

## Chapter 16

# MAC-Forced Forwarding

Introduction .....	16-2
Overview .....	16-2
Configuring an Ethernet Access Node .....	16-3
Monitoring and Troubleshooting .....	16-6
Debugging .....	16-6
Logging .....	16-7
Configuration Examples .....	16-7
Command Reference .....	16-8
add macff server .....	16-8
delete macff server .....	16-9
disable macff interface .....	16-9
disable macff interface debug .....	16-10
enable macff interface .....	16-10
enable macff interface debug .....	16-11
reset macff counter .....	16-12
set macff server .....	16-12
show macff .....	16-13
show macff database .....	16-16
show macff interface .....	16-17
show macff interface counter .....	16-19

## Introduction

---

This chapter describes MAC-Forced Forwarding, how it is implemented, and how to configure it on x900-48FE and AT-9900 switches.

MAC-Forced Forwarding is a method for subscriber separation on a network. It is appropriate for IPv4 Ethernet based networks, where a layer 2 bridged segment separates downstream clients from their upstream IPv4 gateways, known as Access Routers (ARs). MAC-Forced Forwarding directs all traffic from a client to a specific AR. This stops the clients from having direct access to one another through the bridged segment, despite being within the same subnet.

MAC-Forced Forwarding benefits your network in the following ways:

- Monitors, filters, and polices any traffic between separate clients within the same subnet. This lets you account for all traffic to and from a client.
- Allows efficient use of limited resources. MAC-Forced Forwarding allows IPv4 addresses to be efficiently assigned by DHCP, and uses less bandwidth and configuration than other Ethernet solutions, such as PPPoE.
- Provides greater security within the subnet. Because malicious clients cannot discover MAC addresses of their neighbouring clients, they cannot launch Ethernet-level attacks on these clients.

The switch's implementation of MAC-Forced Forwarding is compatible with RFC 4562 *MAC-Forced Forwarding: A Method for Subscriber Separation on an Ethernet Access Network*.

## Overview

---

MAC-Forced Forwarding is suitable for Ethernet networks where a Layer 2 bridging device, known as an *Ethernet Access Node* (EAN), connects ARs to their clients. The protocol is implemented on the EANs in a network.

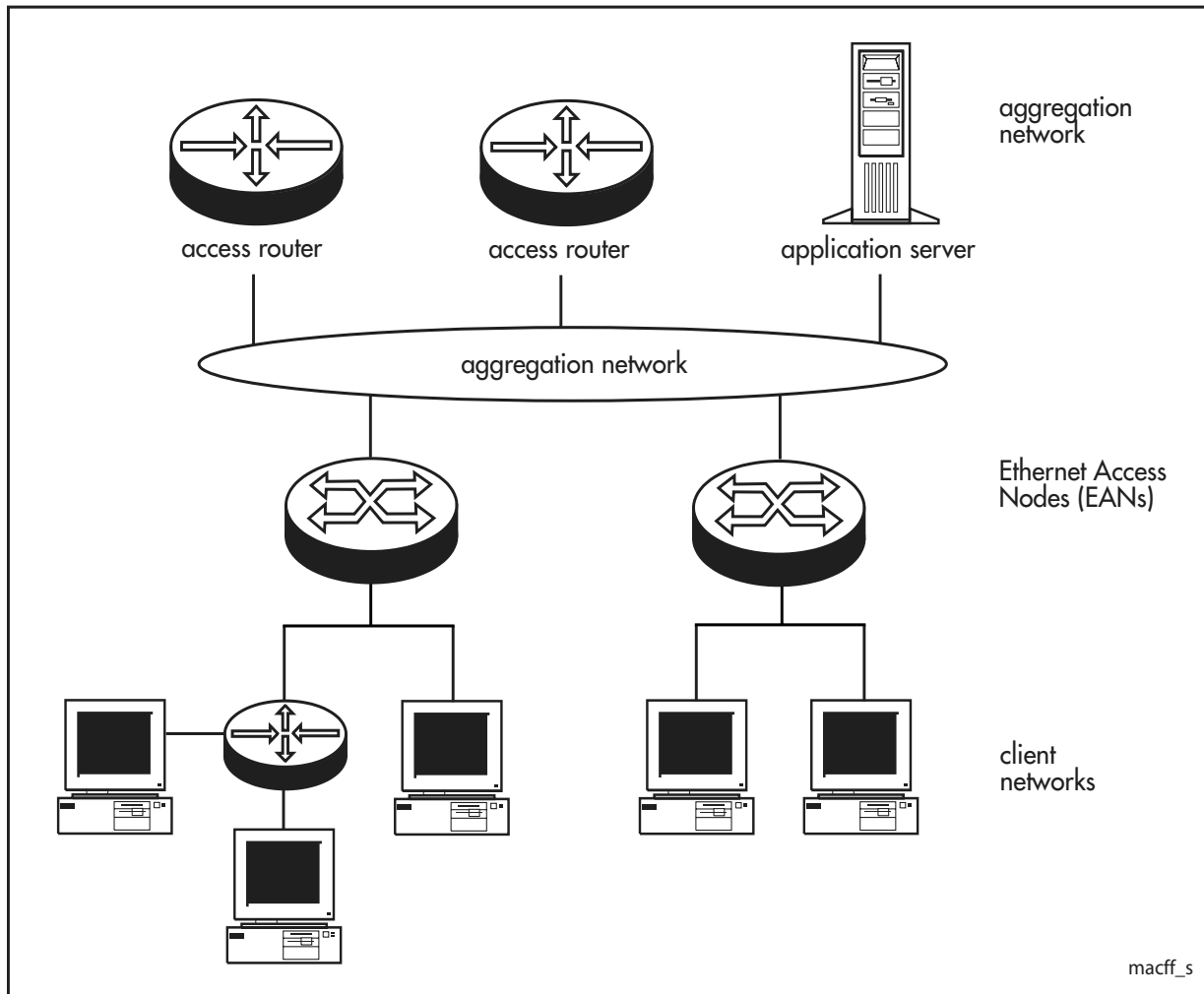
[Figure 16-1 on page 16-3](#) shows an example network with EANs.

