How To | Use MAC-Forced Forwarding with DHCP Snooping to Create Enhanced Private VLANs

Introduction

In a large network where internal users cannot be trusted, it is nearly impossible to stop a host from seeing network traffic that is destined for other hosts. This is especially difficult with layer 2 switches. Some of the major security problems in layer 2 networks occur because switches (by default):

- send broadcasts to all ports in a VLAN
- flood traffic when the switch cannot find the layer 2 destination
- permit any inter-host communication within a VLAN
- cannot determine who is, or is not, allowed to access the physical media

MAC-forced forwarding, in conjunction with private VLANs and DHCP snooping, gives you full control of these issues.

This How To document describes how to set up a Triple Play network, which could be used by a service provider who offers TV, internet and VoIP telephony. It features:

- MAC-Forced Forwarding (MACFF) on edge switches to send all traffic to one Access Router
- DHCP snooping to facilitate MACFF, validate per-user access, and add option 82 information to DHCP requests
- hardware filters on the Access Router for granular VLAN control

  The VLAN control allows VoIP phone calls between hosts in the network, but does not allow any other inter-host communication. Hosts cannot snoop on other hosts' TV, movies or data
- IGMP filtering to stop hosts from joining groups that they are not entitled to belong to
- a DHCP server on the Access Router, to serve the edge network
- Residential Gateways (RGs) at customer sites

Careful consideration of the network design is critical, but each aspect of the configuration is not overly complex.

What information will you find in this document?

This How To Note begins with essential background information, in the following section:

Then it describes the configuration, in the following sections:

Then it describes how to troubleshoot the configuration, in the following sections:

Which products and software version does this document apply to?

MAC-forced forwarding is available on Rapier i, AT-8800, AT-8700XL, AT-8600, AT-8900, AT-9900, and x900-48 Series switches, running Software Version 2.9.1 or later. However, other aspects of this example determine which products the example applies to.

This example gives configuration details for:

- 3 edge switches
- 1 Access Router
- 3 residential gateways

Edge switches

The edge switches use private VLANs as well as MACFF, and both uplink ports on each edge switch belong to the private VLAN (as uplinks). Therefore, each edge switch must support this combination of features, which means you can use any of the following switches:

- Rapier 16fi and Rapier 24i (but not Rapier 48i)
- AT-8724XL (but not AT-8748XL)
- AT-8824 and AT-8848
- AT-8624T/2M, AT-8624PoE, and AT-8648T/2SP

We used AT-8848 switches.

While AT-8948, AT-9900, and x900-48 Series switches support MACFF and private VLANs, they can only have one uplink (a port or trunk group) per private VLAN. This means they cannot be used as edge switches in this example, although they would work in configurations that did not have a ring of edge switches.

Access Router

In this example, the Access Router needs to support advanced hardware filtering, as well as providing WAN links. Therefore, we used a Rapier 24i.

Residential gateways

For the residential gateways, we used AT-RG613TX RGs.

Servers

We used a single server machine for both the SIP server and multicast server. The SIP server software was partysip. The multicast server software was VLC. This document does not describe how to configure these servers; instead detailed instructions are available at www.partysip.org and www.videolan.org.

How this solution provides security

This solution uses a number of features to provide security:

- private VLANs prevent hosts on the same switch from talking to each other
- DHCP snooping ensures that the processes of DHCP—Discover, Offer, Request and ACK—are only seen by the untrusted host, the DHCP server, and the network devices between them
- MACFF intercepts ARP packets on untrusted ports and ensures that these broadcasts are never forwarded
- the combination of DHCP snooping and MACFF extends the private VLANs across switches
- the Access Router controls the inter-host communication. You can control this to a highly granular level

How MAC-forced forwarding works

MAC-forced forwarding is suitable for Ethernet networks where a layer 2 bridging device, known as an Ethernet Access Node (EAN), connects Access Routers to their clients. MACFF is configured on the EANs.

The Allied Telesis implementation of MAC-forced forwarding is based on the concept described in RFC 4562, *MAC-Forced Forwarding: A Method for Subscriber Separation on an Ethernet Access Network*.

The Allied Telesis implementation uses DHCP snooping to maintain a database of the hosts that appear on each switch port. When a host tries to access the network through a switch port, DHCP snooping checks the host’s IP address against the database to ensure that the host is valid.

MACFF then uses DHCP snooping to check whether the host has a gateway Access Router. If it does, MACFF uses a form of proxy ARP to reply to any ARP requests, giving the router's MAC address. This forces the host to send all traffic to the router, even traffic destined to a host in the same subnet as the source. The router receives the traffic and makes forwarding decisions based on a set of forwarding rules, typically a QoS policy or a set of filters.

Note that this implementation requires you to disable ICMP redirection on the Access Router.

The DHCP snooping database

The following figure shows an example of the DHCP snooping database. Observe that four entries exist in the “Current valid entries” section, one of which is for host 172.16.3.200 (shown in **bold**). If this host sends an ARP request, DHCP snooping checks its database for an entry for this host. The entry exists, so DHCP snooping passes the ARP request to MACFF.

```
Manager Edge Switch 1> show dhcpsnooping database

DHCP Snooping Binding Database
-------------------------------------------------------------------------------
Full Leases/Max Leases ... 4/55
Check Interval ........... 30 seconds
Database Listeners ....... CLASSIFIER
                           MACFF

Current valid entries
MAC Address        IP Address       Expires(s)  VLAN  Port       ID     Source
-------------------------------------------------------------------------------
00-0d-da-00-0b-11  172.16.1.201     3790        100   15         2      Dynamic
00-0e-2e-7d-4b-40  172.16.2.202     1935        200   15         11     Dynamic
00-0e-2e-65-05-17  172.16.3.200     180         300   15         12     Dynamic
00-0d-da-00-0b-11  172.16.4.201     Static      400   15         1      User
-------------------------------------------------------------------------------
.
.
.
```

MACFF uses information in the DHCP snooping database to determine how to reply to the ARP request. So when MACFF receives an ARP request from host 172.16.3.200, it checks the database and finds an entry for the host's router (shown in **bold** in the following figure). Therefore, it returns the router’s MAC (00-00-cd-11-79-a0) in an ARP reply.

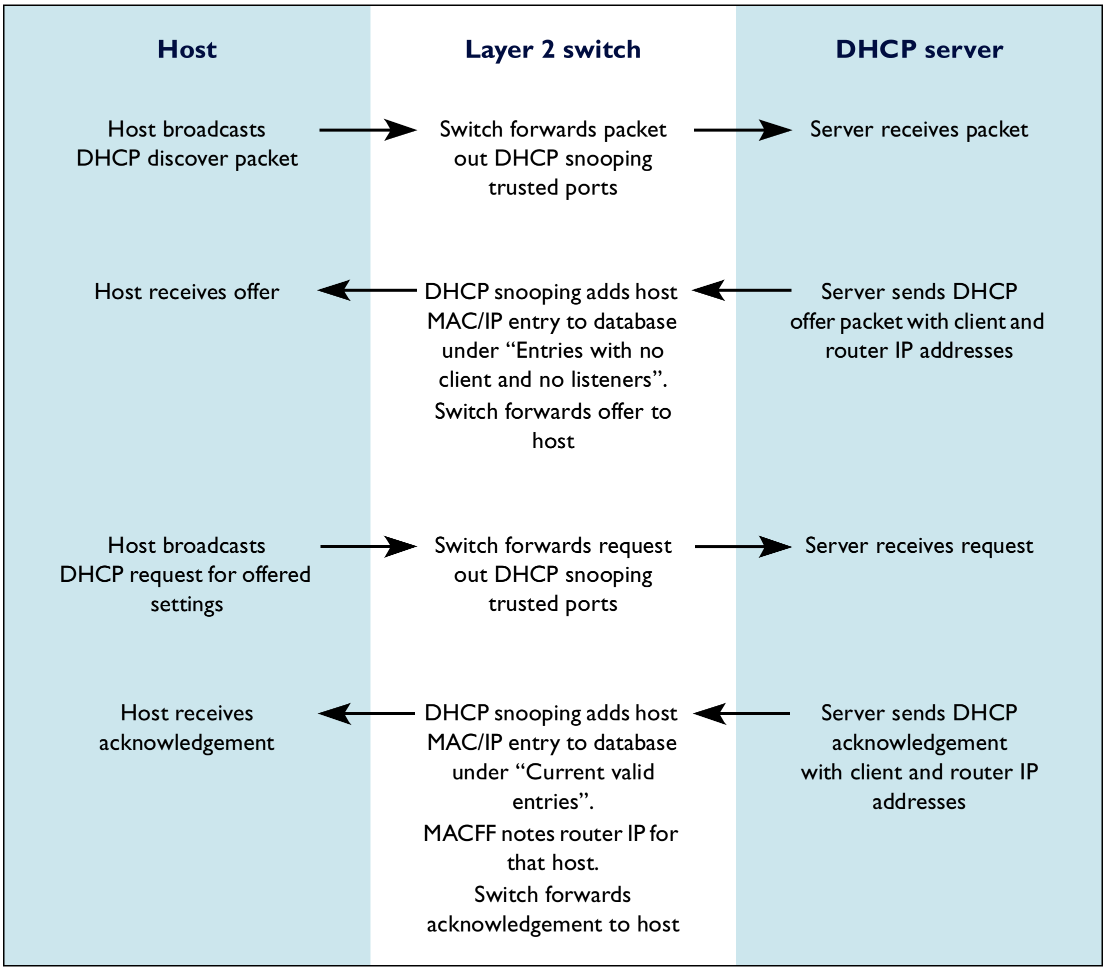
```
Manager Edge Switch 1> show macff database

Vlan ................... Voice
IP Address ............. 172.16.1.254
Description ............ -
MAC Address ............ 00-00-cd-11-79-a0
Server Type ............ Dynamic(1)

Vlan ................... Data
IP Address ............. 172.16.3.254
Description ............ -
MAC Address ............ 00-00-cd-11-79-a0
Server Type ............ Dynamic(1)
.
.
.
```

