

# MultiNode Load Balancing Forwarding Agent

---

12.0(5)T

December 17, 1999

## Feature Overview

The MultiNode Load Balancing (MNLB) forwarding agent is the IOS-based packet redirector component of the MNLD Feature Set for LocalDirector, a product in the Cisco family of load balancing solutions.

The forwarding agent discovers the destination of specific connection requests and forwards packets between the client and the chosen destination. When a forwarding agent receives a connection request, the request is forwarded to the MNLB services manager, the LocalDirector-based component of the MNLD Feature Set for LocalDirector. The services manager makes the load balancing decision and sends the forwarding agent the optimal destination. After the destination is specified, session data is forwarded directly to the destination by the forwarding agent, without further services manager participation. There is no limit to the number of forwarding agents that can be configured in the MNLD Feature Set for LocalDirector.

## Benefits

The MNLD Feature Set for LocalDirector comprises hardware and software that runs on multiple network components. The services manager runs on Cisco's LocalDirector chassis and makes the load-balancing decisions. The forwarding agents run on Cisco IOS router and switch platforms and forward packets to and from the selected destination. Separating the decision-making and packet-forwarding tasks enables much faster packet throughput. The underlying Cisco architecture, ContentFlow architecture, enables high availability, unbounded scalability, application-aware balancing, no single point of failure, and unmatched performance.

## Restrictions

Configure the forwarding agent only if you are installing the MNLD Feature Set for LocalDirector. If you are installing the MNLD Feature Set for LocalDirector, refer to the *MultiNode Load Balancing Feature Set for LocalDirector User Guide* for information about which other hardware and software components are required.

## Related Features and Technologies

The MNLB forwarding agent is an implementation of Cisco's ContentFlow architecture flow delivery agent (FDA).

## Related Documents

Refer to the *MultiNode Load Balancing Feature Set for LocalDirector User Guide* for more information about how the forwarding agent is configured and for more information about the product.

## Supported Platforms

This feature is supported on these platforms:

- Cisco 7500 series
- Cisco 7200 series
- Cisco Cat5000/RSM
- Cisco 4700
- Cisco 3600 series

## Supported Standards, MIBs, and RFCs

This feature supports the following MIB:

- cisco-casa-fa-mib.my

For descriptions of supported MIBs and how to use MIBs, see the Cisco MIB web site on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

No RFCs are supported by this feature.

## Prerequisites

MNLB Feature Set for LocalDirector requires Cisco LocalDirector release 3.1.1 or higher and Cisco IOS Release 12.0(5)T.

## Configuration Tasks

The following sections describe forwarding agent configuration tasks:

- Enabling Cisco Express Forwarding
- Enabling NetFlow Switching
- Enabling IP Multicast Routing
- Configuring the Router as an MNLB Forwarding Agent

## Enabling Cisco Express Forwarding

Cisco Express Forwarding (CEF) is advanced Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns, such as the Internet, on networks characterized by intensive Web-based applications, or interactive sessions.

To enable CEF, use the following command in global configuration mode:

Command	Purpose
Router (config) <b>ip cef distributed</b>	Enables CEF.

**Note** When you enable CEF globally, all interfaces that support CEF are enabled by default. If you want to turn off CEF on a particular interface, you can do so.

## Enabling NetFlow Switching

You must enable NetFlow switching on all interfaces that will carry ContentFlow traffic. To enable NetFlow switching, use the following commands, beginning in interface configuration mode:

Step	Command	Purpose
1	Router(config-if)# <b>interface</b> <i>type</i> <i>slot/port-adapter/port</i> (Cisco 7500 series routers) Router(config-if)# <b>interface</b> <i>type slot/port</i> (Cisco 7200 series routers)	Specifies the interface, and enters interface configuration mode.
2	Router(config-if)# <b>ip route-cache flow</b>	Enables flow switching on the interface.

Normally the size of the NetFlow cache will meet your needs. However, you can increase or decrease the number of entries maintained in the cache by using the following command in global configuration mode

Command	Purpose
Router (config)# <b>ip flow-cache entries</b> <i>number</i>	Changes the number of entries maintained in the NetFlow cache. The number of entries can be 1024 to 524288. The default is 64536.

### Enabling IP Multicast Routing

You must enable multicast routing on all interfaces to the services manager.

To enable multicast routing on all interfaces, use the following command in global configuration mode:

Command	Purpose
Router (config) # <b>ip multicast routing</b>	Enables multicast routing.

