



## Command Reference

This appendix describes the Firewall Services Module commands that are unique to this module and the commands that have been changed from the PIX command implementation for use with the Firewall Services Module.

For detailed information about the PIX software commands, refer to the PIX documentation located at these URLs:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_60/](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_60/)

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_62/](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/)

Command	Command
<a href="#">access-list, page B-2</a>	<a href="#">route-map, page B-30</a>
<a href="#">access-list (ospf), page B-7</a>	<a href="#">set metric, page B-32</a>
<a href="#">area, page B-8</a>	<a href="#">set metric-type, page B-33</a>
<a href="#">clear console-output, page B-11</a>	<a href="#">show console-output, page B-34</a>
<a href="#">clear logging rate-limit, page B-12</a>	<a href="#">show crashdump, page B-35</a>
<a href="#">default-information originate, page B-13</a>	<a href="#">show firewall module, page B-36</a>
<a href="#">distance, page B-14</a>	<a href="#">show firewall vlan-group, page B-37</a>
<a href="#">firewall module, page B-15</a>	<a href="#">show interface, page B-38</a>
<a href="#">firewall vlan-group, page B-16</a>	<a href="#">show ip ospf, page B-39</a>
<a href="#">interface, page B-17</a>	<a href="#">show logging rate-limit, page B-41</a>
<a href="#">ip prefix-list, page B-18</a>	<a href="#">show vlan, page B-42</a>
<a href="#">logging rate-limit, page B-19</a>	<a href="#">summary-address, page B-43</a>
<a href="#">match, page B-21</a>	<a href="#">timers lsa-group-pacing, page B-44</a>
<a href="#">nameif, page B-22</a>	<a href="#">timers spf, page B-45</a>
<a href="#">network, page B-23</a>	<a href="#">upgrade-mp, page B-46</a>
<a href="#">ospf, page B-24</a>	
<a href="#">redistribute, page B-26</a>	
<a href="#">route, page B-28</a>	
<a href="#">router ospf, page B-29</a>	

# access-list

To configure access rules, use the **access-list** command. Use the **no** form of this command to remove access rules from the configuration.


**Note**

The configuration options for the access-lists in module are the same as those supported in PIX 6.0. module also supports access rules configuration using the **object group** command as supported in PIX 6.2.


**Note**

Every interface on the module requires you to explicitly define access lists. By default access lists are defined as **deny any any**.

```
access-list acl_ID deny | permit { protocol | object-group protocol_obj_grp_id }
{ host source_addr | local_addr | source_addr | local_addr source_mask | local_mask |
object-group network_obj_grp_id } { [ operator port [ port ] | object-group service_obj_grp_id
] } { host destination_addr | remote_addr | destination_addr | remote_addr destination_mask |
remote_mask | object-group network_obj_grp_id { [ operator port [ port ] | object-group
service_obj_grp_id ] }
```

```
no access-list acl_ID deny | permit { protocol | object-group protocol_obj_grp_id }
{ host source_addr | local_addr | source_addr | local_addr source_mask | local_mask |
object-group network_obj_grp_id } { [ operator port [ port ] | object-group service_obj_grp_id
] } { host destination_addr | remote_addr | destination_addr | remote_addr destination_mask |
remote_mask | object-group network_obj_grp_id { [ operator port [ port ] | object-group
service_obj_grp_id ] }
```

```
access-list acl_ID deny | permit icmp { host source_addr | local_addr | source_addr | local_addr
source_mask | local_mask | object-group network_obj_grp_id } { host destination_addr |
remote_addr | destination_addr | remote_addr destination_mask | remote_mask | object-group
network_obj_grp_id } { [ icmp_type | object-group icmp_type_obj_grp_id ] }
```

```
no access-list acl_ID deny | permit icmp { host source_addr | local_addr | source_addr |
local_addr source_mask | local_mask | object-group network_obj_grp_id } { host
destination_addr | remote_addr | destination_addr | remote_addr destination_mask | remote_mask
| object-group network_obj_grp_id } { [ icmp_type | object-group icmp_type_obj_grp_id ] }
```

```
clear access-list [acl_ID]
```

```
show access-list [acl_ID]
```

## Syntax Description

<i>acl_ID</i>	Name of an access list. You can use either a name or number.
<b>deny</b>	<p>(Optional) Used with the <b>access-list</b> command to not allow a packet to traverse the PIX firewall. By default, the PIX firewall denies all inbound or outbound packets unless you specifically permit access.</p> <p>When used with a <b>crypto map</b> command statement, <b>deny</b> does not select a packet for IPsec protection. The deny option prevents traffic from being protected by IPsec in the context of that particular crypto map entry. In other words, it does not allow the policy as specified in the crypto map command statements to be applied to this traffic.</p>
<b>permit</b>	<p>Used with the <b>access-list</b> command to select a packet to traverse the PIX firewall. By default, PIX firewall denies all inbound or outbound packets unless you specifically permit access.</p> <p>When used with a crypto map command statement, permit selects a packet for IPsec protection. The permit option causes all IP traffic that matches the specified conditions to be protected by IPsec using the policy described by the corresponding crypto map command statements.</p>
<b>permit icmp</b>	<p>Used with the <b>access-list</b> command to allow an ICMP packet to traverse the PIX firewall. By default, PIX firewall denies all inbound or outbound packets unless you specifically permit access.</p> <p>When used with a crypto map command statement, permit selects a packet for IPsec protection. The permit option causes all IP traffic that matches the specified conditions to be protected by IPsec using the policy described by the corresponding crypto map command statements.</p>
<i>protocol</i>	Name or number of an IP protocol. This value can be one of the keywords <b>icmp</b> , <b>ip</b> , <b>tcp</b> , or <b>udp</b> , or an integer in the range 1 to 254 representing an IP protocol number. To match any Internet protocol, including ICMP, TCP, and UDP, use the keyword <b>ip</b> .
<b>object-group</b>	Identifies the object group.
<i>protocol_obj_grp_id</i>	Identification of the object group.
<b>host</b>	Identifies the host.
<i>source_addr</i>	Address of the network or host from which the packet is being sent. Use this field when an <b>access-list</b> command statement is used in conjunction with an <b>access-list</b> command statement, or with the <b>aaa match access-list</b> command and the <b>aaa authorization</b> command.
<i>local_addr</i>	Address of the network or host local to the PIX firewall. Specify a <i>local_addr</i> when the <b>access-list</b> command statement is used in conjunction with a crypto access-list command statement, a nat 0 access-list command statement, or a vpngroup split-tunnel command statement. The <i>local_addr</i> is the address after NAT has been performed.
<i>source_mask</i>	Netmask bits (mask) to be applied to <i>source_addr</i> , if the source address is for a network mask.
<i>local_mask</i>	Netmask bits (mask) to be applied to <i>local_addr</i> , if the local address is a network mask.
<i>network_obj_grp_id</i>	Name of the network object group containing a group of hosts and networks

