MNLB Feature Set for LD: Command Reference

This section documents the commands used to configure the MNLB Services Manager, Forwarding Agent, and Workload Agent. The commands are listed alphabetically. Parentheses indicate the component for which the command is used.

- **bind** (SM)
- **casa service-manager multicast-ttl** (SM)
- **casa service-manager port** (SM)
- **forwarding-agent** (FA)
- **forwarding-agent pool**
- **ip casa** (FA)
- **real** (SM)
- **redirection** (SM)
- **route** (SM)
- **show ip casa affinities** (FA)
- **show ip casa oper** (FA)
- **show ip casa stats** (FA)
- **show ip casa wildcard** (FA)
- **virtual** (SM)

bind

To associate a virtual server with one or more real servers, use the **bind** command. Use **no bind** to release an association between a real server and virtual server.

bind *virtual_id real_id* [*real_id...*]
[**no**] **bind** *virtual_id real_id* [*real_id...*]

Syntax Description

virtual_id	Virtual server IP address or name, port number, bind-id, and protocol.
real_id	(Optional) The IP address or name, port (if a port-bound server), bind-id, and protocol of a real server.

Command Modes

Configuration and Replication modes.

Usage Guidelines

Use the **virtual** and **real** commands to define the virtual server and real server addresses before using the **bind** command. Use the **bind** command to direct network traffic from a virtual server to a real server. If binding a real server to more than one virtual server, each real server must use a unique bind-id.

Example

```
LocalDirector(config)# bind 172.31.17.1 80 192.168.1.1 192.168.1.2
LocalDirector(config)# bind 172.31.17.1 192.168.1.3 192.168.1.4
LocalDirector(config)# show bind
               Virtual                    Real
    172.31.17.1      80 (IS)
                              192.168.1.2 (IS)
                              192.168.1.1 (IS)
    172.31.17.1 default (IS)
                              192.168.1.4 (IS)
                              192.168.1.3 (IS)
LocalDirector(config)# no bind 172.31.17.1 192.168.1.3
LocalDirector(config)# show bind
               Virtual                    Real
    172.31.17.1      80 (IS)
                              192.168.1.2 (IS)
                              192.168.1.1 (IS)
    172.31.17.1 default (IS)
                              192.168.1.4 (IS)
```

The following is an example of the binding for a UDP virtual and real server:

```
Localdirector(config)# bind 192.10.10.101:300:0:udp 192.10.10.1:200:0:udp
Localdirector(config)#
Localdirector(config)# show bind
       Virtual Machine(s)       Real Machines
  192.10.10.101:300:0:udp(OOS)
                              192.10.10.1:200:0:udp(OOS)
```

Related Command

show bind

casa service-manager multicast-ttl

Use the **casa service-manager multicast-ttl** command to change the multicast time-to-live value. Use the **no casa service-manager multicast-ttl** command to disable the multicast time-to-live value.

casa service-manager multicast-ttl *value*
[**no**] **casa service-manager multicast-ttl** *value*

Syntax Description

multicast-ttl — The time-to-live interval for IP multicast packet communication between Service Manager and Forwarding Agent components.

Note: If you are running CASA, you must configure **ip pim dense**. Some Forwarding Agents might be many hops away, so TTL=1 might not work in some cases.

value — The time-to-live value. The default is 3 hops.

Default

The default time-to-live value is 3 hops.

Command Modes

Configuration and Replication modes.

Related Command

casa service-manager port

casa service-manager port

Use the **casa service-manager port** command to change the Service Manager mulitcast port. Use the **no casa service-manager port** command to disable the Service Manager mulitcast port.

casa service-manager port *port* [**password** *password* [*password_timeout*]]
[**no**] **casa service-manager port** *port* [**password** *password* [*password_timeout*]]

Syntax Description

port	The address of the Service Manager port. By default, 1638 is used.
password	(Optional) Specifies the password option.
password	(Optional) The password to enable MD5 encryption for Service Manager communications.
password_timeout	(Optional) The timeout value for the MD5 encryption password, in seconds. A maximum of 65,535 seconds can be specified.

Default

By default, the Service Manager port is 1638.

Command Modes

Configuration and Replication modes.

Usage Guidelines

Use the **casa service-manager port** command to change the UDP port for the Service Manager used for multicast communication between the components. An optional password and password timeout can be used, which is disabled by default.

The *password* is the password to be used in MD5 encryption of packets between the Service Manager and Forwarding Agents. A *password_timeout* value is assigned for two reasons:

- The *password_timeout* provides a time interval during which non-secured messages are accepted. When you assign a new password, the security feature is enabled. The *password_timeout* is the grace period during which you can apply this password to all components. After this time interval expires, all non-secure messages are discarded.
- When you remove, delete, or change a password, the *password_timeout* determines how long the old password is accepted, as well as how long to wait before using the new password when sourcing messages. Again, this gives you a grace period to change the password on all components.