### How it works

MAC-Forced Forwarding uses a feature of proxy Address Resolution Protocol (ARP) to stop MAC address resolution between clients. Without MAC-Forced Forwarding, the EANs in a network forward valid ARP messages to the requested destination. With MAC-Forced Forwarding, EANs intercept all ARP messages from clients and send proxy ARP replies on behalf of the client's AR. This stops the clients from learning the MAC addresses of any other devices, and directs all traffic from the client directly to the AR.

An exception to this rule occurs when the network has an Application Server (AS), and the client sends an ARP request for the AS. In these cases the EAN sends a proxy ARP reply back on behalf of the AS rather than the AR.

Figure 16-1: Example Ethernet network with layer 2 bridging devices separating ARs and their clients



### MAC-Forced Forwarding with DHCP snooping

MAC-Forced Forwarding is designed to work in conjunction with DHCP snooping. DHCP snooping looks for DHCP ACK messages sent from DHCP servers to clients. These specify the IP address of a client, and the ARs that the client is allowed to access. Using DHCP snooping, the EAN can dynamically discover the clients and ARs that are attached to the network.

It is possible for a client to have multiple IP addresses, with access rights to different ARs. The EAN keeps track of a client's access rights by comparing the assigned IP address with the valid ARs for that address.

## Configuring an Ethernet Access Node

When configuring the EAN, we suggest the following sequence.

To do this...	See this section...
isolate clients within a subnet from one another	<a href="#">Isolating clients using VLANs</a>
prevent malicious spoofing or traffic from clients	<a href="#">Using DHCP filtering and ARP security</a>
gather the details of any clients ARs and ASs on the network	<a href="#">Using the DHCP snooping database</a>
proxy ARP on behalf of ARs and ASs	<a href="#">Enabling MAC-forced forwarding</a>

For an example of how to configure the switch to perform MAC-Forced Forwarding, see *How to Use MAC-Forced Forwarding with DHCP Snooping to Create Enhanced Private VLANs*. This How To Note is available from [www.alliedtelesis.co.uk/site/solutions/techdocs.asp?area=howto](http://www.alliedtelesis.co.uk/site/solutions/techdocs.asp?area=howto).

### Isolating clients using VLANs

To isolate the clients attached to the EAN, you must configure private VLANs. A private VLAN contains switch ports that are isolated from other ports in the VLAN, but can access another network through an uplink port or uplink trunk group. These ports are called *private ports*. Each private VLAN contains private and uplink ports.

When you have configured a private VLAN, the EAN only forwards traffic from a client to the upstream network, regardless of the original destination details. This blocks all direct traffic between private ports. To create private VLANs, follow these steps:

#### 1. Create the private VLAN.

Use the command:

```
create vlan=vlan-name vid=2..4094 private
```

#### 2. Add the uplink port to the private VLAN.

Use the command:

```
add vlan={vlan-name|2..4094} port=port-list
[frame={untagged|tagged}] uplink
```

#### 3. Add the private ports to the private VLAN.

Use the command:

```
add vlan={vlan-name|2..4094} port={port-list|all}
[frame={untagged|tagged}] [group]
```

For further information about the behaviour of private VLANs and how to configure them on the EAN, see [Chapter 7, Switching](#).

### Using the DHCP snooping database

MAC-Forced Forwarding gathers the AR, AS and client details from the DHCP snooping database. DHCP snooping adds entries to this database when:

- a client uses DHCP to obtain an IP address. DHCP snooping checks the DHCP ACK packets sent between the client and its DHCP server.
- you configure the entry manually through a DHCP snooping binding entry.