To have the router join a multicast group and enable IGMP, use the following command in interface configuration mode:

Command	Purpose
Router (config-if) # <b>ip igmp join-group</b> <sup>1</sup> <i>group-address</i> <sup>2</sup>	Joins a multicast group.

- 1 This command must be configured on all interfaces that will listen for the services manager multicasts.
- 2 The group address must match that configured within the services manager configuration.

### Configuring the Router as an MNLB Forwarding Agent

To configure the router as a forwarding agent, use the following commands, beginning in global configuration mode:

Step	Command	Purpose
1	Router (config) # <b>ip casa control-address</b> <i>igmp-address</i>	Specify the control address and IGMP address of the forwarding agent. The control address is a unique ip address used by forwarding-agent to send and receive control message between the service manager and the forwarding-agent. The recommended IGMP address is 224.0.1.2.
2	Router (config-casa) # <b>forwarding-agent pool</b> <i>initial_affinity_pool max_affinity_pool</i>	Adjusts the memory allocated for the forwarding agent's affinity pools. The default pool size is 5000 and there is no maximum pool size.
3	Router (config-casa) # <b>forwarding-agent</b> num [passwd [timeout]]	Specifies the port number.

---

**Note** The forwarding agent IGMP address and port must match the IGMP address and port configured on the services manager and the **ip igmp join-group** command.

---

### Monitoring the MNLB Forwarding Agent

To monitor the status of the forwarding agent, use the following commands in EXEC mode:

Command	Purpose
Router# <b>show ip casa affinities</b>	Displays the status of affinities.
Router# <b>show ip casa oper</b>	Displays the operational status of the forwarding agent.
Router# <b>show ip casa stats</b>	Displays statistical information about the forwarding agent.
Router# <b>show ip casa wildcard</b>	Displays information about wildcard blocks.

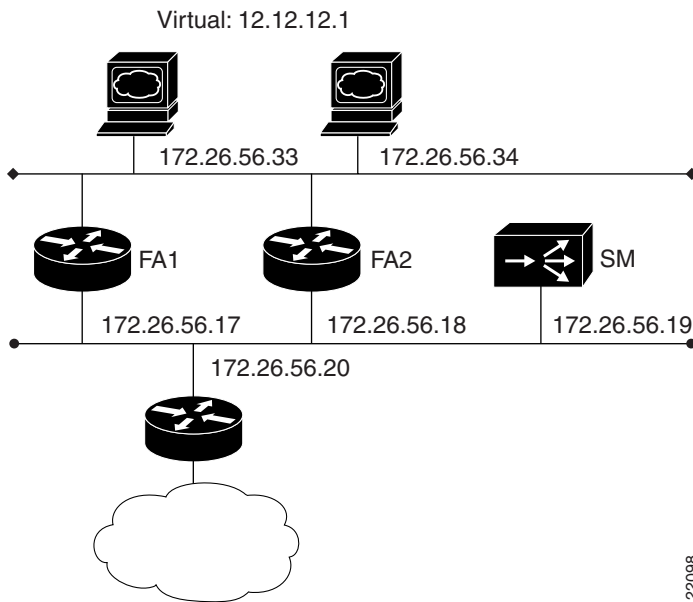
## Configuration Examples

This section provides the following configuration examples:

- Forwarding Agent Configuration for FA2
- Services Manager Configuration for SM

The network configured is shown in Figure 1.

**Figure 1 MultiNode Load Balancing Network Configuration**



22098

### Forwarding Agent Configuration for FA2

The following is a sample, of a router configured as a forwarding agent. In this example all disabled interfaces have been omitted to simplify the display.

```
FA2#wr t
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname FA2
!
!
microcode CIP flash slot0:cip26-5
microcode reload
ip subnet-zero
no ip domain-lookup
!
ip cef distributed
ip casa 206.10.20.34 224.0.1.2
```

## Configuring the Router as an MNLB Forwarding Agent

---

```
forwarding-agent 1637
!
interface Ethernet0/0
 ip address 172.26.56.18 255.255.255.224
 no ip directed-broadcast
 ip route-cache flow
 ip igmp join-group 224.0.1.2
 no ip mroute-cache
!
interface Ethernet0/1
 ip address 172.26.56.37 255.255.255.224
 no ip directed-broadcast
!
!
!
router eigrp 777
 network 172.26.0.0
!

no ip classless
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 exec-timeout 0 0
 login
!
end
```