<b>operator</b>	<p>A comparison operand that allows you to specify a port or a port range. Use without an operator and port to indicate all ports; for example:</p> <pre>access-list acl_out permit tcp any host 209.165.201.1</pre> <p>Use eq and a port to permit or deny access to only that port. For example, use <b>eq ftp</b> to permit or deny access only to FTP:</p> <pre>access-list acl_out deny tcp any host 209.165.201.1 eq ftp</pre> <p>Use lt and a port to permit or deny access to all ports less than the port you specify. For example, use lt 1024 to permit or deny access to the well known ports (1 to 1024):</p> <pre>access-list acl_dmz1 permit tcp any host 192.168.1.1 lt 1025</pre> <p>Use gt and a port to permit or deny access to all ports greater than the port you specify. For example, use gt 42 to permit or deny ports 43 to 65535:</p> <pre>access-list acl_dmz1 deny udp any host 192.168.1.2 gt 42</pre> <p>Use neq and a port to permit or deny access to every port except the ports that you specify. For example, use neq 10 to permit or deny ports 1-9 and 11 to 65535:</p> <pre>access-list acl_dmz1 deny tcp any host 192.168.1.3 neq 10</pre> <p>Use range and a port range to permit or deny access to only those ports named in the range. For example, use range 10 to 1024 to permit or deny access only to ports 10 through 1024. All other ports are unaffected. The use of port ranges can dramatically increase the number of IPsec tunnels. For example, if a port range of 5000 to 65535 is specified for a highly dynamic protocol, up to 60,535 tunnels can be created.</p> <pre>access-list acl_dmz1 deny tcp any host 192.168.1.4 range 21 1024</pre>
<b>port</b>	<p>Service you permit or deny access to. Specify services by the port that handles it, such as smtp for port 25, www for port 80, and so on. You can specify ports by either a literal name or a number in the range of 1 to 65535.</p> <p>You can view valid port numbers online at the following website:  <a href="http://www.isi.edu/in-notes/iana/assignments/port-numbers">http://www.isi.edu/in-notes/iana/assignments/port-numbers</a>.</p> <p>You can also specify numbers.</p>
<i>service_obj_grp_id</i>	Name of the port object group containing a group of services
<i>destination_addr</i>	IP address of the network or host to which the packet is being sent. Specify a <i>destination_addr</i> when the access-list command statement is used in conjunction with an access-list command statement, or with the <b>aaa match access-list</b> command and the <b>aaa authorization</b> command. For inbound connections, <i>destination_addr</i> is the address after NAT has been performed. For outbound connections, <i>destination_addr</i> is the address before NAT has been performed.
<i>destination_mask</i>	Netmask bits (mask) to be applied to <i>destination_addr</i> , if the destination address is a network mask.
<i>remote_addr</i>	IP address of the network or host remote to the firewall. Specify a <i>remote_addr</i> when the <b>access-list</b> command statement is used in conjunction with a <b>crypto access-list</b> command statement, a <b>nat 0 access-list</b> command statement, or a <b>vpngroup split-tunnel</b> command statement.

<i>remote_mask</i>	Netmask bits (mask) to be applied to <i>remote_addr</i> , if the remote address is a network mask.
<i>icmp_type</i>	[Non-IPSec use only]—Permit or deny access to ICMP message types. Omit this option to mean all ICMP types.  ICMP message types are not supported for use with IPSec when the <b>access-list</b> command is used in conjunction with the <b>crypto map</b> command. The <i>icmp_type</i> is ignored.
<i>icmp_type_obj_grp_id</i>	Name of the port object group containing a group of ICMP message types.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged mode.

**Command History**

Release	Modification
1.1(1)	This command is the same as the PIX 6.0 command with the addition of object grouping support from the PIX 6.2 command and other implementation-related changes as noted in the usage guidelines.

**Usage Guidelines**

The access list behavior on the module differs from that on PIX 6.0 as follows:

- By default all traffic is denied through the module. Explicit access rules need to be configured using the **access-list** command and attached to the appropriate interface using the **access-list** command to allow traffic to pass through that interface.
- The module does not support the **outbound**, **conduit** and **apply** configuration commands that are supported in PIX.
- The access lists used in the module are compiled by the software and loaded into a supervisor engine for subsequent lookup. Each time an access rule is added using any of the following commands a short delay occurs before a new compilation begins to catch any additional configurations: **filter**, **fixup**, **icmp**, **telnet**, **ssh**, **access-list**, **established**, **aaa authentication**, **aaa authorization** and **aaa accounting**

After the compilation begins, it may take some time for the new rule set to be downloaded to the hardware. In the interim, the old access rule set is applied to the incoming traffic. After successfully download the new set is used to determine access permissions.

- During compilation, if the compilation process runs out of resources, an error message is printed on the console when the access lists configured on the module are different from those currently being used in the hardware. To synchronize the configuration, remove the newly added rules that began the compilation and add fewer rules.
- Access rules with port ranges have a negative impact on the total number of access rules that the module can support. You should avoid configuring access rules with large port ranges.

---

**Examples**

This example shows how to define an access list allowing any host to access server 121.23.65.12 using Telnet:

```
FWSM(config)# access-list in_acl permit tcp any host 121.23.65.12 eq 23
```

For further examples, refer to the *Configuration Guide for the Cisco Secure PIX Firewall Version 6*.

For examples on using access-lists with the **object group** command, refer to the *Cisco PIX Firewall and VPN Configuration Guide Version 6.2*.

---

**Related Commands**

**access-list** (PIX 6.0)  
**object-group**

# access-list (ospf)

To configure access rules, use the **access list** (ospf) command. Use the **no** form of this command to remove access rules from the configuration.

```
access-list id deny | permit {any | ip mask}
```

```
[no] access-list id deny | permit {any | ip mask}
```

Syntax Description		
<i>id</i>		Sets the access list identification.
<b>deny</b>		Denies access if the conditions are matched.
<b>permit</b>		Permits access if the conditions are matched.
<b>any</b>		Used as an abbreviation for an IP address of 0.0.0.0 and a mask of 255.255.255.0.
<i>ip mask</i>		Sets the IP address and mask for the network.

**Defaults** This command has no default settings.

**Command Modes** Privileged mode.

Command History	Release	Modification
	1.1(1)	This command was introduced.

**Usage Guidelines** This access list syntax is used only in the context of OSPF. Access lists created with this syntax are then used for defining route maps to be applied to redistributed routes. An access list containing any access elements defined using the command syntax cannot be applied to an interface using the **access-list** command.

**Examples** This example shows how to create an access list:

```
FWSM(config)# access-list ospf1 permit 10.2.0.0 255.255.255.0.0
FWSM(config)# show access-list
access-list ospf1; 1 elements
access-list ospf1 permit 10.2.0.0 255.255.255.0 (hitcnt=0)
```

**Related Commands** [match](#)  
[route-map](#)

# area

To specify an area name in the router configuration submode, use the **area** command.