To enable DHCP snooping on the EAN, use the command:

```
enable dhcpsnooping
```

You must configure any uplink ports to ARs as trusted ports before DHCP snooping can successfully operate. To add a trusted port, use the command:

```
set dhcpsnooping port={port-list|all} trusted=yes
[other-options]
```

DHCP snooping plays an integral role in MAC-Forced Forwarding operation. For details about configuring DHCP snooping, see [Chapter 15, DHCP Snooping](#).

### Manually Adding Entries

You can create static entries for clients, ARs and ASs. This allows you to use MAC-Forced Forwarding for clients on the subnet that do not use DHCP for IP address assignment. This also allows you to define any ASs available on the network, as DHCP snooping does not create dynamic entries for ASs.

To add a static client entry, use the command:

```
add dhcp snooping binding [=macaddr] interface=vlan ip=ipadd
port=port-number router=[ipadd, ipadd...]
```

To add a static AR or AS entry, use the command:

```
add macff server interface=vlan ipaddress={ipadd}
[description=desc]
```

### Viewing Entries

To view the list of clients in the DHCP snooping database, use the command:

```
show dhcp snooping database
```

To display the list of ARs and ASs in the database, use the command:

```
show macff database
```

### Enabling MAC-forced forwarding

To enable the EAN to proxy ARP on behalf of ARs and ASs on a VLAN, use the command:

```
enable macff interface=vlan
```

To disable MAC-Forced Forwarding on a VLAN, use the command:

```
disable macff interface=vlan
```

### Using DHCP filtering and ARP security

You can prevent IP addresses from being falsified or “spoofed” using DHCP filtering. This guarantees that malicious devices cannot avoid detection by spoofing IP addresses that are not actually allocated to them. DHCP filtering allows packets to only enter a given port if their source IP address is currently allocated to a client attached to that port.

To configure DHCP filtering, you must create classifiers and incorporate them into a QoS configuration. To create classifiers, enter one or both of the **dhcp snooping** options in the command:

```
create classifier=rule-id [macsaddress=dhcp snooping]
[ipsaddress=dhcp snooping]
```

Treat these classifiers like all other classifiers, and use them as part of any QoS or filtering configuration. See [Chapter 26, Generic Packet Classifier](#) for further information about creating classifiers.

To enhance DHCP filtering so that all IGMP queries sent from a client are dropped, use the command:

```
enable dhcp snooping strictunicast
```

This command protects the wider network from being flooded with IGMP queries. For further details, see “[DHCP Filtering](#)” on page 15-4 of [Chapter 15, DHCP Snooping](#).

To permit only trusted clients to access the network, you must enable ARP security. This ensures that only the clients listed in the DHCP snooping database can send ARP messages into the network. To enable ARP security, use the command:

```
enable dhcp snooping arpsecurity
```

For more information, see “DHCP Snooping ARP Security” on page 15-5 of Chapter 15, DHCP Snooping.

## Monitoring and Troubleshooting

---

To see a summary of the VLANs with MAC-Forced Forwarding enabled, use the command:

```
show macff [counter]
```

To see details about a specific VLAN, use the command:

```
show macff interface=vlan
```

To see detailed counters for the traffic flowing through a VLAN, or through specific ports on a VLAN, use the command:

```
show macff interface=vlan [port=port-list] counter
```

To see a detailed list of clients in the DHCP snooping database, use the command:

```
show dhcp snooping database
```

To see a detailed list of the ARs and ASs held in the database, use the command:

```
show macff database
```

## Debugging

The MAC-Forced Forwarding debugging feature allows you to generate information useful for troubleshooting VLANs on the EAN. To enable or disable debugging, use the commands:

```
enable macff interface=vlan
debug={all|arp|dhcp|error|packet|server|trace}

disable macff interface=vlan
debug={all|arp|dhcp|error|packet|server|trace}
```

## Logging

MAC-Forced Forwarding automatically generates log messages to record when:

- an AR or AS is added or removed from the DHCP snooping database
- the MAC address for any routers associated with a client cannot be resolved
- a client ARP request arrives when the client has no ARs associated with it
- a routine poll of the DHCP snooping database shows that an AR or AS is unavailable
- one of the above log types is generating an excessive amount of logs; the log type is temporarily suspended

DHCP snooping also generates log messages that are related to MAC-Forced Forwarding, such as when a client is added to or removed from the DHCP snooping database.

## Configuration Examples

---

For an example of how to configure the switch to perform MAC-Forced Forwarding, see *How to Use MAC-Forced Forwarding with DHCP Snooping to Create Enhanced Private VLANs*. This How To Note is available from [www.alliedtelesis.co.uk/site/solutions/techdocs.asp?area=howto](http://www.alliedtelesis.co.uk/site/solutions/techdocs.asp?area=howto).

## Command Reference

This section describes the commands available on the switch to configure MAC-Forced Forwarding.

The shortest valid command is denoted by capital letters in the Syntax section. See [“Conventions” on page xlix of About this Software Reference](#) in the front of this manual for details of the conventions used to describe command syntax. See [Appendix A, Messages](#) for a complete list of messages and their meanings.

