match e – match q

match ehlo-reply-parameter

To configure a match condition on the ESMTP ehlo reply parameter, use the **match ehlo-reply-parameter** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **ehlo-reply-parameter** *parameter*
no match [**not**] **ehlo-reply-parameter** *parameter*

Syntax Description

parameter	Specifies the ehlo reply parameter.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure a match condition for an ehlo reply parameter in an ESMTP inspection policy map:

```
ciscoasa
(config)#
 policy-map type inspect esmtp esmtp_map
```

ciscoasa (config-pmap)# **match ehlo-reply-parameter auth**

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.

Command	Description
show running-config class-map	Displays the information about the class map configuration.

match filename

To configure a match condition for a filename for FTP transfer, use the **match filename** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **filename regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **filename regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class regex_class_name	Specifies a regular expression class map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in an FTP class map or policy map. Only one entry can be entered in a FTP class map.

Examples

The following example shows how to configure a match condition for an FTP transfer filename in an FTP inspection class map:

```
ciscoasa(config)# class-map type inspect ftp match-all ftp_class1
ciscoasa(config-cmap)# description Restrict FTP users ftp1, ftp2, and ftp3 from accessing
/root
ciscoasa(config-cmap)# match username regex class ftp_regex_user
ciscoasa(config-cmap)# match filename regex ftp-file
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.

Command	Description
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match filetype

To configure a match condition for a filetype for FTP transfer, use the **match filetype** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **filetype regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **filetype regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class regex_class_name	Specifies a regular expression class map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in an FTP class map or policy map. Only one entry can be entered in a FTP class map.

Examples

The following example shows how to configure a match condition for an FTP transfer filetype in an FTP inspection policy map:

```
ciscoasa(config-pmap)# match filetype class regex ftp-regex-filetype
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.

Command	Description
show running-config class-map	Displays the information about the class map configuration.

match flow ip destination-address

To specify the flow IP destination address in a class map, use the **match flow ip destination-address** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

matchflowipdestination-address
nomatchflowipdestination-address

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **match** commands are used to identify the traffic included in the traffic class for a class map. They include different criteria to define the traffic included in a class-map. Define a traffic class using the **class-map** global configuration command as part of configuring a security feature using Modular Policy Framework. From class-map configuration mode, you can define the traffic to include in the class using the **match** command.

After a traffic class is applied to an interface, packets received on that interface are compared to the criteria defined by the **match** statements in the class map. If the packet matches the specified criteria, it is included in the traffic class and is subjected to any actions associated with that traffic class. Packets that do not match any of the criteria in any traffic class are assigned to the default traffic class.

To enable flow-based policy actions on a tunnel group, use the **match flow ip destination-address** and **match tunnel-group** commands with the **class-map**, **policy-map**, and **service-policy** commands. The criteria to define flow is the destination IP address. All traffic going to a unique IP destination address is considered a flow. Policy action is applied to each flow instead of the entire class of traffic. QoS action police is applied using the **match flow ip destination-address** command. Use **match tunnel-group** to police every tunnel within a tunnel group to a specified rate.

Examples

The following example shows how to enable flow-based policing within a tunnel group and limit each tunnel to a specified rate:

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
```

```
 tunnel-group
ciscoasa(config-cmap)# match flow ip destination-address
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# police 56000
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.
match access-list	Identifies access list traffic within a class map.
show running-config class-map	Displays the information about the class map configuration.
tunnel-group	Creates and manages the database of connection-specific records for VPN.

match header (policy-map type inspect esmtp)

To configure a match condition on the ESMTP header, use the **match header** command in policy-map type inspect esmtp configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **header** [[**length** | **line length**] **gt** *bytes* | **to-fields count gt** *to_fields_number*]
no match [**not**] **header** [[**length** | **line length**] **gt** *bytes* | **to-fields count gt** *to_fields_number*]

Syntax Description

length gt bytes	Specifies to match on the length of the ESMTP header message.
line length gt bytes	Specifies to match on the length of a line of an ESMTP header message.
to-fields count gt to_fields_number	Specifies to match on the number of To: fields.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy-map type inspect esmtp configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure a match condition for a header in an ESMTP inspection policy map:

```
ciscoasa
(config)#
 policy-map type inspect esmtp esmtp_map
```

ciscoasa (config-pmap)# **match header length gt 512**

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.