**area** *area id* **authentication**

**area** *area id* **authentication message-digest**

**area** *area id* **default-cost** *cost*

**area** *area id* **filter-list** *prefix name* [**in** | **out**]

**area** *area id* **nssa** [**no-redistribution**] [**default-information-originate**]

**area** *area id* **range** *prefix mask* [**advertise** | **not-advertise**]

**area** *area id* **stub** [**no-summary**]

**area** *area id* **virtual-link** *router id* [**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [[**authentication-key** *key*]| [**message-digest-key** *key id md5 key*]]

## Syntax Description

<i>area id</i>	Specifies the ID of an area.
<b>authentication</b>	Enables cleartext authentication for this area.
<b>message-digest</b>	Specifies MD5 authentication.
<b>default-cost</b> <i>cost</i>	Assigns a default cost to the default summary route used for the stub area.
<b>filter-list</b> <i>prefix name</i>	Specifies a filter list and assign a filter list name.
<b>in</b>   <b>out</b>	(Optional) Specifies that a list is enabled or disabled.
<b>nssa</b>	Specifies the area is for NSSA.
<b>no-redistribution</b>	(Optional) Specifies there is no area redistribution.
<b>default-information-originate</b>	(Optional) Specifies the default information generated from this area.
<b>range</b> <i>prefix mask</i>	Specifies an address range for which a single summary LSA is generated from this area.
<b>advertise</b>	(Optional) Specifies that an LSA is advertised.
<b>not-advertise</b>	(Optional) Specifies LSA is not advertised.
<b>stub</b>	Defines the area as a stub.
<b>no-summary</b>	(Optional) Specifies that summary (type 3) LSAs are not generated into this area.
<b>virtual-link</b>	Creates a virtual link.
<i>router id</i>	Specifies the router ID for the virtual link.
<b>null</b>	Specifies no authentication.
<b>hello-interval</b> <i>seconds</i>	(Optional) Specifies the time between hello messages.
<b>retransmit-interval</b>	(Optional) Specifies the time between hello message retransmissions.
<b>transmit-delay</b>	(Optional) Specifies the delay between hello message retransmissions.

<b>dead-interval</b>	(Optional) Sets the time to wait for hello messages before declaring a neighbor down.
<b>authentication-key</b>	Assigns a password used by neighbors on a network segment using simple (cleartext) password authentication.
<i>key</i>	Used between the client and server for encrypting data between them, the key must be the same on both the client and server systems. You can use up to 127 alphanumeric characters which are case-sensitive. This key has the same value of a TACACS+ server. Any characters entered past 127 are ignored. You cannot use spaces in the key, but you can use other special characters. If you do not specify a key, encryption does not occur.
<b>message-digest-key</b> <i>keyed md5</i> <i>key</i>	Specifies a key ID and value for an interface using MD5 authentication.

**Defaults**

This command has no default settings.

**Command Modes**

Router configuration submode.

**Command History**

Release	Modification
1.1(1)	This command was introduced.

**Examples**

The following example mandates authentication for areas 0 and 36.0.0.0 of OSPF routing process 201. Authentication keys are also provided.

```
Router(config)# interface ethernet 0
ip address 131.119.251.201 255.255.255.0
ip ospf authentication-key adcdefgh
!
Router(config)# interface ethernet 1
ip address 36.56.0.201 255.255.0.0
ip ospf authentication-key ijklmnop
!
Router(config)# router ospf 201
network 36.0.0.0 0.255.255.255 area 36.0.0.0
network 131.119.0.0 0.0.255.255 area 0
area 36.0.0.0 authentication
area 0 authentication
```

The following example assigns a default cost of 20 to stub network 36.0.0.0:

```
Router(config)# interface ethernet 0
ip address 36.56.0.201 255.255.0.0
!
Router(config)# router ospf 201
network 36.0.0.0 0.255.255.255 area 36.0.0.0
area 36.0.0.0 stub
area 36.0.0.0 default-cost 20
```

The following example filters prefixes that are sent from all other areas to area 1:

```
Router(config)# area 1 filter-list prefix-list AREA_1 in
```

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 36.0.0.0 and for all hosts on network 192.42.110.0:

```
Router(config)# interface ethernet 0
ip address 192.42.110.201 255.255.255.0
!
Router(config)# interface ethernet 1
ip address 192.42.120.201 255.255.255.0
!
Router(config)# router ospf 201
network 192.42.110.0 0.0.0.255 area 0
area 36.0.0.0 range 36.0.0.0 255.0.0.0
area 0 range 192.42.110.0 255.255.0.0
```

The following example establishes a virtual link with default values for all optional parameters:

```
Router(config)# router ospf 201
network 36.0.0.0 0.255.255.255 area 36.0.0.0
area 36.0.0.0 virtual-link 36.3.4.5
```

The following example establishes a virtual link with MD5 authentication:

```
Router(config)# router ospf 201
network 36.0.0.0 0.255.255.255 area 36.0.0.0
area 36.0.0.0 virtual-link 36.3.4.5 message-digest-key 3 md5 sa5721bk47
```

For further examples refer to the *Cisco IOS Configuration Guides* and *Command References*.

# clear console-output

To clear the contents of the message buffer, use the **clear console-output** command.

**clear console-output**

---

**Defaults**

This command has no default settings.

---

**Command Modes**

Privileged mode.

---

**Command History**

Release	Modification
1.1(1)	This command was introduced.

---

**Examples**

This example shows how to clear the message buffer.

```
Router(config)# clear console-output
```

---

**Related Commands**

[show console-output](#)

# clear logging rate-limit

To clear the log rate, use the **clear logging rate-limit** command.

**clear logging rate-limit**

## Defaults

This command has no default settings.

## Command Modes

Privileged mode.

## Command History

Release	Modification
1.1(1)	This command was introduced.

## Examples

This example shows how to clear the logging rate.

```
Router(config)# clear logging rate-limit
```

## Related Commands

[logging rate-limit](#)  
[show logging rate-limit](#)

# default-information originate

To control the redistribution of a default route, use the **default-information originate** command.

**default-information originate** [**always**] [**metric** *value* | **metric-type** {**1** | **2**} | [**route-map** *map*]

Syntax Description		
<b>always</b>	(Optional)	Specifies that a default gateway must be advertised even if it is not present in the routing table.
<b>metric</b> <i>value</i>	(Optional)	Specifies the number of hops to the gateway. You can obtain the hop information by using the <b>traceroute</b> command or by asking your WAN administrator.
<b>metric-type</b>	(Optional)	Specifies the metric type.
<b>1</b>	(Optional)	Specifies metric type 1.
<b>2</b>	(Optional)	Specifies metric type 2.
<b>route-map</b>	(Optional)	Specifies a route map.
<i>map</i>	(Optional)	Route map ID.

## Defaults

This command has no default settings.

## Command Modes

Router configuration submenu.

## Command History

Release	Modification
1.1(1)	This command was introduced.

## Examples

This example shows how to control the redistribution of a default route:

```
Router(config)# default-information originate
```

# distance

To define OSPF administrative distances based on route type, use the **distance** command. To restore the default value, use the **no** form of this command.