Populating the database

DHCP snooping adds address entries to its database when:

- you configure the entry manually through a DHCP snooping binding entry. For an example of how to do this, see Step 9 on page 13
- a host uses DHCP to obtain an IP address. MACFF monitors DHCP acknowledgements (ACK packets) for gateway Access Router information and records that information. For details of this process, see the following figure

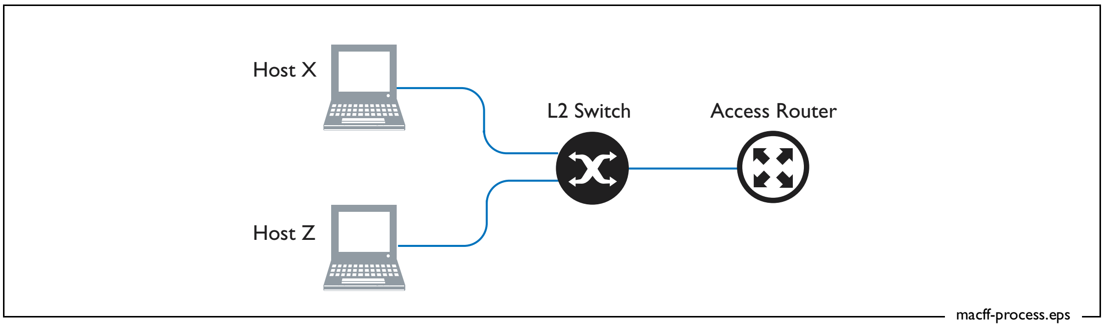
The following figure shows one of the process flows for learning through DHCP. Note that the actual DHCP messages exchanged depends on the host's initial IP settings.



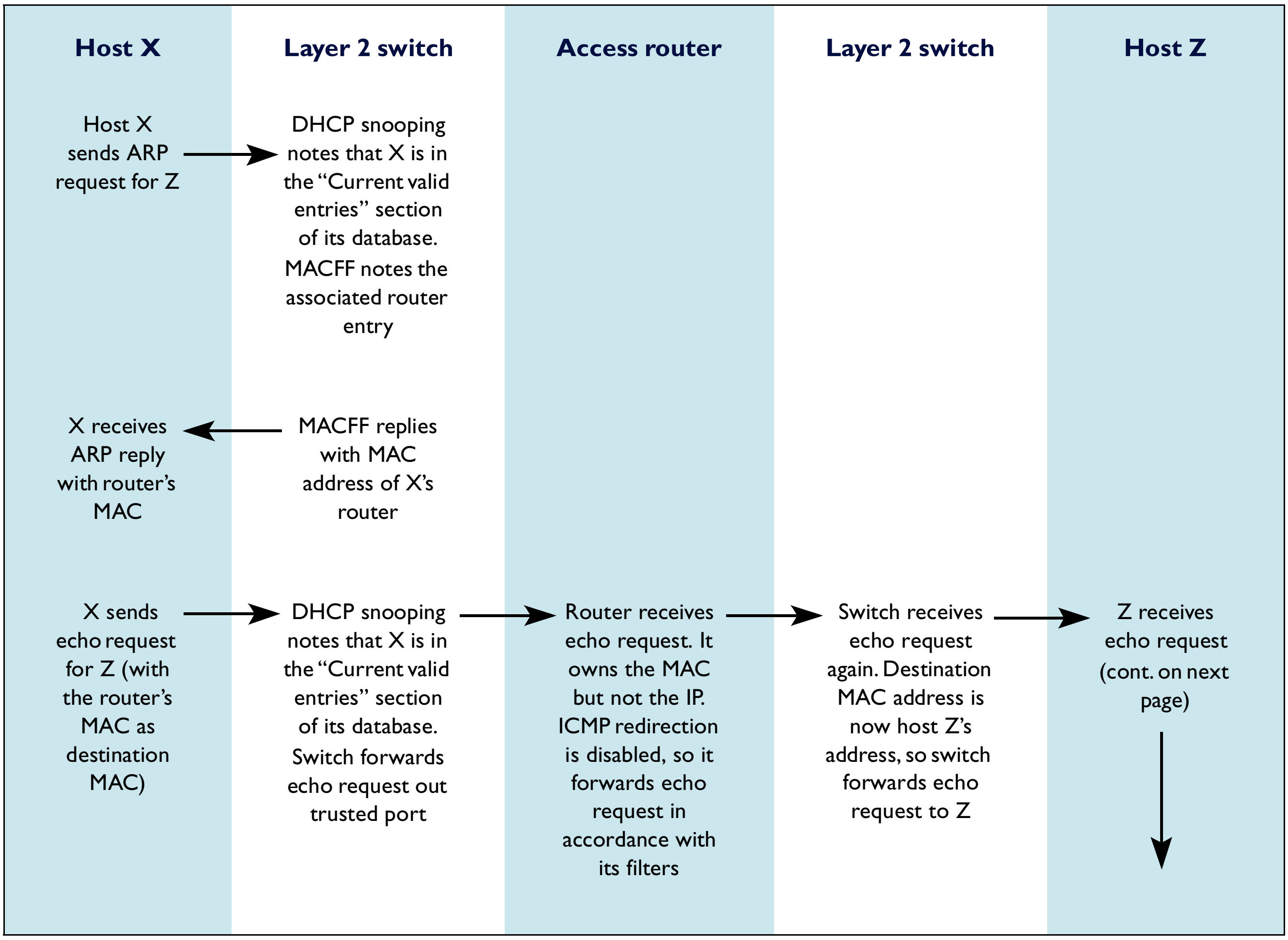
Host		Layer 2 switch		DHCP server
Host broadcasts DHCP discover packet	→	Switch forwards packet out DHCP snooping trusted ports	→	Server receives packet
Host receives offer	←	DHCP snooping adds host MAC/IP entry to database under "Entries with no client and no listeners". Switch forwards offer to host	←	Server sends DHCP offer packet with client and router IP addresses
Host broadcasts DHCP request for offered settings	→	Switch forwards request out DHCP snooping trusted ports	→	Server receives request
Host receives acknowledgement	←	DHCP snooping adds host MAC/IP entry to database under "Current valid entries". MACFF notes router IP for that host. Switch forwards acknowledgement to host	←	Server sends DHCP acknowledgement with client and router IP addresses