Related Command

casa service-manager multicast-ttl

forwarding-agent

Use the **forwarding-agent** CASA-port configuration command to specify the port on which the Forwarding Agent will listen for wildcard and fixed affinities. Use the **no** form of the command to disable listening on that port.

forwarding-agent *num* [*password* [*password_timeout*]]
no forwarding-agent *num*

Syntax Description

num — Port number on which the Forwarding Agent will listen for wildcards and fixed affinities multicast from the Services Manager. This is also the port used for directed messages to the control address. This number must match the port number defined on the MNLB Services Manager.

password — (Optional) Text password used for generating the MD5 digest.

password_timeout — (Optional) Duration in seconds during which the Forwarding Agent will accept the new and old password. Valid range is between 0 and 3600 seconds. The default is 180 seconds.

Default

The default password timeout is 180 seconds.

The default port for the MNLB Services Manager is 1637.

Command Mode

CASA-port configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(5)T.

The *password* is the password to be used in MD5 encryption of packets between the Service Manager and Forwarding Agents. A *password_timeout* value is assigned for two reasons:

- The *password_timeout* provides a time interval during which non-secured messages are accepted. When you assign a new password, the security feature is enabled. The *password_timeout* is the grace period during which you can apply this password to all components. After this time interval expires, all non-secure messages are discarded.
- When you remove, delete, or change a password, the *password_timeout* determines how long the old password is accepted, as well as how long to wait before using the new password when sourcing messages. Again, this gives you a grace period to change the password on all components.

Example

The following example specifies that the Forwarding Agent will listen for wildcard and fixed affinities on port 1637:

```
forwarding-agent 1637
```

Related Commands

show ip casa oper

forwarding-agent pool

To to adjust the memory allocated for the forwarding agent's affinity pools, use the **forwarding-agent pool** CASA-port configuration command. Use the **no** form of the command to restore the default memory allocation.

forwarding-agent pool *initial_affinity_pool max_affinity_pool*

[**no**] **forwarding-agent pool**

Syntax Description

initial_affinity_pool	Initial number of memory blocks allocated for use as affinities. The default is 5000.
max_affinity_pool	Maximum number of memory blocks that can be allocated for use as affinities. The default is no maximum.

Defaults

The default initial affinity pool size is 5000 memory blocks. There is no maximum.

Command Modes

CASA-port configuration

Command History

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

Examples

The following example specifies a configuration of 100,000 initial affinity memory block that can increase to a maximum of 1,000,000 entries:

```
forwarding-agent pool 100000 1000000
```

Related Commands

Command	Description
show ip casa oper	Displays operational information about the forwarding agent.

ip casa

Use the **ip casa** global configuration command to configure the router to function as a Forwarding Agent. Use the **no** form of the command to remove the Forwarding Agent.

ip casa *control-address igmp-address*
no ip casa

Syntax Description

control-address	IP address of the Forwarding Agent side of the Services Manager/Forwarding Agent tunnel used for sending signals. This address is unique for each Forwarding Agent.
igmp-address	IGMP address on which the Forwarding Agent will listen for wildcard and fixed affinities.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(5)T.

Example

The following example specifies the IP address (10.10.4.1) and IGMP address (224.0.1.2) for the Forwarding Agent:

```
ip casa 10.10.4.1 224.0.1.2
```

Related Commands

port
show ip casa oper

real

Use the **real** command to define a real server. Use the **no** form of the command to remove a real server definition.

real *real_name* | *real_ip*[**:**[*port*]**:**[*bind-id*]**:**[*protocol*]] [*service-state*]
[**no**] **real** *real_name* | *real_ip*[**:**[*port*]**:**[*bind-id*]**:**[*protocol*]] [*service-state*]

Syntax Description

real_name Name of a real server.

real_ip IP address of a real server.

port (Optional) Port to use for traffic to run on the real server. Use a colon as a delimiter between the IP address and port number. If you do not identify a specific port, all traffic is allowed to the server and the port is labeled “default.” Zero is the same as default. Servers with a port specified are referred to as “port-bound” servers.

bind-id (Optional) Used with the **assign** command to direct traffic to a specific location. Use a colon as a delimiter between the bind-id and port number. If you do not specify a bind-id when defining a real server, the default is 0. Any client IP address *not* identified by an **assign** command statement is directed to the default bind-id of 0.

protocol (Optional) Protocol to use. The default value is **tcp**, but **udp** and **gre** are available options. Use a colon as a delimiter between the port number and protocol.

service-state (Optional) In-service (**is**) or out-of-service (**oos**). The default is **oos**.

Command Modes

Configuration and Replication modes.

Usage Guidelines

Real servers are actual host machines with unique IP addresses that provide IP services to the network. Real servers can still be accessed using their actual IP address.

Use the **show real** command to check the service state of real servers. Possible service states are:

- In-service (IS)

  The server is online and accepting connections.