**distance** [**intra-area** *dist1*] [**inter-area** *dist2*] [**external** *dist3*]

**no distance**

## Syntax Description

<b>intra-area</b> <i>dist1</i>	(Optional) Sets the distance for all routes within an area.
<b>intra-area</b> <i>dist2</i>	(Optional) Sets the distance for all routes from one area to another area.
<b>external</b> <i>dist3</i>	(Optional) Sets the distance for routes from other routing domains learned by redistribution.

## Defaults

dist1, dist2, and dist3 values are 110.

## Command Modes

Router configuration submode.

## Command History

Release	Modification
1.1(1)	This command was introduced.

## Examples

The following example changes the external distance to 200, making it less reliable:

### Router A Configuration

```
Router(config)# router ospf 1
Router(config)# redistribute ospf 2 subnet
Router(config)# distance external 200
```

### Router B Configuration

```
Router(config)# router ospf 2
Router(config)# redistribute ospf 1 subnet
Router(config)# distance external 200
```

## Related Commands

[area](#)

# firewall module

To attach a group of controlled VLANs to a module, use the **firewall module** command.

```
firewall module module_number vlan-group firewall_group
```

Syntax Description		
	<i>module_number</i>	Specifies the module to attach the VLAN group.
	<b>vlan-group</b>	Specifies a VLAN group
	<i>firewall_group</i>	Names the VLAN group.

**Defaults** This command has no default settings.

**Command Modes** Privileged mode.

Command History	Release	Modification
	1.1(1)	This command was introduced.

**Examples** This example shows how to attach a VLAN group to a module:

```
Router(config)# firewall 6 vlan-group 20
```

**Related Commands** [firewall vlan-group](#)

# firewall vlan-group

To configure a group of controlled VLANs, use the **firewall vlan-group** command.

```
firewall vlan-group firewall_group vlan_range
```

Syntax Description		
	<i>firewall_group</i>	Names the VLAN group.
	<i>vlan_range</i>	Lists the VLANs in the group.

**Defaults** This command has no default settings.

**Command Modes** Privileged mode.

Command History	Release	Modification
	1.1(1)	This command was introduced.

**Examples** This example shows how to configure a group of controlled VLANs:

```
Router(config)# firewall vlan-group 20 8, 10-15
```

**Related Commands** [firewall module](#)

# interface

To enter the interface configuration submode to enter OSPF commands or the **shutdown** command, use the **interface** command.

**interface** *interface-name*

<b>Syntax Description</b>	<i>interface-name</i> Specifies a perimeter interface on the firewall.				
<b>Defaults</b>	This command has no default settings.				
<b>Command Modes</b>	Privileged mode.				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>1.1(1)</td> <td>This command was modified from the PIX version command.</td> </tr> </tbody> </table>	Release	Modification	1.1(1)	This command was modified from the PIX version command.
Release	Modification				
1.1(1)	This command was modified from the PIX version command.				
<b>Examples</b>	<p>This example shows how to enter the interface configuration submode:</p> <pre>Router(config)# <b>interface sweden</b></pre>				
<b>Related Commands</b>	<a href="#">show interface</a>				

# ip prefix-list

To configure a prefix list, use the **ip prefix-list** command.

**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** | **permit** *network/length*} [*ge ge-value*] [**le** *le-value*]

**no ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** | **permit** *network/length*} [*ge ge-value*] [**le** *le-value*]

## Syntax Description

<i>list-name</i>	Specifies the prefix list.
<b>seq</b> <i>seq-value</i>	(Optional) Specifies a sequence name.
<b>deny</b>	(Optional) Denies access if the conditions of the command are not met.
<b>permit</b>	(Optional) Selects a packet to travel through the firewall.
<i>network/length</i>	(Optional) Specifies the network from which the packet originated, or the packets length.
<b>ge</b> <i>ge-value</i>	(Optional) Specifies a generation number.
<b>le</b> <i>le-value</i>	(Optional) Specifies the packets length.

## Defaults

This command has no default settings.

## Command Modes

Privileged mode.

## Command History

Release	Modification
1.1(1)	This command was introduced.

## Examples

This example shows how to deny the default route 0.0.0.0/0:

```
Router(config)# ip prefix-list abc deny 0.0.0.0/0
```

This example shows how to permit the prefix 35.0.0.0/8:

```
Router(config)# ip prefix-list abc permit 35.0.0.0/8
```

For further examples refer to the *Cisco IOS Configuration Guides* and *Command References*.

# logging rate-limit

To rate limit the number of syslogs generated from the module, use the **logging rate-limit** command. To remove access lists from the configuration, use the **no** form of this command.

**logging rate-limit** *num* [*interval*] **message** *syslog\_id*

**no logging rate-limit** *num* [*interval*] **message** *syslog\_id*

**logging rate-limit** *num* [*interval*] **level** *syslog\_level*

**no logging rate-limit** *num* [*interval*] **level** *syslog\_level*

**show logging rate-limit**

**clear logging rate-limit**

## Syntax Description

<i>num</i>	Specifies the syslog limit number.
<i>interval</i>	(Optional) Specifies the time interval in seconds over which the syslogs should be limited to the <i>num</i> instances.
<b>message</b> <i>syslog_id</i>	Specifies the syslog ID of the message being rate limited.
<b>level</b> <i>syslog_level</i>	Sets the syslog level.

## Defaults

This command has no default settings.

## Command Modes

Privileged mode.

## Command History

Release	Modification
1.1(1)	This command was introduced.

## Examples

These examples show how to set up logging rate limits:

- If you want to see only 10 message per second for syslog id 106023, use the following command:

```
logging rate-limit 10 1 message 106023
```

Because the [*interval*] is optional and defaults to 1 second, you can specify:

```
logging rate-limit 10 message 106023
```

- If you want to limit all the syslogs in level 3 to be generated only 5 times per second, use the following command:

```
logging rate-limit 5 level 3
```

- Precedence in setting up logging determines the result of the command action as follows:
  - The **logging rate-limit message** command forms an exception for the **logging rate-limit level** command if the level is defined. For example:

```
logging rate-limit 10 message 106023
logging rate-limit 5 level 1
```

All syslogs other than 106023 in level 1 will be generated at the maximum 5 times per second. 106023 will be generated up to 10 times per second.

- If you set up a configuration in this order:

```
logging rate-limit 10 message 106023
logging rate-limit 5 level 1
no logging rate-limit 10 message 106023
```

The configuration will be equivalent to only the following:

```
logging rate-limit 5 level 1
```

If you set up a configuration in this order:

```
logging rate-limit 10 message 106023
logging rate-limit 5 level 1
no logging rate-limit 5 level 1
```

This configuration is equivalent to the following:

```
logging rate-limit 10 message 106023
```

- To rate limit syslogs from more than 1 level, use the level version of the command multiple times:
 

```
logging rate-limit 5 level 1
logging rate-limit 6 level 3
logging rate-limit 5 2 level 4
```

The last 1 in the configuration limits the rate of all syslogs in level 4 to 5 in 2 second intervals.

