS XE Release 3.4S	
Entomb	TCP/UDP	775	Entomb	entomb	Cisco IOS XE Release 3.1S	
Entrust-AAAS	TCP/UDP	680	Entrust-aaas	entrust-aaas	Cisco IOS XE Release 3.1S	
Entrust-AAMS	TCP/UDP	681	Entrust-aams	entrust-aams	Cisco IOS XE Release 3.1S	
Entrust-ASH	TCP/UDP	710	Entrust Administration Service Handler	entrust-ash	Cisco IOS XE Release 3.1S	
Entrust-KMSH	TCP/UDP	709	Entrust Key Management Service Handler	entrust-kmsh	Cisco IOS XE Release 3.1S	
Entrust-SPS	TCP/UDP	640	entrust-sps	entrust-sps	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
ERPC	TCP/UDP	121	Encore Expedited Remote Pro.Call	erpc	Cisco IOS XE Release 3.1S	
ESCP-IP	TCP/UDP	621	escp-ip	escp-ip	Cisco IOS XE Release 3.1S	
	ESRO-GEN	TCP/UDP	259	Efficient Short Remote Operations	esro-gen	Cisco IOS XE Release 3.1S
ESRP-EMSDP	TCP/UDP	642	ESRO-EMSDP V1.3	esro-emsdp	Cisco IOS XE Release 3.1S	
EtherIP	TCP/UDP	97	Ethernet-within-IP Encapsulation	etherip	Cisco IOS XE Release 3.1S	
Eudora-Set	TCP/UDP	592	Eudora Set	eudora-set	Cisco IOS XE Release 3.1S	
EXEC	TCP/UDP	512	remote process execution;	exec	Cisco IOS XE Release 3.1S	
Fatserv	TCP/UDP	347	Fatmen Server	fatserv	Cisco IOS XE Release 3.1S	
FC	TCP/UDP	133	Fibre Channel	fc	Cisco IOS XE Release 3.1S	
FCP	TCP/UDP	510	FirstClass Protocol	fcp	Cisco IOS XE Release 3.1S	
Finger	TCP/UDP	79	Finger	finger	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
FIRE	TCP/UDP	125	FIRE	fire	Cisco IOS XE Release 3.1S	
FlexLM	TCP/UDP	744	Flexible License Manager	flexlm	Cisco IOS XE Release 3.1S	
FLN-SPX	TCP/UDP	221	Berkeley rlogind with SPX auth	fln-spx	Cisco IOS XE Release 3.1S	
FTP-Agent	TCP/UDP	574	FTP Software Agent System	ftp-agent	Cisco IOS XE Release 3.1S	
FTP-Data	TCP/UDP	20	File Transfer	ftp-data	Cisco IOS XE Release 3.1S	
FTPS-Data	TCP/UDP	989	ftp protocol, data, over TLS/SSL	ftps-data	Cisco IOS XE Release 3.1S	
Fujitsu-Dev	TCP/UDP	747	Fujitsu Device Control	fujitsu-dev	Cisco IOS XE Release 3.1S	
GACP	TCP/UDP	190	Gateway Access Control Protocol	gacp	Cisco IOS XE Release 3.1S	
GDOMAP	TCP/UDP	538	gdomap	gdomap	Cisco IOS XE Release 3.1S	
Genie	TCP/UDP	402	Genie Protocol	genie	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
	Genrad-MUX	TCP/UDP	176	Genrad-mux	genrad-mux	Cisco IOS XE Release 3.1S
	GGF-NCP	TCP/UDP	678	GNU Generation Foundation NCP	ggf-ncp	Cisco IOS XE Release 3.1S
GGP	TCP/UDP	3	Gateway-to-Gateway	ggp	Cisco IOS XE Release 3.1S	
Ginad	TCP/UDP	634	ginad	ginad	Cisco IOS XE Release 3.1S	
GMTP	TCP/UDP	100	GMTP	gmtp	Cisco IOS XE Release 3.1S	
Go-Login	TCP/UDP	491	Go-login	go-login	Cisco IOS XE Release 3.1S	
Gopher	TCP/UDP	70	Gopher	gopher	Cisco IOS XE Release 3.1S	
Graphics	TCP/UDP	41	Graphics	graphics	Cisco IOS XE Release 3.1S	
GRE	TCP/UDP	47	General Routing Encapsulation	gre	Cisco IOS XE Release 3.1S	
Groove	TCP/UDP	2492	Groove	groove	Cisco IOS XE Release 3.1S	
GSS-HTTP	TCP/UDP	488	gss-http	gss-http	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
GSS-XLICEN	TCP/UDP	128	GNU Generation Foundation NCP	gss-xlicen	Cisco IOS XE Release 3.1S	
GTP-User	TCP/UDP	2152	GTP-User Plane	gtp-user	Cisco IOS XE Release 3.1S	
HA-Cluster	TCP/UDP	694	ha-cluster	ha-cluster	Cisco IOS XE Release 3.1S	
HAP	TCP/UDP	661	hap	hap	Cisco IOS XE Release 3.1S	
Hassle	TCP/UDP	375	Hassle	hassle	Cisco IOS XE Release 3.1S	
HCP-Wismar	TCP/UDP	686	Hardware Control Protocol Wismar	hcp-wismar	Cisco IOS XE Release 3.1S	
HDAP	TCP/UDP	263	hdap	hdap	Cisco IOS XE Release 3.1S	
Hello-port	TCP/UDP	652	HELLO_PORT	hello-port	Cisco IOS XE Release 3.1S	
HEMS	TCP/UDP	151	hems	hems	Cisco IOS XE Release 3.1S	
	HIP	TCP/UDP	139	Host Identity Protocol	hip	Cisco IOS XE Release 3.1S
	HL7	TCP	Dynamically assigned	Health Level Seven	hl7	12.2(18)ZYA 12.2(18)ZYA1
HMMP-IND	TCP/UDP	612	HMMP Indication	hmmp-ind	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
HMMP-OP	TCP/UDP	613	HMMP Operation	hmmp-op	Cisco IOS XE Release 3.1S	
HMP	TCP/UDP	20	Host Monitoring	hmp	Cisco IOS XE Release 3.1S	
HOPOPT	TCP/UDP	0	IPv6 Hop-by-Hop Option	hopopt	Cisco IOS XE Release 3.1S	
Hostname	TCP/UDP	101	NIC Host Name Server	hostname	Cisco IOS XE Release 3.1S	
HP-Alarm-Mgr	TCP/UDP	383	HP performance data alarm manager	hp-alarm-mgr	Cisco IOS XE Release 3.1S	
HP-Collector	TCP/UDP	381	HP performance data collector	hp-collector	Cisco IOS XE Release 3.1S	
HP-Managed-Node	TCP/UDP	382	HP performance data managed node	hp-managed-node	Cisco IOS XE Release 3.1S	
HTTP-ALT	TCP/UDP	8080	HTTP Alternate	http-alt	Cisco IOS XE Release 3.1S	
HTTP-Mgmt	TCP/UDP	280	http-mgmt	http-mgmt	Cisco IOS XE Release 3.1S	
HTTP-RPC-EPMAP	TCP/UDP	593	HTTP RPC Ep Map	http-rpc-epmap	Cisco IOS XE Release 3.1S	
Hybrid-POP	TCP/UDP	473	Hybrid-pop	hybrid-pop	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Hyper-G	TCP/UDP	418	Hyper-g	hyper-g	Cisco IOS XE Release 3.1S	
Hyperwave-ISP	TCP/UDP	692	Hyperwave-isp	hyperwave-isp	Cisco IOS XE Release 3.1S	
IAFDBase	TCP/UDP	480	iafdbase	iafdbase	Cisco IOS XE Release 3.1S	
IAFServer	TCP/UDP	479	iafserver	iafserver	Cisco IOS XE Release 3.1S	
IASD	TCP/UDP	432	iasd	iasd	Cisco IOS XE Release 3.1S	
IATP	TCP/UDP	117	Interactive Agent Transfer Protocol	iatp	Cisco IOS XE Release 3.1S	
IBM-App	TCP/UDP	385	IBM Application	ibm-app	Cisco IOS XE Release 3.1S	
	IBM-DB2	TCP/UDP	523	IBM-DB2	ibm-db2	Cisco IOS XE Release 3.1S
IBProtocol	TCP/UDP	6714	Internet Backplane Protocol	ibprotocol	Cisco IOS XE Release 3.1S	
ICLCNet-Locate	TCP/UDP	886	ICL coNETion locate server	iclcnet-locate	Cisco IOS XE Release 3.1S	
ICLNet_SVInfo	TCP/UDP	887	ICL coNETion server info	iclcnet_svinfo	Cisco IOS XE Release 3.1S	
ICMP	TCP/UDP	1	Internet Control Message	icmp	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
IDFP	TCP/UDP	549	idfp	idfp	Cisco IOS XE Release 3.1S	
IDPR	TCP/UDP	35	Inter-Domain Policy Routing Protocol	idpr	Cisco IOS XE Release 3.1S	
IDPRr-CMTP	TCP/UDP	38	IDPR Control Message Transport Protocol	idpr-cmtp	Cisco IOS XE Release 3.1S	
IDRP	TCP/UDP	45	Inter-Domain Routing Protocol	idrp	Cisco IOS XE Release 3.1S	
IEEE-MMS	TCP/UDP	651	ieee-mms	ieee-mms	Cisco IOS XE Release 3.1S	
IEEE-MMS-SSL	TCP/UDP	695	ieee-mms-ssl	ieee-mms-ssl	Cisco IOS XE Release 3.1S	
IFMP	TCP/UDP	101	Ipsilon Flow Management Protocol	ifmp	Cisco IOS XE Release 3.1S	
IGRP	TCP/UDP	9	Cisco interior gateway	igrp	Cisco IOS XE Release 3.1S	
IIOP	TCP/UDP	535	iiop	iiop	Cisco IOS XE Release 3.1S	
IL	TCP/UDP	40	IL Transport Protocol	il	Cisco IOS XE Release 3.1S	
IMSP	TCP/UDP	406	Interactive Mail Support Protocol	imsp	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
InBusiness	TCP/UDP	244	Inbusiness	inbusiness	Cisco IOS XE Release 3.1S	
Infoseek	TCP/UDP	414	InfoSeek	infoseek	Cisco IOS XE Release 3.1S	
Ingres-Net	TCP/UDP	134	INGRES-NET Service	ingres-net	Cisco IOS XE Release 3.1S	
	I-NLSP	TCP/UDP	52	Integrated Net Layer Security TUBA	i-nlsp	Cisco IOS XE Release 3.1S
Intecourier	TCP/UDP	495	Intecourier	intecourier	Cisco IOS XE Release 3.1S	
Integra-SME	TCP/UDP	484	Integra Software Management Environment	integra-sme	Cisco IOS XE Release 3.1S	
Intrinsia	TCP/UDP	503	intrinsa	intrinsa	Cisco IOS XE Release 3.1S	
IPCD	TCP/UDP	576	ipcd	ipcd	Cisco IOS XE Release 3.1S	
IPComp	TCP/UDP	108	IP Payload Compression Protocol	ipcomp	Cisco IOS XE Release 3.1S	
IPCServer	TCP/UDP	600	Sun IPC server	ipcserver	Cisco IOS XE Release 3.1S	
IPCV	TCP/UDP	71	Internet Packet Core Utility	ipcv	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
IPDD	TCP/UDP	578	ipdd	ipdd	Cisco IOS XE Release 3.1S	
IPINIP	TCP/UDP	4	IP in IP	ipinip	Cisco IOS XE Release 3.1S	
IPIP	TCP/UDP	94	IP-within-IP Encapsulation Protocol	ipip	Cisco IOS XE Release 3.1S	
IPLT	TCP/UDP	129	IPLT	iplt	Cisco IOS XE Release 3.1S	
IPP	TCP/UDP	631	Internet Printing Protocol	ipp	Cisco IOS XE Release 3.1S	
IPPC	TCP/UDP	67	Internet Pluribus Packet Core	ippc	Cisco IOS XE Release 3.1S	
Ipv6-Frag	TCP/UDP	44	Fragment Header for IPv6	ipv6-frag	Cisco IOS XE Release 3.1S	
Ipv6-ICMP	TCP/UDP	58	ICMP for IPv6	ipv6-icmp	Cisco IOS XE Release 3.1S	
Ipv6INIP	TCP/UDP	41	Ipv6 encapsulated	ipv6inip	Cisco IOS XE Release 3.1S	
ipv6-NonXT	TCP/UDP	59	No Next Header for IPv6	ipv6-nonxt	Cisco IOS XE Release 3.1S	
	Ipv6-OPTS	TCP/UDP	60	Destination Options for IPv6	ipv6-opts	Cisco IOS XE Release 3.1S
Ipv6-Route	TCP/UDP	43	Routing Header for IPv6	ipv6-route	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
IRC	TCP/UDP	194	Internet Relay Chat	irc	Cisco IOS XE Release 3.1S	
IRC-SERV	TCP/UDP	529	IRC-SERV	irc-serv	Cisco IOS XE Release 3.1S	
IRTP	TCP/UDP	28	Internet Reliable Transaction	irtp	Cisco IOS XE Release 3.1S	
IS99C	TCP/UDP	379	TIA/EIA/IS-99 modem client	is99c	Cisco IOS XE Release 3.1S	
IS99S	TCP/UDP	380	TIA/EIA/IS-99 modem server	is99s	Cisco IOS XE Release 3.1S	
ISAKMP	UDP	500, 4500	Internet Security Association & Key Management Protocol	isakmp	Cisco IOS XE Release 3.1S	
ISI-GI	TCP/UDP	55	ISI Graphics Language	isi-gl	Cisco IOS XE Release 3.1S	
ISIS	TCP/UDP	124	ISIS over IPv4	isis	Cisco IOS XE Release 3.1S	
ISO-ILL	TCP/UDP	499	ISO ILL Protocol	iso-ill	Cisco IOS XE Release 3.1S	
ISO-IP	TCP/UDP	147	iso-ip	iso-ip	Cisco IOS XE Release 3.1S	
ISO-TP0	TCP/UDP	146	iso-tp0	iso-tp0	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
ISO-TP4	TCP/UDP	29	ISO Transport Protocol Class 4	iso-tp4	Cisco IOS XE Release 3.1S	
ISO-TSAP	TCP/UDP	102	ISO-TSAP Class 0	iso-tsap	Cisco IOS XE Release 3.1S	
ISO-TSAP-C2	TCP/UDP	399	ISO Transport Class 2 Non-Control	iso-tsap-c2	Cisco IOS XE Release 3.1S	
ITM-MCELL-S	TCP/UDP	828	itm-mcell-s	itm-mcell-s	Cisco IOS XE Release 3.1S	
IXP-IN-IP	TCP/UDP	111	IPX in IP	ixp-in-ip	Cisco IOS XE Release 3.1S	
Jargon	TCP/UDP	148	Jargon	jargon	Cisco IOS XE Release 3.1S	
	Kali	TCP/UDP	2213	Kali	kali	Cisco IOS XE Release 3.1S
	K-Block	TCP/UDP	287	K-block	k-block	Cisco IOS XE Release 3.1S
Keyserver	TCP/UDP	584	Key Server	keyserver	Cisco IOS XE Release 3.1S	
KIS	TCP/UDP	186	KIS Protocol	kis	Cisco IOS XE Release 3.1S	
Klogin	TCP/UDP	543	klogin	klogin	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Knet-CMP	TCP/UDP	157	KNET/VM Command/Message Protocol	knet-cmp	Cisco IOS XE Release 3.1S	
Konspire2b	TCP/UDP	6085	Konspire2b p2p network	Konspire2b	Cisco IOS XE Release 3.1S	
Kpasswd	TCP/UDP	464	Kpasswd	kpasswd	Cisco IOS XE Release 3.1S	
Kryptolan	TCP/UDP	398	Kryptolan	kryptolan	Cisco IOS XE Release 3.1S	
Kshell	TCP/UDP	544	Kshell	kshell	Cisco IOS XE Release 3.1S	
L2TP	TCP/UDP	1701	l2tp	l2tp	Cisco IOS XE Release 3.1S	
LA-Maint	TCP/UDP	51	IMP Logical Address Maintenance	la-maint	Cisco IOS XE Release 3.1S	
LANServer	TCP/UDP	637	lanserver	lanserver	Cisco IOS XE Release 3.1S	
LARP	TCP/UDP	91	Locus Address Resolution Protocol	larp	Cisco IOS XE Release 3.1S	
LDAP	TCP/UDP	389	Lightweight Directory Access Protocol	ldap	Cisco IOS XE Release 3.1S	
LDP	TCP/UDP	646	LDP	ldp	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Leaf-1	TCP/UDP	25	Leaf-1	leaf-1	Cisco IOS XE Release 3.1S	
Leaf-2	TCP/UDP	26	Leaf-2	leaf-2	Cisco IOS XE Release 3.1S	
Legent-1	TCP/UDP	373	Legent Corporation	legent-1	Cisco IOS XE Release 3.1S	
	Legent-2	TCP/UDP	374	Legent Corporation	legent-2	Cisco IOS XE Release 3.1S
LJK-Login	TCP/UDP	472	ljk-login	ljk-login	Cisco IOS XE Release 3.1S	
Lockd	TCP/UDP	4045	NFS Lock Daemon Manager	lockd	Cisco IOS XE Release 3.1S	
Locus-Con	TCP/UDP	127	Locus PC-Interface Conn Server	locus-con	Cisco IOS XE Release 3.1S	
Locus-Map	TCP/UDP	125	Locus PC-Interface Net Map Ser	locus-map	Cisco IOS XE Release 3.1S	
MAC-SRVR-Admin	TCP/UDP	660	MacOS Server Admin	mac-srvr-admin	Cisco IOS XE Release 3.1S	
Magenta-Logic	TCP/UDP	313	Magenta-logic	magenta-logic	Cisco IOS XE Release 3.1S	
Mailbox-LM	TCP/UDP	505	Mailbox-lm	mailbox-lm	Cisco IOS XE Release 3.1S	
Mailq	TCP/UDP	174	MAILQ	mailq	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Maitrd	TCP/UDP	997	Maitrd	maitrd	Cisco IOS XE Release 3.1S	
MANET	TCP/UDP	138	MANET Protocols	manet	Cisco IOS XE Release 3.1S	
MasqDialer	TCP/UDP	224	Masqdialer	masqdialer	Cisco IOS XE Release 3.1S	
Matip-Type-A	TCP/UDP	350	MATIP Type A	matip-type-a	Cisco IOS XE Release 3.1S	
Matip-Type-B	TCP/UDP	351	MATIP Type B	matip-type-b	Cisco IOS XE Release 3.1S	
MCIDAS	TCP/UDP	112	McIDAS Data Transmission Protocol	mcidas	Cisco IOS XE Release 3.1S	
MCNS-Sec	TCP/UDP	638	mcns-sec	mcns-sec	Cisco IOS XE Release 3.1S	
MDC-Portmapper	TCP/UDP	685	mdc-portmapper	mdc-portmapper	Cisco IOS XE Release 3.1S	
MeComm	TCP/UDP	668	MeComm	mecomm	Cisco IOS XE Release 3.1S	
	MeRegister	TCP/UDP	669	MeRegister	meregister	Cisco IOS XE Release 3.1S
Merit-INP	TCP/UDP	32	MERIT Internodal Protocol	merit-inp	Cisco IOS XE Release 3.1S	
Meta5	TCP/UDP	393	Meta5	meta5	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Metagram	TCP/UDP	99	Metagram	metagram	Cisco IOS XE Release 3.1S	
Meter	TCP/UDP	570	Meter	meter	Cisco IOS XE Release 3.1S	
Mfcobol	TCP/UDP	86	Micro Focus Cobol	mfcobol	Cisco IOS XE Release 3.1S	
MFE-NSP	TCP/UDP	31	MFE Network Services Protocol	mfe-nsp	Cisco IOS XE Release 3.1S	
MFTP	TCP/UDP	349	mftp	mftp	Cisco IOS XE Release 3.1S	
Micom-PFS	TCP/UDP	490	Micom-pfs	micom-pfs	Cisco IOS XE Release 3.1S	
MICP	TCP/UDP	95	Mobile Internetworking Control Pro.	micp	Cisco IOS XE Release 3.1S	
Micromuse-LM	TCP/UDP	1534	micromuse-lm	micromuse-lm	Cisco IOS XE Release 3.1S	
MIT-DOV	TCP/UDP	91	MIT Dover Spooler	mit-dov	Cisco IOS XE Release 3.1S	
MIT-ML-Dev	TCP/UDP	83	MIT ML Device	mit-ml-dev	Cisco IOS XE Release 3.1S	
Mobile	TCP/UDP	55	IP Mobility	mobile	Cisco IOS XE Release 3.1S	
MobileIP-Agent	TCP/UDP	434	mobileip-agent	mobileip-agent	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
MobilIP-MN	TCP/UDP	435	mobilip-mn	mobilip-mn	Cisco IOS XE Release 3.1S	
Mondex	TCP/UDP	471	Mondex	mondex	Cisco IOS XE Release 3.1S	
Monitor	TCP/UDP	561	Monitor	monitor	Cisco IOS XE Release 3.1S	
Mortgageware	TCP/UDP	367	Mortgageware	mortgageware	Cisco IOS XE Release 3.1S	
	MPLS-IN-IP	TCP/UDP	137	MPLS-in-IP	mpls-in-ip	Cisco IOS XE Release 3.1S
MPM	TCP/UDP	45	Message Processing Module	mpm	Cisco IOS XE Release 3.1S	
MPM-Flags	TCP/UDP	44	MPM FLAGS Protocol	mpm-flags	Cisco IOS XE Release 3.1S	
MPM-SND	TCP/UDP	46	MPM [default send]	mpm-snd	Cisco IOS XE Release 3.1S	
MPP	TCP/UDP	218	Netix Message Posting Protocol	mpp	Cisco IOS XE Release 3.1S	
MPTN	TCP/UDP	397	Multi Protocol Transport Network	mptn	Cisco IOS XE Release 3.1S	
MRM	TCP/UDP	679	mrm	mrm	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
MSDP	TCP/UDP	639	msdp	msdp	Cisco IOS XE Release 3.1S	
MSExch-Routing	TCP/UDP	691	MS Exchange Routing	msexch-routing	Cisco IOS XE Release 3.1S	
MSFT-GC	TCP/UDP	3268	Microsoft Global Catalog	msft-gc	Cisco IOS XE Release 3.1S	
MSFT-GC-SSL	TCP/UDP	3269	Microsoft Global Catalog with LDAP/SSL	msft-gc-ssl	Cisco IOS XE Release 3.1S	
MSG-AUTH	TCP/UDP	31	msg-auth	msg-auth	Cisco IOS XE Release 3.1S	
MSG-ICP	TCP/UDP	29	msg-icp	msg-icp	Cisco IOS XE Release 3.1S	
MSNP	TCP/UDP	1863	msnp	msnp	Cisco IOS XE Release 3.1S	
MS-OLAP	TCP/UDP	2393	Microsoft OLAP	ms-olap	Cisco IOS XE Release 3.1S	
MSP	TCP/UDP	18	Message Send Protocol	msp	Cisco IOS XE Release 3.1S	
MS-Rome	TCP/UDP	569	Microsoft rome	ms-rome	Cisco IOS XE Release 3.1S	
MS-Shuttle	TCP/UDP	568	Microsoft shuttle	ms-shuttle	Cisco IOS XE Release 3.1S	
MS-SQLl-M	TCP/UDP	1434	MicrosoftSQL-Monitor	ms-sql-m	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
	MS-wbt	TCP	3389/Heuristic	Microsoft Windows based Terminal Services	ms-wbt	Cisco IOS XE Release 3.4S
	MTP	TCP/UDP	92	Multicast Transport Protocol	mtp	Cisco IOS XE Release 3.1S
Multiling-HTTP	TCP/UDP	777	Multiling HTTP	multiling-http	Cisco IOS XE Release 3.1S	
Multiplex	TCP/UDP	171	Network Innovations Multiplex	multiplex	Cisco IOS XE Release 3.1S	
Mumps	TCP/UDP	188	Plus Fives MUMPS	mumps	Cisco IOS XE Release 3.1S	
MUX	TCP/UDP	18	Multiplexing	mux	Cisco IOS XE Release 3.1S	
Mylex-MAPD	TCP/UDP	467	mylex-mapd	mylex-mapd	Cisco IOS XE Release 3.1S	
MySQL	TCP/UDP	3306	MySQL	mysql	Cisco IOS XE Release 3.1S	
Name	TCP/UDP	42	Host Name Server	name	Cisco IOS XE Release 3.1S	
NAMP	TCP/UDP	167	namp	namp	Cisco IOS XE Release 3.1S	
NARP	TCP/UDP	54	NBMA Address Resolution Protocol	narp	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
NAS	TCP/UDP	991	Netnews Administration System	nas	Cisco IOS XE Release 3.1S	
NCED	TCP/UDP	404	nced	nced	Cisco IOS XE Release 3.1S	
NCLD	TCP/UDP	405	ncld	ncld	Cisco IOS XE Release 3.1S	
NCP	TCP/UDP	524	NCP	ncp	Cisco IOS XE Release 3.1S	
NDSAuth	TCP/UDP	353	NDSAUTH	ndsauth	Cisco IOS XE Release 3.1S	
Nest-Protocol	TCP/UDP	489	Nest-protocol	nest-protocol	Cisco IOS XE Release 3.1S	
Net8-CMAN	TCP/UDP	1830	Oracle Net8 CMan Admin	net8-cman	Cisco IOS XE Release 3.1S	
Net-Assistant	TCP/UDP	3283	net-assistant	net-assistant	Cisco IOS XE Release 3.1S	
Netblt	TCP/UDP	30	Bulk Data Transfer Protocol	netblt	Cisco IOS XE Release 3.1S	
	NetGW	TCP/UDP	741	netgw	netgw	Cisco IOS XE Release 3.1S
	NetNews	TCP/UDP	532	readnews	netnews	Cisco IOS XE Release 3.1S
NetRCS	TCP/UDP	742	Network based RCS	netrcs	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
NetRJS-1	TCP/UDP	71	Remote Job Service	netrjs-1	Cisco IOS XE Release 3.1S	
NetRJS-2	TCP/UDP	72	Remote Job Service	netrjs-2	Cisco IOS XE Release 3.1S	
NetRJS-3	TCP/UDP	73	Remote Job Service	netrjs-3	Cisco IOS XE Release 3.1S	
NetRJS-4	TCP/UDP	74	Remote Job Service	netrjs-4	Cisco IOS XE Release 3.1S	
NETSC-Dev	TCP/UDP	155	NETSC	netsc-dev	Cisco IOS XE Release 3.1S	
NETSC-Prod	TCP/UDP	154	NETSC	netsc-prod	Cisco IOS XE Release 3.1S	
NetViewDM1	TCP/UDP	729	IBM NetView M	netviewdm1	Cisco IOS XE Release 3.1S	
NetviewDM2	TCP/UDP	730	IBM NetView DM	netviewdm2	Cisco IOS XE Release 3.1S	
NetviewDM3	TCP/UDP	731	IBM NetView DM	netviewdm3	Cisco IOS XE Release 3.1S	
Netwall	TCP/UDP	533	for emergency broadcasts	netwall	Cisco IOS XE Release 3.1S	
Netware-IP	TCP/UDP	396	Novell Netware over IP	netware-ip	Cisco IOS XE Release 3.1S	
New-RWHO	TCP/UDP	550	new who	new-rwho	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
NextStep	TCP/UDP	178	NextStep Window Server	nextstep	Cisco IOS XE Release 3.1S	
NFS	TCP/UDP	2049	Network File System	nfs	Cisco IOS XE Release 3.1S	
NicName	TCP/UDP	43	Who Is	nicname	Cisco IOS XE Release 3.1S	
NI-FTP	TCP/UDP	47	NI FTP	ni-ftp	Cisco IOS XE Release 3.1S	
NI-Mail	TCP/UDP	61	NI MAIL	ni-mail	Cisco IOS XE Release 3.1S	
	Nlogin	TCP/UDP	758	nlogin	nlogin	Cisco IOS XE Release 3.1S
	NMAP	TCP/UDP	689	nmap	nmap	Cisco IOS XE Release 3.1S
NMSP	TCP/UDP	537	Networked Media Streaming Protocol	nmsp	Cisco IOS XE Release 3.1S	
NNSP	TCP/UDP	433	nnsp	nnsp	Cisco IOS XE Release 3.1S	
Notes	TCP/UDP	1352	Lotus Notes(R)	notes	Cisco IOS XE Release 3.1S	
NovaStorBakcup	TCP/UDP	308	Novastor Backup	novastorbakcup	Cisco IOS XE Release 3.1S	
NPMP-GUI	TCP/UDP	611	npmp-gui	npmp-gui	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
NPMP-Local	TCP/UDP	610	npmp-local	npmp-local	Cisco IOS XE Release 3.1S	
NPMP-Trap	TCP/UDP	609	npmp-trap	npmp-trap	Cisco IOS XE Release 3.1S	
NPP	TCP/UDP	92	Network Printing Protocol	npp	Cisco IOS XE Release 3.1S	
NQS	TCP/UDP	607	nqs	nqs	Cisco IOS XE Release 3.1S	
NS	TCP/UDP	760	ns	ns	Cisco IOS XE Release 3.1S	
NSFNET-IGP	TCP/UDP	85	NSFNET-IGP	nsfnet-igp	Cisco IOS XE Release 3.1S	
NSIIOPS	TCP/UDP	261	IIOP Name Service over TLS/SSL	nsiiops	Cisco IOS XE Release 3.1S	
NSRMP	TCP/UDP	359	Network Security Risk Management Protocol	nsrmp	Cisco IOS XE Release 3.1S	
NSS-Routing	TCP/UDP	159	NSS-Routing	nss-routing	Cisco IOS XE Release 3.1S	
NSW-FE	TCP/UDP	27	NSW User System FE	nsw-fe	Cisco IOS XE Release 3.1S	
Ntalk	TCP/UDP	518	Ntalk	ntalk	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
NTP	TCP/ UDP	123	Network Time Protocol	ntp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S	
	NVP-II	TCP/UDP	11	Network Voice Protocol	nvp-ii	Cisco IOS XE Release 3.1S
NXEdit	TCP/UDP	126	nxedit	nxedit	Cisco IOS XE Release 3.1S	
OBCBinder	TCP/UDP	183	ocbinder	ocbinder	Cisco IOS XE Release 3.1S	
OBEX	TCP/UDP	650	obex	obex	Cisco IOS XE Release 3.1S	
ObjCall	TCP/UDP	94	Tivoli Object Dispatcher	objcall	Cisco IOS XE Release 3.1S	
OCS_AMU	TCP/UDP	429	ocs_amu	ocs_amu	Cisco IOS XE Release 3.1S	
OCS_CMU	TCP/UDP	428	ocs_cmu	ocs_cmu	Cisco IOS XE Release 3.1S	
OCServer	TCP/UDP	184	ocserver	ocserver	Cisco IOS XE Release 3.1S	
ODMR	TCP/UDP	366	odmr	odmr	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
OHIMSRV	TCP/UDP	506	ohimsrv	ohimsrv	Cisco IOS XE Release 3.1S	
OLSR	TCP/UDP	698	olsr	olsr	Cisco IOS XE Release 3.1S	
OMGInitialRefs	TCP/UDP	900	omginitialrefs	omginitialrefs	Cisco IOS XE Release 3.1S	
OMServ	TCP/UDP	764	omserv	omserv	Cisco IOS XE Release 3.1S	
ONMUX	TCP/UDP	417	onmux	onmux	Cisco IOS XE Release 3.1S	
Opalis-RDV	TCP/UDP	536	Opalis-rdv	opalis-rdv	Cisco IOS XE Release 3.1S	
Opalis-Robot	TCP/UDP	314	oOpalis-robot	opalis-robot	Cisco IOS XE Release 3.1S	
OPC-Job-Start	TCP/UDP	423	IBM Operations Planning and Control Start	opc-job-start	Cisco IOS XE Release 3.1S	
OPC-Job-Track	TCP/UDP	424	IBM Operations Planning and Control Track	opc-job-track	Cisco IOS XE Release 3.1S	
	Openport	TCP/UDP	260	Openport	openport	Cisco IOS XE Release 3.1S
OpenVMS-Sysipc	TCP/UDP	557	Openvms-sysipc	openvms-sysipc	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
OracleNames	TCP/UDP	1575	Oraclenames	oraclenames	Cisco IOS XE Release 3.1S	
OracleNet8CMAN	TCP/UDP	1630	Oracle Net8 Cman	oraclenet8cman	Cisco IOS XE Release 3.1S	
ORA-Srv	TCP/UDP	1525	Oracle TCP/IP Listener	ora-srv	12.2(18)ZYA 12.2(18)ZYA Cisco IOS XE Release 3.1S	
Orbix-Config	TCP/UDP	3076	Orbix 2000 Config	orbix-config	Cisco IOS XE Release 3.1S	
Orbix-Locator	TCP/UDP	3075	Orbix 2000 Locator	orbix-locator	Cisco IOS XE Release 3.1S	
Orbix-Loc-SSL	TCP/UDP	3077	Orbix 2000 Locator SSL	orbix-loc-ssl	Cisco IOS XE Release 3.1S	
OSPF	TCP/UDP	89	Open Shortest Path First	ospf	Cisco IOS XE Release 3.1S	
OSU-NMS	TCP/UDP	192	OSU Network Monitoring System	osu-nms	Cisco IOS XE Release 3.1S	
Parsec-Game	TCP/UDP	6582	Parsec Gameserver	parsec-game	Cisco IOS XE Release 3.1S	
Passgo	TCP/UDP	511	Passgo	passgo	Cisco IOS XE Release 3.1S	
Passgo-Tivoli	TCP/UDP	627	Passgo-tivoli	passgo-tivoli	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Password-Chg	TCP/UDP	586	Password Change	password-chg	Cisco IOS XE Release 3.1S	
Pawserv	TCP/UDP	345	Perf Analysis Workbench	pawserv	Cisco IOS XE Release 3.1S	
PCMail-SRV	TCP/UDP	158	PCMail Server	pcmail-srv	Cisco IOS XE Release 3.1S	
PDAP	TCP/UDP	344	Prospero Data Access Protocol	pdap	Cisco IOS XE Release 3.1S	
Personal-link	TCP/UDP	281	Personal-link	personal-link	Cisco IOS XE Release 3.1S	
PFTP	TCP/UDP	662	Parallel File Transfer Protocol	pftp	Cisco IOS XE Release 3.1S	
	PGM	TCP/UDP	113	PGM Reliable Transport Protocol	pgm	Cisco IOS XE Release 3.1S
Philips-VC	TCP/UDP	583	Philips Video-Conferencing	philips-vc	Cisco IOS XE Release 3.1S	
Phonebook	TCP/UDP	767	Phone	phonebook	Cisco IOS XE Release 3.1S	
Photuris	TCP/UDP	468	Photuris	photuris	Cisco IOS XE Release 3.1S	
PIM	TCP/UDP	103	Protocol Independent Multicast	pim	Cisco IOS XE Release 3.1S	
PIM-RP-DISC	TCP/UDP	496	PIM-RP-DISC	pim-rp-disc	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
PIP	TCP/UDP	1321	pip	pip	Cisco IOS XE Release 3.1S	
PIPE	TCP/UDP	131	Private IP Encapsulation within IP	pipe	Cisco IOS XE Release 3.1S	
PIRP	TCP/UDP	553	pirp	pirp	Cisco IOS XE Release 3.1S	
PKIX-3-CA-RA	TCP/UDP	829	PKIX-3 CA/RA	pkix-3-ca-ra	Cisco IOS XE Release 3.1S	
PKIX-Timestamp	TCP/UDP	318	pkix-timestamp	pkix-timestamp	Cisco IOS XE Release 3.1S	
PNNI	TCP/UDP	102	PNNI over IP	pnni	Cisco IOS XE Release 3.1S	
Pop2	TCP/UDP	109	Post Office Protocol - Version 2	pop2	Cisco IOS XE Release 3.1S	
Pop3	TCP/UDP	110, Heuristic	Post Office Protocol 3	pop3	Cisco IOS XE Release 3.1S	
POV-Ray	TCP/UDP	494	pov-ray	pov-ray	Cisco IOS XE Release 3.1S	
Powerburst	TCP/UDP	485	Air Soft Power Burst	powerburst	Cisco IOS XE Release 3.1S	
PPStream	TCP/UDP	Heuristic	P2P TV Application	ppstream	Cisco IOS XE Release 3.3S	
PPTP	TCP/UDP	1723	Point-to-Point Tunneling Protocol	pptp	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
	Printer	TCP/UDP	515	spooler	printer	12.1(2)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S
Print-SRV	TCP/UDP	170	Network PostScript	print-srv	Cisco IOS XE Release 3.1S	
PRM	TCP/UDP	21	Packet Radio Measurement	prm	Cisco IOS XE Release 3.1S	
PRM-NM	TCP/UDP	409	Prospero Resource Manager Node Man	prm-nm	Cisco IOS XE Release 3.1S	
PRM-SM	TCP/UDP	408	Prospero Resource Manager Sys. Man	prm-sm	Cisco IOS XE Release 3.1S	
Profile	TCP/UDP	136	PROFILE Naming System	profile	Cisco IOS XE Release 3.1S	
Prospero	TCP/UDP	191	Prosper Directory Service	prospero	Cisco IOS XE Release 3.1S	
PTCNameService	TCP/UDP	597	PTC Name Service	ptcnameservice	Cisco IOS XE Release 3.1S	
PTP	TCP/UDP	123	Performance Transparency Protocol	ptp	Cisco IOS XE Release 3.1S	
PTP-Event	TCP/UDP	319	PTP Event	ptp-event	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
PTP-General	TCP/UDP	320	PTP General	ptp-general	Cisco IOS XE Release 3.1S	
Pump	TCP/UDP	751	Pump	pump	Cisco IOS XE Release 3.1S	
PUP	TCP/UDP	12	PUP	pup	Cisco IOS XE Release 3.1S	
Purenoise	TCP/UDP	663	purenoise	purenoise	Cisco IOS XE Release 3.1S	
PVP	TCP/UDP	75	Packet Video Protocol	pvp	Cisco IOS XE Release 3.1S	
PWDGen	TCP/UDP	129	Password Generator Protocol	pwdgen	Cisco IOS XE Release 3.1S	
QBIKGDP	TCP/UDP	368	qbikgdp	qbikgdp	Cisco IOS XE Release 3.1S	
QFT	TCP/UDP	189	Queued File Transport	qft	Cisco IOS XE Release 3.1S	
QMQP	TCP/UDP	628	qmqp	qmqp	Cisco IOS XE Release 3.1S	
	QMTP	TCP/UDP	209	The Quick Mail Transfer Protocol	qmtp	Cisco IOS XE Release 3.1S
	QNX	TCP/UDP	106	QNX	qnx	Cisco IOS XE Release 3.1S
QoTD	TCP/UDP	17	Quote of the Day	qotd	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
QRH	TCP/UDP	752	qrh	qrh	Cisco IOS XE Release 3.1S	
QUOTD	TCP/UDP	762	quotad	quotad	Cisco IOS XE Release 3.1S	
r-commands	TCP	Dynamically assigned	rsh, rlogin, rexec	rcmd	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1	
RAP	TCP/UDP	38	Route Access Protocol	rap	Cisco IOS XE Release 3.1S	
RCMD	TCP	512–514	BSD r-commands	rcmd	Cisco IOS XE Release 3.3S	
RCP	TCP/UDP	469	Radio Control Protocol	rcp	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S	
RDA	TCP/UDP	630	rda	rda	Cisco IOS XE Release 3.1S	
RDB-DBS-DISP	TCP/UDP	1571	Oracle Remote Data Base	rdb-dbs-disp	Cisco IOS XE Release 3.1S	
RDP	TCP/UDP	27	Reliable Data Protocol	rdp	Cisco IOS XE Release 3.1S	
Realm-RUSD	TCP/UDP	688	ApplianceWare managment protocol	realm-rusd	Cisco IOS XE Release 3.1S	
RE-Mail-CK	TCP/UDP	50	Remote Mail Checking Protocol	re-mail-ck	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
RemoteFS	TCP/UDP	556	rfs server	remotefs	Cisco IOS XE Release 3.1S	
Remote-KIS	TCP/UDP	185	Remote-kis	remote-kis	Cisco IOS XE Release 3.1S	
REPCMD	TCP/UDP	641	repcmd	repcmd	Cisco IOS XE Release 3.1S	
REPSCMD	TCP/UDP	653	repscmd	repscmd	Cisco IOS XE Release 3.1S	
RESCAP	TCP/UDP	283	rescap	rescap	Cisco IOS XE Release 3.1S	
RIP	TCP/UDP	520	Routing Information Protocol	rip	Cisco IOS XE Release 3.1S	
	RIPING	TCP/UDP	521	ripng	ripng	Cisco IOS XE Release 3.1S
	RIS	TCP/UDP	180	Intergraph	ris	Cisco IOS XE Release 3.1S
RIS-CM	TCP/UDP	748	Russell Info Sci Calendar Manager	ris-cm	Cisco IOS XE Release 3.1S	
RJE	TCP/UDP	5	Remote Job Entry	rje	Cisco IOS XE Release 3.1S	
RLP	TCP/UDP	39	Resource Location Protocol	rlp	Cisco IOS XE Release 3.1S	
RLZDBASE	TCP/UDP	635	rlzdbase	rlzdbase	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
RMC	TCP/UDP	657	rmc	rmc	Cisco IOS XE Release 3.1S	
RMIActivation	TCP/UDP	1098	rmiactivation	rmiactivation	Cisco IOS XE Release 3.1S	
RMIRegistry	TCP/UDP	1099	rmiregistry	rmiregistry	Cisco IOS XE Release 3.1S	
RMonitor	TCP/UDP	560	Rmonitord	rmonitor	Cisco IOS XE Release 3.1S	
RMT	TCP/UDP	411	Remote MT Protocol	rmt	Cisco IOS XE Release 3.1S	
RPC2Portmap	TCP/UDP	369	rpc2portmap	rpc2portmap	Cisco IOS XE Release 3.1S	
RRH	TCP/UDP	753	rrh	rrh	Cisco IOS XE Release 3.1S	
RRP	TCP/UDP	648	Registry Registrar Protocol	rrp	Cisco IOS XE Release 3.1S	
RSH-SPX	TCP/UDP	222	Berkeley rshd with SPX auth	rsh-spx	Cisco IOS XE Release 3.1S	
RSVD	TCP/UDP	168	rsvd	rsvd	Cisco IOS XE Release 3.1S	
RSVP_Tunnel	TCP/UDP	363	rsvp_tunnel	rsvp_tunnel	Cisco IOS XE Release 3.1S	
RSVP-E2E-Ignore	TCP/UDP	134	RSVP-E2E-IGNORE	rsvp-e2e-ignore	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Rsync	TCP/UDP	873	Rsync	rsync	Cisco IOS XE Release 3.1S	
RTelnet	TCP/UDP	107	Remote Telnet Service	rtelnet	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S	
	RTIP	TCP/UDP	771	Real Time Streaming Protocol	rtip	Cisco IOS XE Release 3.1S
RTMP	TCP	Heuristic	Real Time Messaging Protocol	rtmp	Cisco IOS XE Release 3.4S	
RTSPS	TCP/UDP	322	RTSPS	rtsps	Cisco IOS XE Release 3.1S	
Rushd	TCP/UDP	696	Rushd	rushd	Cisco IOS XE Release 3.1S	
RVD	TCP/UDP	66	MIT Remote Virtual Disk Protocol	rvd	Cisco IOS XE Release 3.1S	
RXE	TCP/UDP	761	rxe	rxe	Cisco IOS XE Release 3.1S	
SAFT	TCP/UDP	487	saft Simple Asynchronous File Transfer	saft	Cisco IOS XE Release 3.1S	
Sanity	TCP/UDP	643	Sanity	sanity	Cisco IOS XE Release 3.1S	
SAT-EXPAK	TCP/UDP	64	SATNET and Backroom EXPAK	sat-expak	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
SAT-Mon	TCP/UDP	69	SATNET Monitoring	sat-mon	Cisco IOS XE Release 3.1S	
SCC-Security	TCP/UDP	582	scc-security	scc-security	Cisco IOS XE Release 3.1S	
SCC-SP	TCP/UDP	96	Semaphore Communications Sec. Pro.	scc-sp	Cisco IOS XE Release 3.1S	
SCO-DTMgr	TCP/UDP	617	SCO Desktop Administration Server	sco-dtmgr	Cisco IOS XE Release 3.1S	
SCOHELP	TCP/UDP	457	scohelp	scohelp	Cisco IOS XE Release 3.1S	
SCOI2ODialog	TCP/UDP	360	scoi2odialog	scoi2odialog	Cisco IOS XE Release 3.1S	
SCO-Inetmgr	TCP/UDP	615	Internet Configuration Manager	sco-inetmgr	Cisco IOS XE Release 3.1S	
SCO-SysMgr	TCP/UDP	616	SCO System Administration Server	sco-sysmgr	Cisco IOS XE Release 3.1S	
SCO-WebsrvrMg3	TCP/UDP	598	SCO Web Server Manager 3	sco-websrvrmg3	Cisco IOS XE Release 3.1S	
SCO-WebsrvrMgr	TCP/UDP	620	SCO WebServer Manager	sco-websrvrmgr	Cisco IOS XE Release 3.1S	
	SCPS	TCP/UDP	105	SCPS	scps	Cisco IOS XE Release 3.1S