- Out-of-service (OOS)

The **out-of-service** command is used to take the server out of service, and connections are not sent to it via the virtual server. Connections addressed to the server’s actual IP address are bridged by LocalDirector.

- Failed

  The server has not responded to the number of connections set by the **threshold** command or has responded with the same number of TCP RSTs.

- Testing

  After the time set by the **retry** command has passed, LocalDirector puts a failed real server into testing mode where it gets one live connection from a virtual server. If the real server does not respond or responds with TCP RST, then it goes back to a failed state and a SYSLOG message is generated. If the server responds to the connection, then its state is changed to in-service. Note that LocalDirector does not generate any traffic to test the real server. Instead, a live connection is sent to the server in testing state. If the real server fails and there is no traffic to the virtual server that it is bound to, it stays in testing mode.

Example

Although a space can be used as a delimiter for port-bound servers, a colon is preferred. Note that the port is 0 by default, and the **is** (in-service) command is used to put the port 80 server in-service when it is defined:

```
ld(config) 1# real 192.168.1.1
ld(config) 2# real 192.168.1.1:80:tcp is
ld(config) 3# real 192.168.1.1 23
ld(config) 4# show real
Real Machines:
                                               No Answer    TCP Reset    DataIn
Machine             Connect   State  Thresh    Reassigns    Reassigns    Conns
192.168.1.1:23         0       OOS     8          0            0          0
192.168.1.1:80:tcp     0       IS      8          0            0          0
192.168.1.1:0          0       OOS     8          0            0          0
```

The **show real** command provides the following information:

Table 4-1 show real Command Field Descriptions

Field	Description
Machine	IP address, port (if a port-bound server), bind_id, and protocol, or name of the server.
Connect	The current number of connections to the server. This does not include direct connections to the server that are bridged by LocalDirector.
State	IS (in-service), OOS (out-of-service), failed, or testing.
Thresh	Threshold value for reassignments before server is marked as failed.
No Answer Reassigns	Number of connections that are not answered by a real server.
TCP Reset Reassigns	Number of connections that are reassigned because a real server responded with a RST on a new connection.
DataIn Conns	Number of clients requesting but not receiving data.

Related Command

show real

redirection

Use the **redirection** command to set the type of load balancing redirection for the virtual server.

redirection *virtual_id* {**directed** | **dispatched**} [**local** | **casa**] [**igmp** *igmp_address*] [**port** *port*] [**wildcard-ttl** *seconds*] [**fixed-ttl** *seconds*]

Syntax Description

virtual_id The IP address or name, port (if a port-bound server), bind-id, and protocol of a virtual server.

directed Uses NAT to pass packets to the real server. (NAT replaces the virtual IP address with IP address of the real server.)

dispatched The IP address of the virtual server is aliased on each real server, making address translation unnecessary. (LocalDirector replaces the MAC address on a packet with that of the real server. Packets are then passed on to a real server, retaining the IP address.)

local (Optional) Use LocalDirector style of architecture; that is, the style used since version 1.0

casa (Optional) Use the ContentFlow environment.This keyword is not functional unless LocalDirector is part of the ContentFlow environment.

igmp (Optional) Multicast group for Service Manager and Forwarding Agent components. This keyword is not functional unless LocalDirector is part of the ContentFlow environment.

igmp_address (Optional) Multicast group address. The default address is 224.0.1.2.

port (Optional) Configure the port for ContentFlow communications. This keyword is not functional unless LocalDirector is part of the ContentFlow environment.

port (Optional) The address of the Forwarding Agent port. By default, 1638 is used.

wildcard-ttl (Optional) The wildcard-ttl connection objects. This keyword is not functional unless LocalDirector is part of the ContentFlow environment.

fixed-ttl (Optional) The fixed-ttl connection objects (connections). This keyword is not functional unless LocalDirector is part of the ContentFlow environment.

seconds (Optional) The number of seconds.

Default

By default, directed mode with local architecture is used.

Command Modes

Configuration and Replication modes.

Usage Guidelines

The **redirection** command allows you to change the way packets pass through LocalDirector.

Directed mode uses Network Address Translation (NAT) to translate the IP headers in packets. NAT, supported in LocalDirector since version 1.0, provides quick setup with no network address changes, reducing system administration time.

Using NAT may not always be the best solution. Since some protocols embed the IP address within the payload, this can be a problem when a packet is encrypted. Additionally, searching though an entire payload for an IP address is processor-intensive and time-consuming. In these cases, performance can be increased using Dispatched mode.

Dispatched mode increases traffic throughput, but requires assigning an aliased IP address on a real server that matches the virtual IP address on LocalDirector. Dispatched mode should be used for UDP and TCP when the IP address information needs to remain unchanged.