### add macff server

**Syntax** ADD MACFF SERVER INTERface=*vlan* IPaddress=*ipadd*  
[DESCription=*desc*]

**Description** This command adds a static AR or AS entry to the DHCP snooping database. MAC-Forced Forwarding sends proxy ARP replies on behalf of devices in this database.

This command requires a user with security officer privilege when the switch is in security mode.

Parameter	Description
INTERface	The interface that the AR or AS is attached to. <i>vlan</i> is the name of a VLAN interface such as vlan46 or vlan122.
IPaddress	The IPv4 address of the AR or AS, in dotted decimal notation.
DESCription	An arbitrary description for the AR or AS. This can be between 0 to 255 characters long, and use any printable character.

**Examples** To add a new access router called “Primary DHCP Server (Asuka)” with the IP address 192.168.5.1, which is attached to vlan5, use the command:

```
add macff server int=vlan5 ip=192.168.5.1 desc="Primary DHCP  
Server (Asuka) "
```

**Related Commands** [delete macff server](#)  
[set macff server](#)  
[show macff](#)  
[show macff interface](#)



## delete macff server

**Syntax** `DELEte MACFF SERVER INTErface=vlan IPaddress=ipadd`

**Description** This command deletes a static AR or AS entry from the DHCP snooping database. The switch no longer sends proxy ARP replies on behalf of the AR or AS, and clients can no longer access the AR or AS.

This command requires a user with security officer privilege when the switch is in security mode.

Parameter	Description
INTErface	The interface that the AR or AS is attached to. <i>vlan</i> is the name of a VLAN interface such as <i>vlan46</i> or <i>vlan122</i> .
IPaddress	The IPv4 address of the AR or AS, in dotted decimal notation.

**Examples** To delete an existing application server with the IP address 192.168.5.1, which is attached to *vlan5*, use the command:

```
del macff server int=vlan5 ip=192.168.5.1
```

**Related Commands** [add macff server](#)  
[set macff server](#)  
[show macff](#)

## disable macff interface

**Syntax** `DISAbLe MACFF INTErface=vlan`

**Description** This command disables MAC-Forced Forwarding on the specified VLAN. Normal ARP behaviour recommences on this VLAN.

*vlan* is the name of a VLAN interface such as *vlan46* or *vlan122*. The specified VLAN must be a private VLAN. The switch's default interface, *vlan1*, is public and cannot have MAC-Forced Forwarding enabled (or disabled) on it.

You must disable MAC-Forced Forwarding debugging on the VLAN before you can disable MAC-Forced Forwarding for that VLAN. Use the **disable macff interface debug** command to disable any debugging.

This command requires a user with security officer privilege when the switch is in security mode.

**Examples** To disable MAC-Forced Forwarding on *vlan12*, use the command:

```
dis macff int=vlan12
```

**Related Commands** [disable macff interface debug](#)  
[enable macff interface debug](#)  
[enable macff interface](#)  
[show macff](#)

## disable macff interface debug

**Syntax** `DISable MACFF INTerface=vlan`  
`DEBug={ALL | ARP | DHCP | ERRor | PACKet | SERVER | TRAcE}`

**Description** This command disables debugging for MAC-Forced Forwarding. This command requires a user with security officer privilege when the switch is in security mode.

Parameter	Description
INTerface	The interface that debugging is disabled on. <i>vlan</i> is the name of a VLAN interface such as <i>vlan46</i> or <i>vlan122</i> .
DEBug	Entering one of the following options disables debugging of: Default: no default
ALL	All debugging options.
ARP	ARP requests made by MAC-Forced Forwarding to ARs and ASs.
DHCP	Information passed to MAC-Forced Forwarding from DHCP snooping.
ERRor	Any errors in MAC-Forced Forwarding processing.
PACKet	ARP requests processed by MAC-Forced Forwarding, and the ARP replies sent back to clients.
SERVER	The addition and removal of ARs and ASs.
TRAcE	Selected MAC-Forced Forwarding processing.

**Examples** To disable MAC-Forced Forwarding server debugging on *vlan3*, use the command:

```
dis macff int=vlan3 deb=server
```

**Related Commands** [disable macff interface](#)  
[enable macff interface debug](#)  
[enable macff interface](#)  
[show macff](#)

## enable macff interface

**Syntax** `ENAbLe MACFF INTerface=vlan`

**Description** This command enables MAC-Forced Forwarding on the specified VLAN. When a client attached to the VLAN sends an ARP request, MAC-Forced Forwarding responds by sending a proxy ARP reply on behalf of the client's AR. This prevents clients from learning the MAC addresses of other clients within their subnet, and ensures that all traffic is routed to a specific AR.

*vlan* is the name of a VLAN interface such as *vlan46* or *vlan122*. The VLAN specified must be a private VLAN. The switch's default interface, *vlan1*, is public and cannot have MAC-Forced Forwarding enabled on it.