# match

To define route matching criteria for a route map, use the **no** form of this command. To disable matching, use the **no** form of this command.

**match** [**interface** | **route-type** | **metric** | **ip address** | **ip next-hop** | **ip route-source**]

[**no**] **match** [**interface** | **route-type** | **metric** | **ip address** | **ip next-hop** | **ip route-source**]

## Syntax Description

<b>interface</b>	(Optional) Specifies an interface.
<b>metric</b>	(Optional) Specifies the number of hops to the gateway. You can obtain the hop information by using the <b>traceroute</b> command or by asking your WAN administrator.
<b>ip address</b>	(Optional) Specifies the IP address to match.
<b>ip next-hop</b>	(Optional) Specifies that the next IP address is matched.
<b>ip route-source</b>	(Optional) Specifies that the match is to the route source IP address.

## Defaults

This command has no default settings.

## Command Modes

Route-map configuration submode.

## Command History

Release	Modification
1.1(1)	The <b>no</b> form of this command was introduced.

## Examples

This example shows how create a route map that can be used to redistribute internal routes:

```
Router(config-route-map)# route-map name
Router(config-route-map)# match route-type internal
```

## Related Commands

**set**  
[route-map](#)

# nameif

To assign a name to an interface, use the **nameif** command. To remove the interface name, use the **no** form of this command.

**nameif** *vlan\_number if\_name security\_level*

**no nameif** *vlan\_number [if\_name] [security\_level]*

## Syntax Description

<i>vlan_number</i>	Specifies a VLAN.
<i>if_name</i>	Specifies the perimeter interface name.
<i>security_level</i>	Indicates the security level for the perimeter interface. Range is from 1 to 99.

## Defaults

This command has no default settings.

## Command Modes

Privileged mode.

## Command History

Release	Modification
1.1(1)	This command was modified from the PIX version command.

## Usage Guidelines

Specifies the perimeter interface VLAN, name, and security level on an interface.

## Examples

This example shows how to assign a name to an interface:

```
Router(config)# nameif vlan 10 inside security 100
```

# network

To define the interfaces on which OSPF runs and to define the area ID for those interfaces, use the **network area router** command. To disable OSPF routing for interfaces defined with the address wildcard-mask pair, use the **no** form of this command.

**network** *ip-address wildcard-mask area area id*

**no network** *ip-address wildcard-mask area area id*

## Syntax Description

<i>ip-address</i>	Specifies the IP address.
<i>wildcard-mask</i>	Specifies the IP address type mask that includes “don’t care” bits.
<b>area</b> <i>area id</i>	(Optional) Specifies an area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address. If you intend to associate areas with IP subnets, you can specify a subnet address as the area ID.

## Defaults

This command has no default settings.

## Command Modes

Router configuration submode.

## Command History

Release	Modification
1.1(1)	This command was introduced.

## Examples

This example shows how to initialize the OSPF routing process 109, and defines four OSPF areas: 10.9.50.0, 2, 3, and 0. Areas 10.9.50.0, 2, and 3 mask specific address ranges, while area 0 enables OSPF for all other networks.

```
Router(config)# interface ethernet 0
Router(config)# ip address 131.108.20.1 255.255.255.0
Router(config)# router ospf 109
Router(config-router)# network 131.108.20.0 0.0.0.255 area 10.9.50.0
Router(config-router)# network 131.108.0.0 0.0.255.255 area 2
Router(config-router)# network 131.109.10.0 0.0.0.255 area 3
Router(config-router)# network 0.0.0.0 255.255.255.255 area 0:
```

# ospf

To configure OSPF use the **ospf** commands.

**ospf authentication-key** *key*

**ospf authentication** [**message-digest** | **null**]

**ospf cost** *cost*

**ospf dead-interval** *seconds*

**ospf hello-interval** *seconds*

**ospf message-digest-key** *keyed md5 key*

**ospf priority** *number*

**ospf retransmit-interval** *seconds*

**ospf transmit-delay** *seconds*

Syntax	Description
<b>authentication-key</b>	Assigns a password used by neighbors on a network segment using simple (cleartext) password authentication.
<i>key</i>	The key is used between the client and server for encrypting data between them, the key must be the same on both the client and server systems. You can use up to 127 alphanumeric characters which are case-sensitive. This key has the same value of a TACACS+ server. Any characters entered past 127 are ignored. You cannot use spaces in the key, but you can use other special characters. If you do not specify a key, encryption does not occur.
<b>authentication</b>	Specifies authentication.
[ <b>message-digest</b>   <b>null</b> ]	(Optional) Specifies the authentication type for an interface as either cleartext, message digest, or no authentication.
<b>cost</b> <i>cost</i>	Specifies the cost of sending a packet on an OSPF interface.
<b>dead-interval</b> <i>seconds</i>	Sets the time to wait for hello messages before declaring a neighbor down.
<b>message-digest-key</b> <i>keyed</i> <b>md5</b> <i>key</i>	Specifies a key ID and value for an interface using MD5 authentication.
<b>priority</b> <i>number</i>	Sets the priority of the OSPF router for DR (designated router) or BDR (backup designated router) election.
<b>ospf hello-interval</b> <i>seconds</i>	Sets a delay value in seconds between hello messages.
<b>retransmit-interval</b> <i>seconds</i>	Specifies a delay between LSA retransmissions.
<b>transmit-delay</b>	Specifies the estimated time taken to transmit an LSA on an OSPF interface.

## Defaults

This command has no default settings.

**Command Modes** Interface configuration submode.

Command History	Release	Modification
	1.1(1)	This command was introduced.

**Examples** The following example sets the interface cost value to 65:

```
Router(config)# ospf cost 65
```

The following example sets the interval between hello packets to 15 seconds:

```
Router(config)# ospf hello-interval 15
```

The following example sets a new key 19 with the password 8ry4222:

```
Router(config)# ospf message-digest-key 19 md5 8ry4222
```

For further examples, refer to the corresponding **ip ospf** commands in *Cisco IOS Configuration Guides* and *Command References*.