The process for MAC-forced forwarding

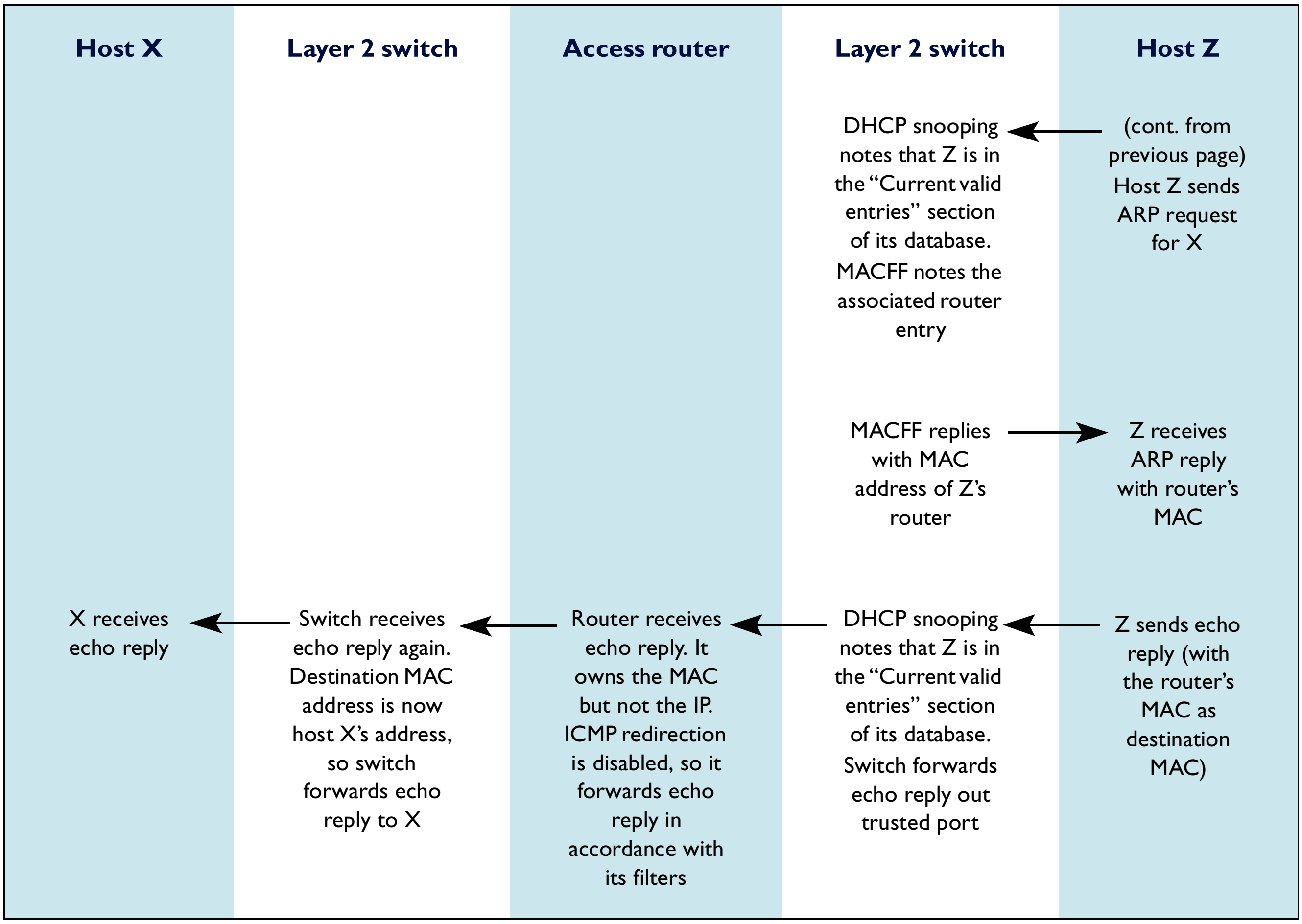
Once DHCP snooping has learned the router for a given host, MACFF can force frames from that host to go to the desired router. To illustrate this process, consider the following simple network.



The following figure shows the process flow when host X pings host Z. MACFF already knows about both hosts.



Host X	Layer 2 switch	Access router	Layer 2 switch	Host Z
Host X sends ARP request for Z →	DHCP snooping notes that X is in the "Current valid entries" section of its database. MACFF notes the associated router entry			
X receives ARP reply with router's MAC	← MACFF replies with MAC address of X's router			
X sends echo request for Z (with the router's MAC as destination MAC) →	DHCP snooping notes that X is in the "Current valid entries" section of its database. Switch forwards echo request out trusted port →	Router receives echo request. It owns the MAC but not the IP. ICMP redirection is disabled, so it forwards echo request in accordance with its filters →	Switch receives echo request again. Destination MAC address is now host Z's address, so switch forwards echo request to Z →	Z receives echo request (cont. on next page) ↓



Host X

Layer 2 switch

Access router

Layer 2 switch

Host Z

(cont. from previous page) Host Z sends ARP request for X

DHCP snooping notes that Z is in the "Current valid entries" section of its database. MACFF notes the associated router entry

MACFF replies with MAC address of Z's router

Z receives ARP reply with router's MAC

Z sends echo reply (with the router's MAC as destination MAC)

DHCP snooping notes that Z is in the "Current valid entries" section of its database. Switch forwards echo reply out trusted port

Router receives echo reply. It owns the MAC but not the IP. ICMP redirection is disabled, so it forwards echo reply in accordance with its filters

Switch receives echo reply again. Destination MAC address is now host X's address, so switch forwards echo reply to X

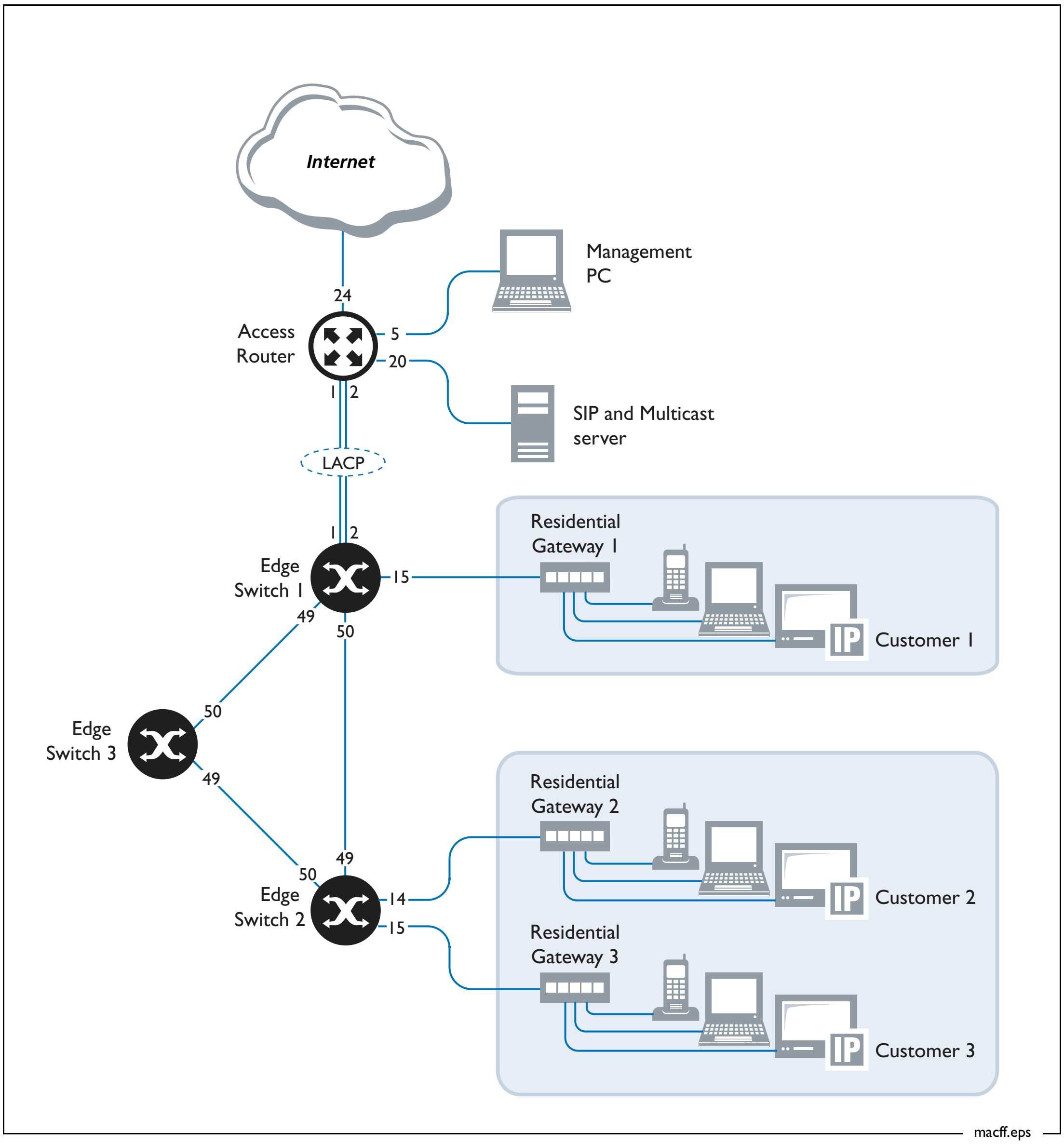
X receives echo reply

Overview of the example

In this example, three customers connect through residential gateways to a ring of edge switches, which act as layer 2 EANs. The ring connects to an Access Router, which connects to a server for voice and video, a management PC, and the Internet.

The network has redundancy through the layer 2 switch ring and through LACP (trunked ports) between edge switch 1 and the Access Router. However, the Access Router and switch 1 are both single points of failure.

The following figure shows the network configuration.



macff.eps

There are six VLANs:

- vlan28—for the servers and Internet access port. This VLAN only occurs on the Access Router, not the edge switches
- vlan100—for voice traffic
- vlan200—for video traffic such as TV and movies
- vlan300—for data and the Internet
- vlan400—for management of the residential gateways
- vlan500—for management of the Access Router and the EAN of edge switches

The residential gateways and the switches may be managed by different people, so this configuration puts them in different VLANs for security reasons.

On the edge switches, all the VLANs are private VLANs and MACFF pushes traffic from each switch up to the Access Router. On the Access Router, classifiers and hardware filters enforce the communication policy described in the following table.

Hosts in...	Cannot talk to hosts in...	Can talk to...
vlan100	vlan200, vlan300, vlan400, vlan500	Other hosts in vlan100, and Hosts outside the EAN domain, such as vlan28 for the SIP server
vlan200	vlan100, vlan200, vlan300, vlan400, vlan500	Hosts outside the EAN domain, such as vlan28 for the multicast server
vlan300	vlan100, vlan200, vlan300, vlan400, vlan500	Hosts outside the EAN domain, such as vlan28 and the Internet
vlan400	vlan100, vlan200, vlan300, vlan400, vlan500	The management PC 172.16.5.250 Hosts outside the EAN domain
vlan500	vlan100, vlan200, vlan300, vlan400, vlan500	The management PC 172.16.5.250 Hosts outside the EAN domain

This example only controls traffic flow within and between the VLANs in the table above. The configuration allows traffic to and from hosts outside these VLANs. For example, all hosts can talk to hosts in vlan28. If your network requires more controls than this, you can use the methods in this How To Note to configure this.