This command requires a user with security officer privilege when the switch is in security mode.

**Examples** To enable MAC-Forced Forwarding on vlan12 use the command:

```
ena macff int=vlan12
```

**Related Commands** [disable macff interface debug](#)  
[disable macff interface](#)  
[enable macff interface debug](#)  
[show macff](#)  
[show macff interface](#)  
[show macff interface counter](#)

## enable macff interface debug

**Syntax** ENABle MACFF INTerface=*vlan*  
DEBUg={ALL | ARP | DHCP | ERRor | PACKet | SERVER | TRAcE}

**Description** This command enables debugging of MAC-Forced Forwarding on the specified VLAN. You can use debugging to find out what information is coming in on a VLAN, when a new client, AR or AS is discovered or deleted, and to do in-depth packet debugging of MAC-Forced Forwarding on your network. You can enable debugging only on one VLAN at a time.

This command requires a user with security officer privilege when the switch is in security mode.

Parameter	Description
INTerface	The VLAN that this command enables debugging on. <i>vlan</i> is the name of a VLAN interface such as vlan46 or vlan122.
DEBUg	Entering one of the following options enables debugging of: Default: no default
ALL	All debugging modes.
ARP	ARP requests made by MAC-Forced Forwarding to ARs and ASs.
DHCP	Information passed to MAC-Forced Forwarding from DHCP snooping.
ERRor	Any errors in MAC-Forced Forwarding processing.
PACKet	ARP requests processed by MAC-Forced Forwarding, and the ARP replies sent back to clients.
SERVER	The addition and removal of ARs and ASs.
TRAcE	Selected MAC-Forced Forwarding processing.

See *How to Use MAC-Forced Forwarding with DHCP Snooping to Create Enhanced Private VLANs* for examples of MAC-Forced Forwarding debug output. This How To Note is available from [www.alliedtelesis.co.uk/site/solutions/techdocs.asp?area=howto](http://www.alliedtelesis.co.uk/site/solutions/techdocs.asp?area=howto).

**Examples** To enable MAC-Forced Forwarding ARP debugging on vlan3, use the command:

```
ena macff int=vlan3 deb=arp
```

**Related Commands** [disable macff interface debug](#)  
[enable macff interface](#)  
[reset macff counter](#)  
[show macff](#)

## reset macff counter

**Syntax** RESET MACFF COUNTER [Port=*port-list*]

**Description** This command resets all the current MAC-Forced Forwarding counter information for a range of ports, or all ports.

The **port** parameter allows you to reset a subset of port counters. *port-list* is either a specific port, a range of ports using a hyphen to specify the range (*n-m*), or a comma-separated list of ports or ranges. Port numbers start at 1 and end at *m*, where *m* is the highest numbered switch Ethernet port, including uplink ports.

This command requires a user with security officer privilege when the switch is in security mode.

**Examples** To reset the MAC-Forced Forwarding counters for ports 2, 3, 4, 5 and 8, use the command:

```
res macff count po=2-5,8
```

**Related Commands**

- [disable macff interface](#)
- [enable macff interface](#)
- [show macff](#)
- [show macff interface counter](#)

## set macff server

**Syntax** SET MACFF SERVER INTERface=*vlan* IPaddress=*ipadd*  
DESCription={*desc*}

**Description** This command allows you to change the description of a statically configured AR or AS. You cannot modify the IP address or interface, as these two values are used as unique keys to permit device identification.

This command requires a user with security officer privilege when the switch is in security mode.

Parameter	Description
INTERface	The interface that the AR or AS is attached to. <i>vlan</i> is the name of a VLAN interface such as <i>vlan46</i> or <i>vlan122</i> .
IPaddress	The IPv4 address of the AR or AS, in dotted decimal notation.
DESCription	An arbitrary description for the AR or AS. This can be between 0 to 255 characters long, and use any printable character. Leaving the option blank removes the current description without adding a new description.

**Examples** To set the description of an AR with the IP address 192.168.5.2, which is attached to *vlan5*, to "Main LAN Gateway (Eva)", use the command:

```
set macff serv int=vlan5 ip=192.168.5.2 desc="Main LAN  
Gateway (Eva)"
```

To remove the description of an AS with the IP address 192.168.5.3, which is attached to *vlan7*, use the command:

```
set macff serv int=vlan7 ip=192.168.5.3 desc=
```

**Related Commands** [add macff server](#)  
[delete macff server](#)

## show macff

**Syntax** SHow MACFF [COUnTer]

**Description** This command displays a summary of the VLANs with MAC-Forced Forwarding enabled on them, and MAC-Forced Forwarding status details (Figure 16-2, Figure 16-3, Table 16-1 on page 16-14). The **counter** parameter displays the combined counters for all VLANs, and counters for server activity on all VLANs.