Command	Description
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match header (policy-map type inspect ipv6)

To configure a match condition on the IPv6 header, use the **match header** command in policy-map type inspect ipv6 configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **header** { **ah** | **count gt** *number* | **destination-option** | **esp** | **fragment** | **hop-by-hop** | **routing-address count gt** *number* | **routing-type** { **eq** | **range** } *number* }
no match [**not**] **header** { **ah** | **count gt** *number* | **destination-option** | **esp** | **fragment** | **hop-by-hop** | **routing-address count gt** *number* | **routing-type** { **eq** | **range** } *number* }

Syntax Description

ah	Matches the IPv6 Authentication extension header
count gt *number*	Specifies the maximum number of IPv6 extension headers, from 0 to 255.
destination-option	Matches the IPv6 destination-option extension header.
esp	Matches the IPv6 Encapsulation Security Payload (ESP) extension header.
fragment	Matches the IPv6 fragment extension header.
hop-by-hop	Matches the IPv6 hop-by-hop extension header.
not	(Optional) Does not match the specified parameter.
routing-address count gt *number*	Sets the maximum number of IPv6 routing header type 0 addresses, greater than a number between 0 and 255.
routing-type {**eq** | **range**} *number*	Matches the IPv6 routing header type, from 0 to 255. For a range, separate values by a space, for example, **30 40**.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy-map type inspect ipv6 configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

Specifies the headers you want to match. By default, the packet is logged (**log**); if you want to drop (and optionally also log) the packet, enter the **drop** and optional **log** commands in match configuration mode.

Re-enter the **match** command and optional **drop** action for each extension you want to match:

Examples

The following example creates an inspection policy map that will drop and log all IPv6 packets with the hop-by-hop, destination-option, routing-address, and routing type 0 headers:

```
policy-map type inspect ipv6 ipv6-pm
 parameters
 match header hop-by-hop
  drop log
 match header destination-option
  drop log
 match header routing-address count gt 0
  drop log
 match header routing-type eq 0
  drop log
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match header-flag

To configure a match condition for a DNS header flag, use the **match header-flag** command in class-map or policy-map configuration mode. To remove a configured header flag, use the **no** form of this command.

match [**not**] **header-flag** [**eq**] { *f_well_known* | *f_value* }
no match [**not**] **header-flag** [**eq**] { *f_well_known* | *f_value* }

Syntax Description

eq	Specifies an exact match. If not configured, specifies a match-all bit mask match.
f_well_known	Specifies DNS header flag bits by well-known name. Multiple flag bits may be entered and logically OR'd. QR (Query, note: QR=1, indicating a DNS response) AA (Authoritative Answer) TC (TrunCation) RD (Recursion Desired) RA (Recursion Available)
f_value	Specifies an arbitrary 16-bit value in hexadecimal form.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in a DNS class map or policy map. Only one entry can be entered in a DNS class map.

Examples

The following example shows how to configure a match condition for a DNS header flag in a DNS inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match header-flag AA
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match im-subscriber

To configure a match condition for a SIP IM subscriber, use the **match im-subscriber** command in class-map or policy-map configuration mode. To remove the match condtion, use the **no** form of this command.

match [**not**] **im-subscriber regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **im-subscriber regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class regex_class_name	Specifies a regular expression class map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in a SIP class map or policy map. Only one entry can be entered in a SIP class map.

Examples

The following example shows how to configure a match condition for a SIP IM subscriber in a SIP inspection class map:

```
ciscoasa(config-cmap)# match im-subscriber regex class im_sender
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.

Command	Description
show running-config class-map	Displays the information about the class map configuration.

match interface

To distribute any routes that have their next hop out one of the interfaces specified, use the **match interface** command in route-map configuration mode. To remove the match interface entry, use the **no** form of this command.

match interface *interface-name*
no match interface *interface-name*

Syntax Description

interface-name	Name of the interface (not the physical interface). Multiple interface names can be specified.

Command Default

No match interfaces are defined.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the interface-type interface-number arguments.

The **route-map global** configuration command and the **match** and **set** configuration commands allow you to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. You can give the **match** commands in any order. All **match** commands must "pass" to cause the route to be redistributed according to the set actions that are given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria. If there is more than one interface specified in the **match** command. then the **no match interface** interface-name can be used to remove a single interface.

A route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command is ignored. If you want to modify only some data, you must configure a second route map section and specify an explicit match.