The following **casa** options are not functional unless LocalDirector is part of the ContentFlow environment:

- Use the **casa igmp** keyword to set the multicast group address for the components on the LocalDirector. Messages between the Service Manager and Forwarding Agent are sent using multicast to the members of this group. By default, the igmp group address is 224.0.1.2.
- Use the **casa wildcard-ttl** keyword to set the time-to-live value for the wildcard-affinity connection objects on the Forwarding Agents. The Service Manager is responsible for ensuring the wildcard-affinities are refreshed before they time out. The default value is 1 minute.
- Use the **casa fixed-ttl** keyword to set the time-to-live value for the fixed-affinity connection objects. The fixed-affinity connection objects default time-to-live value is 1 minute.

Related Command

show redirection

route

Use the **route** command to add a static route to the IP routing table. Use the **no route** command to clear the route

route *dest_net net_mask gateway* [*metric*]
[**no**] **route** *dest_net net_mask gateway* [*metric*]

Syntax Description

dest_net	Destination IP network address; if default route, specify as all zeros (0.0.0.0).
net_mask	Subnet mask for the network; if default route, specify as all zeros (0.0.0.0).
gateway	The adjacent gateway to reach the destination IP network.
metric	(Optional) Distance metric (defaults to one).

Command Modes

Configuration and Replication modes.

Usage Guidelines

If you want to change an existing route, you must first use the **no route** command to clear the route, and then specify the new route with the **route** command. Defining a new IP route with the **route** command does not overwrite a route that is already established.

Example

```
LocalDirector(config)# route 0.0.0.0 0.0.0.0 192.168.1.1 1
LocalDirector(config)#
```

Related Commands

clear route
show route

show ip casa affinities

Use the **ip casa affinities** EXEC command to display statistics about affinities.

> **show ip casa affinities** [**stats**] | [**saddr** *ipaddr* [**detail**]] | [**daddr** *ipaddr* [**detail**]] | **[sport** *sport* [**detail**]] | [**dport** *dport* [**detail**]] | [**protocol** *protocol* [**detail**]]

Syntax Description

daddr *ipaddr* — (Optional) Displays affinities for a destination address.

detail — (Optional) Displays detailed affinity information.

dport *dport* — (Optional) Displays affinities for a destination port.

internal — (Optional) Displays internal ContentFlow information.

protocol *protocol* — (Optional) Displays protocol of a given TCP connection.

saddr *ipaddr* — (Optional) Displays source address of a given TCP connection.

sport *sport* — (Optional) Displays source port of a given TCP connection.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(5)T.

Sample Displays

The following is sample output of the **show ip casa affinities** command:

```
Router# show ip casa affinities

                        Affinity Table
Source Address  Port  Dest Address    Port  Prot
161.44.36.118   1118  172.26.56.13    19    TCP
172.26.56.13    19    161.44.36.118   1118  TCP
```

The following is sample output of the **show ip casa affinities detail** command

```
Router# show ip casa affinities detail

                        Affinity Table
Source Address  Port  Dest Address    Port  Prot
161.44.36.118   1118  172.26.56.13    19    TCP
  Action Details:
    Interest Addr:          172.26.56.19      Interest Port: 1638
    Interest Packet: 0x0102 SYN FRAG
    Interest Tickle: 0x0005 FIN RST
    Dispatch (Layer 2):     YES               Dispatch Address: 172.26.56.33

Source Address  Port  Dest Address    Port  Prot
172.26.56.13    19    161.44.36.118   1118  TCP
  Action Details:
    Interest Addr:          172.26.56.19      Interest Port: 1638
    Interest Packet: 0x0104 RST FRAG
    Interest Tickle: 0x0003 FIN SYN
    Dispatch (Layer 2):     NO                Dispatch Address: 0.0.0.0
```

Table 1 describes significant fields shown in the display.

Table 1 Show IP Casa Affinities Field Descriptions

Field	Description
Source Address	Source address of a given connection.
Port	Source port of a given connection.
Dest Address	Destination address of a given connection.
Port	Destination of a given connection.
Prot	Protocol of a given connection.
Action Details	Actions to be taken on a match.
Interest Addr	Service Manager that is to receive interest packets for this affinity.
Interest Port	Service Manager port to which interest packets are sent.
Interest Packet	List of packet types that the Service Manager is interested in.
Interest Tickle	List of packet types for which the Service Manager wants entire packet.
Dispatch (Layer 2)	Layer 2 destination information will be modified.
Dispatch Address	Address of the real serve.

Related Commands

port
show ip casa oper

show ip casa oper

Use the **show ip casa oper** command to display operational information.

show ip casa oper

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(5)T.

Sample Displays

The following is sample output of the **show ip casa oper** command:

```
Router# show ip casa oper

Casa is Active
  Casa control address is 206.10.20.34/32
  Casa multicast address is 224.0.1.2
  Listening for wildcards on:
    Port:1637
      Current passwd:NONE Pending passwd:NONE
      Passwd timeout:180 sec (Default)
```

Table 2 describes significant fields shown in the display.