To configure this example, follow the steps in the following sections:

- "How to configure the edge switches" on page 11
  - "Configure edge switch 1" on page 11
  - "Configure edge switch 2" on page 14
  - "Configure edge switch 3" on page 16
- "How to configure the Access Router" on page 17
- "How to configure the residential gateways" on page 22
  - "Configure residential gateway 1" on page 23
  - "Configure residential gateway 2" on page 25
  - "Configure residential gateway 3" on page 26

How to configure the edge switches

This section describes how to configure edge switch 1 in detail. Then it gives the configurations for edge switches 2 and 3, highlighting the differences between them and switch 1.

Configure edge switch 1

Edge switch 1 is directly connected to the Access Router.

1. Name the switch

Give the switch a name to appear at the command prompt, by using the command:

```
set system name="Edge Switch 1"
```

2. Create the VLANs

The five VLANs are all private VLANs. Create them by using the commands:

```
create vlan=Voice vid=100 private

create vlan=Video vid=200 private

create vlan=Data vid=300 private

create vlan=Management vid=400 private

create vlan=EAN_Management vid=500 private
```

3. Configure spanning tree

Spanning tree prevents loops in the ring. Enable it by using the commands:

```
enable stp=default

set stp=default mode=rapid
```

4. Add ports to the private VLANs

Private VLANs have uplink and private ports. This switch has four uplink ports: ports 1 and 2, which are the LACP connection to the Access Router, and ports 49 and 50, which connect to the neighbouring switches. The private port (port 15) connects to the residential gateway.

Add the ports by using the commands:

```
add vlan=100 port=1-2,49-50 uplink frame=tagged
add vlan=100 port=15 frame=tagged
add vlan=200 port=1-2,49-50 uplink frame=tagged
add vlan=200 port=15 frame=tagged
add vlan=300 port=1-2,49-50 uplink frame=tagged
add vlan=300 port=15 frame=tagged
add vlan=400 port=1-2,49-50 uplink frame=tagged
add vlan=400 port=15 frame=tagged
add vlan=500 port=1-2,49-50 uplink frame=tagged
```

5. Specify the ports that do not connect to a switch

Hosts connect more quickly initially when STP knows which ports do not have a switch connected to them—in other words, which ports are edge ports. Set this by using the command:

```
set stp=default port=3-48 edgeport=yes
```

6. Enable DHCP snooping

Enable DHCP snooping, ARP security and (if desired) option 82, by using the commands:

```
enable dhcpsnooping
enable dhcpsnooping arpsecurity
enable dhcpsnooping option82
```

ARP security ensures that ARP packets received on untrusted ports are only forwarded if they originate from an IP in the DHCP snooping database of current valid entries.

In this example we have enabled option 82 because you may choose to use a DHCP server that supports the logging of option 82 information. This example uses the DHCP server on the Rapier i switch, which does not log option 82 information.

7. Specify the trusted ports

Private VLAN uplink ports need to be trusted ports, so that they can forward DHCP packets. Ports that are connected to hosts need to be untrusted ports. The default state is untrusted, so specify the trusted ports by using the commands:

```
set dhcpsnooping port=1 trusted=yes

set dhcpsnooping port=2 trusted=yes

set dhcpsnooping port=49 trusted=yes

set dhcpsnooping port=50 trusted=yes
```

8. Set the number of leases on the port that connects the residential gateway

A residential gateway is connected to port 15, so multiple IP addresses will appear on that port. In this example, the RG has separate IP addresses for the Voice, Video, Data, and Management VLANs. Therefore, set the maximum allowed number to 4 by using the command:

```
set dhcpsnooping port=15 maxleases=4
```

9. Specify the static IP of the residential gateway

DHCP Snooping must be told about any static IP addresses, because it cannot learn them through DHCP. In this example, the residential gateway connected to port 15 has a static management IP address of 172.16.4.201 on VLAN400. Specify this static binding by using the command:

```
add dhcpsnooping binding=00-0d-da-00-0b-11 ip=172.16.4.201
  interface=vlan400 port=15 router=172.16.4.254
```

This static lease uses one port lease out of the maximum number of leases (which you specified in the previous step).

Other solutions could have a static IP address on the Voice VLAN, for example. If so, you would also need to bind that IP address.

10. Add a remote management IP address

Add an IP to vlan500 for remote management purposes, by using the commands:

```
enable ip

add ip int=vlan500 ip=172.16.5.101 mask=255.255.255.0
```

11. Enable MAC-forced forwarding

Enable MAC-forced forwarding on all VLANs by using the commands:

```
enable macff int=vlan100

enable macff int=vlan200

enable macff int=vlan300

enable macff int=vlan400

enable macff int=vlan500
```

12. Configure LACP

LACP sets up a dynamic trunk between the Access Router and this switch. By default, it operates on all ports unless you specifically remove ports from the LACP configuration. In this example, ports 1 and 2 connect this switch to the Access Router, and for security reasons we recommend removing the other ports.

Remove the unwanted ports from the trunk and enable LACP, by using the commands:

```
delete lacp port=3-50

enable lacp
```

13. Save the configuration

Save the configuration and set the switch to use it on start-up, by using the command:

```
create config=macffedge1.cfg set
```

Configure edge switch 2

Edge switch 2 is connected to port 50 of edge switch 1. The configuration is similar to edge switch 1, except that:

- the name is different
- there are two uplink ports—to switches 1 and 3—instead of the four on switch 1. This changes the VLAN configuration and the STP edge ports and means LACP is not needed
- two residential gateways are connected to switch 2 so the configuration includes their ports, and adds static bindings for them for DHCP snooping
- the management IP address is different

The configuration for switch 2 follows, with these differences in **bold**:

```
# System configuration
set system name="Edge Switch 2"

# VLAN general configuration
create vlan=Voice vid=100 private
create vlan=Video vid=200 private
create vlan=Data vid=300 private
create vlan=Management vid=400 private
create vlan=EAN_Management vid=500 private

# STP general configuration
enable stp=default
set stp=default mode=rapid

# VLAN port configuration
# ports 1 and 2 are not in any VLANs
add vlan=100 port=49-50 uplink frame=tagged
add vlan=100 port=15 frame=tagged
add vlan=100 port=14 frame=tagged
add vlan=200 port=49-50 uplink frame=tagged
add vlan=200 port=15 frame=tagged
add vlan=200 port=14 frame=tagged
add vlan=300 port=49-50 uplink frame=tagged
add vlan=300 port=15 frame=tagged
add vlan=300 port=14 frame=tagged
add vlan=400 port=49-50 uplink frame=tagged
add vlan=400 port=15 frame=tagged
add vlan=400 port=14 frame=tagged
add vlan=500 port=49-50 uplink frame=tagged

# STP port configuration
set stp="default" port=1-48 edgeport=yes

# DHCP Snooping configuration
enable dhcpsnooping
enable dhcpsnooping arpsecurity
enable dhcpsnooping option82
set dhcpsnooping port=14 maxleases=4
set dhcpsnooping port=15 maxleases=4
set dhcpsnooping port=49 trusted=yes
set dhcpsnooping port=50 trusted=yes
add dhcpsnooping binding=00-0d-da-00-00-37 ip=172.16.4.202 interface=vlan400
port=14 router=172.16.4.254
add dhcpsnooping binding=00-0d-da-00-02-eb ip=172.16.4.203 interface=vlan400
port=15 router=172.16.4.254

# IP configuration
enable ip
add ip int=vlan500 ip=172.16.5.102 mask=255.255.255.0

# MACFF configuration
enable macff int=vlan100
enable macff int=vlan200
enable macff int=vlan300
enable macff int=vlan400
enable macff int=vlan500
```

Configure edge switch 3

Edge switch 3 is connected to port 49 of edge switch 1. The configuration is similar to edge switch 1, except that:

- the name is different
- there are two uplink ports—to switches 1 and 2—instead of the four on switch 1. This changes the VLAN configuration and the STP edge ports and means LACP is not needed
- no residential gateways are connected to switch 3 so the configuration has no static bindings for DHCP snooping
- the management IP address is different

The configuration for switch 3 follows, with these differences in **bold**:

```
# System configuration
set system name="Edge Switch 3"

# VLAN general configuration
create vlan=Voice vid=100 private
create vlan=Video vid=200 private
create vlan=Data vid=300 private
create vlan=Management vid=400 private
create vlan=EAN_Management vid=500 private

# STP general configuration
enable stp=default
set stp=default mode=rapid

# VLAN port configuration
# unlike switch 1, ports 1, 2 and 15 are not in any VLANs
add vlan=100 port=49-50 uplink frame=tagged
add vlan=200 port=49-50 uplink frame=tagged
add vlan=300 port=49-50 uplink frame=tagged
add vlan=400 port=49-50 uplink frame=tagged
add vlan=500 port=49-50 uplink frame=tagged

# STP port configuration
set stp=default port=1-48 edgeport=yes

# DHCP Snooping configuration
# unlike switch 1, there is no maxlease setting for port 15 or static bindings
enable dhcpsnooping
enable dhcpsnooping arpsecurity
enable dhcpsnooping option82
set dhcpsnooping port=49 trusted=yes
set dhcpsnooping port=50 trusted=yes

# IP configuration
enable ip
add ip int=vlan500 ip=172.16.5.103 mask=255.255.255.0

# MACFF configuration
enable macff int=vlan100
enable macff int=vlan200
enable macff int=vlan300
enable macff int=vlan400
enable macff int=vlan500
```

How to configure the Access Router

The Access Router—in this case a Rapier 24i switch—is a critical point in the network. It deals with access control for all five private VLANs, and is the path to the Internet, the SIP server (for VoIP telephony) and multicast groups (for TV and movies).