Examples

The following example shows that the routes with their next hop outside is distributed:

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match interface outside
```

Related Commands

Command	Description
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address that is specified by the access lists.
match metric	Redistributes routes with the metric specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

match invalid-recipients

To configure a match condition on the ESMTP invalid recipient address, use the **match invalid-recipients** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **invalid-recipients count gt** *number*
no match [**not**] **invalid-recipients count gt** *number*

Syntax Description

count gt number	Specifies to match on the invalid recipient number.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure a match condition for invalid recipients count in an ESMTP inspection policy map:

```
ciscoasa
(config)#
 policy-map type inspect esmtp esmtp_map
```

ciscoasa (config-pmap)# **match invalid-recipients count gt 1000**

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.

Command	Description
show running-config class-map	Displays the information about the class map configuration.

match ip address

To redistribute any routes that have a route address or match packet that is passed by one of the access lists specified, use the **match ip address** command in route-map configuration mode. To restore the default settings, use the **no** form of this command.

match ip address { *acl_id* . . . | **prefix-list** *prefix_list_id* . . . }
no match ip address { *acl_id* . . . | **prefix-list** *prefix_list_id* . . . }

Syntax Description

acl_id	Specifies the name of an access-list. Multiple access lists can be specified.
prefix-list *prefix_list_id*	Specifies the name of a prefix-list. Multiple prefix lists can be specified. **Note** Not supported for OSPF.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.20(2)	For OSPF, prefix lists are no longer supported.

Usage Guidelines

The **route-map** command and the **match** and **set** configuration commands allow you to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is enforced by the **match** commands are met. The **no route-map** command deletes the route map.

Examples

The following example shows how to redistribute internal routes:

```
ciscoasa(config)# route-map test
ciscoasa(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

Related Commands

Command	Description
match interface	Distributes any routes that have their next hop out one of the interfaces specified,
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
match ipv6 address	Distributes any routes that have an IPv6 route address or match packet that is passed by one of the access lists specified.
match metric	Redistributes routes with the metric specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

match ip next-hop

To redistribute any routes that have a next-hop router address that is passed by one of the access lists specified, use the **match ip next-hop** command in route-map configuration mode. To remove the next-hop entry, use the **no** form of this command.

match ip next-hop { *acl . . .* } | **prefix-list** *prefix_list*
no match ip next-hop { *acl . . .* } | **prefix-list** *prefix_list*

Syntax Description

acl	Name of an ACL. Multiple ACLs can be specified.
prefix-list *prefix_list*	Name of prefix list.

Command Default

Routes are distributed freely, without being required to match a next-hop address.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *acl* argument.

The **route-map global** configuration command and the **match** and **set** configuration commands allow you to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. You can enter the **match** commands in any order. All **match** commands must "pass" to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command is ignored. To modify only some data, you must configure a second route map section and specify an explicit match.

Examples

The following example shows how to distribute routes that have a next-hop router address passed by access list acl_dmz1 or acl_dmz2:

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ip next-hop acl_dmz1 acl_dmz2
```

Related Commands

Command	Description
match interface	Distributes distribute any routes that have their next hop out one of the interfaces specified.
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
match metric	Redistributes routes with the metric specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

match ip route-source

To redistribute routes that have been advertised by routers and access servers at the address that is specified by the ACLs, use the **match ip route-source** command in the route-map configuration mode. To remove the next-hop entry, use the **no** form of this command.

match ip route-source { *acl . . .* } **prefix-list** *prefix_list*
match ip route-source { *acl . . .* }

Syntax Description

acl	Name of an ACL. Multiple ACLs can be specified.
prefix_list	Name of prefix list.

Command Default

No filtering on a route source.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the access-list-name argument.

The **route-map global** configuration command and the **match** and **set** configuration commands allow you to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. You can enter the **match** commands in any order. All **match** commands must "pass" to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command is ignored. To modify only some data, you must configure a second route map section

and specify an explicit match. The next-hop and source-router address of the route are not the same in some situations.

Examples

The following example shows how to distribute routes that have been advertised by routers and access servers at the addresses specified by ACLs acl_dmz1 and acl_dmz2:

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ip route-source acl_dmz1 acl_dmz2
```

Related Commands

Command	Description
match interface	Distributes distribute any routes that have their next hop out one of the interfaces specified.
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the ACLs specified.
match metric	Redistributes routes with the metric specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

match ipv6 address

To redistribute any routes that have an IPv6 route address or match packet that is passed by one of the access lists specified, use the **match ipv6 address** command in route-map configuration mode. To restore the default settings, use the **no** form of this command.

match ipv6 address { *acl . . .* } **prefix-list**
no match ipv6 address { *acl . . .* } **prefix-list**

Syntax Description

acl	Specifies the name of an access list. Multiple access lists can be specified.
prefix-list	Specifies the name of a match prefix list.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

The **route-map global** configuration command and the **match** and **set** configuration commands allow you to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is enforced by the **match** commands are met. The **no route-map** command deletes the route map.