Figure 16-2: Example output from the **show macff** command

```
MAC Forced Forwarding Information:
-----
VLAN Interface          Dbg IP Address      State    Servers
-----
vlan2                   <*> 20.1.1.1        ENABLED   6
vlan3                   30.1.1.1           ENABLED   0
vlan6                   -                   ENABLED   0
-----
```

Figure 16-3: Example output from the **show macff counter** command

```
MAC Forced Forwarding Information:
-----
VLAN Interface          Dbg IP Address      State    Servers
-----
vlan2                   <*> 20.1.1.1        ENABLED   6
vlan3                   30.1.1.1           ENABLED   0
vlan6                   -                   ENABLED   0

Overall Status:
Number of Servers ..... 6
Servers Lost ..... 0

ARP Counters( All Ports ):
ARP Counters:
Requests ..... 2301   Replies ..... 0
Resolution Request ..... 48   Resolutions Failed ..... 43
Src : No DHCP SN ENTRY .... 42   Src : Inconsistent Data .. 0
Src : No Routers ..... 1   Src : No Routers Found ... 0
Dest: No DHCP SN ENTRY .... 0   S/D : Same Port ..... 0

Server Counter:
ARP Resolution Requests .. 345   ARP Resolutions ..... 0
ARP Resolutions Failed ... 345   ARP Still Valid ..... 0
Static Add ..... 0   Static Delete ..... 0
Dynamic Add ..... 0   Dynamic Delete ..... 0
Dynamic Update Add ..... 0   Dynamic Update Delete .... 0
Dynamic Update: No New ... 0   Static Add Fail ..... 0
Dynamic Add Fail ..... 0   Static Delete Fail ..... 0
Dynamic Delete Fail ..... 0
-----
```

Table 16-1: Parameters in the output of the **show macff [counter]** command

Parameter	Meaning
VLAN Interface	The VLAN for which MAC-Forced Forwarding information is displayed.
Dbg	Whether debugging is currently executing on the VLAN; "<*>" indicates yes, a blank space indicates no.
IP Address	Current IP address assigned to the specified VLAN.
State	Whether MAC-Forced Forwarding is enabled on the VLAN.
Servers	Number of active ARs and ASs configured on the VLAN. This includes both statically defined and dynamically found devices.
<b>Overall Status</b>	
Number of Servers	Number of ARs and ASs currently in the DHCP snooping database.
Servers Lost	Number of ARs and ASs that have been deleted or lost, and have been removed from the DHCP snooping database.
<b>ARP Counters (All Ports)</b>	
Requests	Number of ARP Requests received by MAC-Forced Forwarding.
Replies	Number of ARP Replies that MAC-Forced Forwarding has sent on behalf of an AR or AS.
Resolution Requests	Number of ARP resolution Requests for an AR or AS that required MAC address resolution.
Resolutions Failed	Number of ARP Requests that failed to determine the MAC address of the AR or AS.
Src : No DHCPSPN Entry	Number of ARP requests where the source client is not in the DHCP snooping database.
Src : Inconsistent Data	Number of ARP requests where the source client information in the DHCP snooping database does not match the source client information in the ARP request.
Src : No Routers	Number of ARP requests where the source client does not have a valid AR in the DHCP snooping database.
Src : No Routers Found	Number of ARP requests where MAC-Forced Forwarding could not contact any of the valid ARs for that client.
Dest : No DNCPSN Entry	Number of ARP requests between clients within a subnet where the destination client is not in the DHCP snooping database. The switch drops these requests.
S/D : Same Port	Number of ARP requests where the source and destination clients are on the same port (within a private network). The switch drops these requests.
<b>Server Counter</b>	
ARP Resolution Requests	Number of ARP resolution requests received for an AR or AS.
ARP Resolutions	Number of ARP resolution requests that MAC-Forced Forwarding successfully replied to.
ARP Resolutions Failed	Number of ARP resolution requests where MAC-Forced Forwarding was unable to reply with the MAC address of a valid AR or AS.

Table 16-1: Parameters in the output of the **show macff [counter]** command (cont.)

Parameter	Meaning
ARP Still Valid	Number of ARP resolution requests where the correct details for the AR or AS are already in the DHCP snooping database.
Static Add	Number of entries in the DHCP snooping database that were added using <b>add macff server</b> .
Static Delete	Number of entries in the DHCP snooping database that were removed using <b>delete macff server</b> .
Dynamic Add	Number of entries in the DHCP snooping database that DHCP snooping has dynamically added.
Dynamic Delete	Number of entries in the DHCP snooping database that DHCP snooping has dynamically deleted.
Dynamic Update Add	Number of entries in the DHCP snooping database that DHCP snooping added after its dynamic updating process.
Dynamic Update Delete	Number of entries in the DHCP snooping database that DHCP snooping deleted after its dynamic updating process.
Dynamic Update: No New	Number of times that all the valid servers associated with a client were removed from the DHCP snooping database after the DHCP snooping update process.
Static Add Fail	Number of times a static entry attempt failed to add an entry to the DHCP snooping database.
Dynamic Add Fail	Number of times DHCP snooping attempted and failed to add an entry to the DHCP snooping database.
Static Delete Fail	Number of times a static entry attempt failed to delete an entry from the DHCP snooping database.
Dynamic Delete Fail	Number of times DHCP snooping attempted and failed to delete an entry from the DHCP snooping database.