Table 2 Show IP Casa Oper Field Descriptions

Field	Description
Casa is Active	The ContentFlow architecture is active.
Casa control address	Unique address for this Forwarding Agent.
Casa multicast address	Services Manager broadcast address.
Listening for wildcards on	Port on which the forwarding agent will listen.
Port	Services Manager broadcast port.
Current passwd	Current password.
Pending passwd	Password that will override the current password.
Passwd timeout	Interval after which the pending password becomes the current password.

show ip casa stats

Use the **show ip casa stats** command to display statistical information.

show ip casa stats

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(5)T.

Sample Displays

The following is sample output of the **show ip casa stats** command:

```
Router# show ip casa stat

Casa is active:
  Wildcard Stats:
    Wildcards:       6           Max Wildcards:    6
    Wildcard Denies: 0           Wildcard Drops:   0
    Pkts Throughput: 441         Bytes Throughput: 39120
  Affinity Stats:
    Affinities:      2           Max Affinities:   2
    Cache Hits:      444         Cache Misses:     0
    Affinity Drops:  0
  Casa Stats:
    Int Packet:      4           Int Tickle:       0
    Casa Denies:     0           Drop Count:       0
```

Table 3 describes significant fields shown in the display.

Table 3 Show IP Casa Stats Field Descriptions

Field	Description
Casa is Active	**Description**
Wildcard Stats	The ContentFlow architecture is active.
Wildcards	Wildcard statistics.
Max Wildcards	Number of current wildcards.
Wildcard Denies	Maximum number of wildcards since the ContentFlow architecture became active.
Wildcard Drops	Protocol violations.
Pkts Throughput	No memory to install wildcard.
Bytes Throughput	Number of packets passed through all wildcards.
Affinity Stats	Number of bytes passed through all wildcards.
Affinities	Affinity statistics.
Max Affinities	Current number of affinities.

Table 3 Show IP Casa Stats Field Descriptions

Field	Description
Cache Hits	Maximum number of affinities since the ContentFlow architecture became active.
Cache Misses	Number of packets that match wildcards and fixed affinities.
Affinity Drops	Matched wildcard, missed fix.
Casa Stats	Number of times an affinity could not be created.
Int Packet	ContentFlow statistics.
Int Tickle	Interest packets.
Casa Denies	Interest tickles.
Drop Count	Protocol violation.

show ip casa wildcard

Use the **show ip casa wildcard** command to display information about wildcard affinities.

show ip casa wildcard [**detail**]

Syntax Description

detail	(Optional) Displays detailed statistics.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(5)T.

Sample Displays

The following is sample output of the **show ip casa wildcard** command:

```
Router# show ip casa wildcard

Source Address  Source Mask     Port  Dest Address    Dest Mask       Port  Prot
0.0.0.0         0.0.0.0         0     172.26.56.2     255.255.255.255 0     ICMP
0.0.0.0         0.0.0.0         0     172.26.56.2     255.255.255.255 0     TCP
0.0.0.0         0.0.0.0         0     172.26.56.13    255.255.255.255 0     ICMP
0.0.0.0         0.0.0.0         0     172.26.56.13    255.255.255.255 0     TCP
172.26.56.2     255.255.255.255 0     0.0.0.0         0.0.0.0         0     TCP
172.26.56.13    255.255.255.255 0     0.0.0.0         0.0.0.0         0     TCP
```

The following is sample output of the **show ip casa wildcard detail** command:

```
router#sh ip casa wild detail
Source Address  Source Mask     Port  Dest Address    Dest Mask       Port  Prot
0.0.0.0         0.0.0.0         0     172.26.56.2     255.255.255.255 0     ICMP
  Service Manager Details:
    Manager Addr:           172.26.56.19      Insert Time: 08:21:27 UTC 04/18/96
  Affinity Statistics:
    Affinity Count:         0                 Interest Packet Timeouts: 0
  Packet Statistics:
    Packets:                0                 Bytes: 0
  Action Details:
    Interest Addr:          172.26.56.19      Interest Port: 1638
    Interest Packet: 0x8000 ALLPKTS
    Interest Tickle: 0x0107 FIN SYN RST FRAG
    Dispatch (Layer 2):     NO                Dispatch Address: 0.0.0.0
    Advertise Dest Address: YES               Match Fragments:  NO

Source Address  Source Mask     Port  Dest Address    Dest Mask       Port  Prot
0.0.0.0         0.0.0.0         0     172.26.56.2     255.255.255.255 0     TCP
  Service Manager Details:
    Manager Addr:           172.26.56.19      Insert Time: 08:21:27 UTC 04/18/96
  Affinity Statistics:
    Affinity Count:         0                 Interest Packet Timeouts: 0
  Packet Statistics:
    Packets:                0                 Bytes: 0
  Action Details:
    Interest Addr:          172.26.56.19      Interest Port: 1638
    Interest Packet: 0x8102 SYN FRAG ALLPKTS
    Interest Tickle: 0x0005 FIN RST
    Dispatch (Layer 2):     NO                Dispatch Address: 0.0.0.0
    Advertise Dest Address: YES               Match Fragments:  NO
```

Table 4 describes significant fields shown in the display.