Examples

The following example shows how to redistribute internal routes: access-list acl_dmz1 extended permit ipv6 any <net> <mask>

```
ciscoasa(config)# access-list acl_dmz1 extended permit ipv6 any <net> <mask>
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ipv6 address acl_dmz1 acl_dmz2
```

Related Commands

Command	Description
match interface	Distributes any routes that have their next hop out one of the interfaces specified,

Command	Description
match ip address	Distributes any routes that have a route address or match packet that is passed by one of the access lists specified.
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
match metric	Redistributes routes with the metric specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

match login-name

To configure a match condition for a client login name for instant messaging, use the **match login-name** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **login-name regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **login-name regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class regex_class_name	Specifies a regular expression class map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in an IM class map or policy map. Only one entry can be entered in a IM class map.

Examples

The following example shows how to configure a match condition for a client login name in an instant messaging class map:

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match login-name regex login
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
show running-config class-map	Displays the information about the class map configuration.

match media-type

To configure a match condition on the H.323 media type, use the **match media-type** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **media-type** [**audio** | **data** | **video**]
no match [**not**] **media-type** [**audio** | **data** | **video**]

Syntax Description

audio	Specifies to match audio media type.
data	Specifies to match data media type.
video	Specifies to match video media type.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure a match condition for audio media type in an H.323 inspection class map:

```
ciscoasa(config-cmap)# match media-type audio
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match message class

To configure a match condition for the message class and type of M3UA messages, use the **match message class** command in policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **message class** *class_id* [**id** *message_id*]
no match [**not**] **message class** *class_id* [**id** *message_id*]

Syntax Description

class_id	The message class. See the usage section for a list of supported classes and types.
id *message_id*	The message type within the specified class.

Command Default

M3UA inspection allows all message classes and types without rate limits.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

You can configure this command in an M3UA inspection policy map. You can drop or rate limit packets based on the message class and type. The following table lists the possible values. Consult M3UA RFCs and documentation for detailed information about these messages.

M3UA Message Class	Message ID Type
0 (Management Messages)	0-1
1 (Transfer Messages)	1
2 (SS7 Signaling Network Management Messages)	1-6
3 (ASP State Maintenance Messages)	1-6
4 (ASP Traffic Maintenance Messages)	1-4
9 (Routing Key Management Messages)	1-4

Examples

The following example shows how to configure a match condition for M3UA messages.

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# match message class 2 id 6
ciscoasa(config-pmap-c)# drop
ciscoasa(config-pmap-c)# match message class 9
ciscoasa(config-pmap-c)# drop
```

Related Commands

Command	Description
inspect m3ua	Enables M3UA inspection.
policy-map type inspect	Creates an inspection policy map.

match message id

To configure a match condition for a GTP message ID, use the **match message id** command in policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **message** { **v1** | **v2** } **id** [*message_id* | **range** *lower_range upper_range* }
no match [**not**] **message** { **v1** | **v2** } **id** [*message_id* | **range** *lower_range upper_range* }

Syntax Description

{**v1** | **v2**}	(Starting with 9.5(1).) Indicates the GTP version. Use **v1** for GTPv0-1, and **v2** for GTPv2.
message_id	The message ID, which can be 1 to 255.
range *lower_range upper_range*	A range of message IDs. Specify the lower and upper boundaries of the range.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
9.5(1)	The {**v1** | **v2**} keywords were added.

Usage Guidelines

This command can be configured in a GTP policy map.

Examples

The following example shows how to configure a match condition for a message ID in a GTP inspection policy map:

```
ciscoasa(config-pmap)# match message id 33
```

Starting with release 9.5(1), you need to add the {**v1** | **v2**} keyword:

```
ciscoasa(config-pmap)# match message v2 id 33
```

Related Commands

Command	Description
inspect gtp	Configures inspection of GTP traffic.

match message length

To configure a match condition for a GTP message ID, use the **match message length** command in policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **message length min** *min_length* **max** *max_length*
no match [**not**] **message length min** *min_length* **max** *max_length*

Syntax Description

min *min_length*	Specifies a minimum message ID length. Value is between 1 and 65536.
max *max_length*	Specifies a maximum message ID length. Value is between 1 and 65536.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in a GTP policy map.