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
SCTP	TCP/UDP	132	Stream Control Transmission Protocol	sctp	Cisco IOS XE Release 3.1S	
SCX-Proxy	TCP/UDP	470	scx-proxy	scx-proxy	Cisco IOS XE Release 3.1S	
SDNSKMP	TCP/UDP	558	SDNSKMP	sdnskmp	Cisco IOS XE Release 3.1S	
SDRP	TCP/UDP	42	Source Demand Routing Protocol	sdrp	Cisco IOS XE Release 3.1S	
Secure-ftp	TCP/UDP	990	ftp protocol, control, over TLS/SSL	secure-ftp	Cisco IOS XE Release 3.1S	
Secure-IRC	TCP/UDP	994	irc protocol over TLS	secure-irc	Cisco IOS XE Release 3.1S	
Secure-LDAP	TCP/UDP	636	ldap protocol over TLS	secure-ldap	Cisco IOS XE Release 3.1S	
Secure-NNTP	TCP/UDP	563	nntp protocol over TLS	secure-nntp	Cisco IOS XE Release 3.1S	
Secure-Pop3	TCP/UDP	995	pop3 protocol over TLS	secure-pop3	Cisco IOS XE Release 3.1S	
Secure-Telnet	TCP/UDP	992	telnet protocol over TLS	secure-telnet	Cisco IOS XE Release 3.1S	
Secure-VMTP	TCP/UDP	82	SECURE-VMTP	secure-vmtp	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Semantix	TCP/UDP	361	Semantix	semantix	Cisco IOS XE Release 3.1S	
Send	TCP/UDP	169	SEND	send	Cisco IOS XE Release 3.1S	
Server-IPX	TCP/UDP	213	Internetwork Packet Exchange Protocol	server-ipx	Cisco IOS XE Release 3.1S	
Servstat	TCP/UDP	633	Service Status update	servstat	Cisco IOS XE Release 3.1S	
SET	TCP/UDP	257	Secure Electronic Transaction	set	Cisco IOS XE Release 3.1S	
SFS-Config	TCP/UDP	452	Cray SFS config server	sfs-config	Cisco IOS XE Release 3.1S	
	SFS-SMP-Net	TCP/UDP	451	Cray Network Semaphore server	sfs-smp-net	Cisco IOS XE Release 3.1S
SFTP	TCP/UDP	115	Simple File Transfer Protocol	sftp	Cisco IOS XE Release 3.1S	
SGCP	TCP/UDP	440	sgcp	sgcp	Cisco IOS XE Release 3.1S	
SGMP	TCP/UDP	153	sgmp	sgmp	Cisco IOS XE Release 3.1S	
SGMP-Traps	TCP/UDP	160	sgmp-traps	sgmp-traps	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Shockwave	TCP/UDP	1626	Shockwave	shockwave	Cisco IOS XE Release 3.1S	
Shrinkwrap	TCP/UDP	358	Shrinkwrap	shrinkwrap	Cisco IOS XE Release 3.1S	
SIAM	TCP/UDP	498	siam	siam	Cisco IOS XE Release 3.1S	
SIFT-UFT	TCP/UDP	608	Sender-Initiated/Unsolicited File Transfer	sift-uft	Cisco IOS XE Release 3.1S	
SILC	TCP/UDP	706	silc	silc	Cisco IOS XE Release 3.1S	
SitaraDir	TCP/UDP	2631	Sitaradir	sitaradir	Cisco IOS XE Release 3.1S	
SitaraMgmt	TCP/UDP	2630	Sitaramgmt	sitaramgmt	Cisco IOS XE Release 3.1S	
Sitaraserver	TCP/UDP	2629	sitaraserver	sitaraserver	Cisco IOS XE Release 3.1S	
SKIP	TCP/UDP	57	SKIP	skip	Cisco IOS XE Release 3.1S	
SKRONK	TCP/UDP	460	skronk	skronk	Cisco IOS XE Release 3.1S	
SM	TCP/UDP	122	SM	sm	Cisco IOS XE Release 3.1S	
Smakynet	TCP/UDP	122	Smakynet	smakynet	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
SmartSDP	TCP/UDP	426	Smartsdp	smartsdp	Cisco IOS XE Release 3.1S	
SMP	TCP/UDP	121	Simple Message Protocol	smp	Cisco IOS XE Release 3.1S	
	SMPNameRes	TCP/UDP	901	smpnameres	smpnameres	Cisco IOS XE Release 3.1S
	SMSD	TCP/UDP	596	smsd	smsd	Cisco IOS XE Release 3.1S
SMSP	TCP/UDP	413	Storage Management Services Protocol	smsp	Cisco IOS XE Release 3.1S	
SMUX	TCP/UDP	199	SMUX	smux	Cisco IOS XE Release 3.1S	
SNAGas	TCP/UDP	108	SNA Gateway Access Server	snagas	Cisco IOS XE Release 3.1S	
Snare	TCP/UDP	509	Snare	snare	Cisco IOS XE Release 3.1S	
S-Net	TCP/UDP	166	Sirius Systems	s-net	Cisco IOS XE Release 3.1S	
SNP	TCP/UDP	109	Sitara Networks Protocol	snp	Cisco IOS XE Release 3.1S	
SNPP	TCP/UDP	444	Simple Network Paging Protocol	snpp	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
SNTP-Heartbeat	TCP/UDP	580	SNTP HEARTBEAT	sntp-heartbeat	Cisco IOS XE Release 3.1S	
SoftPC	TCP/UDP	215	Insignia Solutions	softpc	Cisco IOS XE Release 3.1S	
Sonar	TCP/UDP	572	Sonar	sonar	Cisco IOS XE Release 3.1S	
SPMP	TCP/UDP	656	spmp	spmp	Cisco IOS XE Release 3.1S	
Sprite-RPC	TCP/UDP	90	Sprite RPC Protocol	sprite-rpc	Cisco IOS XE Release 3.1S	
SPS	TCP/UDP	130	Secure Packet Shield	sps	Cisco IOS XE Release 3.1S	
SPSC	TCP/UDP	478	spsc	spsc	Cisco IOS XE Release 3.1S	
SQL*Net	TCP/UDP	66	Oracle SQL*NET	sql*net	Cisco IOS XE Release 3.1S	
SQLExec	TCP/UDP	9088	SQL Informix	sqlexec	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.1S	
SQL-Net	TCP/UDP	150	SQL-NET	sql-net	Cisco IOS XE Release 3.1S	
	SQLServ	TCP/UDP	118	SQL Services	sqlserv	Cisco IOS XE Release 3.1S