1. Name the switch

Give the switch a name to appear at the command prompt, by using the command:

```
set system name="Access Router"
```

2. Create the VLANs

On the Access Router, none of the VLANs are private VLANs.

Create a VLAN for access to the Internet, the SIP server and multicast groups, by using the command:

```
create vlan=CoreNetwork vid=28
```

Create the other VLANs by using the commands:

```
create vlan=Voice vid=100
create vlan=Video vid=200
create vlan=Data vid=300
create vlan=Management vid=400
create vlan=EAN_Management vid=500
```

3. Configure spanning tree

Spanning tree prevents loops in the ring. Enable it by using the commands:

```
enable stp=default
set stp=default mode=rapid
```

4. Add ports to the VLANs

The Access Router connects to:

- edge switch 1 through ports 1 and 2, using LACP
- the SIP and multicast server through port 20 in vlan28
- the Internet through port 24 in vlan28
- a management PC in vlan500 through port 5. This PC has an IP address of 172.16.5.250

Add the ports to the VLANs by using the commands:

```
add vlan=28 port=20,24
add vlan=500 port=5
add vlan=100 port=1-2 frame=tagged
add vlan=200 port=1-2 frame=tagged
add vlan=300 port=1-2 frame=tagged
add vlan=400 port=1-2 frame=tagged
add vlan=500 port=1-2 frame=tagged
```

5. Specify the ports that do not connect to a switch

Hosts connect more quickly initially when STP knows which ports do not have a switch connected to them—in other words, which ports are edge ports. Set this by using the command:

```
set stp=default port=3-23 edgeport=yes
```

6. Configure IP

The Access Router is the next hop for all VLANs in the network, so IP must be configured. Enable IP, give each VLAN an IP address, and set up IP routing, by using the commands:

```
enable ip
add ip int=vlan28 ip=172.28.40.60
add ip int=vlan100 ip=172.16.1.254 mask=255.255.255.0
add ip int=vlan200 ip=172.16.2.254 mask=255.255.255.0
add ip int=vlan300 ip=172.16.3.254 mask=255.255.255.0
add ip int=vlan400 ip=172.16.4.254 mask=255.255.255.0
add ip int=vlan500 ip=172.16.5.254 mask=255.255.255.0
add ip rou=0.0.0.0 mask=0.0.0.0 int=vlan28 next=172.28.0.1
```

7. Control VLAN traffic flow: classify packets

Traffic within and between the VLANs should be discarded, except for traffic between:

- hosts within vlan100. This allows hosts to phone each other
- the management PC and hosts in vlan400 and vlan500. This allows you to manage the edge switches and the RGs from the management PC
- hosts in vlan100-500 and hosts outside these VLANs. This allows hosts to connect through vlan28 to the SIP and multicast server and to the Internet

The first step is to create classifiers to match traffic in VLANs 100-500 because this is the traffic you need to control. The classifiers match on the basis of source and destination IP addresses. Create the classifiers by using the commands:

```
create class=10 ipsa=172.16.0.0/16 ipda=172.16.0.0/16
create class=100 ipsa=172.16.1.0/24 ipda=172.16.1.0/24
create class=401 ipsa=172.16.4.0/24 ipda=172.16.5.250/32
create class=402 ipsa=172.16.5.250/32 ipda=172.16.4.0/24
create class=501 ipsa=172.16.5.0/24 ipda=172.16.5.250/32
create class=502 ipsa=172.16.5.250/32 ipda=172.16.5.0/24
```

8. Control VLAN traffic flow: discard undesirable packets

Almost all traffic within and between VLANs 100-500 needs to be discarded, so this example creates a filter to discard everything in those VLANs, then specifies exceptions. Hardware filters specify such exceptions through an action of **nodrop**, which stops the switch from discarding a packet that an earlier filter would discard.

First create the filter to drop everything, by using the command:

```
add switch hwfilter classifier=10 action=discard
```

Then create filters to allow the exceptions, by using the commands:

```
add switch hwfilter classifier=100 action=nodrop
add switch hwfilter classifier=401 action=nodrop
add switch hwfilter classifier=402 action=nodrop
add switch hwfilter classifier=501 action=nodrop
add switch hwfilter classifier=502 action=nodrop
```

The switch processes hardware filters in order, and processes every filter in the list. This means later filters override the effect of earlier filters, so the generic “drop-everything” filter must come first. Any packet that matches classifiers 100-502 also matches classifier 10 and therefore matches the generic filter.

Note that the configuration does not need a filter to allow vlan100-500 to contact other VLANs, such as vlan28. This happens by default, because there is no filter to block such traffic.

The following table summarises the effect of the classifiers and filters.

Classifier ID	Source	Destination	Action of filter
10	172.16.0.0/16 (all hosts in VLANs 100-500)	172.16.0.0/16 (all hosts in VLANs 100-500)	Drop
100	172.16.1.0/24 (all hosts in vlan100)	172.16.1.0/24 (all hosts in vlan100)	Override the drop action so permit
401	172.16.4.0/24 (all hosts in vlan400)	172.16.5.250/32 (the management PC)	Override the drop action so permit
402	172.16.5.250/32 (the management PC)	172.16.4.0/24 (all hosts in vlan400)	Override the drop action so permit
501	172.16.5.0/24 (all hosts in vlan500)	172.16.5.250/32 (the management PC)	Override the drop action so permit
502	172.16.5.250/32 (the management PC)	172.16.5.0/24 (all hosts in vlan500)	Override the drop action so permit

9. Disable ICMP redirection

ICMP redirection must be disabled when MACFF is used, to stop the Access Router from sending ICMP redirects to hosts. The Access Router would otherwise send an ICMP redirect message whenever it found itself having to route a packet out of the interface that the packet arrived on.

Disable ICMP redirection by using the command:

```
disable ip icmp=redirect
```

10. Enable IGMP for multicast group management

IGMP needs to be enabled on any interface that could see IGMP hosts, by using the commands:

```
enable ip igmp
enable ip igmp int=vlan28
enable ip igmp int=vlan200
enable ip igmp int=vlan300
```

11. Enable PIM for routing multicast traffic

PIM sparse mode routes multicast data between VLANs. Configure it by using the commands:

```
add pim interface=vlan28

add pim interface=vlan200

add pim bsrcandidate interface=vlan28

add pim rpcandidate group=224.0.0.0 mask=240.0.0.0
  interface=vlan28

enable pim
```

12. Configure the DHCP server

The Access Router also acts as a DHCP server to dynamically configure IP on network hosts. To configure DHCP, you create a policy and apply a range of IP addresses to it. The range defines the IP address pool. For this configuration, note that:

- there are separate policies for voice, video and data traffic. Each policy assigns IP settings for the appropriate VLAN
- DHCP always gives each residential gateway the same IP settings. The configuration achieves this through static MAC address to IP address mapping in the range that is attached to the Voice_DHCP policy. For example, when a DHCP request on vlan100 arrives with a source MAC of 00-0d-da-00-0b-11, the server will only ever offer the IP address 172.16.1.201

Configure DHCP by using the commands:

```
create dhcp poli=Voice_DHCP lease=7200

add dhcp poli=Voice_DHCP subn=255.255.255.0 router=172.16.1.254
  dnss=10.0.0.100,10.0.0.101 maskdiscovery=off masksupplier=off

create dhcp range=Voice_range poli=Voice_DHCP ip=172.16.1.200
  number=5

add dhcp range=Voice_range ip=172.16.1.201 a=00-0d-da-00-0b-11

add dhcp range=Voice_range ip=172.16.1.202 a=00-0d-da-00-00-37

add dhcp range=Voice_range ip=172.16.1.203 a=00-0d-da-00-02-eb

create dhcp poli=Video_DHCP lease=3600

add dhcp poli=Video_DHCP subn=255.255.255.0 router=172.16.2.254
  maskdiscovery=off masksupplier=off

create dhcp range=Video_range poli=Video_DHCP ip=172.16.2.200
  number=5

create dhcp poli=Data_DHCP lease=300

add dhcp poli=Data_DHCP subn=255.255.255.0 router=172.16.3.254
  dnss=10.0.0.100,10.0.0.101 maskdiscovery=off masksupplier=off

create dhcp range=Data_range poli=Data_DHCP ip=172.16.3.200
  number=5

enable dhcp
```

13. Enable LACP

LACP sets up a dynamic trunk between edge switch 1 and this switch, using ports 1 and 2. For security purposes, the other ports should be manually removed from the trunk, because they should never be part of it. Therefore, set up LACP by using the commands:

```
delete lacp port=3-24

enable lacp
```

14. Save the configuration

Save the configuration and set the switch to use it on start-up, by using the command:

```
create config=macffar.cfg set
```

How to configure the residential gateways

This section gives basic example configurations for the three residential gateways (RGs), to get you underway.