## Services Manager Configuration for SM

```
SM# wr t
Building configuration...
: Saved
: LocalDirector 420 Version 3.0.0.127
syslog output 20.3
no syslog console
enable password 00000000000000000000000000000000 encrypted
hostname SM
no shutdown ethernet 0
no shutdown ethernet 1
no shutdown ethernet 2
no shutdown ethernet 3
interface ethernet 0 auto
interface ethernet 1 auto
interface ethernet 2 auto
interface ethernet 3 auto
mtu 0 1500
mtu 1 1500
mtu 2 1500
mtu 3 1500
multiring all
no secure 0
no secure 1
no secure 2
no secure 3
ping-allow 0
ping-allow 1
ping-allow 2
ping-allow 3
ip address 172.26.56.19 255.255.255.248
route 172.26.10.249 255.255.255.255 172.26.56.20 1
```

```

route 206.10.20.33 255.255.255.255 172.26.56.17 1
route 206.10.20.34 255.255.255.255 172.26.56.18 1
no rip passive
failover ip address 0.0.0.0
failover
password cisco
telnet 161.0.0.0 255.0.0.0
no snmp-server contact
no snmp-server location
casa service-manager port 1638
casa service-manager multicast-ttl 60
tftp-server 172.26.10.249 /tftpboot/LD
virtual 172.26.56.13:0:0:tcp is
virtual 172.26.56.2:0:0:tcp is
redirection 172.26.56.13:0:0:tcp dispatched casa wildcard-ttl 60 fixed-ttl 60 igmp
224.0.1.2 port 1637
redirection 172.26.56.2:0:0:tcp dispatched casa wildcard-ttl 60 fixed-ttl 60 igmp
224.0.1.2 port 1637
real 172.26.56.34:0:0:tcp is
real 172.26.56.33:0:0:tcp is
real 172.26.56.6:0:0:tcp is
real 172.26.56.10:0:0:tcp is
bind 172.26.56.13:0:0:tcp 172.26.56.33:0:0:tcp
bind 172.26.56.13:0:0:tcp 172.26.56.34:0:0:tcp
bind 172.26.56.2:0:0:tcp 172.26.56.10:0:0:tcp
bind 172.26.56.2:0:0:tcp 172.26.56.6:0:0:tcp
: end

```

## Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command reference publication.

In Cisco IOS Release 12.0(1)T or later, you can search and filter the output for **show** and **more** commands. This functionality is useful when you need to sort through large amounts of output, or if you want to exclude output that you do not need to see.

To use this functionality, enter a **show** or **more** command followed by the “pipe” character (**|**), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search or filter on:

```
command | {begin | include | exclude} regular-expression
```

Following is an example of the **show atm vc** command in which you want the command output to begin with the first line where the expression “PeakRate” appears:

```
show atm vc | begin PeakRate
```

For more information on the search and filter functionality, refer to the Cisco IOS Release 12.0(1)T feature module titled *CLI String Search*.

## forwarding-agent

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

**forwarding-agent** *num* [*password* [*timeout*]]

**[no] forwarding-agent**

### Syntax Description

<i>num</i>	Port numbers on which the forwarding agent will listen for wildcards broadcast from the services manager. This must match the port number defined on the services manager.
<i>password</i>	(Optional) Text password used for generating the MD5 digest.
<i>timeout</i>	(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.

### Defaults

The default password timeout is 180 seconds.

The default port for the services manager is 1637.

### Command Modes

CASA-port configuration

### Command History

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

### Examples

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

```
forwarding-agent 1637
```

### Related Commands

Command	Description
<b>show ip casa oper</b>	Displays operational information about the forwarding agent.

## 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

<i>initial_affinity_pool</i>	Initial number of memory blocks allocated for use as affinities. The default is 5000.
<i>max_affinity_pool</i>	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
<b>show ip casa oper</b>	Displays operational information about the forwarding agent.

## ip casa

To configure the router to function as an MNLB forwarding agent, use the **ip casa** global configuration command. Use the **no** form of the command to disable the forwarding agent.

**ip casa** *control-address igmp-addr*

**[no] ip casa**

### Syntax Description

<i>control-address</i>	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.
<i>igmp-addr</i>	IGMP address on which the forwarding agent will listen for wildcard and fixed affinities.

### Defaults

No default behavior or values.