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
SQLServer	TCP/UDP	1433	Microsoft-SQL-Server	sqlserver	Cisco IOS XE Release 3.1S	
SRC	TCP/UDP	200	IBM System Resource Controller	src	Cisco IOS XE Release 3.1S	
SRMP	TCP/UDP	193	Spider Remote Monitoring Protocol	srmp	Cisco IOS XE Release 3.1S	
SRP	TCP/UDP	119	SpectraLink Radio Protocol	srp	Cisco IOS XE Release 3.1S	
SRSSend	TCP/UDP	362	srssend	srssend	Cisco IOS XE Release 3.1S	
SS7NS	TCP/UDP	477	ss7ns	ss7ns	Cisco IOS XE Release 3.1S	
SSCOPMCE	TCP/UDP	128	SSCOPMCE	sscopmce	Cisco IOS XE Release 3.1S	
SSH	TCP/UDP	22	Secure Shell Protocol	ssh	Cisco IOS XE Release 3.1S	
Sshell	TCP/UDP	614	SSLshell	sshell	Cisco IOS XE Release 3.1S	
SST	TCP/UDP	266	SCSI on ST	sst	Cisco IOS XE Release 3.1S	
ST	TCP/UDP	5	Stream	st	Cisco IOS XE Release 3.1S	
StatSRV	TCP/UDP	133	Statistics Service	statsrv	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
STMF	TCP/UDP	501	stmf	stmf	Cisco IOS XE Release 3.1S	
STP	TCP/UDP	118	Schedule Transfer Protocol	stp	Cisco IOS XE Release 3.1S	
StreetTalk	TCP/UDP	566	Streettalk	streettalk	Cisco IOS XE Release 3.1S	
Stun-NAT	TCP/UDP	3478	STUN	stun-nat	Cisco IOS XE Release 3.1S	
STX	TCP/UDP	527	Stock IXChange	stx	Cisco IOS XE Release 3.1S	
Submission	TCP/UDP	587	Submission	submission	Cisco IOS XE Release 3.1S	
	Subntbcst_TFTP	TCP/UDP	247	subntbcst_tftp	subntbcst_tftp	Cisco IOS XE Release 3.1S
SU-MIT-TG	TCP/UDP	89	SU/MIT Telnet Gateway	su-mit-tg	Cisco IOS XE Release 3.1S	
Sun-DR	TCP/UDP	665	sun-dr	sun-dr	Cisco IOS XE Release 3.1S	
Sun-ND	TCP/UDP	77	SUN ND PROTOCOL-Temporary	sun-nd	Cisco IOS XE Release 3.1S	
SupDup	TCP/UDP	95	SUPDUP	supdup	Cisco IOS XE Release 3.1S	
Surf	TCP/UDP	1010	Surf	surf	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Sur-Meas	TCP/UDP	243	Survey Measurement	sur-meas	Cisco IOS XE Release 3.1S	
Svrloc	TCP/UDP	427	Server Location	svrloc	Cisco IOS XE Release 3.1S	
Swift-RVF	TCP/UDP	97	Swift Remote Virtual File Protocol	swift-rvf	Cisco IOS XE Release 3.1S	
Swipe	TCP/UDP	53	IP with Encryption	swipe	Cisco IOS XE Release 3.1S	
Synoptics-Trap	TCP/UDP	412	Trap Convention Port	synoptics-trap	Cisco IOS XE Release 3.1S	
Synotics-Broker	TCP/UDP	392	SynOptics Port Broker Port	synotics-broker	Cisco IOS XE Release 3.1S	
Synotics-Relay	TCP/UDP	391	SynOptics SNMP Relay Port	synotics-relay	Cisco IOS XE Release 3.1S	
Systat	TCP/UDP	11	Active Users	systat	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S	
TACACS	TCP/UDP	49, 65	Terminal Access Controller Access Control System	tacacs	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S	
TAC News	TCP/UDP	98	TAC News	tacnews	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release	
Talk	TCP/UDP	517	Talk	talk	Cisco IOS XE Release 3.1S		
		TCF	TCP/UDP	87	TCF	tcf	Cisco IOS XE Release 3.1S
TD-Replica	TCP/UDP	268	Tobit David Replica	td-replica	Cisco IOS XE Release 3.1S		
TD-Service	TCP/UDP	267	Tobit David Service Layer	td-service	Cisco IOS XE Release 3.1S		
Teedtap	TCP/UDP	559	Teedtap	teedtap	Cisco IOS XE Release 3.1S		
Tell	TCP/UDP	754	Send	tell	Cisco IOS XE Release 3.1S		
Telnet	TCP/UDP	23	Telnet	telnet	Cisco IOS XE Release 3.1S		
Tempo	TCP/UDP	526	newdate	tempo	Cisco IOS XE Release 3.1S		
Tenfold	TCP/UDP	658	Tenfold	tenfold	Cisco IOS XE Release 3.1S		
Texar	TCP/UDP	333	Texar Security Port	texar	Cisco IOS XE Release 3.1S		
TICF-1	TCP/UDP	492	Transport Independent Convergence for FNA	ticf-1	Cisco IOS XE Release 3.1S		