Note If a filter is not set, the filter is not active.

Table 4 Show IP Casa Wildcard Field Descriptions

Field	Description
Source Address	Source address of a given TCP connection.
Source Mask	Mask to apply to source address before matching.
Port	Source port of a given TCP connection.
Dest Address	Destination address of a given TCP connection.
Dest Mask	Mask to apply to destination address before matching.
Port	Destination port of a given TCP connection.
Prot	Protocol of a given TCP connection.
Service Manager Details	Service Manager details.
Manager Addr	Source address of this wildcard.
Insert Time	System time at which this wildcard was inserted.
Affinity Statistics	Affinity statistics.
Affinity Count	Number of affinities created on behalf of this wildcard.
Interest Packet Timeouts	Number of unanswered interest packets.

Table 4 Show IP Casa Wildcard Field Descriptions

Field	Description
Packet Statistics	Packet statistics.
Packets	Number of packets that match this wildcard.
Bytes	Number of bytes that match this wildcard.
Action Details	Actions to be taken on a match.
Interest Addr	Service Manager that is to receive interest packets for this wildcard.
Interest Port	Service Manager port to which interest packets are sent.
Interest Packet	List of packet types that the Service Manager is interested in.
Interest Tickle	List of packet types for which the Service Manager wants the entire packet.
Dispatch (Layer 2)	Layer 2 destination information will be modified.
Dispatch Address	Address of the real server.
Advertise Dest Address	Destination address.
Match Fragments	Does wildcard also match fragments? (boolean)

virtual

Create a virtual server to accept a connection from the network.

virtual *virtual_name* | *virtual_ip* [**:**[*virtual_port*]**:**[*bind-id*]**:**[*protocol*]]
[*service-state*]
[**no**] **virtual** *virtual_name* | *virtual_ip* [**:**[*virtual_port*]**:**[*bind-id*]**:**[*protocol*]] [*service-state*]

Syntax Description

virtual_name Name of the virtual server being defined.

virtual_ip IP address of the virtual server being defined.

virtual_port (Optional) Port traffic that runs on the server. Use a colon as a delimiter between the IP address and port number. If you do not identify a specific port, all traffic is allowed to the server and the port is labeled 0. Servers with a port specified are referred to as "port-bound" servers.

bind-id (Optional) Used with the **assign** command to direct traffic to a specific location. Use a colon as a delimiter between the bind-id and port number. If you do not specify a bind-id when defining a virtual server, the default is 0. Any client IP address *not* identified by an **assign** command statement will be directed to the default bind-id of 0.

protocol (Optional) Protocol to use. The default value is **tcp**, but **udp** and **gre** are available options. Use a colon as a delimiter between the bind-id and protocol.

service-state (Optional) In-service (**is**) or out-of-service (**oos**). The default is **oos**.

Command Mode

Configuration

Usage Guidelines

The **virtual** command creates a virtual server to accept a connection from the network. Virtual servers present a single address for a group of real servers and load balance service requests between the real servers in a site. The virtual server IP address is published to the user community, but the real IP address remain unpublished.

If you are using directed mode, and the published or "advertised" addresses are different from internal addresses, the IP address of LocalDirector must be on the network from which you want to access LocalDirector. That is, if your virtual servers are on network 204.31.17.x, and your real servers are on network 192.168.89.x, then the IP address of LocalDirector should be either 204.31.17.x (if accessing LocalDirector from outside) or 192.168.89.x (if accessing LocalDirector from inside). Here *accessing* means using Telnet, SNMP, or SYSLOG to connect to LocalDirector. Virtual server addresses can only be accessed from the client side of LocalDirector.

If you are using dispatched mode, you can create an alias IP address on LocalDirector and keep it in a subnet different from the location of the real servers.

Specify the IP address of LocalDirector with the **ip address** command before defining virtual servers. If no real servers are bound to the virtual server, the **no virtual** command can be used to remove the virtual server from LocalDirector.

Note If you define a port-bound virtual server and there is no real server with that port defined (or a real server configured for default ports), the client is sent a TCP RST when a connection to that port is attempted.

On Catalyst 6000 Family Switches, if you use FTP sessions with MNLB you must configure a port-bound virtual server bound to port 21 on the MNLB Services Manager.