**Related Commands** [router ospf](#)

# redistribute

To enable redistribution of static or connected routes or routes from another OSPF process, use the **redistribute** command. To remove redistribution from the configuration, use the **no** form of this command.

```
redistribute {ospf id | static | connect} [{match {internal | external extern-type} metric
metric-value | metric-type metric-type [internal | external] tag tag-value | subnets}]
route-map map value
```

```
[no] redistribute {ospf id | static | connect} [{match {internal | external extern-type} metric
metric-value | metric-type metric-type [internal | external] tag tag-value | subnets}]
route-map map value
```

## Syntax Description

<b><i>ospf id</i></b>	Specifies the OSPF routing process from which routes are to be distributed.
<b>static</b>	Redistributes static routes.
<b>connect</b>	Redistributes connected routes.
<b>match</b>	(Optional) Specifies the criteria by which OSPF routes are redistributed into other routing domains.
<b>internal</b>	(Optional) Specifies routes that are internal to a specific autonomous system.
<b>external 1</b>	Specifies routes that are external to the autonomous system, but are imported into OSPF as Type 1 external route.
<b>external 2</b>	Specifies routes that are external to the autonomous system, but are imported into OSPF as Type 2 external route.
<b>metric</b> <i>metric-value</i>	(Optional) Specifies the metric for the redistributed route. If a value is not specified for this option, and no value is specified using the <b>default-metric</b> command, the default metric value is 0. In the case of OSPF, the default metric is 20. Use a value consistent with the destination protocol.
<b>metric-type</b> <i>metric-type</i>	(Optional) Specifies the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values: <ul style="list-style-type: none"> <li>Type 1 external route</li> <li>Type 2 external route</li> </ul>
<b>tag</b> <i>tag-value</i>	(Optional) Specifies the 32-bit decimal value attached to each external route. This value is not used by OSPF itself. It may be used to communicate information between Autonomous System Boundary Routers (ASBRs). If none is specified, then the remote autonomous system number is used for routes from Border Gateway Protocol (BGP) and Exterior Gateway Protocol (EGP); for other protocols, zero (0) is used.

<b>subnets</b>	(Optional) Specifies the redistribution of routes into OSPF, the scope of redistribution for the specified protocol.
<b>route-map</b> <i>map value</i>	(Optional) Specifies a route map that should be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol. If not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported.

**Defaults**

Metric value is 0 or 20 depending upon the destination protocol.

**Command Modes**

Privileged mode.

**Command History**

Release	Modification
1.1(1)	The <b>no</b> form of this command was introduced.

**Examples**

This example shows how to specify a network 172.16.0.0 that will appear as an external link-state advertisement (LSA) in OSPF 1 with a cost of 100 (the cost is preserved):

```
Router(config)# ip address inside 172.16.0.1 255.0.0.0
Router(config)# interface inside
Router(config)# ospf cost 100

Router(config)# ip address outside 10.0.0.1 255.0.0.0
Router(config)# interface outside
Router(config)# ip address 10.0.0.1 255.0.0.0

Router(config)# router ospf 1
Router(config-router)# network 10.0.0.0 0.255.255.255 area 0
Router(config)# redistribute ospf 2 subnet
Router(config)# router ospf 2
Router(config-router)# network 172.16.0.0 0.255.255.255 area 0
```

# route

To define a static or default route for an interface, use the **route** command.

```
route if_name ip_address netmask gateway_ip [metric]
```

```
[no] route [if_name ip_address [mask gateway]]
```

Syntax Description	
<i>if_name</i>	Specifies the perimeter interface name.
<i>ip_address</i>	Specifies the network IP address. Use 0.0.0.0 to specify a default route. The 0.0.0.0 IP address can be abbreviated as 0.
<i>netmask</i>	Specifies a network mask to apply to the <i>ip_address</i> . Use 0.0.0.0 to specify a default route. The 0.0.0.0 netmask can be abbreviated as 0.
<i>gateway_ip</i>	Specifies the IP address of the gateway router (the next hop address for this route).
<b>metric</b>	(Optional) Specifies the number of hops to the <i>gateway_ip</i> . If you are not sure, enter 1. Your network administrator can supply this information or you can use a <b>tracert</b> command to obtain the number of hops.

**Defaults**  
 Netmask value is 255.255.255.0.  
 Metric value is 1.

**Command Modes**  
 Privileged mode.

Command History	Release	Modification
	1.1(1)	This command was modified from the PIX version command.

**Examples**  
 This example shows how to configure a route on the interface “inside” for the network 10.2.2.0/24 with next hop 10.2.1.5:

```
FWSM(config)# route inside 10.2.2.0 255.255.255.0 10.2.1.5
FWSM(config)# show route
S    0.0.0.0 0.0.0.0 [0/0] via 10.6.13.1, dmz
C    10.2.1.0 255.255.255.0 is directly connected, inside
S    10.2.2.0 255.255.255.0 [1/0] via 10.2.1.5, inside
C    10.3.1.0 255.255.255.0 is directly connected, outside
C    10.6.13.0 255.255.255.0 is directly connected, dmz
C    127.0.0.0 255.255.255.0 is directly connected, eobc
```

**Related Commands**    [show route](#)

# router ospf

To create or configure an OSPF routing process, use the **router ospf** command. To remove the routing process from the configuration, use the **no** form of this command.

**router ospf** *autonomous-system id*

**no router ospf** *autonomous-system id*

Syntax Description	<i>autonomous-system id</i>	Specifies the autonomous system configured for routing.
--------------------	-----------------------------	---

Defaults	This command has no default settings.
----------	---------------------------------------

Command Modes	Privileged mode.
---------------	------------------

Command History	Release	Modification
	1.1(1)	This command was introduced.

Examples	This example shows how to create and OSPF routing process:
----------	--

```
Router(config)# router ospf 12345
```

Related Commands	<a href="#">ospf network</a>
------------------	------------------------------

# route-map

To create a route map, use the **route-map** command. To remove a route map from the configuration, use the **no** form of this command.

```
route-map map-tag [permit | deny] [seq-num]
```

```
[no] route-map map-tag [permit | deny] [seq-num]
```

## Syntax Description

<i>map-tag</i>	Defines a meaningful name for the route map. The <b>redistribute router configuration</b> command uses this name to reference this route map. Multiple route maps may share the same map tag name.
<b>permit</b>	(Optional) Specifies the match criteria are met for this route map. When this keyword is specified, the route is redistributed as controlled by the set actions. In the case of policy routing, the packet is policy routed. If the match criteria are not met, and this keyword is specified, the next route map with the same map tag is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set.
<b>deny</b>	(Optional) Specifies the match criteria are met for the route map. When the deny keyword is specified, the route is not redistributed. In the case of policy routing, the packet is not policy routed, and no further route maps sharing the same map tag name will be examined. If the packet is not policy routed, the normal forwarding algorithm is used.
<i>seq-num</i>	(Optional) The number that indicates the position a new route map occupies in the list of route maps already configured with the same name. If the <b>no</b> form of this command is used, the position of the route map should be deleted.

## Defaults

Permit is the default.

## Command Modes

Privileged mode.

## Command History

Release	Modification
1.1(1)	The <b>no</b> form of this command was introduced.

## Examples

This example shows how to create a route map:

```
FWSM# route-map disco permit
FWSM# show route-map
route-map disco permit 10
```

**Related Commands** [match](#)  
[set](#)

# set metric

To define the actions taken on routes that match the criteria defined for a route map, use the **set metric** command. To disable metric criteria, use the **no** form of this command.

**set metric** [+ | -] *metric-value*

[no] **set metric** [+ | -] *metric-value*

Syntax Description	
+   -	(Optional) Specifies a positive or negative metric.
<i>metric-value</i>	Specifies a metric value.