**Example** To display summary details for VLANs using MAC-Forced Forwarding, use the command:

```
sh macff
```

**Related Commands** [show macff interface](#)  
[show macff interface counter](#)

## show macff database

**Syntax** SHOW MACFF DATABASE

**Description** This command displays a detailed list of the ARs and ASs held in the DHCP snooping database (Figure 16-4, Table 16-2).

Figure 16-4: Example output from the **show macff database** command

```
Vlan ..... vlan2
IP Address ..... 82.20.54.1
Description ..... DHCP Server (Nerv)
MAC Address ..... 00-00-04-01-16-13
Server type ..... Static, Dynamic(4)

Vlan ..... vlan2
IP Address ..... 82.20.54.2
Description ..... Main LAN Gateway (EVA)
MAC Address ..... -
Server type ..... Static

Vlan ..... vlan3
IP Address ..... 82.20.57.4
Description ..... -
MAC Address ..... 00-00-cd-23-b3-03
Server type ..... Dynamic(2)

Vlan ..... vlan3
IP Address ..... 82.20.57.7
Description ..... -
MAC Address ..... -
Server type ..... Dynamic(4)

Vlan ..... vlan3
IP Address ..... 82.20.57.12
Description ..... Second Unit (Asuka)
MAC Address ..... 00-22-53-20-ba-12
Server type ..... Static, Dynamic(2)
```

Table 16-2: Parameters in the output of the **show macff database** command

Parameter	Meaning
Vlan	VLAN interface to which the AR or AS is attached.
IP Address	IP address of the AR or AS.
Description	Description given to a statically defined AR or AS, as set with the <b>add macff server</b> and <b>set macff server</b> commands. A "-" is shown for dynamically defined entries, or static entries without a description.
MAC Address	MAC address of the AR or AS.
Server type	How the EAN knows of the AR or AS. "Dynamic" means that DHCP snooping added the AR. The number in brackets is the number of DHCP snooping clients that can access this AR. "Static" means the AR or AS was statically defined using the <b>add macff server</b> command. "Static" and "Dynamic" are both displayed when DHCP snooping has discovered an AR that is also statically defined. Dynamic AR entries remain in the database until there are no clients in the database that are allowed to access this AR.



**Example** To display the list of servers that the DHCP snooping database currently holds, use the command:

```
sh macff datab
```

**Related Commands**

- [add macff server](#)
- [delete macff server](#)
- [set macff server](#)
- [show macff interface](#)
- [show macff interface counter](#)

## show macff interface

**Syntax** SHow MACFF INTerface=*vlan*

**Description** This command displays the current status of MAC-Forced Forwarding on the specified VLAN (Figure 16-5, Table 16-3). *vlan* is the name of a VLAN interface such as vlan46 or vlan122.

Figure 16-5: Example output from the **show macff interface** command

```
MAC Forced Forwarding Information:
-----
Interface ..... vlan2
Status ..... ENABLED
IP address..... 20.1.1.1
Ports:
  Tagged ..... None
  Untagged ..... 2,22
Active servers ..... 6
Debugging ..... ALL - ARP, DHCP, PACKET, TRACE, SERVER, ERROR

Upstream Servers:

IP Address ..... 82.20.54.1
Description ..... Default Gateway (Shojun)
MAC Address ..... 00-00-04-01-16-13
Server type ..... Static

IP Address ..... 82.20.57.4
Description ..... -
MAC Address ..... 00-00-cd-23-b3-04
Server type ..... Dynamic(2)
-----
```

Table 16-3: Parameters in the output of the **show macff interface** command

Parameter	Meaning
Interface	VLAN interface on which MAC-Forced Forwarding is configured.
Status	Whether MAC-Forced Forwarding is enabled on the VLAN.
IP Address	IP address assigned to the VLAN.
Ports: Tagged	The tagged ports assigned to the VLAN; tagged ports transmit VLAN tagged frames.
Ports: Untagged	The untagged ports assigned to the VLAN; untagged ports transmit frames without VLAN tags.

Table 16-3: Parameters in the output of the **show macff interface** command (cont.)