### Command Modes

Global configuration

### Command History

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

### Examples

The following example specifies the internet 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

Command	Description
<b>forwarding-agent</b>	Specifies the port on which the forwarding agent will listen for wildcard and fixed affinities.

# show ip casa affinities

To display statistics about affinities, use the **show ip casa affinities** EXEC command.

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

## Syntax Description

<b>stats</b>	(Optional) Displays limited statistics.
<b>saddr</b> <i>ipaddr</i>	(Optional) Displays source address of a given TCP connection.
<b>daddr</b> <i>ipaddr</i>	(Optional) Displays destination address of a given TCP connection.
<b>sport</b> <i>sport</i>	(Optional) Displays source port of a given TCP connection.
<b>dport</b> <i>dport</i>	(Optional) Displays destination port of a given TCP connection.
<b>protocol</b> <i>protocol</i>	(Optional) Displays protocol of a given TCP connection.
<b>detail</b>	(Optional) Displays detailed statistics.

## Command Modes

EXEC

## Command History

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

## Examples

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

Related Commands

Command	Description
<b>forwarding-agent</b>	Specifies the port number on which the forwarding agent will listen for wildcards and fixed affinities.
<b>show ip casa oper</b>	Shows operational information about the forwarding agent.

# show ip casa oper

To display operational information about the forwarding agent, use the **show ip casa oper EXEC** command.

```
show ip casa oper
```

## Syntax Description

This command has no arguments or keywords.

## Command Modes

EXEC

## Command History

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

## Examples

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 forwarding agent 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.

Related Commands

<b>Command</b>	<b>Description</b>
<b>ip casa</b>	Configures the router to function as an MNLB forwarding agent.

## show ip casa stats

To display statistical information about the forwarding agent, use the **show ip casa stats EXEC** command.

```
show ip casa stats
```

### Syntax Description

This command has no arguments or keywords.

### Command Modes

EXEC

### Command History

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

### Examples

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

```
Router# show ip casa stats

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	The forwarding agent is active.
Wildcard Stats	Wildcard statistics.
Wildcards	Number of current wildcards.
Max Wildcards	Maximum number of wildcards since the forwarding agent became active.
Wildcard Denies	Protocol violations.
Wildcard Drops	No memory to install wildcard.
Pkts Throughput	Number of packets passed through all wildcards.

**Table 3 Show IP Casa Stats Field Descriptions (continued)**

<b>Field</b>	<b>Description</b>
Bytes Throughput	Number of bytes passed through all wildcards.
Affinity Stats	Affinity statistics.
Affinities	Current number of affinities.
Max Affinities	Maximum number of affinities since the forwarding agent became active.
Cache Hits	Number of packets that match wildcards and fixed affinities.
Cache Misses	Matched wildcard, missed fix.
Affinity Drops	Number of times an affinity could not be created.
Casa Stats	Forwarding agent statistics.
Int Packet	Interest packets.
Int Tickle	Interest tickles.
Casa Denies	Protocol violation.
Security Drops	Packets dropped due to password or authentication mismatch.
Drop Count	Number of messages dropped.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show ip casa oper</b>	Shows operational information about the forwarding agent.

# show ip casa wildcard

To display information about wildcard blocks, use the **show ip casa wildcard EXEC** command.

**show ip casa wildcard [detail]**

## Syntax Description

detail (Optional) Displays detailed statistics.

## Command Modes

EXEC

## Command History

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

## Examples

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# show 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
    
```

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

Table 4 describes significant fields shown in the display.

**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	Services 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.

**Table 4 Show IP Casa Wildcard Field Descriptions (continued)**

<b>Field</b>	<b>Description</b>
Interest Packet Timeouts	Number of unanswered interest packets.
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	Services manager that is to receive interest packets for this wildcard.
Interest Port	Services manager port to which interest packets are sent.
Interest Packet	List of packet types that the services manager is interested in.
Interest Tickle	List of packet types for which the services 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)

#### Related Commands

<b>Command</b>	<b>Description</b>
<b>show ip casa oper</b>	Shows operational information about the forwarding agent.

## debug ip casa affinities

To display debug messages for affinities, use the **debug ip casa affinities** privileged EXEC command. Use the **no** form of the command to disable debugging.

**[no] debug ip casa affinities**

### Syntax Description

This command has no arguments or keywords.

### Defaults

Debugging for affinities is not enabled.