Examples

The following example shows how to configure a match condition for a message length in a GTP inspection policy map:

```
ciscoasa(config-pmap)# match message length min 8 max 200
```

Related Commands

Command	Description
inspect gtp	Configures inspection of GTP traffic.
match message id	Matches traffic based on message ID.

match message-path

To configure a match condition for the path taken by a SIP message as specified in the Via header field, use the **match message-path** command in class-map or policy-map configuration mode. To remove the match condtion, use the **no** form of this command.

match [**not**] **message-path regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **message-path regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class regex_class_name	Specifies a regular expression class map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in a SIP class map or policy map. Only one entry can be entered in a SIP class map.

Examples

The following example shows how to configure a match condition for the path taken by a SIP message in a SIP inspection class map:

```
ciscoasa(config-cmap)# match message-path regex class sip_message
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match metric

To redistribute routes with the metric specified, use the **match metric** command in route-map configuration mode. To remove the entry, use the **no** form of this command.

match metric *number*
no match metric *number*

Syntax Description

number	Route metric, which can be an IGRP five-part metric; valid values are from 0 to 4294967295.

Command Default

No filtering on a metric value.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **route-map global** configuration command and the **match** and **set** configuration commands allow you to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command is ignored. To modify only some data, you must configure a second route map section and specify an explicit match.

Examples

The following example shows how to redistribute routes with the metric 5:

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match metric 5
```

Related Commands

Command	Description
match interface	Distributes distribute any routes that have their next hop out one of the interfaces specified,
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

match mime

To configure a match condition on the ESMTP mime encoding type, mime filename length, or mime file type, use the **match mime** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **mime** [**encoding** *type* | **filename length gt** *bytes* | **filetype** *regex*]
no match [**not**] **mime** [**encoding** *type* | **filename length gt** *bytes* | **filetype** *regex*]

Syntax Description

encoding type	Specifies to match on the encoding type.
filename length gt bytes	Specifies to match on the filename length.
filetype regex	Specifies to match on the file type.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure a match condition for a mime filename length in an ESMTP inspection policy map:

```
ciscoasa
(config)#
 policy-map type inspect esmtp esmtp_map
```

ciscoasa (config-pmap)# **match mime filename length gt 255**

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.

Command	Description
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match msisdn

To configure a match condition for a GTP Mobile Station International Subscriber Directory Number (MSISDN) information element in the Create PDP Context request, Create Session request, and Modify Bearer Response messages, use the **match msisdn** command in policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **msisdn regex** { *regex_name* | **class** *class_name* }
no match [**not**] **msisdn regex** { *regex_name* | **class** *class_name* }

Syntax Description

regex_name	The name of a regular expression object.
class *class_name*	The name of a regular expression class.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.10(1)	This command was introduced.

Usage Guidelines

This command can be configured in a GTP policy map.

You can filter on the Mobile Station International Subscriber Directory Number (MSISDN) information element in the Create PDP Context request. You can drop and optionally log messages based on a specific MSISDN, or on a range of MSISDNs based on the first x number of digits. You use a regular expression to specify the MSISDN. MSISDN filtering is supported for GTPv1 and GTPv2 only.

Examples

The following example shows how to configure an MSISDN match condition using a regular expression object.

```
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# match msisdn regex msisdn1
ciscoasa(config-pmap-c)# drop log
```

The following example shows how to configure an MSISDN match condition using a regular expression class.

```
ciscoasa(config)# policy-map type inspect gtp gtp-map

ciscoasa(config-pmap)# match msisdn regex class msisdn2

ciscoasa(config-pmap-c)# drop log
```

Related Commands

Command	Description
drop	Drop packets that match the criteria.
log	Log packets that match the criteria.
inspect gtp	Enables GTP application inspection.
policy-map type inspect gtp	Creates or edits a GTP inspection policy map.

match opc

To configure a match condition for the originating point code (OPC) of M3UA data messages, use the **match opc** command in policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **opc** *code*
no match [**not**] **opc** *code*

Syntax Description

code	The originating point code in *zone -region -sp* format.