Parameter	Meaning
Active Servers	Number of ARs and ASs in use by clients on this VLAN.
Debugging	Debugging modes that are enabled on the VLAN.
<b>Upstream Servers</b>	Lists the active ARs and ASs for this VLAN.
IP Address	IP address of the AR or AS attached to this VLAN.
Description	Description of the AR or AS, if it has been statically defined using the <b>add macff server</b> or <b>set macff server</b> commands.
MAC Address	MAC address of the AR or AS.
Server Type	How the EAM knows of the AR or AS. <p>“Dynamic” means that DHCP snooping added the AR. The number in brackets is the number of DHCP snooping clients that can access this AR.</p> <p>“Static” means the AR or AS was statically defined using the <b>add macff server</b> command.</p> <p>“Static” and “Dynamic” are both displayed when DHCP snooping has discovered an AR that is also statically defined. Dynamic AR entries remain in the database until there are no clients in the database that are allowed to access this AR.</p>

**Example** To see the current status of MAC-Forced Forwarding on vlan5, such as which debugging options are enabled, use the command:

```
sh macff int=vlan5
```

**Related Commands**

- [add macff server](#)
- [delete macff server](#)
- [disable macff interface](#)
- [enable macff interface](#)
- [set macff server](#)
- [show macff](#)
- [show macff interface counter](#)

## show macff interface counter

**Syntax** `SHoW MACFF INTeRface=vlan [POrt=port-list] COUNTeR`

**Description** This command displays MAC-Forced Forwarding counters for each port on an VLAN (Figure 16-6, Table 16-4).

The **port** parameter allows you to select only a subset of ports to display information about. *port-list* is either a specific port, a range of ports using a hyphen to specify the range (n-m), or a comma-separated list of ports or port ranges. Port numbers start at 1 and end at m, where m is the highest numbered switch Ethernet port, including uplink ports.

Figure 16-6: Example output from the **show macff interface counter** command

```
MAC Forced Forwarding Information:
-----
Interface ..... vlan2
Status ..... ENABLED
IP address..... 20.1.1.1
Ports:
  Tagged ..... None
  Untagged ..... 2,22
Active servers ..... 6
Debugging ..... NONE

Counters for Port: 2
ARP Counters:
  Requests ..... 2301    Replies ..... 0
  Resolution Request ..... 48    Resolutions Failed ..... 43
  Src : No DHCP SN ENTRY .... 42    Scr : Inconsistent Data .. 0
  Src : No Routers ..... 1    Scr : No Routers Found ... 0
  Dest: No DHCP SN ENTRY .... 0    S/D : Same Port ..... 0

Counters for Port: 22
ARP Counters:
  Requests ..... 1    Replies ..... 0
  Resolution Request ..... 8    Resolutions Failed ..... 0
  Src : No DHCP SN ENTRY .... 2    Scr : Inconsistent Data .. 0
  Src : No Routers ..... 0    Scr : No Routers Found ... 0
  Dest: No DHCP SN ENTRY .... 0    S/D : Same Port ..... 0
-----
```

Table 16-4: Parameters in the output of the **show macff interface counter** command

Parameter	Meaning
Interface	VLAN that MAC-Forced Forwarding is configured on.
Status	Whether MAC-Forced Forwarding is enabled on the VLAN.
IP Address	IP address assigned to the VLAN.
Ports: Tagged	The tagged ports assigned to the VLAN; tagged ports transmit VLAN tagged frames.
Ports: Untagged	The untagged ports assigned to the VLAN; untagged ports transmit frames without VLAN tags.
Active Servers	Number of ARs and ASs in use by clients on this VLAN.
Debugging	Debugging modes that are enabled on the VLAN.
Counters for Port:	Specific port that the counters are for.

Table 16-4: Parameters in the output of the **show macff interface counter** command (cont.)

Parameter	Meaning
<b>ARP Counters</b>	
Requests	Number of ARP Requests received by MAC-Forced Forwarding from clients on this port.
Replies	Number of ARP Replies that MAC-Forced Forwarding has sent to clients on this port on behalf of an AR or AS.
Resolution Requests	Number of ARP Resolution Requests from clients on this port for an AR or AS that required MAC address resolution.
Resolutions Failed	Number of ARP Requests from clients on this port that failed to determine the MAC address of the AR or AS.
Src : No DHCP SN Entry	Number of ARP requests from clients on this port, where the source client is not in the DHCP snooping database.
Src : Inconsistent Data	Number of ARP requests from clients on this port where the source client information in the DHCP snooping database does not match the source client information in the ARP request.
Src : No Routers	Number of ARP requests from clients on this port where the source client does not have a valid AR in the DHCP snooping database.
Src : No Routers Found	Number of ARP requests from clients on this port where MAC-Forced Forwarding could not contact any of the valid ARs for that client.
Dest : No DNCP SN Entry	Number of ARP requests sent from clients on this port to another client within the same subnet, where the destination client is not in the DHCP snooping database. The switch drops these requests.
S/D : Same Port	Number of ARP requests from clients on this port where the source and destination clients are on the same port (within a private network). The switch drops these requests.

**Example** To see the counters for ports 2 to 10, 14 and 18, on vlan5 use the command:

```
sh macff int=vlan5 po=2-10,14,18
```

**Related Commands**

- [disable macff interface](#)
- [enable macff interface](#)
- [reset macff counter](#)
- [show macff](#)
- [show macff interface](#)