### Command History

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

### Examples

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 services manager.
flags	Bit field indicating actions to be taken on this affinity.
fwd addr	Address to which packets will be directed.
interest	Services manager that's interested in packets for this affinity.
int ip:port	Services manager port to which interest packets are sent.

**Table 5          Debug IP Casa Affinities Field Descriptions**

<b>Field</b>	<b>Description</b>
sequence delta	Used to adjust TCP sequence numbers for this affinity.

## debug ip casa packets

To display debug messages for packets, use the **debug ip casa packets** privileged EXEC command. Use the **no** form of the command to disable debugging.

**[no] debug ip casa packets**

### Syntax Description

This command has no arguments or keywords.

### Defaults

Debugging for packets is not enabled.

### Command History

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

### Examples

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**

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

## debug ip casa wildcards

To display debug messages for wildcards, use the **debug ip casa wildcards** privileged EXEC command. Use the **no** form of this command to disable debugging.

**[no] debug ip casa wildcards**

### Syntax Description

This command has no arguments or keywords.

### Defaults

Debugging for wildcards is not enabled.

### Command History

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

### Examples

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 connection.
dest mask	Destination of 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	Services manager that's interested in packets for this affinity.
int ip: port	Services manager port to which interest packets are sent.

**Table 7          Debug IP Casa Wildcards Field Descriptions**

<b>Field</b>	<b>Description</b>
sequence delta	Used to adjust sequence numbers for this affinity.

## Glossary

**affinity**—The set of information that uniquely describes the association of a client to a particular host within a server cluster. It relates the addresses found in the IP packet (protocol, client IP address, port, local port, cluster address) to the IP address of the local host that has been assigned to handle all packets with that unique set of addresses.

**CEF**—Cisco Express Forwarding.

**cluster**—A set of computer systems that are connected together through multisystem hardware or software to provide services traditionally provided by a single system. This arrangement provides higher availability and better scalability.

**cluster address**—The IP address that represents the entire cluster of hosts. It is defined in each server and each forwarding agent router. The routers advertise routes to their internal instances of this address. The servers do not advertise the address, but recognize it as one of their local, or loopback addresses.

**ContentFlow architecture**—A Cisco protocol that enables communication between a services manager and a forwarding agent.

**control address**—An IP address assigned to the IP cluster function within each router. It is unique to each router and is used for management flows.

**forwarding agent**—MultiNode Load Balancing forwarding agent. Fulfills routing decisions made by the services manager. The forwarding agent filters packets coming into the virtual network and sends to the services manager packets that are without a known server destination.

**IGMP**—The forwarding agent uses Internet Group Management Protocol (IGMP) multicast to listen to the services manager broadcasts. IP hosts use IGMP to report their group membership to directly-connected multicast routers. IGMP uses group addresses, which are Class D IP addresses. The high-order four bits of a Class D address are 1110. This means that host group addresses can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is guaranteed not to be assigned to any group. The address 224.0.0.1 is assigned to all systems on a subnet. The address 224.0.0.2 is assigned to all routers on a subnet.

**load balancing**—Spreading user requests among available servers within a cluster of servers, based on a variety of algorithms.

**LocalDirector**—Cisco LocalDirector is hardware and software that provide one of the platforms for the MNLB services manager.

**MD5**— Message Digest Algorithm Version 5, a neighbor router authentication scheme used to ensure reliability and security when routing updates are to be exchanged between neighbor routers.

**NetFlow switching**—High-performance network-layer switching path that captures as part of its switching function a rich set of traffic statistics including user, protocol, port, and type of service information.

**services manager**—MultiNode Load Balancing services manager. Using load balancing and server/application feedback, the services manager determines a real server for the packet flow. Once the optimal destination is decided, all other packets in the packet flow are directed to a forwarding agent and real server, increasing packet throughput. In the MNLD Feature Set for LocalDirector, the services manager function is performed by the LocalDirector.

**server farm**—Also called a server cluster, a group of real servers that provide various applications and services.

**tag switching**—Packet-forwarding strategy that maps Layer 3 header contents into a fixed-length, unstructured value called a tag. In effect, a tag represents a forwarding equivalence class; that is, a set of packets that, however different they may be, are indistinguishable to the forwarding function. The tag does not represent a particular path through the network. In general the path continues to be chosen by the existing Layer 3 routing algorithms.

**virtual server**—Presents a single address that represents an application server farm for clients.