**Defaults** This command has no default settings.

**Command Modes** Route-map configuration submenu.

Command History	Release	Modification
	1.1(1)	This command was introduced.

**Examples** This example shows how to set the metric value for the routing protocol to 100:

```
Router(config-route-map)# route-map set-metric
Router(config)# set metric 100
```



**Note**

We recommend that you consult your Cisco technical support representative before changing the default value. For further information, refer to the *Cisco IOS Configuration Guide* and *Command Reference*.

**Related Commands** [set metric-type](#)

# set metric-type

To specify a metric type for a route map, use the **set metric-type** command.

```
set metric-type type-1 | type-2
```

```
[no] set metric-type type-1 | type-2
```

Syntax Description	type-1	type-2
	Specifies the open Shortest Path First (OSPF) external Type 1 metric.	Specifies the OSPF external Type 2 metric

**Defaults** This command has no default settings.

**Command Modes** Route-map configuration submode.

Command History	Release	Modification
	1.1(1)	This command was introduced.

**Examples** This example shows how to set the metric type of the destination protocol to OSPF external Type 1:

```
Router(config-route-map)# route-map map-type
Router(config-route-map)# set metric-type type-1:
```

**Related Commands** [set metric](#)

# show console-output

To view the contents of the message buffer, use the **show console-output** command.

**show console-output** [*start\_message\_number*-*end\_message\_number*]

Syntax Description		
	<i>start_message_number</i>	Specifies the starting serial number of the message to be displayed.
	<i>end_message_number</i>	Specifies the end serial number of the message to be displayed.

**Defaults** This command has no default settings.

**Command Modes** Privileged mode.

Command History	Release	Modification
	1.1(1)	This command was introduced.

**Usage Guidelines** Messages appearing on the console are redirected to all active Telnet sessions. When no Telnet session is available, the output is saved to a buffer. The buffer output can be subsequently examined when you Telnet to the module application software partition. Individual messages are numbered.

**Examples** This example shows how to display the buffer output:

```
FWSM# show console-output
Message #1 :Initializing debugger.....:
Message #2 :Found PCI card in slot:1 bus:2 dev:9 (vendor:0x8086 deviceid:0x1001)
Message #3 :Found PCI card in slot:2 bus:2 dev:8 (vendor:0x8086 deviceid:0x1001)
Message #4 :Found PCI card in slot:3 bus:1 dev:6 (vendor:0x1014 deviceid:0x1e8)
Message #5 :Ignoring PCI card in slot:3 (vendor:0x1014 deviceid:0x1e8)
Message #6 :Found PCI card in slot:4 bus:1 dev:5 (vendor:0x1014 deviceid:0x1e8)
Message #7 :Ignoring PCI card in slot:4 (vendor:0x1014 deviceid:0x1e8)
Message #8 :Found PCI card in slot:5 bus:1 dev:4 (vendor:0x1014 deviceid:0x1e8)
Message #9 :Ignoring PCI card in slot:5 (vendor:0x1014 deviceid:0x1e8)
Message #10 :Found PCI card in slot:7 bus:0 dev:2 (vendor:0x1011 deviceid:0x22)
```

**Related Commands** [clear console-output](#)

# show crashdump

To display the contents of the crashdump partition, use the **show crashdump** command.

**show crashdump**

---

**Defaults**

This command has no default settings.

---

**Command Modes**

Privileged mode.

---

**Command History**

Release	Modification
1.1(1)	This command was modified from the PIX version command.

---

**Examples**

This example shows how to display the contents of the crashdump partition:

```
Router(config)# show crashdump
```

# show firewall module

To display the module configuration, use the **show firewall module** command.

**show firewall module**

---

**Defaults**

This command has no default settings.

---

**Command Modes**

Privileged mode.

---

**Command History**

<b>Release</b>	<b>Modification</b>
1.1(1)	This command was introduced.

---

**Examples**

This example shows how to display the module configuration:

```
Router(config)# show firewall module
```

# show firewall vlan-group

To display the configured firewall VLAN groups, use the **show firewall** command.

**show firewall vlan-group**

---

**Defaults**

This command has no default settings.

---

**Command Modes**

Privileged mode.

---

**Command History**

Release	Modification
1.1(1)	This command was introduced.

---

**Examples**

This example shows how to display the configured firewall VLAN groups:

```
Router(config)# show firewall 20
```

# show interface

To show all of the VLANs configured, use the **show interface** command.

**show interface** [*interface name*] **stats**

Syntax Description		
	<i>interface_name</i>	Specifies the perimeter interface name.
	<b>stats</b>	Displays the interface state and counters.

**Defaults** This command has no default settings.

**Command Modes** Privileged mode.

Command History	Release	Modification
	1.1(1)	This command was modified from the PIX version command.

**Usage Guidelines** If VLANs are not configured on the MSFC, you will not be able to define any new VLAN interfaces on the Firewall Services Module.

**Examples** This example shows how to display the firewall VLANs configured on all interfaces:

```
Router(config)# show interface domino
```

**Related Commands** [interface](#)

# show ip ospf

To show the OSPF configuration, use the **show ip ospf** command.

**show ip ospf border-routers**

**show ip ospf database [router][network][external]**

**show ip ospf interface**

**show ip ospf neighbor**

**show ip ospf request-list**

**show ip ospf retransmission-list**

**show ip ospf summary-address**

**show ip ospf virtual-link**

Syntax	Description
<b>border-routers</b>	Displays the internal OSPF routing table entries to an area border router and autonomous system boundary router.
<b>database</b> <b>[router][network][external]</b>	Displays lists of information related to the OSPF database, for a specific router, for network LSAs or external LSAs.
<b>interface</b>	Displays the information on the interfaces for which OSPF is enabled.
<b>neighbor</b>	Displays the OSPF-neighbor information on a per-interface basis.
<b>request-list</b>	Displays a list of all LSAs requested by a router.
<b>retransmission-list</b>	Displays a list of all LSAs waiting to be resent.
<b>summary-address</b>	Displays a list of all summary address redistribution information configured under an OSPF process.
<b>virtual-link</b>	Displays parameters and the current state of OSPF virtual links.

## Defaults

This command has no default settings.

## Command Modes

Privileged mode.

## Command History

Release	Modification
1.1(1)	This command was introduced.

---

**Examples**

This example shows how to show the IP OSPF configuration:

```
Router(config)# show ip ospf border routers
Routing Process "ospf 201" with ID 192.42.110.200 Supports only single TOS(TOS0) route It
is an area border and autonomous system boundary router Redistributing External Routes
from, igrp 200 with metric mapped to 2, includes subnets in redistribution
ip with metric mapped to 2
igrp 2 with metric mapped to 100
igrp 32 with metric mapped to 1
Number of areas in this router is 3
Area 192.42.110.0
Number of interfaces in this area is 1
Area has simple password authentication
SPF algorithm executed 6 times
```

For further examples, refer to the *Cisco IOS Configuration Guides* and *Command References*.

---

**Related Commands**

[ospf](#)

# show logging rate-limit

To display the logging rate, use the **show logging rate-limit** command.