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
TICF-2	TCP/UDP	493	Transport Independent Convergence for FNA	ticf-2	Cisco IOS XE Release 3.1S	
Timbuktu	TCP/UDP	407	Timbuktu	timbuktu	Cisco IOS XE Release 3.1S	
Time	TCP/UDP	37	Time	time	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S	
Timed	TCP/UDP	525	Timeserver	timed	Cisco IOS XE Release 3.1S	
TINC	TCP/UDP	655	tinc	tinc	Cisco IOS XE Release 3.1S	
TLISRV	TCP/UDP	1527	Oracle	tlisrv	Cisco IOS XE Release 3.1S	
TLSP	TCP/UDP	56	Transport Layer Security Protocol	tlsp	Cisco IOS XE Release 3.1S	
TNETOS	TCP/UDP	377	NEC Corporation	tnETOS	Cisco IOS XE Release 3.1S	
TNS-CML	TCP/UDP	590	tns-cml	tns-cml	Cisco IOS XE Release 3.1S	
TN-TL-FD1	TCP/UDP	476	tn-tl-fd1	tn-tl-fd1	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
TP++	TCP/UDP	39	TP++ Transport Protocol	tp++	Cisco IOS XE Release 3.1S	
TPIP	TCP/UDP	594	tpip	tpip	Cisco IOS XE Release 3.1S	
Trunk-1	TCP/UDP	23	Trunk-1	trunk-1	Cisco IOS XE Release 3.1S	
Trunk-2	TCP/UDP	24	Trunk-2	trunk-2	Cisco IOS XE Release 3.1S	
TServer	TCP/UDP	450	Computer Supported Telecomunication Applications	tserver	Cisco IOS XE Release 3.1S	
TTP	TCP/UDP	84	TTP	ttp	Cisco IOS XE Release 3.1S	
UAAC	TCP/UDP	145	UAAC Protocol	uaac	Cisco IOS XE Release 3.1S	
UARPs	TCP/UDP	219	Unisys ARPs	uarps	Cisco IOS XE Release 3.1S	
UDPLite	TCP/UDP	136	UDPLite	udplite	Cisco IOS XE Release 3.1S	
UIS	TCP/UDP	390	uis	uis	Cisco IOS XE Release 3.1S	
uLISTProc	TCP/UDP	372	List Processor	ulistproc	Cisco IOS XE Release 3.1S	
ULP	TCP/UDP	522	ulp	ulp	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
ULPNet	TCP/UDP	483	ulpnet	ulpnet	Cisco IOS XE Release 3.1S	
Unidata-LDM	TCP/UDP	388	Unidata LDM	unidata-ldm	Cisco IOS XE Release 3.1S	
Unify	TCP/UDP	181	Unify	unify	Cisco IOS XE Release 3.1S	
UPS	TCP/UDP	401	Uninterruptible Power Supply	ups	Cisco IOS XE Release 3.1S	
	URM	TCP/UDP	606	Cray Unified Resource Manager	urm	Cisco IOS XE Release 3.1S
	UTI	TCP/UDP	120	UTI	uti	Cisco IOS XE Release 3.1S
Utime	TCP/UDP	519	Unixtime	utime	Cisco IOS XE Release 3.1S	
UTMPCD	TCP/UDP	431	utmpcd	utmpcd	Cisco IOS XE Release 3.1S	
UTMPSD	TCP/UDP	430	utmpsd	utmpsd	Cisco IOS XE Release 3.1S	
UUCP	TCP/UDP	540	uucpd	uucp	Cisco IOS XE Release 3.1S	
UUCP-Path	TCP/UDP	117	UUCP Path Service	uucp-path	Cisco IOS XE Release 3.1S	
UUCP-rLogin	TCP/UDP	541	uucp-rlogin	uucp-rlogin	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
UUIDGEN	TCP/UDP	697	UUIDGEN	uuidgen	Cisco IOS XE Release 3.1S	
VACDSM-App	TCP/UDP	671	VACDSM-APP	vacdsm-app	Cisco IOS XE Release 3.1S	
VACDSM-SWS	TCP/UDP	670	VACDSM-SWS	vacdsm-sws	Cisco IOS XE Release 3.1S	
VATP	TCP/UDP	690	Velazquez Application Transfer Protocol	vatp	Cisco IOS XE Release 3.1S	
VEMMI	TCP/UDP	575	vemmi	vemmi	Cisco IOS XE Release 3.1S	
VID	TCP/UDP	769	vid	vid	Cisco IOS XE Release 3.1S	
Videotex	TCP/UDP	516	videotex	videotex	Cisco IOS XE Release 3.1S	
VISA	TCP/UDP	70	VISA Protocol	visa	Cisco IOS XE Release 3.1S	
VNC	TCP/UDP	5800, 5900, 5901	Virtual Network Computing	vnc	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3	
VMNet	TCP/UDP	175	vmnet	vmnet	Cisco IOS XE Release 3.1S	
VMPWSCS	TCP/UDP	214	vmpwscs	vmpwscs	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
VMTP	TCP/UDP	81	VMTP	vmtp	Cisco IOS XE Release 3.1S	
	VNAS	TCP/UDP	577	vnas	vnas	Cisco IOS XE Release 3.1S
VPP	TCP/UDP	677	Virtual Presence Protocol	vpp	Cisco IOS XE Release 3.1S	
VPPS-QUA	TCP/UDP	672	vpps-qua	vpps-qua	Cisco IOS XE Release 3.1S	
VPPS-VIA	TCP/UDP	676	vpps-via	vpps-via	Cisco IOS XE Release 3.1S	
VRRP	TCP/UDP	112	Virtual Router Redundancy Protocol	vrrp	Cisco IOS XE Release 3.1S	
VSINet	TCP/UDP	996	vsinet	vsinet	Cisco IOS XE Release 3.1S	
VSLMP	TCP/UDP	312	vslmp	vslmp	Cisco IOS XE Release 3.1S	
WAP-Push	TCP/UDP	2948	WAP PUSH	wap-push	Cisco IOS XE Release 3.1S	
WAP-Push-HTTP	TCP/UDP	4035	WAP Push OTA-HTTP port	wap-push-http	Cisco IOS XE Release 3.1S	
WAP-Push-HTTPS	TCP/UDP	4036	WAP Push OTA-HTTP secure	wap-push-https	Cisco IOS XE Release 3.1S	
WAP-Pushsecure	TCP/UDP	2949	WAP PUSH SECURE	wap-pushsecure	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
WAP-VACL-S	TCP/UDP	9207	WAP vCal Secure	wap-vcal-s	Cisco IOS XE Release 3.1S	
WAP-VCAL	TCP/UDP	9205	WAP vCal	wap-vcal	Cisco IOS XE Release 3.1S	
WAP-VCARD	TCP/UDP	9204	WAP vCard	wap-vcard	Cisco IOS XE Release 3.1S	
WAP-VCARD-S	TCP/UDP	9206	WAP vCard Secure	wap-vcard-s	Cisco IOS XE Release 3.1S	
WAP-WSP	TCP/UDP	9200	WAP connectionless session service	wap-wsp	Cisco IOS XE Release 3.1S	
WAP-WSP-S	TCP/UDP	9202	WAP secure connectionless session service	wap-wsp-s	Cisco IOS XE Release 3.1S	
WAP-WSP-WTP	TCP/UDP	9201	WAP session service	wap-wsp-wtp	Cisco IOS XE Release 3.1S	
WAP-WSP-WTP-S	TCP/UDP	9203	WAP secure session service	wap-wsp-wtp-s	Cisco IOS XE Release 3.1S	
	WB-Expak	TCP/UDP	79	WIDEBAND EXPAK	wb-expak	Cisco IOS XE Release 3.1S
WB-Mon	TCP/UDP	78	WIDEBAND Monitoring	wb-mon	Cisco IOS XE Release 3.1S	
Webster	TCP/UDP	765	Webster	webster	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Webex Meeting	TCP	Heuristic	Webex Meeting	webex-meeting	Cisco IOS XE Release 3.4S	
WhoAmI	TCP/UDP	565	whoami	whoami	Cisco IOS XE Release 3.1S	
Whois++	TCP/UDP	63	whois++ Service	whois++	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S	
Windows Update	TCP	80, 443, Heuristic	Windows Update	windows-update	Cisco IOS XE Release 3.4S	
WorldFusion	TCP/UDP	2595	World Fusion	worldfusion	Cisco IOS XE Release 3.1S	
WPGS	TCP/UDP	780	wpgs	wpgs	Cisco IOS XE Release 3.1S	
WSN	TCP/UDP	74	Wang Span Network	wsn	Cisco IOS XE Release 3.1S	
XAct-Backup	TCP/UDP	911	Xact-backup	xact-backup	Cisco IOS XE Release 3.1S	
X-Bone-CTL	TCP/UDP	265	Xbone CTL	x-bone-ctl	Cisco IOS XE Release 3.1S	
XDMCP	TCP/UDP	177	X Display Manager Control Protocol	xdmcp	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
XDTP	TCP/UDP	3088	eXtensible Data Transfer Protocol	xdtp	Cisco IOS XE Release 3.1S	
XFER	TCP/UDP	82	XFER Utility	xfer	Cisco IOS XE Release 3.1S	
XNET	TCP/UDP	15	Cross Net Debugger	xnet	Cisco IOS XE Release 3.1S	
XNS-Auth	TCP/UDP	56	XNS Authentication	xns-auth	Cisco IOS XE Release 3.1S	
XNS-CH	TCP/UDP	54	XNS Clearinghouse	xns-ch	Cisco IOS XE Release 3.1S	
	XNS-Courier	TCP/UDP	165	Xerox	xns-courier	Cisco IOS XE Release 3.1S
XNS-IDP	TCP/UDP	22	XEROX NS IDP	xns-idp	Cisco IOS XE Release 3.1S	
XNS-Mail	TCP/UDP	58	XNS mail	xns-mail	Cisco IOS XE Release 3.1S	
XNS-Time	TCP/UDP	52	XNS Time Protocol	xns-time	Cisco IOS XE Release 3.1S	
XTP	TCP/UDP	36	XTP	xtp	Cisco IOS XE Release 3.1S	
XVTTP	TCP/UDP	508	xvttp	xvttp	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
XYPlex-Mux	TCP/UDP	173	Xyplex	xyplex-mux	Cisco IOS XE Release 3.1S	
X Windows	TCP	6000-6003	X Window System	xwindows	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S	
z39.50	TCP/UDP	210	ANSI Z39.50	z39.50	Cisco IOS XE Release 3.1S	
Zannet	TCP/UDP	317	Zannet	zannet	Cisco IOS XE Release 3.1S	
ZServ	TCP/UDP	346	Zebra server	zserv	Cisco IOS XE Release 3.1S	
AN	IP	107	Active Networks	an	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
AOL-Protocol[8]		TCP	5190	America OnLine Protocol	aol-protocol	Cisco IOS XE Release 3.3S
ARGUS		IP	13	ARGUS	argus	Cisco IOS XE Release 3.1S
ARIS		IP	104	ARIS	aris	Cisco IOS XE Release 3.1S
AX25		IP	93	AX.25 Frames	ax25	Cisco IOS XE Release 3.1S
BBNR RCC Mon		IP	10	BBN RCC Monitoring	bbnrccmon	Cisco IOS XE Release 3.1S
BLIZWOW		TCp, UDP	3724	World of Warcraft Gaming Protocol	blizwow	Cisco IOS XE Release 3.3S
BNA		IP	49	BNA	bna	Cisco IOS XE Release 3.1S
	BR-SAT-Mon	IP	76	Backroom SATNET Monitoring	br-sat-mon	Cisco IOS XE Release 3.1S
	CBT	IP	7	CBT	cbt	Cisco IOS XE Release 3.1S
CFTP	IP	62	CFTP	cftp	Cisco IOS XE Release 3.1S	
Choas	IP	16	Chaos	chaos	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Compaq-Peer	IP	110	Compaq Peer Protocol	compaq-peer	Cisco IOS XE Release 3.1S	
CPHB	IP	73	Computer Protocol Heart Beat	cphb	Cisco IOS XE Release 3.1S	
CPNX	IP	72	Computer Protocol Network Executive	cpnx	Cisco IOS XE Release 3.1S	
CRTP	IP	126	Combat Radio Transport Protocol	crtp	Cisco IOS XE Release 3.1S	
CRUDP	IP	127	Combat Radio User Datagram	crudp	Cisco IOS XE Release 3.1S	
DCCP	IP	33	Datagram Congestion Control Protocol	dccp	Cisco IOS XE Release 3.1S	
DCN-Meas	IP	19	DCN Measurement Subsystems	dcn-meas	Cisco IOS XE Release 3.1S	
DDP	IP	37	Datagram Delivery Protocol	ddp	Cisco IOS XE Release 3.1S	
DDX	IP	116	D-II Data Exchange	ddx	Cisco IOS XE Release 3.1S	
DGP	IP	86	Dissimilar Gateway Protocol	dgp	Cisco IOS XE Release 3.1S	
DSR	IP	48	Dynamic Source Routing Protocol	dsr	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
EGP	IP	8	Exterior Gateway Protocol	egp	Cisco IOS XE Release 3.1S	
EIGRP	IP	88	Enhanced Interior Gateway Routing Protocol	eigrp	Cisco IOS XE Release 3.1S	
EMCON	IP	14	EMCON	emcon	Cisco IOS XE Release 3.1S	
Encap	IP	98	Encapsulation Header	encap	15.1(3)T	
EtherIP	IP	97	Ethernet-within-IP Encapsulation	etherip	Cisco IOS XE Release 3.1S	
	FC	IP	133	Fibre Channel	fc	Cisco IOS XE Release 3.1S
FIRE	IP	125	FIRE	fire	Cisco IOS XE Release 3.1S	
GGP	IP	3	Gateway-to-Gateway	ggp	Cisco IOS XE Release 3.1S	
GMTP	IP	100	GMTP	gmtp	Cisco IOS XE Release 3.1S	
GRE	IP	47	General Routing Encapsulation	gre	Cisco IOS XE Release 3.1S	
HIP	IP	139	Host Identity Protocol	hip	Cisco IOS XE Release 3.1S	
HMP	IP	20	Host Monitoring	hmp	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
HopOpt	IP	0	IPv6 Hop-by-Hop Option	hopopt	Cisco IOS XE Release 3.1S	
ICQ	TCP	80, Heuristic	I seek you Instant Messaging Protocol	icq	Cisco IOS XE Release 3.3S	
IATP	IP	117	Interactive Agent Transfer Protocol	iatp	Cisco IOS XE Release 3.1S	
ICMP	IP	1	Internet Control Message	icmp	Cisco IOS XE Release 3.1S	
IDPR	IP	35	Inter-Domain Policy Routing Protocol	idpr	Cisco IOS XE Release 3.1S	
IDPR-CMTP	IP	38	IDPR Control Message Transport Protocol	idpr-cmtp	Cisco IOS XE Release 3.1S	
IDRP	IP	45	Inter-Domain Routing Protocol	idrp	Cisco IOS XE Release 3.1S	
IFMP	IP	101	Ipsilon Flow Management Protocol	ifmp	Cisco IOS XE Release 3.1S	
IGRP	IP	9	Cisco interior gateway	igrp	Cisco IOS XE Release 3.1S	
IL	IP	40	IL Transport Protocol	il	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
I-NLSP	IP	52	Integrated Net Layer Security TUBA	i-nlsp	Cisco IOS XE Release 3.1S	
IMPCOMP	IP	108	IP Payload Compression Protocol	ipcomp	Cisco IOS XE Release 3.1S	
	IPCU	IP	71	Internet Packet Core Utility	ipcv	Cisco IOS XE Release 3.1S
IPinIP	IP	4	IP in IP	ipinip	Cisco IOS XE Release 3.1S	
IPIP	IP	94	IP-within-IP Encapsulation Protocol	ipip	Cisco IOS XE Release 3.1S	
IPLT	IP	129	IPLT	iplt	Cisco IOS XE Release 3.1S	
IPPC	IP	67	Internet Pluribus Packet Core	ippc	Cisco IOS XE Release 3.1S	
IPv6-Frag	IP	44	Fragment Header for IPv6	ipv6-frag	Cisco IOS XE Release 3.1S	
IPv6-ICMP	IP	58	ICMP for IPv6	ipv6-icmp	Cisco IOS XE Release 3.1S	
IPv6INIP	IP	41	Ipv6 encapsulated	ipv6inip	Cisco IOS XE Release 3.1S	
IPv6-NONXT	IP	59	No Next Header for IPv6	ipv6-nonxt	Cisco IOS XE Release 3.1S	
IPv6-Opts	IP	60	Destination Options for IPv6	ipv6-opts	Cisco IOS XE Release 3.1S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
IPv6-Route	IP	43	Routing Header for IPv6	ipv6-route	Cisco IOS XE Release 3.1S	
IRTP	IP	28	Internet Reliable Transaction	irtp	Cisco IOS XE Release 3.1S	
ISIS	IP	124	ISIS over IPv4	isis	Cisco IOS XE Release 3.1S	
ISO-TP4	IP	29	ISO Transport Protocol Class 4	iso-tp4	Cisco IOS XE Release 3.1S	
IXP-in-IP	IP	111	IPX in IP	ixp-in-ip	Cisco IOS XE Release 3.1S	
LARP	IP	91	Locus Address Resolution Protocol	larp	Cisco IOS XE Release 3.1S	
Leaf-1	IP	25	Leaf-1	leaf-1	Cisco IOS XE Release 3.1S	
6to4 IPv6 Tunneled	L3 Protocol	--	6to4 IPv6 Tunneled	6to4 IPv6 Tunneled	Cisco IOS XE Release 3.2S	
	AYIYA IPv6 Tunneled	UDP	5072	IPv6 Tunneled based on AYIYA traffic	AYIYA IPv6 Tunneled	Cisco IOS XE Release 3.2S
	BabelGum	TCP, UDP	80 + Heuristic	BabelGum	BabelGum	Cisco IOS XE Release 3.2S
Baidu Movie	TCP, UDP	80 + Heuristic	Baidu Movie	Baidu Movie	Cisco IOS XE Release 3.2S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
DHCP	UDP	67,68	Dynamic Host Configuration Protocol	dhcp	Cisco IOS XE Release 3.2S	
DHT	UDP	Heuristic	Distributed sloppy Hash Table Protocol	DHT	Cisco IOS XE Release 3.2S	
Filetopia	TCP	Heuristic	Filetopia P2P file sharing	filetopia	Cisco IOS XE Release 3.2S	
Fring-VoIP	UDP	Heuristic	Fring VoIP	fring-voip	Cisco IOS XE Release 3.3S	
GoogleEarth	TCP	80 + Heuristic	GoogleEarth	GoogleEarth	Cisco IOS XE Release 3.2S	
Guruguru	TCP	Heuristic	Guruguru	guruguru	Cisco IOS XE Release 3.2S	
IMAP	TCP	143,220	Internet Mail Access Protocol	imap	Cisco IOS XE Release 3.2S	
IRC	TCP	80 + Heuristic	IRC	IRC	Cisco IOS XE Release 3.2S	
ISATAP IPv6 Tunneled	L3 Protocol		Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) IPv6 Tunneled	ISATAP IPv6 Tunneled	Cisco IOS XE Release 3.2S	
iTunes	TCP	80 + Heuristic	iTunes	iTunes	Cisco IOS XE Release 3.2S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Kuro	TCP	Heuristic	Kuro	kuro	Cisco IOS XE Release 3.3S	
Manolito	TCP, UDP	TCP - Heuristic port, UDP - 41170	Manolito P2P music sharing protocol	manolito	Cisco IOS XE Release 3.2S	
MapleStory	TCP	Heuristic	Maple Story Gaming Protocol	MapleStory	Cisco IOS XE Release 3.2S	
SIP	TCP, UDP	TCP/UDP - 5060 + Heuristic	Session Initiation Protocol	sip	Cisco IOS XE Release 3.2S	
	MGCP	TCP, UDP	UDP 2427/2727 - TCP 2427/2428/2727 + Heuristic	Media Gateway Control Protocol	MGCP	12.2(18)ZYA1 12.3(7)T Cisco IOS XE Release 3.2S
Microsoft-DS	TCP, UDP	445	Microsoft-ds	microsoftds	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.3S	
MSN Messenger	TCP	1080,1863, 80, Hueristic	MSN Messenger	msn-messenger	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.3S	
MyJabber File Transfer	TCP	Heuristic	MyJabber File Transfer	MyJabber File Transfer	Cisco IOS XE Release 3.2S	
Napster	TCP	80 + Heuristic	Napster	napster	Cisco IOS XE Release 3.2S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Netshow	TCP	1755 + Heuristic	Netshow	netshow	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1	
NNTP	TCP	TCP - 119 + Heuristic, UDP -119	Network News Transfer Protocol	NNTP	Cisco IOS XE Release 3.2S	
NTP	UDP	123	Network Time Protocol	NTP	Cisco IOS XE Release 3.2S	
Pando	TCP,UDP	TCP - 80 + Heuristic, UDP - Heuristic	Pando	Pando	Cisco IOS XE Release 3.2S	
POCO	TCP, UDP	Heuristic	POCO File-Sharing Application	POCO	Cisco IOS XE Release 3.2S	
POP3	TCP	110, Heuristic	POP3	POP3	Cisco IOS XE Release 3.2S	
PPTP	TCP	1723	Point-to-Point Tunneling Protocol	pptp	Cisco IOS XE Release 3.2S	
RADIUS	UDP	1812, 1813	Remote Authentication Dial In User Service protocol	radius	Cisco IOS XE Release 3.3S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
	SCCP/Skinny	TCP	2000-2002	Skinny Call Control Protocol	skinny	Cisco IOS XE Release 3.3S
	Soribada	TCP	TCP - 80 + Heuristic, UDP - Heuristic	Soribada, Korean P2P music sharing Protocol	soribada	Cisco IOS XE Release 3.2S
	Soulseek	TCP	Heuristic	SoulSeek internet download manager Protocol	soulseek	Cisco IOS XE Release 3.3S
	TeamSpeak	UDP	Heuristic	TeamSpeak internet based voice-conferencing Protocol	TeamSpeak	Cisco IOS XE Release 3.2S
TelePresence	TCP/UDP	Dynamically assigned	Cisco TelePresence System	telepresence-media	12.2(18)ZYA2	
Telepresence-control	TCP,UDP	TCP- 5060, UDP- Heuristic	Telepresence-control	telepresence-control	Cisco IOS XE Release 3.2S	
Teredo IPv6 Tunneled	TCP,UDP	TCP- Heuristic, UDP - 3544 + Heuristic	Teredo IPv6 Tunneled	teredo-ipv6-tunneled	Cisco IOS XE Release 3.2S	
TFTP	UDP	69	Trivial File Transfer Protocol	tftp	Cisco IOS XE Release 3.2S	
TomatoPang	TCP	Heuristic	TomatoPang P2P Sharing Protocol	TomatoPang	Cisco IOS XE Release 3.2S	
Tunnel-HTTP	TCP	80 + Heuristic	HTTP Tunneling	tunnel-http	Cisco IOS XE Release 3.2S	