Command Default

M3UA inspection allows all originating point codes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

You can configure this command in an M3UA inspection policy map. You can drop packets based on the originating point code. Point code is in *zone -region -sp* format, where the possible values for each element depend on the SS7 variant. You define the variant on the **ss7 variant** command in the policy map.

- ITU—Point codes are 14 bit in 3-8-3 format. The value ranges are [0-7]-[0-255]-[0-7]. This is the default SS7 variant.
- ANSI—Point codes are 24 bit in 8-8-8 format. The value ranges are [0-255]-[0-255]-[0-255].
- Japan—Point codes are 16 bit in 5-4-7 format. The value ranges are [0-31]-[0-15]-[0-127].
- China—Point codes are 24 bit in 8-8-8 format. The value ranges are [0-255]-[0-255]-[0-255].

Examples

The following example shows how to configure a match condition for a specific originating point code for ITU.

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# match opc 1-5-1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# ss7 variant ITU
```

Related Commands

Command	Description
inspect m3ua	Enables M3UA inspection.
match dpc	Matches the M3UA destination point code.
policy-map type inspect	Creates an inspection policy map.
ss7 variant	Identifies the SS7 variant to use in the policy map.

match peer-ip-address

To configure a match condition for the peer IP address for instant messaging, use the **match peer-ip-address** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **peer-ip-address** *ip_address ip_address_mask*
no match [**not**] **peer-ip-address** *ip_address ip_address_mask*

Syntax Description

ip_address	Specifies a hostname or IP address of the client or server.
ip_address_mask	Specifies the netmask for the client or server IP address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in an IM class map or policy map. Only one entry can be entered in a IM class map.

Examples

The following example shows how to configure a match condition for the peer IP address in an instant messaging class map:

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match peer-ip-address 10.1.1.0 255.255.255.0
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
show running-config class-map	Displays the information about the class map configuration.

match peer-login-name

To configure a match condition for the peer login name for instant messaging, use the **match peer-login-name** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **peer-login-name regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **peer-login-name regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class regex_class_name	Specifies a regular expression class map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in an IM class map or policy map. Only one entry can be entered in a IM class map.

Examples

The following example shows how to configure a match condition for the peer login name in an instant messaging class map:

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match peer-login-name regex peerlogin
```

Related Commands

Command	Description
class-map type inspect	Creates an inspection class map.
show running-config class-map	Displays the information about the class map configuration.

match port

When using the Modular Policy Framework, match the ports to which you want to apply actions by using the **match port** command in class-map configuration mode. To remove the **match port** command, use the **no** form of this command.

match port { **tcp** | **udp** | **sctp** } { **eq** *port* | **range** *beg_port end_port* }
no match port { **tcp** | **udp** | **sctp** } { **eq** *port* | **range** *beg_port end_port* }

Syntax Description

eq *port*	Specifies a single port name or number.
range *beg_port end_port*	Specifies beginning and ending port range values between 1 and 65535.
tcp	Specifies a TCP port.
sctp	Specifies an SCTP port.
udp	Specifies a UDP port.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	The **sctp** keyword was added.

Usage Guidelines

Configuring Modular Policy Framework consists of four tasks:

1. Identify the Layer 3 and 4 traffic to which you want to apply actions using the **class-map** or **class-map type management** command.

After you enter the **class-map** command, you can enter the **match port** command to identify the traffic. Alternatively, you can enter a different type of **match** command, such as the **match access-list** command (the **class-map type management** command only allows the match port command). You can only include one **match port** command in the class map, and you cannot combine it with other types of **match** commands.

1. (Application inspection only) Define special actions for application inspection traffic using the **policy-map type inspect** command.
2. Apply actions to the Layer 3 and 4 traffic using the **policy-map** command.
3. Activate the actions on an interface using the **service-policy** command.

Examples

The following example shows how to define a traffic class using a class map and the **match port** command:

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq 8080
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match access-list	Matches traffic according to an access list.
match any	Includes all traffic in the class map.
show running-config class-map	Displays the information about the class map configuration.

match ppid

To configure a match condition for the payload protocol identifier (PPID) for SCTP inspection, use the **match ppid** command in inspection policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **ppid** *ppid_1* [*ppid_2*]
no match [**not**] **ppid** *ppid_1* [*ppid_2*]

Syntax Description

ppid_1 [*ppid_2*]	Specifies an SCTP PPID, either by the PPID number (0-4294967295) or name (see the CLI help for the available names). You can include a second (higher) PPID to specify a range.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Inspection policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

This command can be configured in an SCTP inspection policy map. Use it to filter on PPID to apply special actions to those IDs, such as drop, log, or rate limit.