Note that this section's configuration is a less secure configuration because it does not include advanced but highly recommended features such as authentication. You should expand the configuration to match your network's needs.

The configurations give each RG a static IP address on the management interface, which is vlan400. This is a different management VLAN to the EAN management VLAN, which is vlan500. Separating the management like this allows you to give residential customers some control over their RGs, without compromising the security of the EAN switches.

Note that the DHCP server on the Access Router always assigns the same IP address to each RG's voice VLAN (see Step 12 on page 21). This simplifies ongoing IP management of the RG.

Note: If you see a message like the following one when you are configuring an RG, you can ignore it. The command has still worked.

```
--> vlan add Data port lan2 frame untagged
webserver:Couldn't find node with attribute
```

Configure residential gateway 1

RG 1 is attached to port 15 of edge switch 1.

1. Configure the voice VLAN, vlan100

Create the VLAN, set it to obtain its IP address through DHCP, and add the wan port to it, by using the commands:

```
vlan add Voice vid 100
ethernet add transport Voice
ip add interface Voice
ip set interface Voice dhcp enabled
ip attach Voice Voice
vlan add Voice port wan frame tagged
```

2. Configure the video VLAN, vlan200

Create the VLAN and add the wan and lan1 ports to it, by using the commands:

```
vlan add Video vid 200
vlan add Video port lan1 frame untagged
vlan add Video port wan frame tagged
```

3. Configure the data VLAN, vlan300

Create the VLAN and add the wan and lan2 ports to it, by using the commands:

```
vlan add Data vid 300
vlan add Data port lan2 frame untagged
vlan add Data port wan frame tagged
```

4. Configure the management VLAN, vlan400

Create the VLAN, give it a static IP address, and add the wan port to it, by using the commands:

```
vlan add Management vid 400
ethernet add transport Management
ip add interface Management 172.16.4.201 255.255.255.0
ip attach Management Management
vlan add Management port wan frame tagged
```

5. Configure SIP

Configure SIP, by using the commands:

```
voip sip protocol enable
voip sip protocol set netinterface Voice
voip sip locationserver create default contact 172.28.255.122
voip sip proxyserver create default contact 172.28.255.122
voip ep analogue create a11 type al-fxs-del physical-port tel1
voip ep analogue create a12 type al-fxs-del physical-port tel2
voip sip user create user11 address 711 domain 172.28.255.122
voip sip user create user12 address 712 domain 172.28.255.122
voip sip user add user11 port a11
voip sip user add user12 port a12
```

6. Save the configuration

The commands for saving the configuration depend on the RG’s software version. Either use the two commands:

```
system config create myconfig.cfg
system config set myconfig.cfg
```

or use the single command:

```
system config save
```

Configure residential gateway 2

RG 2 is attached to port 14 of edge switch 2. The configuration is similar to RG 1, except that:

- the management IP address is different
- the SIP ports and users are different

The configuration for RG 2 follows, with these differences in **bold**:

```
vlan add Voice vid 100
ethernet add transport Voice
ip add interface Voice
ip set interface Voice dhcp enabled
ip attach Voice Voice
vlan add Voice port wan frame tagged

vlan add Video vid 200
vlan add Video port lan1 frame untagged
vlan add Video port wan frame tagged

vlan add Data vid 300
vlan add Data port lan2 frame untagged
vlan add Data port wan frame tagged
vlan add Management vid 400
ethernet add transport Management
ip add interface Management 172.16.4.202 255.255.255.0
ip attach Management Management
vlan add Management port wan frame tagged

voip sip protocol enable
voip sip protocol set netinterface Voice
voip sip locationserver create default contact 172.28.255.122
voip sip proxyserver create default contact 172.28.255.122
voip ep analogue create a21 type al-fxs-del physical-port tel1
voip ep analogue create a22 type al-fxs-del physical-port tel2
voip sip user create user21 address 721 domain 172.28.255.122
voip sip user create user22 address 722 domain 172.28.255.122
voip sip user add user21 port a21
voip sip user add user22 port a22
```

Configure residential gateway 3

RG 3 is attached to port 15 of edge switch 2. The configuration is similar to RG 1, except that:

- the management IP address is different
- the SIP ports and users are different

The configuration for RG 3 follows, with these differences in **bold**:

```
vlan add Voice vid 100
ethernet add transport Voice
ip add interface Voice
ip set interface Voice dhcp enabled
ip attach Voice Voice
vlan add Voice port wan frame tagged

vlan add Video vid 200
vlan add Video port lan1 frame untagged
vlan add Video port wan frame tagged

vlan add Data vid 300
vlan add Data port lan2 frame untagged
vlan add Data port wan frame tagged

vlan add Management vid 400
ethernet add transport Management
ip add interface Management 172.16.4.203 255.255.255.0
ip attach Management Management
vlan add Management port wan frame tagged

voip sip protocol enable
voip sip protocol set netinterface Voice
voip sip locationserver create default contact 172.28.255.122
voip sip proxyserver create default contact 172.28.255.122
voip ep analogue create a31 type al-fxs-del physical-port tel1
voip ep analogue create a32 type al-fxs-del physical-port tel2
voip sip user create user31 address 731 domain 172.28.255.122
voip sip user create user32 address 732 domain 172.28.255.122
voip sip user add user31 port a31
voip sip user add user32 port a32
```

Configuration extensions

This section extends the example with the following optional extras:

- "Add a server to the MACFF configuration" on page 27
- "Block unwanted multicast groups" on page 30

Add a server to the MACFF configuration

In the configuration described in previous sections, the Access Router handles all communication between clients and the SIP and multicast servers. This is necessary in the example because the servers and clients are in different VLANs (the servers are in vlan28 and the clients are in vlan100-300).

If instead your server and clients are in the same VLAN, it is more efficient to forward traffic directly between server and client. This section describes how to do this by adding the server statically to the MACFF configuration.

When you add the server to MACFF, the switch responds to ARP requests with the right MAC address for that server, instead of responding with the Access Router's MAC address. This establishes client → server connectivity, instead of client → Access Router → server connectivity. The direct connectivity gives clients faster access to critical servers and makes the Access Router less congested.

How to add a server

In this example, we add a server to the Data VLAN, vlan300, by connecting it to the trusted port 10 on edge switch 3. The server has an IP address of 172.16.3.250 and a MAC address of 00-0e-2e-65-15-18. To add the server to the MACFF configuration, use the following steps.

1. Add the server to MACFF

Add the server, by using the following command on each of the three edge switches:

```
add macff server interface=vlan300 ip=172.16.3.250
  description="Data LAN Server"
```

2. If your server is on an untrusted port, bind the server to DHCP snooping

In this example, the new server is attached to a trusted port on edge switch 3. if instead you attached it to an **untrusted** port, you would need to add a static DHCP snooping binding for the server, to stop DHCP snooping from blocking the server traffic. To do this, you would use the command:

```
add dhcpsnooping binding=00-0e-2e-65-15-18 ip=172.16.3.250
  interface=vlan300 port=10 router=172.16.3.254
```

If the server is on an untrusted port, packets go directly from the client to the server, but packets from the server to the client go through the Access Router. This reduces the efficiency of the packet flow.

3. Check the configuration

MACFF registers the new server against the Data VLAN. You can see the number of servers for each VLAN by using the command:

```
show macff
```

The following figure shows the resulting output. Note that the Data VLAN now has a server (shown in **bold**).

```
MAC Forced Forwarding Information:
----------------------------------------------------------------------
VLAN Interface                   Dbg IP Address      State     Servers
----------------------------------------------------------------------
Voice                                -               ENABLED         1
Video                                -               ENABLED         1
Data                                 -               ENABLED         1
Management                           -               ENABLED         1

----------------------------------------------------------------------
```

You can see more information about this server by checking the information that MACFF uses from the DHCP snooping database, by using the command:

```
show macff database
```

The following figure shows the resulting output, with the new server's information shown in **bold**. The MAC address is the MAC address of the router (not the new server). Note that the MAC address would be missing if the switch was unable to resolve an ARP for the server.

```
Vlan ................... Voice
IP Address ............. 172.16.1.254
Description ............ -
MAC Address ............ 00-00-cd-11-79-a0
Server Type ............ Dynamic(1)

Vlan ................... Video
IP Address ............. 172.16.2.254
Description ............ -
MAC Address ............ 00-00-cd-11-79-a0
Server Type ............ Dynamic(1)

Vlan ................... Data
IP Address ............. 172.16.3.250
Description ............ Data LAN Server
MAC Address ............ 00-0e-2e-65-15-18
Server Type ............ Static

Vlan ................... Management
IP Address ............. 172.16.4.254
Description ............ -
MAC Address ............ 00-00-cd-11-79-a0
Server Type ............ Dynamic(1)
```

Block unwanted multicast groups

When you connect PCs to the network, you may find unwanted multicast traffic occurs in the network. This section describes how to use IGMP filtering to block such traffic.