Category	Protocol	Type	WKP/IP Protocol	Description	Syntax	Cisco IOS XE Release
Ventrilo	TCP, UDP	Heuristic	Ventrilo VoIP Protocol	Ventrilo	Cisco IOS XE Release 3.2S	
Waste	TCP/UDP	Heuristic	Waste	waste	Cisco IOS XE Release 3.3S	
WebThunder	TCP, UDP	TCP-80, UDP-Heuristic	WebThunder Peer-to-Peer File Sharing	WebThunder	Cisco IOS XE Release 3.2S	
Yahoo-Messenger	TCP	TCP-5050/5101/80/1900 /Heuristic	Yahoo Messenger	yahoo-messenger	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.3S	
Yahoo-Messenger-VoIP	TCP/UDP	Heuristic	Yahoo Messenger VoIP	yahoo-voip-messenger	Cisco IOS XE Release 3.3S	
Yahoo VoIP over SIP	TCP/UDP	5060/Heuristic	Yahoo VoIP over SIP	yahoo-voip-over-sip	Cisco IOS XE Release 3.4S	

[1] For Release 12.2(18)ZYA and Cisco IOS XE Release 2.5 Cisco supports Exchange 03 and 07 only. MS client access is recognized, but web client access is not recognized.

[2] In Release 12.3(4)T, the NBAR Extended Inspection for HTTP Traffic feature was introduced. This feature allows NBAR to scan TCP ports that are not well known and to identify HTTP traffic that is traversing these ports. For Cisco IOS XE Release 2.1, classification of HTTP traffic by URL or hostname is not supported. Cisco IOS XE Release 2.5 supports classification of HTTP traffic by URL or hostname.

[3] Skype was introduced in Cisco IOS Release 12.4(4)T. As a result of this introduction, Skype is native in (included with) the Cisco IOS software and uses the NBAR infrastructure new to Cisco IOS Release 12.4(4)T. Cisco software supports Skype 1.0, 2.5, and 3.0. For Cisco IOS XE Release 2.1, Skype is supported in the TCP type only. Note that certain hardware platforms do not support Skype. For instance, Skype is not supported on the Catalyst 6500 series switch that is equipped with a Supervisor/PISA engine. Cisco IOS XE Release 2.5 supports Skype in the TCP and UDP type.

[4] For Release 12.2(18)ZYA, access to YouTube via HTTP only is recognized.

[5] BitTorrent classifies only unencrypted traffic.

[6] eDonkey classifies only unencrypted traffic.

[7] For Release 12.2(18)ZYA, only SIP and Skinny telephone connections (cisco-phone traffic connections) are recognized. H.323 telephone connections are not recognized.

[8] AOL-Protocol classifies traffic shared between ICQ and AOL clients.

Custom Protocols Created with the ip nbar custom Command

The *variable-field-name* argumentis used in conjunction with the **variable***field-namefield-length* options that are entered when you create a custom protocol using the **ipnbarcustom**command. The variable option allows NBAR to match traffic on the basis of a specific value of a custom protocol. For instance, if **ipnbarcustomftdd125variablescid2tcprange50015005** is entered to create a custom protocol, and then a class map using the**matchprotocolftddscid804**is created, the created class map will match all traffic that has the value “804” at byte 125 entering or leaving TCP ports 5001 to 5000.

Up to 24 variable values per custom protocol can be expressed in class maps. For instance, in the following configuration, 4 variables are used and 20 more “scid” values could be used.

```
Router(config)# ip nbar custom ftdd field scid 125 variable 1 tcp range 5001 5005
Router(config)# class-map active-craft
Router(config-cmap)# match protocol ftdd scid 0x15
Router(config-cmap)# match protocol ftdd scid 0x21
Router(config)# class-map passive-craft
Router(config-cmap)# match protocol ftdd scid 0x11
Router(config-cmap)# match protocol ftdd scid 0x22
```

match protocol Command Restrictions (Catalyst 6500 Series Switches Only)

Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) on the basis of a protocol type or application. You can create as many traffic classes as needed.

Cisco IOS Release 12.2(18)ZY includes software intended for use on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine. For this release and platform, note the following restrictions for using policy maps and **matchprotocol** commands:

- A single traffic class can be configured to match a maximum of eight protocols or applications.
- Multiple traffic classes can be configured to match a cumulative maximum of 95 protocols or applications.