Examples

The port and bind-id are optional when defining virtual servers. Although a space can be used as a delimiter for the port, a colon is preferred and must be used with the bind-id. Note that the port and bind-id are 0 by default:

```
ld(config) 5# virtual 10.10.10.1:80:tcp
ld(config) 6# virtual 10.10.10.1:443:1:tcp
ld(config) 7# virtual 10.10.10.1
ld(config) 8# show virtual

Machines:
Machine               Mode       State  Connect  Sticky   Predictor    Slowstart
10.10.10.1:80:0:tcp   directed    OOS     0        0      leastconns   roundrobin*
10.10.10.1:443:1:tcp  directed    OOS     0        0      leastconns   roundrobin*
10.10.10.1:0:0:tcp    directed    OOS     0        0      leastconns   roundrobin*
```

In the following example, note the use of the **name** command. The name is used with the port and bind-id to identify the server (*virtual_id*):

```
ld(config) 9# name 10.10.10.1 lucky
ld(config) 0# is virtual lucky:80
ld(config) 1# sticky lucky:443:1 10
ld(config) 2# show virtual
Virtual Machines:
 Machine      Mode    State  Connect   Sticky    Predictor   Slowstart
   lucky:80:0  directed   IS        0        0   leastconns  roundrobin*
   lucky:443:1 directed  OOS        0       10   leastconns  roundrobin*
   lucky:0:0   directed  OOS        0        0   leastconns  roundrobin*
```

To remove a virtual server you have to first remove any bind association to real servers. For example:

```
LocalDirector(config) 5# show virtual
Virtual Machines:
 Machine          Mode     State  Connect   Sticky    Predictor   Slowstart
 192.168.0.98:0:0  directed  OOS        0        0   leastconns  roundrobin*
 192.168.0.99:0:0     directed     IS        0        0   leastconns  roundrobin*
LocalDirector(config) 6# show bind
               Virtual                      Real
         192.168.0.98:0:0(OOS)
                                 192.168.0.3:0(OOS)
         192.168.0.99:0:0(IS)
                                 192.168.0.1:0(IS)
                                 192.168.0.2:0(IS)
LocalDirector(config) 7# no virtual 192.168.0.98:0:0
Must unbind all reals before removing virtual.
LocalDirector(config) 8# no bind 192.168.0.98:0:0 192.168.0.3:0
LocalDirector(config) 9# no virtual 192.168.0.98:0:0
LocalDirector(config) 0# show virtual
Virtual Machines:
 Machine          Mode    State  Connect   Sticky    Predictor   Slowstart
  2.168.0.99:0:0  directed    IS        0        0   leastconns  roundrobin*
LocalDirector(config) 1#
```

The **show virtual** command indicates the service state of virtual servers. Possible service states are:

- In-service (IS)

  The virtual server accepting connections.

- Out-of-service (OOS)

  The **out-of-service** command was used to take the virtual server off-line, and it is not accepting traffic for load balancing. Connections addressed to the virtual server will be dropped.

- Failed

  The virtual server is unable to direct traffic to real servers. The real servers bound to the virtual server are either out of service or failed.

- Max

  All real servers bound to the virtual server have reached the value set with the **maxconns** command. They are not accepting connections even though the servers are in-service.

Table 4-2 show virtual Command Field Descriptions

Column heading	Description
Machine	IP address or name of the server, port (if a port-bound server), and protocol.
Mode	Directed or dispatched mode.
State	IS (in-service), OOS (out-of-service), or Max. Max means the server has reached maximum connections set with the **maxconns** command.
Connect	Number of connections to the server.
Sticky	Elapsed time of inactivity before connection is sent to another server.
Predictor	Type of load balancing. An asterisk (*) indicates that this predictor is active.
Slowstart	Slowstart option set with **predictor** command (roundrobin or none). An asterisk (*) indicates that this predictor is active.

Related Commands

ip address
show virtual

Debug Commands

This section documents the debug commands. A range of command modifiers is available to limit the output to the specific area of interest.

debug ip casa affinities

Use the **debug ip casa affinities** Global configuration command to enable debugging for affinities. Use the **no** form of this command to disable debugging.

debug ip casa affinities
no debug ip casa affinities

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Privileged EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(5)T.

Sample Display

The following is output from the **debug ip casa affinities** command:

```
Router# debug ip casa affinities

16:15:36:Adding fixed affinity:
16:15:36:    10.10.1.1:54787 -> 10.10.10.10:23 proto = 6
16:15:36:Updating fixed affinity:
16:15:36:    10.10.1.1:54787 -> 10.10.10.10:23 proto = 6
16:15:36:    flags = 0x2, appl addr = 10.10.3.2, interest = 0x5/0x100
16:15:36:    int ip:port = 10.10.2.2:1638, sequence delta = 0/0/0/0
16:15:36:Adding fixed affinity:
16:15:36:    10.10.10.10:23 -> 10.10.1.1:54787 proto = 6
16:15:36:Updating fixed affinity:
16:15:36:    10.10.10.10:23 -> 10.10.1.1:54787 proto = 6
16:15:36:    flags = 0x2, appl addr = 0.0.0.0, interest = 0x3/0x104
16:15:36:    int ip:port = 10.10.2.2:1638, sequence delta = 0/0/0/0
```

Table 5 describes significant fields of the debug output.