For example, the following figure shows that the data VLAN has an entry on port 25 of edge switch 3 for the group 239.255.255.250 (which is associated with UPnP). A PC attached to port 25 is sending reports for this group.

```
Manager Edge Switch 3> show igmpsnooping

IGMP Snooping
------------------------------------------------------------------------
Status ........................... Enabled
Disabled All-groups ports ........ None
.
.
.
Vlan Name (vlan id) ..... Data (300)
Fast Leave .............. Off
Query Solicitation ...... Off
Static Router Ports ..... None
Group List ..............

  Group. 239.255.255.250                    Entry timeout 180 secs
  Ports  25

  All Groups                                Entry timeout 172 secs
  Ports  50
.
.
.
```

For detailed information about filtering, see *How to Configure IGMP on Allied Telesis Routers and Switches for Multicasting*. This How To Note is available in the Resource Center on your switch's Documentation and Tools CDROM, or from http://www.alliedtelesis.com/resources/literature/howto.aspx.

How to filter

In this example, we specify the groups from which the switch **accepts** IGMP messages, instead of the groups which are blocked. On port 25 on edge switch 3, we only want to accept IGMP messages from groups in the range 224.x.x.x, and we only want report and leave messages—query messages will never arrive on this port. To create such a filter, use the following steps.

1. Create the filter

Create the filter by using the command:

```
create igmp filter=1
```

2. Add entries to the filter

Add the desired groups and message types to the filter by using the commands:

```
add igmp filter=1 entry=1 groupaddress=224.0.0.0-224.255.255.255
  msgtype=leave
```

```
add igmp filter=1 entry=2 groupaddress=224.0.0.0-224.255.255.255
  msgtype=report
```

You do not need to specify the action because the default is **action=include**.

Filters end in an implicit blocking entry, so this filter discards all other messages and groups.

3. Apply the filter

Apply the filter on the desired port by using the command:

```
set switch port=25 igmpfilter=1
```

4. Check that the filter works

Wait until the current group entry has timed out, then check that another entry has not replaced it, by using the command:

```
show igmpsnooping
```

The following figure shows that the unwanted entry is no longer there.

```
IGMP Snooping
------------------------------------------------------------------------
Status ........................... Enabled
Disabled All-groups ports ........ None
.
.
.
Vlan Name (vlan id) ..... Data (300)
Fast Leave .............. Off
Query Solicitation ...... Off
Static Router Ports ..... None
Group List ..............

  All Groups                                Entry timeout 176 secs
  Ports  50
.
.
.
```

How to troubleshoot the configuration

A number of different troubleshooting options exist for MACFF, including the following:

- “Show commands” on page 32
- “Counters” on page 33
- “Log messages” on page 34
- “Debugging commands” on page 36

Show commands

Useful **show** commands include:

- **show macff**—lists the VLANs that MACFF is configured on with some information about MACFF on each VLAN
- **show macff interface**—gives detailed information about MACFF on a particular VLAN
- **show dhcpsnooping database**—summarises the hosts that DHCP snooping knows about
- **show macff database**—gives detailed information for servers and routers that MACFF knows about from the DHCP snooping database. For each server or router, it lists the VLAN, the IP address, the MAC address, whether the entry was learned statically or dynamically, and the number of hosts that are bound to dynamically-learnt servers or routers. The following figure shows example output for this command on edge switch 2 for this Note’s example.

```
Vlan .................... Voice
IP Address ............. 172.16.1.254
Description ............ -
MAC Address ............ 00-00-cd-11-79-a0
Server Type ............ Dynamic(2)

Vlan .................... Video
IP Address ............. 172.16.2.254
Description ............ -
MAC Address ............ 00-00-cd-11-79-a0
Server Type ............ Dynamic(1)

Vlan .................... Management
IP Address ............. 172.16.4.254
Description ............ -
MAC Address ............ 00-00-cd-11-79-a0
Server Type ............ Dynamic(2)
```

For detailed information about the above commands, see the *MAC-Forced Forwarding* and *DHCP Snooping* chapters of the Software Reference.

Counters

You can display useful counters by using the commands:

```
show macff counter
show macff interface=vlan port=number counter
```

The following figure shows output of the command **show macff counter** on edge switch 1 for this Note’s example.

```
MAC Forced Forwarding Information:
----------------------------------------------------------------------
VLAN Interface                   Dbg IP Address      State     Servers
----------------------------------------------------------------------
Voice                                -               ENABLED         1
Video                                -               ENABLED         1
Data                                 -               ENABLED         0
Management                           -               ENABLED         1


Overall Status:
  Number of Servers ........     3
  Servers Lost .............    12

ARP Counters( All Ports ):
  Requests .................  1974    Replies ..................   272
  Resolution Requests ......     4    Resolutions Failed .......     0
  Src : No DHCPSN Entry ....     0    Src : Inconsistent Data ..     0
  Src : No Routers .........  1328    Src : No Routers Found ...     0
  Dest: No DHCPSN Entry ....  1328    S/D : Same Port ..........     0

Server Counter:
  ARP Resolution Requests ..   261    ARP Resolutions ..........   256
  ARP Resolutions Failed ...     5    ARP Still Valid ..........  7759
  Static Add ...............     0    Static Delete ............     0
  Dynamic Add ..............     8    Dynamic Delete ...........     1
  Dynamic Update Add .......     7    Dynamic Update Delete ....    11
  Dynamic Update: No New ...    11    Static Add Fail ..........     0
  Dynamic Add Fail .........     0    Static Delete Fail .......     0
  Dynamic Delete Fail ......     0
----------------------------------------------------------------------
```

The following figure shows output of the command **show macff interface=vlan300 port=15 counter** on edge switch 1 for this Note's example.

```
MAC Forced Forwarding Information:
----------------------------------------------------------------------
Interface ................. Data
Status .................... ENABLED
IP Address ................ -
Ports:
  Tagged .................. 1-2,15,49-50
  Untagged ................ 36,38
Active Servers ............ 0
Debugging ................. NONE

Counters for Port: 15
ARP Counters:
  Requests ................  1608    Replies .................   280
  Resolution Requests ......    4    Resolutions Failed .......    0
  Src : No DHCPSN Entry ....    0    Src : Inconsistent Data ..    0
  Src : No Routers .........  1328    Src : No Routers Found ...    0
  Dest: No DHCPSN Entry ....  1328    S/D : Same Port ..........    0
----------------------------------------------------------------------
```

For detailed information about the above commands, see the *MAC-Forced Forwarding* chapter of the Software Reference.

Log messages

When events happen that cause DHCP snooping and MACFF to do something, the switch produces a log message. To see the log messages, use the command:

```
show log
```

This section gives some of the possible actions and the resulting log messages.

▶ MACFF rejects an ARP request

The client 172.16.2.204 tried to ARP for 172.16.2.254 but MACFF rejected it because there was no router mapped to the client 172.16.2.204.

```
01 21:58:37 4 MACF MACF  CLIEN Client 172.16.2.204 ARP for 172.16.2.254 failed
                                 - no routers
```

▶ Router-to-host mapping successfully added

DHCP Snooping has seen the client 172.16.2.204 successfully discover its DHCP lease, including the information that its router is 172.16.2.254. MACFF noted the router-to-host mapping.

```
01 21:58:37 3 DHCP DHCPS UPDAT Updating entry [chaddr 00-0e-2e-7d-4b-40],
                             clientIP 172.16.2.204, vlan200, port15, serverIP
                               172.16.2.254, Expires 22:58:37 01-Jan-2007(*)
01 21:58:37 3 MACF MACF  NEWSE New upstream server acquired -
                               172.16.2.254(00-00-cd-11-79-a0) on Video
```

▶ Client successfully renews its DHCP lease

DHCP Snooping has seen the client 172.16.1.201 successfully renew its DHCP lease. MACFF did nothing.

```
01 22:31:35 3 DHCP DHCPS UPDAT Updating entry [chaddr 00-0d-da-00-0b-11],
                             clientIP 172.16.1.201, vlan100, port15, serverIP
                               172.16.1.254, Expires 00:31:35 02-Jan-2007(*)
```

▶ Client stops getting a router IP through DHCP

MACFF saw DHCP snooping validate a host’s DHCP renewal, but the DHCP packet did not provide the client with a router IP, so MACFF deleted the entry for this router-to-host mapping.

```
01 22:50:36 3 MACF MACF  LOSTS Upstream server lost -
                               172.16.2.254(00-00-cd-11-79-a0) on Video
```

▶ Server statically added but does not resolve

A binding for a static server was added, then MACFF reported that it could not resolve a MAC address for the server’s IP address.

```
02 05:45:35 3 MACF MACF  NEWSE New upstream server acquired -
                               172.16.2.250(00-00-00-00-00-00) on Video
02 05:45:42 4 MACF MACF  LOSTC Upstream server - cannot contact
                               172.16.2.250(00-00-00-00-00-00) on Video
```

Debugging commands

Both DHCP snooping and MACFF debugging produce useful output when you are troubleshooting MACFF configurations. We recommend enabling them both.