Examples

The following example configures NBAR to match FTP traffic:

```
Router(config-cmap)# match protocol ftp
```

In the following example, custom protocol ftdd is created by using a variable. A class map matching this custom protocol based on the variable is also created. In this example, class map matchscidinftdd will match all traffic that has the value “804” at byte 125 entering or leaving TCP ports 5001 to 5005. The variable scid is 2 bytes in length:

```
Router(config)# ip nbar custom ftdd 125 variable scid 2 tcp range 5001 5005
Router(config)# class-map matchscidinftdd
Router(config-cmap)# match protocol ftdd scid 804
```

The following example show the command can also be written using hexadecimal values in the class map as follows:

```
Router(config)#
ip nbar custom ftdd 125 variable scid 2 tcp range 5001 5005
Router(config)# class-map matchscidinftdd
Router(config-cmap)# match protocol ftdd scid 0x324
```

In the following example, the **variable** keyword is used while you create a custom protocol, and class maps are configured to classify different values within the variable field into different traffic classes. Specifically, in the following example, variable scid values 0x15, 0x21, and 0x27 will be classified into class map active-craft, while scid values 0x11, 0x22, and 0x25 will be classified into class map passive-craft.

```
Router(config)# ip nbar custom ftdd field scid 125 variable 1 tcp range 5001 5005
Router(config)# class-map active-craft
Router(config-cmap)# match protocol ftdd scid 0x15
Router(config-cmap)# match protocol ftdd scid 0x21
Router(config-cmap)# match protocol ftdd scid 0x27
Router(config)# class-map passive-craft
Router(config-cmap)# match protocol ftdd scid 0x11
Router(config-cmap)# match protocol ftdd scid 0x22
Router(config-cmap)# match protocol ftdd scid 0x25
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
ip nbar custom	Extends the capability of NBAR Protocol Discovery to classify and monitor additional static port applications, or allows NBAR to classify nonsupported static port traffic.

match protocol citrix

To configure network-based application recognition (NBAR) to match Citrix traffic, use the **matchprotocolcitrix** command in class-map configuration mode. To disable NBAR from matching Citrix traffic, use the **no** form of this command.

match protocol citrix [**app** *application-name-string*] [**ica-tag** *ica-tag-value*]

no match protocol citrix [**app** *application-name-string*] [**ica-tag** *ica-tag-value*]

Syntax Description

app	(Optional) Specifies matching of an application name string.
application-name-string	(Optional) Specifies the string to be used as the subprotocol parameter.
ica-tag	(Optional) Specifies tagging of Independent Computing Architecture (ICA) packets.
ica-tag-value	(Optional) Specifies the priority tag of ICA packets. Priority tag values can be in the range of 0 to 3.

Command Default

No match criteria are specified.

Command Modes

Class-map configuration

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(13)E	This command was implemented on Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
12.4(2)T	This command was modified to include the ica-tag keyword and the *ica-tag-value* argument.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Entering the **matchprotocolcitrix** command without the **app** keyword establishes all Citrix traffic as successful match criteria.

Entering the**matchprotocolcitrix** command with the ica-tag keyword prioritizes Citrix ICA traffic. The priority tag values can be a number from 0 to 3, with 0 having the highest priority and 3 the lowest.

Examples

The following example configures NBAR to match all Citrix traffic:

```
match protocol citrix
```

The following example configures NBAR to match Citrix traffic with the application name of packet1:

```
match protocol citrix app packet1
```

The following example configures NBAR to give Citrix ICA traffic a priority of 1:

```
match protocol citrix ica-tag-1
```

match protocol fasttrack

To configure network-based application recognition (NBAR) to match FastTrack peer-to-peer traffic, use the **matchprotocolfasttrack** command in class-map configuration mode. To disable NBAR from matching FastTrack traffic, use the **no** form of this command.

match protocol fasttrack file-transfer *"regular-expression"*

no match protocol fasttrack file-transfer *"regular-expression"*

Syntax Description

file-transfer	Indicates that a regular expression will be used to identify specific FastTrack traffic.
“ *regular-expression* ”	Regular expression used to identify specific FastTrack traffic. For instance, entering “cisco” as the regular expression would classify the FastTrack traffic containing the string “cisco” as matches for the traffic policy. To specify that all FastTrack traffic be identified by the traffic class, use “*” as the regular expression.

Command Default

NBAR is not configured to match FastTrack peer-to-peer traffic

Command Modes

Class-map configuration

Command History

Release	Modification
12.1(12c)E	This command was introduced.
12.1(13)E	This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

To specify that all FastTrack traffic be identified by the traffic class, use “*” as the regular expression.

Applications that use FastTrack include KaZaA, Grokster, and Morpheus (although newer versions of Morpheus use Gnutella).

Examples

The following example configures NBAR to match all FastTrack traffic:

```
match protocol fasttrack file-transfer “*”
```

In the following example, all FastTrack files that have the “.mpeg” extension will be classified into class map nbar:

```
class-map match-all nbar
 match protocol fasttrack file-transfer "*.mpeg"
```

The following example configures NBAR to match FastTrack traffic that contains the string “cisco”:

```
match protocol fasttrack file-transfer “*cisco*”
```

match protocol gnutella

To configure network-based application recognition (NBAR) to match Gnutella peer-to-peer traffic, use the **matchprotocolgnutella** command in class-map configuration mode. To disable NBAR from matching Gnutella traffic, use the **no** form of this command.

match protocol gnutella file-transfer *"regular-expression"*

no match protocol gnutella file-transfer *"regular-expression"*

Syntax Description

file-transfer	Indicates that a regular expression will be used to identify specific Gnutella traffic.
" *regular-expression* "	The regular expression used to identify specific Gnutella traffic. For instance, entering "cisco" as the regular expression would classify the Gnutella traffic containing the string "cisco" as matches for the traffic policy. To specify that all Gnutella traffic be identified by the traffic class, use "*" as the regular expression.

Command Default

No behavior or values are predefined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.1(12c)E	This command was introduced.
12.1(13)E	This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

To specify that all Gnutella traffic be identified by the traffic class, use "*" as the regular expression.

Applications that use Gnutella include the following:

- BearShare
- Gnewtellium
- Gnucleus
- Gtk-Gnutella
- JTella
- LimeWire
- Morpheus
- Mutella
- Phex
- Qtella
- Swapper
- XoloX
- XCache

Examples

The following example configures NBAR to match all Gnutella traffic:

```
match protocol gnutella file-transfer “*”
```

In the following example, all Gnutella files that have the “.mpeg” extension will be classified into class map nbar:

```
class-map match-all nbar
 match protocol gnutella file-transfer "*.mpeg"
```

In the following example, only Gnutella traffic that contains the characters “cisco” is classified:

```
class-map match-all nbar
 match protocol gnutella file-transfer “*cisco*”
```

match protocol http

To configure Network-Based Application Recognition (NBAR) to match HTTP traffic by URL, host, Multipurpose Internet Mail Extension (MIME) type, or fields in HTTP packet headers, use the **matchprotocolhttp** command in class-map configuration mode. To disable NBAR from matching HTTP traffic by URL, host, or MIME type, or fields in HTTP packet headers, use the **no** form of this command.

match protocol http [**url** *url-string*| **host** *hostname-string*| **mime** *MIME-type*| **c-header-field** *c-header-field-string*| **s-header-field** *s-header-field-string*]

no match protocol http [**url** *url-string*| **host** *hostname-string*| **mime** *MIME-type*| **c-header-field** *c-header-field-string*| **s-header-field** *s-header-field-string*]

match protocol http [**content-encoding** *content-encoding-name-string*| **from** *from-address-string*| **host** *hostname-string*| **location** *location-name-string*| **mime** *MIME-type*| **referer** *referer-address-string*| **server** *server-software-name-string*| **url** *url-string*| **user-agent** *user-agent-software-name-string*]

no match protocol http [**content-encoding** *content-encoding-name-string*| **from** *from-address-string*| **host** *hostname-string*| **location** *location-name-string*| **mime** *MIME-type*| **referer** *referer-address-string*| **server** *server-software-name-string*| **url** *url-string*| **user-agent** *user-agent-software-name-string*]

Syntax Description

url	(Optional) Specifies matching by a URL.
url-string	(Optional) User-specified URL of HTTP traffic to be matched.
host	(Optional) Specifies matching by a hostname.
hostname-string	(Optional) User-specified hostname to be matched.
mime	(Optional) Specifies matching by a MIME text string.
MIME-type	(Optional) User-specified MIME text string to be matched.
c-header-field	(Optional) Specifies matching by a string in the header field in HTTP client messages. **Note** HTTP client messages are often called HTTP request messages.
c-header-field-string	(Optional) User-specified text string within the HTTP client message (HTTP request message) to be matched.
s-header-field	(Optional) Specifies matching by a string in the header field in the HTTP server messages **Note** HTTP server messages are often called HTTP response messages.

s-header-field-string	(Optional) User-specified text within the HTTP server message (HTTP response message) to be matched.
Cisco IOS 15.1(2)T and Later Releases and Catalyst 6500 Series Switch Equipped with the Supervisor 32/PISA Engine	
content-encoding	(Optional) Specifies matching by the encoding mechanism used to package the entity body.
content-encoding-name-string	(Optional) User-specified content-encoding name.
from	(Optional) Specifies matching by the e-mail address of the person controlling the user agent.
from-address-string	(Optional) User-specified e-mail address.
location	(Optional) Specifies matching by the exact location of the resource from request.
location-name-string	(Optional) User-specified location of the resource.
referer	(Optional) Specifies matching by the address from which the resource request was obtained.
referer-address-name-string	(Optional) User-specified address of the referer resource.
server	(Optional) Specifies matching by the software used by the origin server handling the request.
server-software-name-string	(Optional) User-specified software name.
user-agent	(Optional) Specifies matching by the software used by the agent sending the request.
user-agent-software-name-string	(Optional) User-specified name of the software used by the agent sending the request.

Command Default

NBAR does not match HTTP traffic by URL, host, MIME type, or fields in HTTP packet headers.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.0(5)XE2	This command was introduced.

Release	Modification
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(2)E	This command was modified to include the *hostname-string* argument.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(13)E	This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T, and the NBAR Extended Inspection for HTTP Traffic feature was introduced. This feature allows NBAR to scan TCP ports that are not well known and to identify HTTP traffic traversing these ports.
12.4(2)T	The command was integrated into Cisco IOS Release 12.4(2)T and was modified to include the **c-header-field***c-header-field-string* and **s-header-field***s-header-field-string* keywords and arguments.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)ZY2	This command was integrated into Cisco IOS Release 12.2(18)ZY2, and support was provided for the Catalyst 6500 series switch that is equipped with the Supervisor 32/PISA engine. **Note** For this Cisco IOS release and this platform, the **c-header-field***c-header-field-string* and **s-header-field***s-header-field-string* keywords and arguments are not available. To achieve the same functionality, use the individual keywords and arguments as shown in the syntax for the Catalyst 6500 series switch.
15.1(2)T	This command was modified. Support for the **c-header-field***c-header-field-string* and **s-header-field***s-header-field-string* keywords and arguments was removed. The **content-encoding**, **from**, **location**, **referrer**, and **user-agent** keywords and respective arguments were added.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

Classification of HTTP Traffic by Host, URL, or MIME

In Cisco IOS Release 12.3(4)T, the NBAR Extended Inspection for HTTP Traffic feature was introduced. This feature allows NBAR to scan TCP ports that are not well-known and that identify HTTP traffic traversing these ports. This feature is enabled automatically when a service policy containing the **matchprotocolhttp** command is attached to an interface.

When matching by MIME type, the MIME type can contain any user-specified text string. See the following web page for the IANA-registered MIME types:

http://www.iana.org/assignments/media-types/

When matching by MIME type, NBAR matches a packet containing the MIME type and all subsequent packets until the next HTTP transaction.

When matching by host, NBAR performs a regular expression match on the host field contents inside the HTTP packet and classifies all packets from that host.

HTTP client request matching supports GET, PUT, HEAD, POST, DELETE, OPTIONS, CONNECT, and TRACE. When matching by URL, NBAR recognizes the HTTP packets containing the URL and then matches all packets that are part of the HTTP request. When specifying a URL for classification, include only the portion of the URL that follows the www.*hostname .domain* in the **match** statement. For example, for the URL www.cisco.com/latest/whatsnew.html, include only /latest/whatsnew.html with the **match** statement (for instance, **matchprotocolhttpurl/latest/whatsnew.html**).

Note For Cisco IOS Release 12.2(18)ZY2 (and later releases) on the Cisco Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA, up to 56 parameters or subclassifications per protocol per router can be specified with the **matchprotocolhttp** command. These parameters or subclassifications can be a combination of any of the available match choices, such as host matches, MIME matches, server matches, and URL matches. For other Cisco IOS releases and platforms, the maximum is 24 parameters or subclassifications per protocol per router.

To match the www.*anydomain* .com portion, use the hostname matching feature. The parameter specification strings can take the form of a regular expression with the following options.

Option	Description
	Match any zero or more characters in this position.
	Match any one character in this position.
	Match one of a choice of characters.
(|)	Match one of a choice of characters in a range. For example cisco.(gif | jpg) matches either cisco.gif or cisco.jpg.
[ ]	Match any character in the range specified, or one of the special characters. For example, [0-9] is all of the digits. [*] is the "*" character and [[] is the "[" character.

Classification of HTTP Header Fields

In Cisco IOS Release 12.3(11)T, NBAR introduced expanded ability for users to classify HTTP traffic using information in the HTTP Header Fields.

HTTP works using a client/server model: HTTP clients open connections by sending a request message to an HTTP server. The HTTP server then returns a response message to the HTTP client (this response message is typically the resource requested in the request message from the HTTP client). After delivering the response, the HTTP server closes the connection and the transaction is complete.

HTTP header fields are used to provide information about HTTP request and response messages. HTTP has numerous header fields. For additional information on HTTP headers, see section 14 of RFC 2616: Hypertext Transfer Protocol--HTTP/1.1. This document can be read at the following URL:

http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html

For request messages (client to server), the following HTTP header fields can be identified by using NBAR:

- User-Agent
- Referer

For response messages (server to client), the following header fields can be identified by using NBAR:

- Server
- Location
- Content-Encoding
- Content-Base

Note Use of the Content-Base field has not been implemented by the HTTP community. (See RFC 2616 for details.) Therefore, the Content-Base field is not identified by NBAR on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine.

Within NBAR, the **matchprotocolhttpc-header-field** command is used to specify request messages (the “c” in the **c-header-field** portion of the command is for client). The **matchprotocolhttps-header-field** command is used to specify response messages (the “s” in the **s-header-field**portion of the command is for server).

It is important to note that combinations of URL, host, MIME type, and HTTP headers can be used during NBAR configuration. These combinations provide customers with more flexibility to classify specific HTTP traffic based on their network requirements.

Note For Cisco IOS Release 12.2(18)ZY2 and later releases on the Cisco Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA, and for Cisco IOS Release 15.1(2)T and later releases, the **c-header-field** and **s-header-field** keywords and associated arguments in the **matchprotocolhttp** command are not available.

Examples

The following example classifies, within class map class1, HTTP packets based on any URL containing the string whatsnew/latest followed by zero or more characters:

```
class-map class1
 match protocol http url whatsnew/latest*
```

The following example classifies, within class map class2, packets based on any hostname containing the string cisco followed by zero or more characters:

```
class-map class2
 match protocol http host cisco*
```

The following example classifies, within class map class3, packets based on the JPEG MIME type:

```
class-map class3
 match protocol http mime “*jpeg”
```

In the following example, any response message that contains “ gzip” in the Content-Base (if available), Content-Encoding, Location, or Server header fields will be classified by NBAR. Typically, the term “gzip” would be found in the Content-Encoding header field of the response message.

```
class-map class4
 match protocol http s-header-field “gzip”
```

In the following example, HTTP header fields are combined with a URL to classify traffic. In this example, traffic with a User-Agent field of “CERN-LineMode/3.0” and a Server field of “CERN/3.0”, along with URL “www.cisco.com/routers”, will be classified using NBAR.

```
class-map match-all c-http
 match protocol http c-header-field “CERN-LineMode/3.0”
 match protocol http s-header-field “CERN/3.0”
 match protocol http url “www.cisco.com/routers”
```

Examples

In the following two examples, the individual keywords and associated arguments are used to specify traffic (instead of the **c-header-field** and the **s-header-field** keywords).

In the first example, the**user-agent**, **referrer**, and **from** keywords are specified. In the second example, the server, location, content-encoding keywords are specified.

```
class-map match-all test1
 match protocol http user-agent Mozilla
 match protocol http referrer *10.0.10.50”
 match protocol http from *example.com”
class-map match-all test2
 match protocol http server Apache
 match protocol http location *example.com”
 match protocol http content-encoding compress
 match protocol http match protocol http content-base *exmaple.com”
```

Related Commands

Command	Description
show ip nbar protocol-discovery	Displays the statistics gathered by the NBAR Protocol Discovery feature.

match protocol pppoe-discovery

To match and classify PPP over Ethernet (PPPoE) control-plane packets that are sent to the control plane, use the **match protocol pppoe-discovery** command in QoS class-map configuration mode. To remove this match criterion, use the **no** form of this command.

match protocol pppoe-discovery

no match protocol pppoe-discovery

Syntax Description

This command has no arguments or keywords.

Command Default

PPPoE control packets sent to the control plane are not matched or classified.

Command Modes

QoS class-map configuration (config-cmap)

Command History

Release	Modification
Cisco IOS XE Release 2.3	This command was introduced on Cisco ASR 1000 Series Aggregation Routers.

Usage Guidelines

The **match pppoe-discovery** command is associated with control-plane-related features such as Control Plane Policing (CoPP).

When used in a class map, the **match protocol pppoe-discovery** command can classify either ingress PPPoE control-plane packets or egress PPPoE control-plane packets and include them in a specified traffic class. That class can then be configured in a policy map and can receive the desired quality of service (QoS) feature (such as traffic policing).

Note With CSCts20715, the **match protocol pppoe-discovery** command matches PPPoE Active Discovery Initiation (PADI) packets received over Automatic Virtual Circuits (AutoVC) configured on an ATM subinterface. Each ATM cell of PADI packets is punted as a separate packet and is counted towards the PPPOE_DISCOVERY packet count.

Examples

The following is an example of the **match protocol pppoe-discovery** command configured in a class-map called copplass-pppoe-discovery. PPPoE control-plane traffic identified as meeting the match criterion is placed in a class called coppclass-pppoe-discovery.

The coppclass-pppoe-discovery class is then configured in a policy map called copp-policy-pppoe-discovery, and the QoS traffic policing feature is applied using the **police** command.