Table 5 Debug IP Casa Affinities Field Descriptions

Field	Description
Adding fixed affinity	Adding a fixed affinity to affinity table.
Updating fixed affinity	Modifying a fixed affinity table with information from the Service Manager.
flags	Bit field indicating actions to be taken on this affinity.
fwd addr	Address to which packets will be directed.
interest	Service Manager that's interested in packets for this affinity.
int ip:port	Service Manager port to which interest packets are sent.
sequence delta	Used to adjust TCP sequence numbers for this affinity.

debug ip casa packets

Use the **debug ip casa packets** Global configuration command to enable debugging for packets. Use the **no** form of this command to disable debugging.

debug ip casa packets
no debug ip casa packets

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Privileged EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(5)T.

Sample Display

The following is output from the **debug ip casa packets** command:

```
Router# debug ip casa packets

16:15:36:Routing CASA packet - TO_MGR:
16:15:36:    10.10.1.1:55299 -> 10.10.10.10:23 proto = 6
16:15:36:    Interest Addr:10.10.2.2   Port:1638
16:15:36:Routing CASA packet - FWD_PKT:
16:15:36:    10.10.1.1:55299 -> 10.10.10.10:23 proto = 6
16:15:36:    Fwd Addr:10.10.3.2
16:15:36:Routing CASA packet - TO_MGR:
16:15:36:    10.10.10.10:23 -> 10.10.1.1:55299 proto = 6
16:15:36:    Interest Addr:10.10.2.2   Port:1638
16:15:36:Routing CASA packet - FWD_PKT:
16:15:36:    10.10.10.10:23 -> 10.10.1.1:55299 proto = 6
16:15:36:    Fwd Addr:0.0.0.0
16:15:36:Routing CASA packet - TICKLE:
16:15:36:    10.10.10.10:23 -> 10.10.1.1:55299 proto = 6
16:15:36:    Interest Addr:10.10.2.2   Port:1638  Interest Mask:SYN
16:15:36:    Fwd Addr:0.0.0.0
16:15:36:Routing CASA packet - FWD_PKT:
16:15:36:    10.10.1.1:55299 -> 10.10.10.10:23 proto = 6
16:15:36:    Fwd Addr:10.10.3.2
```

Table 6 describes significant fields in the debug output.

Table 6 Debug IP Casa Packets Field Descriptions

Field	Description
Routing CASA packet - TO_MGR	Forwarding Agent is routing a packet to the Service Manager.
Routing CASA packet - FWD_PKT	Forwarding Agent is routing a packet to the forwarding address.
Routing CASA packet - TICKLE	Forwarding Agent is signalling Service Manager while allowing the packet in question to take the appropriate action.
Interest Addr	Service Manager address.
Interest Port	Port on the Service Manager where packet is sent.
Fwd Addr	Address to which packets matching the affinity are sent.
Interest Mask	Service Manager that is interested in packets for this affinity.

debug ip casa wildcards

Use the **debug ip casa wildcards** Global configuration command to enable debugging for wildcards. Use the **no** form of this command to disable debugging.

debug ip casa wildcards
no debug ip casa wildcards

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Privileged EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(5)T.

Sample Display

The following is output from the **debug ip casa wildcards** command:

```
Router# debug ip casa wildcards

16:13:23:Updating wildcard affinity:
16:13:23:    10.10.10.10:0 -> 0.0.0.0:0 proto = 6
16:13:23:    src mask = 255.255.255.255, dest mask = 0.0.0.0
16:13:23:    no frag, not advertising
16:13:23:    flags = 0x0, appl addr = 0.0.0.0, interest = 0x8107/0x8104
16:13:23:    int ip:port = 10.10.2.2:1638, sequence delta = 0/0/0/0
16:13:23:Updating wildcard affinity:
16:13:23:    0.0.0.0:0 -> 10.10.10.10:0 proto = 6
16:13:23:    src mask = 0.0.0.0, dest mask = 255.255.255.255
16:13:23:    no frag, advertising
16:13:23:    flags = 0x0, appl addr = 0.0.0.0, interest = 0x8107/0x8102
16:13:23    int ip:port = 10.10.2.2:1638, sequence delta = 0/0/0/0
```

Table 7 describes significant fields in the debug output.

Table 7 Debug IP Casa Wildcards Field Descriptions

Field	Description
src mask	Source of a given connection.
dest mask	Destination of a given connection.
no frag, not advertising	Not accepting IP fragments.
flags	Bit field indicating actions to be taken on this affinity.
fwd addr	Address to which packets matching the affinity will be directed.
interest	Service Manager that's interested in packets for this affinity.
int ip: port	Service Manager port to which interest packets are sent.
sequence delta	Used to adjust sequence numbers for this affinity.