If you decide to filter on PPID, keep the following in mind:

- PPIDs are in data chunks, and a given packet can have multiple data chunks. If a packet includes data chunks with different PPIDs, the packet will not be filtered, and the assigned action will not be applied to the packet.
- If you use PPID filtering to drop or rate-limit packets, be aware that the transmitter will resend any dropped packets. Although a packet for a rate-limited PPID might make it through on the next attempt, a packet for a dropped PPID will again be dropped. You might want to evaluate the eventual consequence of these repeated drops on your network.

Examples

The following example creates an SCTP inspection policy map that will drop unassigned PPIDs (unassigned at the time this example was written), rate limit PPIDs 32-40, and log the Diameter PPID.

```
policy-map type inspect sctp sctp-pmap
 match ppid 58 4294967295
  drop
 match ppid 26
  drop
 match ppid 49
  drop
 match ppid 32 40
  rate-limit 1000
 match ppid diameter
  log
```

Related Commands

Command	Description
drop	Drops matching traffic.
inspect sctp	Enables SCTP inspection.
log	Logs matching traffic.
policy-map type inspect sctp	Creates an SCTP inspection policy map.
rate-limit	Applies a rate limit to matching traffic.

match precedence

To specify a precedence value in a class map, use the **match precedence** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

matchprecedence*value*
nomatchprecedence*value*

Syntax Description

value	Specifies up to four precedence values separated by a space. Range is 0 to 7.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **match** commands are used to identify the traffic included in the traffic class for a class map. They include different criteria to define the traffic included in a class-map. Define a traffic class using the **class-map** global configuration command as part of configuring a security feature using Modular Policy Framework. From class-map configuration mode, you can define the traffic to include in the class using the **match** command.

After a traffic class is applied to an interface, packets received on that interface are compared to the criteria defined by the **match** statements in the class map. If the packet matches the specified criteria, it is included in the traffic class and is subjected to any actions associated with that traffic class. Packets that do not match any of the criteria in any traffic class are assigned to the default traffic class.

Use the **match precedence** command to specify the value represented by the TOS byte in the IP header.

Examples

The following example shows how to define a traffic class using a class map and the **match precedence** command:

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
 precedence 1
ciscoasa(config-cmap)#
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.
match access-list	Identifies access list traffic within a class map.
match any	Includes all traffic in the class map.
show running-config class-map	Displays the information about the class map configuration.

match protocol

To configure a match condition for a specific instant messaging protocol, such as MSN or Yahoo, use the **match protocol** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **protocol** { **msn-im** | **yahoo-im** }
no match [**not**] **protocol** { **msn-im** | **yahoo-im** }

Syntax Description

msn-im	Specifies to match the MSN instant messaging protocol.
yahoo-im	Specifies to match the Yahoo instant messaging protocol.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in an IM class map or policy map. Only one entry can be entered in a IM class map.

Examples

The following example shows how to configure a match condition for the Yahoo instant messaging protocol in an instant messaging class map:

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match protocol yahoo-im
```

Related Commands

Command	Description
class-map type inspect	Creates an inspection class map.
show running-config class-map	Displays the information about the class map configuration.

match question

To configure a match condition for a DNS question or resource record, use the **match question** command in class-map or policy-map configuration mode. To remove a configured section, use the **no** form of this command.

match { **question** | { **resource-record answer** | **authority** | **additional** } }
no match { **question** | { **resource-record answer** | **authority** | **additional** } }

Syntax Description

question	Specifies the question portion of a DNS message.
resource-record	Specifies the resource record portion of a DNS message.
answer	Specifies the Answer RR section.
authority	Specifies the Authority RR section.
additional	Specifies the Additional RR section.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

By default, this command inspects the DNS header and matches the specified field. It can be used in conjunction with other DNS match commands to define inspection of a particular question or RR type..

This command can be configured within a DNS class map or policy map. Only one entry can be entered within a DNS class-map.

Examples

The following example shows how to configure a match condition for a DNS question in a DNS inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match question
```

Related Commands

Command	Description
class-map type inspect	Creates an inspection class map.
policy-map type inspect	Creates an inspection policy map.