```
Router> enable
```

```
Router# configure terminal
Router(config)# class-map match-all coppclass-pppoe-discovery
Router(config-cmap)# match protocol pppoe-discovery
Router(config-cmap)# exit
Router(config)# policy-map copp-policy-pppoe-discovery
Router(config-pmap)# class coppclass-pppoe-discovery
Router(config-pmap-c)# police rate 8000 bps conform-action transmit exceed-action drop
Router(config-pmap-c-police)# end
```

Related Commands

Command	Description
control-plane	Enters control-plane configuration mode, which allows users to associate or modify attributes or parameters (such as a service policy) that are associated with the control plane of the device.
match protocol	Configures the match criterion for a class map on the basis of the specified protocol.
police rate	Configures traffic policing for traffic that is destined for the control plane.
show policy-map control-plane	Displays the configuration and statistics for a traffic class or all traffic classes in the policy maps attached to the control plane for aggregate or distributed control-plane services.
show pppoe session	Displays information about currently active PPPoE sessions.

match protocol rtp

To configure network-based application recognition (NBAR) to match Real-Time Transfer Protocol (RTP) traffic, use the **matchprotocolrtp** command in class-map configuration mode. To disable NBAR from matching RTP traffic, use the no form of this command.

match protocol rtp [**audio**| **video**| **payload-type** *payload-string*]

no match protocol rtp [**audio**| **video**| **payload-type** *payload-string*]

Syntax Description

audio	(Optional) Specifies matching by audio payload-type values in the range of 0 to 23. These payload-type values are reserved for audio traffic.
video	(Optional) Specifies matching by video payload-type values in the range of 24 to 33. These payload-type values are reserved for video traffic.
payload-type	(Optional) Specifies matching by a specific payload-type value, providing more granularity than is available with the **audio** or **video** keywords.
payload-string	(Optional) User-specified string that contains the specific payload-type values. A *payload-string* argument can contain commas to separate payload-type values and hyphens to indicate a range of payload-type values. A *payload-string* argument can be specified in hexadecimal (prepend 0x to the value) and binary (prepend b to the value) notation in addition to standard number values.

Command Default

No match criteria are specified.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.1(11b)E	This command was integrated into Cisco IOS Release 12.1(11b)E.
12.1(13)E	This command was implemented on Catalyst 6000 family switches without FlexWAN modules.

Release	Modification
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Entering the **matchprotocolrtp** command without any other keywords establishes all RTP traffic as successful match criteria.

RTP is a packet format for multimedia data streams. It can be used for media-on-demand as well as interactive services such as Internet telephony. RTP consists of a data and a control part. The control part is called Real-Time Transport Control Protocol (RTCP). It is important to note that the NBAR RTP Payload Classification feature does not identify RTCP packets and that RTCP packets run on odd-numbered ports while RTP packets run on even-numbered ports.

The payload type field of an RTP packet identifies the format of the RTP payload and is represented by a number. NBAR matches RTP traffic on the basis of this field in the RTP packet. A working knowledge of RTP and RTP payload types is helpful if you want to configure NBAR to match RTP traffic. For more information about RTP and RTP payload types, refer to RFC 1889, *RTP: A Transport Protocol for Real-Time Applications.*

Examples

The following example configures NBAR to match all RTP traffic:

```
class-map class1
 match protocol rtp
```

The following example configures NBAR to match RTP traffic with the payload-types 0, 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, and 64:

```
class-map class2
 match protocol rtp payload-type "0, 1, 4-0x10, 10001b-10010b, 64"
```

match qos-group

To identify a specific quality of service (QoS) group value as a match criterion, use the **matchqos-group**command in class-map configuration or policy inline configuration mode. To remove a specific QoS group value from a class map, use the **no** form of this command.

match qos-group *qos-group-value*

no match qos-group *qos-group-value*

Syntax Description

qos-group-value	The exact value from 0 to 99 used to identify a QoS group value.

Command Default

No match criterion is specified.

Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
11.1CC	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 Series Routers.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

The **matchqos-group** command is used by the class map to identify a specific QoS group value marking on a packet. This command can also be used to convey the received Multiprotocol Label Switching (MPLS) experimental (EXP) field value to the output interface.

The *qos-group-value* argument is used as a marking only. The QoS group values have no mathematical significance. For instance, the *qos-group-value* of 2 is not greater than 1. The value simply indicates that a packet marked with the *qos-group-value* of 2 is different than a packet marked with the *qos-group-value* of 1. The treatment of these packets is defined by the user through the setting of QoS policies in QoS policy-map class configuration mode.

The QoS group value is local to the router, meaning that the QoS group value that is marked on a packet does not leave the router when the packet leaves the router. If you need a marking that resides in the packet, use IP precedence setting, IP differentiated services code point (DSCP) setting, or another method of packet marking.

This command can be used with the **random-detectdiscard-class-based**command.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

Examples

The following example shows how to configure the service policy named priority50 and attach service policy priority50 to an interface. In this example, the class map named qosgroup5 will evaluate all packets entering Fast Ethernet interface 1/0/0 for a QoS group value of 5. If the incoming packet has been marked with the QoS group value of 5, the packet will be treated with a priority level of 50.

```
Router(config)#

class-map qosgroup5
Router(config-cmap)
#
 match qos-group 5
Router(config)#

exit
Router(config)#

policy-map priority50
Router(config-pmap)#

class qosgroup5
Router(config-pmap-c)#

priority 50
Router(config-pmap-c)#

exit
Router(config-pmap)#

exit
Router(config)#

interface fastethernet1/0/0
Router(config-if)#

service-policy output priority50
```

Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria of a QoS value of 4 will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match qosgroup 4
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
random-detect discard-class-based	Bases WRED on the discard class value of a packet.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set precedence	Specifies an IP precedence value for packets within a traffic class.
set qos-group	Sets a group ID that can be used later to classify packets.

match source-address mac

To use the source MAC address as a match criterion, use the **matchsource-addressmac**command in class-map configuration or policy inline configuration mode. To remove a previously specified source MAC address as a match criterion, use the **no**form of this command.

match source-address mac *address-source*

no match source-address mac *address-source*

Syntax Description

address-source	The source source MAC address to be used as a match criterion.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

This command can be used only on an input interface with a MAC address; for example, Fast Ethernet and Ethernet interfaces.

This command cannot be used on output interfaces with no MAC address, such as serial and ATM interfaces.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

Examples

The following example uses the MAC address mac 0.0.0 as a match criterion:

```
Router(config)# class-map matchsrcmac
Router(config-cmap)
#
match source-address mac 0.0.0
```

Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the specified MAC source address will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match source-address mac 0.0.0
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.

match start

Note Effective with Cisco IOS Release 15.2(4)M, the **match start** command is not available in Cisco IOS software.

To configure the match criteria for a class map on the basis of the datagram header (Layer 2) or the network header (Layer 3), use the **match start** command in class-map configuration mode. To remove the specified match criteria, use the **no** form of this command.

match start {**l2-start**| **l3-start**} **offset** *number* **size** *number* {**eq**| **neq**| **gt**| **lt**| **range** *range*| **regex** *string*} {*value* [*value2*]| [*string*]}

no match start {**l2-start**| **l3-start**} **offset** *number* **size** *number* {**eq**| **neq**| **gt**| **lt**| **range** *range*| **regex** *string*} {*value* [*value2*]| [*string*]}

Syntax Description

l2-start	Match criterion starts from the datagram header.
l3-start	Match criterion starts from the network header.
offset *number*	Match criterion can be made according to any aribitrary offset.
size *number*	Number of bytes in which to match.
eq	*Match criteria is met if the* packet is equal to the specified value or mask.
neq	*Match criteria is met if the* packet is not equal to the specified value or mask.
mask	(Optional) Can be used when the **eq** or the **neq** keywords are issued.
gt	*Match criteria is met if the* packet is greater than the specified value.
lt	*Match criteria is met if the* packet is less than the specified value.
range *range*	Match critera is based upon a lower and upper boundary protocol field range.
regex *string*	Match critera is based upon a string that is to be matched.

value	Value for which the packet must be in accordance with.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).
Cisco IOS XE 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines

To the match criteria that is to be used for flexible packet matching, you must first enter the**class-map** command to specify the name of the class whose match criteria you want to establish. Thereafter, you can enter one of the following commands:

- **match field** (which configures the match criteria for a class map on the basis of the fields defined in the protocol header description files [PHDFs])
- **match start** (which can be used if a PHDF is not loaded onto the router)

Examples

The following example shows how to configure FPM for blaster packets. The class map contains the following match criteria: TCP port 135, 4444 or UDP port 69; and pattern 0x0030 at 3 bytes from start of IP header.

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf
class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp
class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp
class-map type access-control match-all blaster1
 match field tcp dest-port eq 135
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster3
 match field udp dest-port eq 69
 match start 13-start offset 3 size 2 eq 0x0030
policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
 drop
policy-map type access-control fpm-udp-policy
 class blaster3
 drop
policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
 service-policy fpm-udp-policy
interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
load protocol	Loads a PHDF onto a router.
match field	Configures the match criteria for a class map on the basis of the fields defined in the PHDFs.

match tag (class-map)

To specify the tag to be matched for a tag type of class map, use the **matchtag** command in class-map configuration mode. To delete the tag, use the **no** form of this command.

match tag *tag-name*

no match tag *tag-name*

Syntax Description

tag-name	Name of the tag.

Command Default

No match tags are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The access control server (ACS) sends the tag attribute to the network access device (NAD) using the Cisco attribute-value (AV) pair. (The tag attribute can also be sent to the NAD using the IETF attribute 88.)

Examples

The following example shows that the tag to be matched is named “healthy”:

```
Router(config)# class-map type tag healthy_class
Router(config-cmap)# match tag healthy
Router(config-cmap)# end
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.

match vlan (QoS)

To match and classify traffic on the basis of the virtual local-area network (VLAN) identification number, use the **matchvlan** command in class-map configuration mode. To remove a previously specified VLAN identification number as a match criterion, use the **no** form of this command.

match vlan *vlan-id-number*

no match vlan *vlan-id-number*

Syntax Description

vlan-id-number	VLAN identification number, numbers, or range of numbers. Valid VLAN identification numbers must be in the range of 1 to 4095.

Command Default

Traffic is not matched on the basis of the VLAN identification number.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced for use on Cisco 10000 series routers only. .
15.1(1)T	This command was modified. Support for this command is no longer limited to the Cisco 10000 series routers.
Cisco IOS XE Release 2.1	This command was modifed. Support for this command was introduced on the Cisco ASR 1000 series routers.

Usage Guidelines

Specifying VLAN Identification Numbers

You can specify a single VLAN identification number, multiple VLAN identification numbers separated by spaces (for example, 2 5 7), or a range of VLAN identification numbers separated by a hyphen (for example, 25-35).

Support Restrictions

The following restrictions apply to the **matchvlan** command:

- The **matchvlan** command is supported for IEEE 802.1q and Inter-Switch Link (ISL) VLAN encapsulations only.
- As of Cisco IOS Release 12.2(31)SB2, the **matchvlan** command is supported on Cisco 10000 series routers only.

Examples

In the following sample configuration, the **matchvlan** command is enabled to classify and match traffic on the basis of a range of VLAN identification numbers. Packets with VLAN identification numbers in the range of 25 to 50 are placed in the class called class1.

```
Router> enable
Router# configure terminal
Router(config)# class-map class1
Router(config-cmap)# match vlan 25-50
Router(config-cmap)# end
```

Note Typically, the next step would be to configure class1 in a policy map, enable a quality of service (QoS) feature (for example, class-based weighted fair queueing [CBWFQ]) in the policy map, and attach the policy map to an interface. To configure a policy map, use the **policy-map** command. To enable CBWFQ, use the **bandwidth** command (or use the command for the QoS feature that you want to enable). To attach the policy map to an interface, use the**service-policy**command. For more information about classifying network traffic on the basis of a match criterion, see the “Classification” part of the Cisco IOS Quality of Service Solutions Configuration Guide , Release 12.4T.

Related Commands

Command	Description
bandwidth (policy-map class)	Specify or modifies the bandwidth allocated for a class belonging to a policy map.
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces.
service-policy	Attached a policy map to an interface.

match vlan inner

To configure a class map to match the innermost VLAN ID in an 802.1q tagged frame, use the **matchvlaninner**command in ATM interface configuration mode. To remove matching on the innermost VLAN ID of an 802.1q tagged frame, use the **no** form of this command.

match vlan inner *vlan-ids*

no match vlan inner *vlan-ids*

Syntax Description

vlan-ids	One or more VLAN IDs to be matched. The valid range for VLAN IDs is from 1 to 4095, and the list of VLAN IDs can include one or all of the following: • Single VLAN IDs, separated by spaces. For example: 100 200 300 • One or more ranges of VLAN IDs, separated by spaces. For example: 1-1024 2000-2499

Command Default

Packets are not matched on the basis of incoming dot1q VLAN inner IDs.

Command Modes

Class map configuration

Command History

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF	This command was implemented on Cisco 7600 series routers.

Examples

The following example creates a class map that matches packets with a VLAN IDs of 100 to 300.

```
Router(config)#
class-map match-all vlan100
Router(config-cmap)# match vlan inner 100
Router(config-cmap)# exit
Router(config)# class-map match-all vlan200
Router(config-cmap)# match vlan inner 200
Router(config-cmap)# exit
Router(config)# class-map match-all vlan300
Router(config-cmap)# match vlan inner 300
```

Related Commands

Command	Description
clear cef linecard	Clears Cisco Express Forwarding (CEF) information on one or more line cards, but does not clear the CEF information on the main route processor (RP). This forces the line cards to synchronize their CEF information with the information that is on the RP.
match qos-group	Identifies a specified QoS group value as a match criterion.
mls qos trust	Sets the trusted state of an interface to determine which incoming QoS field on a packet, if any, should be preserved.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.
show platform qos policy-map	Displays the type and number of policy maps that are configured on the router.

maximum (local policy)

To set the limits for Resource Reservation Protocol (RSVP) resources, use the **maximum** command in local policy configuration mode. To delete the limits, use the **no** form of this command.

maximum [**bandwidth** [**group**| **single**] *bandwidth*| **senders** *maximum-senders*]

no maximum [**bandwidth** [**group**| **single**]| **senders**]

Syntax Description

bandwidth	(Optional) Indicates bandwidth limits for RSVP reservations.
group	(Optional) Specifies the amount of bandwidth, in kbps, that can be requested by all the reservations covered by a local policy.
single	(Optional) Specifies the maximum bandwidth, in kbps, that can be requested by any specific RSVP reservation covered by a local policy.
bandwidth	Maximum limit for the requested bandwidth, in kbps. Range is from 1 to 10000000.
senders	(Optional) Limits the number of RSVP senders affected by a local policy that can be active at the same time on a router.
maximum-senders	Maximum number of senders the specified policy allows. Range is from 1 to 50000; the default is 1000.

Command Default

No maximum bandwidth limit is set and no RSVP senders are configured.

Command Modes

Local policy configuration (config-rsvp-local-if-policy)

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.4(6)T	This command was modified to apply to RESV messages.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

As part of the application ID enhancement, the **maximumbandwidth** command applies to RESV messages. This change has the following benefits:

- Allows the local policy bandwidth limit to be used by RSVP's admission control process for both shared and nonshared reservations. Releases that performed group bandwidth checks on PATH messages could not account for bandwidth sharing and, as a result, you had to account for sharing by creating a larger maximum group bandwidth for the policy.
- Allows a local policy to trigger preemption during the admission control function if there is insufficient policy bandwidth to meet the needs of an incoming RESV message.

Examples

The following example specifies the maximum bandwidth for a group of reservations and for a single reservation, respectively:

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet 1/0
Router(config-if)# ip rsvp policy local identity video
Router(config-rsvp-local-policy)# maximum bandwidth group 500
Router(config-rsvp-local-policy)# maximum bandwidth single 50
```

Related Commands

Command	Description
ip rsvp policy local	Determines how to perform authorization on RSVP requests.

maximum bandwidth ingress

To configure the bandwidth parameters for the ingress policy pool, use the **maximumbandwidthingress** command in local policy configuration mode or local policy interface configuration mode. To disable the bandwidth configuration for the ingress policy pool, use the **no** form of this command.

Command Syntax in Local Policy Configuration Mode

maximum bandwidth ingress {**group**| **single**} *bandwidth*

no maximum bandwidth ingress {**group**| **single**}

Command Syntax in Local Policy Interface Configuration Mode

maximum bandwidth ingress {**group** *bandwidth*| **percent** {**group**| **single**} *percent*| **single** *bandwidth*}

no maximum bandwidth ingress {**group**| **percent** {**group**| **single**}| **single**}

Syntax Description

group	Specifies the maximum ingress bandwidth, in kb/s, that can be requested by all the reservations covered by a local policy.
single	Specifies the maximum ingress bandwidth, in kb/s, that can be requested by any specific RSVP reservation covered by a local policy.
bandwidth	Maximum limit for the requested ingress bandwidth, in kb/s.
percent {**group** | **single**}	Specifies a percentage of the ingress bandwidth of an interface as the maximum bandwidth available to a group of flows or a single flow.
percent	Maximum limit for the requested bandwidth, in percent.

Command Default

RSVP is disabled by default; therefore, maximum bandwidth limit is not set.

Command Modes

Local policy configuration (config-rsvp-local-policy) Local policy interface configuration (config-rsvp-local-if-policy)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Release	Modification
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

You can use the **maximumbandwidthingress**command to configure the maximum bandwidth for a given policy. You can also configure a percentage of the RSVP ingress bandwidth of an interface as the maximum bandwidth available to a group of flows, or a single flow matching the policy. The percentages of the RSVP bandwidth to be configured as the maximum bandwidth are not available for global-based RSVP policies, but are available for interface RSVP policies.

The **maximumbandwidthingresspercent** command is mutually exclusive with the **maximumbandwidthingressgroup** and **maximumbandwidthingresssingle** commands. That is, if you configure the maximum percentage of RSVP ingress bandwidth using the **maximumbandwidthingresspercent** command, any configurations made using the **maximumbandwidthingressgroup** and **maximumbandwidthingresssingle** commands are removed.

Examples

The following example shows how to configure the maximum ingress bandwidth for a group of reservations and for a single reservation respectively, in a global-based RSVP policy:

```
Device> enable
Device# configure terminal
Device(config)# ip rsvp policy local identity rsvp-video
Device(config-rsvp-local-policy)# maximum bandwidth ingress group
 200
Device(config-rsvp-local-policy)# maximum bandwidth ingress single 100
The following example shows how to configure the maximum percentage of RSVP ingress bandwidth
 of an interface for a group of reservations and for a single reservation, respectively:
Device> enable
Device# configure terminal
Device(config)# interface tunnel 0
Device(config-if)# ip rsvp policy local identity rsvp-video
Device(config-rsvp-local-if-policy)# maximum bandwidth ingress percent group 50
Device(config-rsvp-local-if-policy)# maximum bandwidth ingress single 50
```

Related Commands

Command	Description
show ip rsvp ingress	Displays information about the RSVP ingress bandwidth configured on interfaces.

maximum bandwidth percent

To configure the percentage of the Resource Reservation Protocol (RSVP) bandwidth of an interface as the maximum bandwidth available to a group of flows or a single flow, use the **maximumbandiwidthpercent**command in local policy configuration mode. To disable this configuration, use the **no** form of this command.

maximum bandwidth percent {**group**| **single**} *bandwidth-percentage*

no maximum bandwidth percent {**group**| **single**}

Syntax Description

group	Specifies the amount of bandwidth, in kb/s, that can be requested by all the reservations covered by a local policy.
single	Specifies the maximum bandwidth, in kb/s, that can be requested by any specific RSVP reservation covered by a local policy.
bandwidth-percentage	Maximum limit for the requested bandwidth, in kb/s.

Command Default

RSVP is disabled by default; therefore, no percentage bandwidth is set.

Command Modes

Local policy configuration (config-rsvp-local-if-policy)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **maximumbandwidthpercent** command is mutually exclusive with the **maximumbandwidthgroup** and **maximumbandwidthsingle** commands. That is, if you configure the maximum percentage of RSVP using the **maximumbandwidthpercent** command, any configurations made using the **maximumbandwidthgroup** and **maximumbandwidthsingle** commands are removed. The **maximumbandwidthpercent** command is not present in the global RSVP policy.

This maximum percentage of RSVP bandwidth configured for a group of flows is used to do RSVP Call Admission Control (CAC) for the flows matching with the policy. The **maximumbandiwidthpercent** command allows oversubscription. That is, you can configure more than 100 percent of the RSVP bandwidth as the maximum bandwidth for group reservations or as the maximum bandwidth for a single reservation.

Examples

The following example shows how to conifgure the maximum percentage of RSVP bandwidth of an interface for a group of reservations and for a single reservation, respectively:

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet 1/0
Router(config-if)# ip rsvp policy local identity video
Router(config-rsvp-local-policy)# maximum bandwidth percent group 50
Router(config-rsvp-local-policy)# maximum bandwidth single 50
```

Related Commands

Command	Description
ip rsvp policy local	Determines how to perform authorization on RSVP requests.
maximum (local policy)	Sets the limits for RSVP resources.

maximum header

To specify the maximum size of the compressed IP header, use the **maximumheader** command in IPHC-profile configuration mode. To return the maximum size of the compressed IP header to the default size, use the **no** form of this command.

maximum header *number-of-bytes*

no maximum header

Syntax Description

number-of-bytes	The maximum header size, in bytes. Valid entries are numbers from 20 to 168. Default is 168.

Command Default

The maximum size of the compressed IP header is 168 bytes.

Command Modes

IPHC-profile configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

The **maximumheader** command allows you to define the maximum size of the IP header of a packet to be compressed. Any packet with an IP header that exceeds the maximum size is sent uncompressed.

Use the *number-of-bytes* argument of the **maximumheader** command to restrict the size of the IP header to be compressed.

Intended for Use with IPHC Profiles

The **maximumheader** command is intended for use as part of an IPHC profile. An IPHC profile is used to enable and configure header compression on your network. For more information about using IPHC profiles to configure header compression, see the “Header Compression” module and the “Configuring Header Compression Using IPHC Profiles” module of the *Cisco IOS Quality of Service Solutions Configuration Guide* , Release 12.4T.

Prerequisite

Before using the **maximumheader**command, you must enable either TCP header compression or non-TCP header compression. To enable TCP header compression, use the **tcp** command. To enable non-TCP header compression, use the **non-tcp** command.

Examples

The following is an example of an IPHC profile called profile2. In this example, the maximum size of the compressed IP header is set to 75 bytes.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# non-tcp
Router(config-iphcp)# maximum header 75
Router(config-iphcp)# end
```

Related Commands

Command	Description
iphc-profile	Creates an IPHC profile.
non-tcp	Enables non-TCP header compression within an IPHC profile.
tcp	Enables TCP header compression within an IPHC profile.

max-reserved-bandwidth

Note Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **max-reservedbandwidth**command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note Effective with Cisco IOS XE Release 3.2S, the **max-reservedbandwidth**command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To change the percent of interface bandwidth allocated for Resource Reservation Protocol (RSVP), class-based weighted fair queueing (CBWFQ), low latency queueing (LLQ), IP RTP Priority, Frame Relay IP RTP Priority, Frame Relay PVC Interface Priority Queueing (PIPQ), or hierarchical queueing framework (HQF), use the **max-reservedbandwidth** command in interface configuration mode. To restore the default value, use the **no** form of this command.

max-reserved-bandwidth *percent*

no max-reserved-bandwidth

Syntax Description

percent	Amount of interface bandwidth allocated for RSVP, CBWFQ, LLQ, IP RTP Priority, Frame Relay IP RTP Priority, Frame Relay PIPQ, and HQF.

Command Default

75 percent on all supported platforms except the Cisco 7500 series routers, which do not have this restriction.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)T	This command was introduced.

Release	Modification
12.4(20)T	Support was added for HQF using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC). **Note** This is the last T release in which the command is supported.
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.
15.0(1)S	This command was modified. This command was hidden.
15.1(3)T	This command was modified. This command was hidden.
Cisco IOS XE Release 3.2S	This command was replaced by an MQC command (or sequence of MQC commands).

Usage Guidelines

The **max-reserved-bandwidth** command is not supported in Cisco IOS Release 12.2SR or in 12.2SX. It is supported in 12.4T, but only up to the 12.4(20)T release in which HQF functionality was integrated.

The sum of all bandwidth allocation on an interface should not exceed 75 percent of the available bandwidth on an interface. The remaining 25 percent of bandwidth is used for overhead, including Layer 2 overhead, control traffic, and best-effort traffic.

If you need to allocate more than 75 percent for RSVP, CBWFQ, LLQ, IP RTP Priority, Frame Relay IP RTP Priority, Frame Relay PIPQ, or HQF, you can use the **max-reserved-bandwidth** command. The *percent* argument specifies the maximum percentage of the total interface bandwidth that can be used.

If you do use the **max-reserved-bandwidth** command, make sure that not too much bandwidth is taken away from best-effort and control traffic.

Examples

In the following example, the policy map called policy1 is configured for three classes with a total of 8 Mbps configured bandwidth, as shown in the output from the **showpolicy-map** command:

```
Router# show policy-map policy1
 Policy Map policy1
  Weighted Fair Queueing
    Class class1
      Bandwidth 2500 (kbps) Max Threshold 64 (packets)
    Class class2
      Bandwidth 2500 (kbps) Max Threshold 64 (packets)
    Class class3
      Bandwidth 3000 (kbps) Max Threshold 64 (packets)
```

When you enter the **service-policy**command in an attempt to attach the policy map on a 10-Mbps Ethernet interface, an error message such as the following is produced:

```
I/f Ethernet1/1 class class3 requested bandwidth 3000 (kbps) Available only 2500 (kbps)
```

The error message is produced because the default maximum configurable bandwidth is 75 percent of the available interface bandwidth, which in this example is 7.5 Mbps. To change the maximum configurable bandwidth to 80 percent, use the **max-reserved-bandwidth** command in interface configuration mode, as follows:

```
max-reserved-bandwidth 80
service output policy1
end
```

To verify that the policy map was attached, enter the **showpolicy-mapinterface** command:

```
Router# show policy-map interface e1/1
 Ethernet1/1  output :policy1
  Weighted Fair Queueing
    Class class1
      Output Queue:Conversation 265
        Bandwidth 2500 (kbps) Packets Matched 0 Max Threshold 64 (packets)
        (discards/tail drops) 0/0
    Class class2
      Output Queue:Conversation 266
        Bandwidth 2500 (kbps) Packets Matched 0 Max Threshold 64 (packets)
        (discards/tail drops) 0/0
    Class class3
      Output Queue:Conversation 267
        Bandwidth 3000 (kbps) Packets Matched 0 Max Threshold 64 (packets)
        (discards/tail drops) 0/0
```

Examples

The following example configures a strict priority queue in a virtual template configuration with CBWFQ. The **max-reserved-bandwidth** command changes the maximum bandwidth allocated between CBWFQ and IP RTP Priority from the default (75 percent) to 80 percent.

```
multilink virtual-template 1
interface virtual-template 1
 ip address 172.16.1.1 255.255.255.0
 no ip directed-broadcast
 ip rtp priority 16384 16383 25
 service-policy output policy1
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 max-reserved-bandwidth 80
 end
interface Serial0/1
 bandwidth 64
 ip address 10.1.1.2 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 ppp multilink
 end
```

Note To make the virtual access interface function properly, do not configure the **bandwidth** command on the virtual template. Configure it on the actual interface, as shown in the example.

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
ip rtp priority	Reserves a strict priority queue for a set of RTP packet flows belonging to a range of UDP destination ports.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.

Command	Description
show policy-map	Displays the configuration of all classes comprising the specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.

metadata application-params

To enter metadata application entry configuration mode and create new metadata application parameters, use the **metadata application-params** command in global configuration mode. To remove previously configured metadata application parameters, use the **no** form of this command.

metadata application-params *app-param-name*

no metadata application-params *app-param-name*

Syntax Description

app-param-name	Metadata application name that can be used as the match criterion for provisioning control plane classification.

Command Default

The application parameters for metadata-based classification are not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

To create new metadata application parameters that can be used as match criteria for provisioning control plane classification, use the **metadata application-params** command. The **metadata application-params** command places the device in metadata application entry configuration mode. Use the following commands in metadata application entry configuration mode to configure the properties of the application. Configuring the name and ID is mandatory.

- **default—**Default properties for the name, description, and ID for the specified application.
- **description** *description-text***—**Description of the application. Supports up to 55 characters.
- **identifier** *id-value***—**Application ID. Internally maps to the application name. The range is from 1 to 16777215.
- **name** *name***—**Name of the application. Supports up to 24 characters.

Use the **show metadata application table** command to display the details of all metadata applications.

Examples

The following example shows how to create a new metadata application with appropriate parameters:

```
Device(config)# metadata application-params app1
Device(config-md-app-entry)# name instant-messaging-audio
Device(config-md-app-entry)# identifier 243
Device(config-md-app-entry)# description instant messaging audio recordings
```

The following output of the **show metadata application table** command shows the name and ID of all the metadata applications configured on a specific endpoint:

```
Device# show metadata application table

ID     Name                  Vendor                Vendor id
--------------------------------------------------------------------------------
113    telepresence-media    -                     -
114    telepresence-contr$   -                     -
478    telepresence-data     -                     -
414    webex-meeting         -                     -
56     citrix                -                     -
81     cisco-phone           -                     -
472    vmware-view           -                     -
473    wyze-zero-client      -                     -
61     rtp                   -                     -
64     h323                  -                     -
5060   sip                   -                     -
554    rtsp                  -                     -
496    jabber                -                     -
5222   xmpp-client           -                     -
```

The table below describes the significant fields shown in the display.

Table 7: show metadata application table Field Descriptions

Field	Description
ID	Application ID. Internally maps to the application name.
Name	Name of the application.

Related Commands

Command	Description
debug metadata	Enables debugging for metadata flow.
default	Displays default properties for the name, description, and ID for the specified application.
description	Displays the description of the application.
identifier	Displays the Application ID.
name	Displays the name of the application.

Command	Description
show metadata application table	Displays a list of metadata applications defined on a device.
show metadata flow	Displays metadata flow information.
name	Displays the name of the application.

metadata flow

To enable metadata on all interfaces or on a specific interface, use the **metadata flow** command in global configuration mode or interface configuration mode. To disable metadata, use the **no** form of this command.

metadata flow

no metadata flow

Syntax Description

This command has no arguments or keywords.

Command Default

Metadata is disabled on an interface.

Command Modes

Global configuration (config)

Interface configuration (config-if)

Command History

Release	Modification
15.2(1)T	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

If you use the **metadata flow** command in global configuration mode, metadata is enabled at the device level. That is, metadata is enabled on all the interfaces configured on the device. If you use the **metadata flow** command in interface configuration mode, metadata is enabled on the specified interface only. You can use the **no metadata flow** command in interface configuration mode to disable metadata on any one interface. However, metadata flows that enter from other interfaces will not be able to pass through an interface on which metadata has been disabled. In such instances, the flow table will not be populated and classification will not complete successfully. When you explicitly enable or disable metadata on an interface, configuration details are retrieved using the nonvolatile generation (NVGEN) method and are displayed in the configuration.

Examples

The following example shows how to enable metadata at the device level:

```
Device(config)# metadata flow
```

The following example shows how to enable metadata at the per-interface level:

```
Device(config)# interface gigabitethernet 0/0
Device(config-if)# metadata flow
```

Related Commands

Command	Description
metadata flow (troubleshooting)	Creates flow entries for testing and troubleshooting the metadata flow.

metadata flow (troubleshooting)

To simulate the creation of flows for testing and troubleshooting metadata, use the **metadata flow** command in global configuration mode. To remove the flows created for testing and troubleshooting, use the **no** form of this command.

Cisco IOS Release 15.1(1)SY and Later Releases

metadata flow

no metadata flow

Releases Prior to Cisco IOS Release 15.1(1)SY

metadata flow [**entry** *entry-name*| **flow-specifier** *flow-specifier-name* | **session-params** *session-name*]

no metadata flow [**entry** *entry-name*| **flow-specifier** *flow-specifier-name* | **session-params** *session-name*]

Syntax Description

entry *entry-name*	Creates a flow entry with the specified name.
flow-specifier *flow-specifier-name*	Configures source and destination information.
session-params *session-name*	Configures session parameters for the flow.

Command Default

Static metadata flow entries are not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)T	This command was introduced.
15.1(1)SY	The command was modified. The **entry** *entry-name*, **flow-specifier** *flow-specifier-name*, and **session-params** *session-name* keyword-argument pairs were removed.

Usage Guidelines

You can use the **metadata flow** command along with the associated keywords when you need to simulate an environment consisting of virtual endpoints for testing or troubleshooting purposes.

Use the **metadata flow entry** *entry-name* command to create a flow. To create a successful flow, specify the flow specifier and session parameters.

Using the **flow-specifier** *flow-specifier-name* keyword and argument pair creates a flow specifier and places the device in metadata configuration flow specifier mode. Use the following commands in metadata configuration flow specifier mode to configure the flow tuple for the flow:

- **dest-ip** *ip-address* **dest-port** *port-number*—Specifies the destination IPv4 address and destination port number for the endpoint.
- **source-ip** *ip-address* **source-port** *port-number*—Specifies the source IPv4 address and source port number for the endpoint.

Using the **session-params** *session-name* keyword and argument pair places the command in metadata session parameters configuration mode. Use the following related command in metadata session parameters configuration mode to configure the session parameters for the flow:

- **application name** *application-name*—Associates the specified application name to the session.

Using the **entry** *entry-name* keyword and argument pair places the command in metadata entry configuration mode. In metadata entry configuration mode, use the **flow-specifier** keyword with the previously defined flow specifier and the **session-params** keyword with the previously defined session parameter name to associate with the specified flow entry.

Examples

The following examples show how to create a flow entry, a flow specifier, and session parameters, and how to associate the flow specifier and session parameters with the flow entry.

The following configuration shows how to create a flow entry:

```
Device(config)# metadata flow entry e1
```

The following example shows how to create a flow specifier with the source IP address, destination IP address, and source and destination port numbers:

```
Device(config)# metadata flow flow-specifier flow1
Device(config-md-flowspec)# source 209.165.201.3 source-port 1000
Device(config-md-flowspec)# destination 209.165.201.20 dest-port 1000
```

The following example shows how to create a session parameter and the associated parameters:

```
Device(config)# metadata flow session-params session1
Device(config-md-session-params)# application name webex-meeting
```

The following example shows how to associate the flow specifier and session parameters with the flow entry:

```
Device(config)# metadata flow entry e1
Device(config-md-entry)# flow-specifier flow1
Device(config-md-entry)# session-params session1
```

Related Commands

Command	Description
debug metadata	Enables debugging for metadata flow.
show metadata application table	Displays a list of metadata applications defined on a device.
show metadata flow	Displays metadata flow information.

mls ip pbr

To enable the multilayer switching (MLS) support for policy-routed packets, use the **mlsippbr**command in global configuration mode. To disable the MLS support for policy-routed packets, use the **no** form of this command.

mls ip pbr [null0]

no mls ip pbr

Syntax Description

null0	(Optional) Enables the hardware support for the interface null0 in the route-maps.

Command Default

MLS support for policy-routed packets is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17d)SXB	This command was introduced on the Supervisor Engine 2 and introduced into Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed to support the **null0** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

Note Do not enable PBR and SLB on the same interface; PBR-based packets are not forwarded correctly.

When you enable the hardware-policy routing by entering the **mlsippbr** command, all policy routing occurs in the hardware and is applied to all interfaces, regardless of which interface was configured for policy routing.

Use the **null0** keyword when you have routed traffic only to enable the hardware support for the **setinterfacenull0** in the route-maps.

Examples

This example shows how to enable the MLS support for policy-routed packets:

```
Router(config)#
mls ip pbr
```

Related Commands

Command	Description
show tcam interface vlan acl	Displays information about the interface-based TCAM.