**show logging rate-limit**

---

**Defaults**

This command has no default settings

---

**Command Modes**

Privileged mode.

---

**Command History**

Release	Modification
1.1(1)	This command was introduced.

---

**Examples**

This example shows how to display the logging rate:

```
Router(config)# show logging rate limit
```

---

**Related Commands**

[clear logging rate-limit](#)  
[logging rate-limit](#)

# show vlan

To display the list of VLANs assigned to the module through the configuration on the supervisor route process MSFC, use the **show vlan** command.

**show vlan**

---

## Defaults

This command has no default settings

---

## Command Modes

Privileged mode.

---

## Command History

Release	Modification
1.1(1)	This command was modified from the PIX version command.

---

## Examples

This example shows how to display the VLANs assigned to the module:

```
Router(config)# show vlan
10, 33, 100,
```

# summary-address

To create aggregate addresses for external routes, use the **summary-address** command. To disable aggregate addressing for external routes, use the **no** form of this command.

```
summary-address addr mask [not-advertise] [tag tag]
```

```
[no] summary-address addr mask [not-advertise] [tag tag]
```

Syntax Description	
<i>addr</i>	The summary address designated for a range of addresses.
<i>mask</i>	The IP subnet mask used for the summary route.
<b>not-advertise</b>	(Optional) Suppresses routes that match the specified address/mask pair.
<b>tag</b> <i>tag</i>	(Optional) Specifies a tag value that can be used as a match value for controlling redistribution through route maps.

**Defaults** This command has no default settings.

**Command Modes** Router configuration submode.

Command History	Release	Modification
	1.1(1)	This command was introduced.

**Examples** This example shows the summary address 10.1.0.0 includes address 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. Only the address 10.1.0.0 is advertised in an external link-state advertisement.

```
Router(config)# summary-address 10.1.0.0 255.255.0.0
```

## timers lsa-group-pacing

To change the interval at which OSPF link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers lsa-group-pacing** configuration command. To restore the default value, use the **no** form of this command.

**timers lsa-group-pacing** *seconds*

**no timers lsa-group-pacing**

<b>Syntax Description</b>	<i>seconds</i>	Specifies the number of seconds in the interval at which LSAs are grouped and refreshed, checksummed, or aged. The range is from 10 to 1800 seconds.
---------------------------	----------------	--

<b>Defaults</b>	240 seconds
-----------------	-------------

<b>Command Modes</b>	Router configuration submode.
----------------------	-------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	1.1(1)	This command was introduced.

### Usage Guidelines

**Examples** This example shows how to change the OSPF pacing between LSA groups to 60 seconds:

```
Router(config)# router ospf 1
Router(config-router)# timers lsa-group-pacing 60
```

## timers spf

To configure the delay time between when OSPF receives a topology change and when it starts a shortest path first (SPF) calculation, use the **timers spf** command. To configure the hold time between two consecutive SPF calculations, use the **timers spf router** configuration command. To return to the default timer values, use the **no** form of this command.

**timers spf** *spf-delay* *spf-holdtime*

**no timers spf** *spf-delay* *spf-holdtime*

Syntax Description		
	<i>spf-delay</i>	Specifies the delay time (in seconds) between when OSPF receives a topology change and when it starts an SPF calculation. It can be an integer from 0 to 65535. A value of 0 means that there is no delay; that is, the SPF calculation is started immediately.
	<i>spf-holdtime</i>	Specifies the minimum time (in seconds) between two consecutive SPF calculations. It can be an integer from 0 to 65535 seconds. A value of 0 means that there is no delay; that is, two SPF calculations can be done, one immediately after the other.

### Defaults

Delay time is 5 seconds.

Minimum time is 10 seconds.

### Command Modes

Router configuration submode.

### Command History

Release	Modification
1.1(1)	This command was introduced.

### Examples

This example shows how to change the delay to 10 seconds and the hold time to 20 seconds:

```
Router(config)# timers spf 10 20
```

# upgrade-mp

To upgrade the maintenance software image, use the **upgrade-mp** command.

```
upgrade-mp tftp:[[//location] [/tftp_pathname]]
```

Syntax Description		
<b>tftp</b>		Specifies a download of the maintenance software image through TFTP and install the image to the maintenance partition.
<i>//location</i>		Specifies the location of the TFTP server.
<i>/tftp_pathname</i>		This TFTP server must be reachable from the module when the module image is booted up. The pathname can include any directory names in addition to the actual last component of the path to the file on the server.

## Usage Guidelines

The **upgrade-mp** command lets you download a maintenance software image through TFTP. The image is downloaded, installed to the compact Flash and available on the next module reload (reboot).

If the command is used without the location or pathname optional parameters, then the location and filename are obtained from the user interactively through a series of questions similar to those presented by Cisco IOS software. If you only enter a colon (:), parameters are taken from the **tftp-server** command settings. If other optional parameters are supplied, then these values would be used in place of the corresponding **tftp-server** command setting. Supplying any of the optional parameters, such as a colon and anything after it, causes the command to run without prompting for user input.

The location is an IP address that the firewall can reach. The pathname can include any directory names besides the actual last component of the path to the file on the server. The pathname cannot contain spaces. If a directory name has spaces, set the directory in the TFTP server instead of in the **upgrade-mp** command.

If your TFTP server has been configured to point to a directory on the system from which you are downloading the image, you need only use the IP address of the system and the image filename.

For example, the command causes the TFTP server to receive the command and determine the actual file location from its root directory information:

```
Router(config)# upgrade-mp tftp://10.1.1.5/mp.1-1-0-3.bin.gz
```

The server then downloads the TFTP image to the module.

## Examples

This example causes the module to prompt you for the filename and location before you start the TFTP download:

```
Router(config)# upgrade-mp
Address or name of remote host [127.0.0.1]? 10.1.1.5
Source file name [cdisk]? mp.1-1-0-3.bin.gz
copying tftp://10.1.1.5/mp.1-1-0-3.bin.gz to flash
[yes|no|again]? yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Received 1695744 bytes.
Maintenance partition upgraded.
```

To set the filename and location specified in the **tftp-server** command, save memory, and then download the image to Flash memory, use these commands:

```
Router(config)# tftp-server outside 10.1.1.5 mp.1-1-0-3.bin.gz
Warning: 'outside' interface has a low security level (0).
write memory
Building configuration...
Cryptochecksum: 017c452b d54be501 8620ba48 490f7e99
[OK]
Router(config)# upgrade-mp tftp:
copying tftp://10.1.1.5/mp.1-1-0-3.bin.gz to flash
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

To override the information in the **tftp-server** command and specify alternate information about the filename and location, use this command:

```
Router(config)# upgrade-mp tftp://10.0.0.1/mp.1-1-0-3.bin.gz
```

To specify all information, if you have not set the **tftp-server** command, use this command:

```
Router(config)# upgrade-mp tftp://10.0.0.1/mp.1-1-0-3.bin.gz
```