To enable DHCP snooping debug, use the command:

```
enable dhcpsnooping debug=all
```

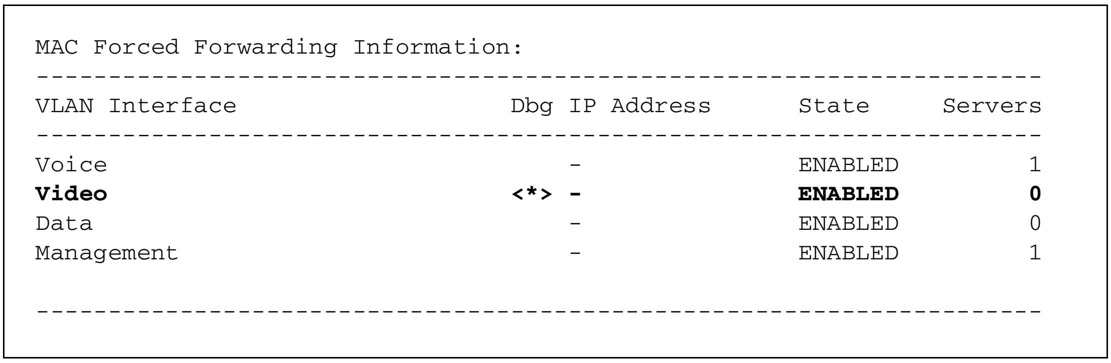
To enable MACFF debugging, use the command:

```
enable macff interface=vlan debug=all
```

Note that you enable MACFF debugging on a single VLAN. You can see which VLAN debugging is enabled on by using the command:

```
show macff
```

The following figure shows that debugging is enabled on the Video VLAN, vlan200.



```
MAC Forced Forwarding Information:
----------------------------------------------------------------------
VLAN Interface                   Dbg IP Address       State      Servers
----------------------------------------------------------------------
Voice                                -                ENABLED          1
Video                            <*> -                ENABLED          0
Data                                 -                ENABLED          0
Management                           -                ENABLED          1

----------------------------------------------------------------------
```

If events occur that apply to another VLAN, you see some information about them, but not as much. See “Events for other VLANs” on page 44 for examples of this.

This section includes the following examples of debugging output:

- “A host renews its DHCP lease” on page 37
- “Different DHCP actions” on page 39
- “Backing up DHCP snooping database” on page 40
- “Uplink port is not trusted” on page 40
- “ARP received on untrusted port” on page 41
- “ARP received on trusted port” on page 42
- “Static server added to MACFF configuration” on page 43
- “Events for other VLANs” on page 44

A host renews its DHCP lease

This section shows the debugging output from edge switch 1 when a host successfully renews its DHCP lease. Note that most of the following output is DHCP snooping debug, which starts with “DHCPSN_”. MACFF debugging starts with “MACFF_”.

1. DHCP snooping processes the renewal request

First, a packet arrives for vlan300 on port 15, requesting the renewal. DHCP snooping processes it and forwards it out its trusted ports.

```
DHCPSN_PROCESS: [0152250c] DHCP Snooping pkt for VLAN 300 from port 15
DHCPSN_PROCESS: [0152250c] Type: REQUEST
DHCPSN_PROCESS: [0152250c] On DHCP Snooping non-trusted port
DHCPSN_PROCESS: [0152250c] Inserting Option 82
Option_82_Info: [0152250c] Inserting Option 82...
Option_82_Info: [0152250c] Inserting Sub-option CircuitID
Option_82_Info: [0152250c] Inserting Sub-option RemoteID
Option_82_Info: [0152250c] Inserted Option 82 (length 20):
  52 12 01 06 00 04 01 2c 00 0f 02 08 00 06 00 00 cd 23 ca e6
DHCPSN_PROCESS: [0152250c] DHCP Snoop forwarding pkt at L2 for VLAN 300
InPort 15
DHCPSN_PROCESS: [0152250c] L2 Dest MAC is broadcast
DHCPSN_PROCESS: [0152250c] Type: REQUEST, L2 forward to trusted ports
DHCPSN_PROCESS: [0152250c] Forward ports (except 15)
DHCPSN_PROCESS: [0152250c]    Tagged:1-2,49-50
DHCPSN_PROCESS: [0152250c]  Untagged:None
```

2. DHCP snooping processes the reply from the DHCP server

The DHCP server (on the Access Router) replies to the request. DHCP snooping sees this reply on port 1. It processes the reply, sees the DHCP acknowledgement and passes the reply to MACFF.

```
DHCPSN_PROCESS: [01f7476c] DHCP Snooping pkt for VLAN 300 from port 1
DHCPSN_PROCESS: [01f7476c] Type: REPLY
DHCPSN_PROCESS: [01f7476c] On DHCP Snooping trusted port
DHCPSN_PROCESS: [01f7476c] Lookup result for CHAddr 00-0e-2e-65-3f-c8: Port
15
DHCPSN_PROCESS: [01f7476c] DHCP ACK Found...
DHCPSN_PROCESS: [01f7476c] Found router option 0304ac1003fe
DHCPSN_DB: Updating entryId 5. Flags 00000210
DHCPSN_DB: Notifying DB listener: CLASSIFIER
DHCPSN_ACL: dhcpSnoopAclListener >> dbEntryPt=0x00cd8bdc flags=0x00000210
DHCPSN_DB: Notifying DB listener: MACFF
```

3. MACFF processes the reply from the DHCP server

MACFF notes the router-to-host mapping, increments counters, and ARPs for the MAC address of the router.

```
MACFF_DHCP: Modify Client 00-0e-2e-65-3f-c8 on VLAN 300.
MACFF_DHCP:    old routers: -
MACFF_DHCP:    new routers: 172.16.3.254
MACFF_SERVER: Add dynamic server 172.16.3.254 on VLAN 300, ref count: 1.
macffCounterServerIncrement: counter=8
macffControllerServerCheckArp: serverPt=00cfdf20, log=1
macffControllerCheckArp( serverPt=, IP=0.0.0.0        , genLog=1 )
MACFF_ARP: Checking server 172.16.3.254 on VLAN 300.
macffCounterServerIncrement: counter=3
MACFF_ARP:   ARP found: 00-00-cd-11-79-a0, port 1.
macffLogGenerate: MT=0, OT=0, IP1=172.16.3.254, IP2=0.0.0.0
macffLogGenerate: IP3=0.0.0.0, eth=00-00-cd-11-79-a0, desc=Data
macffLogGenerate: logCount=0
```

4. DHCP snooping forwards the ARP reply to the requestor

DHCP snooping changes the state of the client in its database and forwards the ARP reply to the client.

```
DHCPSN_DB: Change state for 00-0e-2e-65-3f-c8, in FULL for event
LISTENER_OK
DHCPSN_DB: Changed state for 00-0e-2e-65-3f-c8, to FULL
DHCPSN_PROCESS: [01f7476c] DHCP Snoop forwarding pkt at L2 for VLAN 300
InPort 1
DHCPSN_PROCESS: [01f7476c] L2 Dest MAC is unicast
DHCPSN_PROCESS: [01f7476c] Using chaddr lookup result for dest port(s)
DHCPSN_PROCESS: [01f7476c] L2 forward packet directly to port 15
DHCPSN_PROCESS: [01f7476c] Forward ports (except 1)
DHCPSN_PROCESS: [01f7476c]    Tagged:15
DHCPSN_PROCESS: [01f7476c]  Untagged:None
```

Different DHCP actions

This section describes the debugging output that MACFF displays in response to four different types of DHCP message. The first of these examples is the same as the output shown in Step 3 on page 38 above.

The output was generated on edge switch 1 by using the command:

```
enable macff interface=vlan300 debug=dhcp
```

Existing host requests IP settings and receives address and router IP

A host, identified by MAC address 00-0e-2e-65-3f-c9, sends a DHCP request and is given IP settings with a router IP (172.16.3.254) in the DHCP options part of the packet. MACFF debugging notes that there was previously no router for this host and now there is.

```
MACFF_DHCP: Modify Client 00-0e-2e-65-3f-c9 on VLAN 300.
MACFF_DHCP:    old routers: -
MACFF_DHCP:    new routers: 172.16.3.254
```

Existing host requests IP settings and receives address but no router IP

A host, identified by MAC address 00-0e-2e-65-3f-c9, sends a DHCP request and is given IP settings with no router IP in the DHCP options part of the packet. MACFF debugging notes that there was previously a router for this host and now there is not.

```
MACFF_DHCP: Modify Client 00-0e-2e-65-3f-c9 on VLAN 300.
MACFF_DHCP:    old routers: 172.16.3.254
MACFF_DHCP:    new routers: -
```

New host requests IP settings and receives address and router IP

A new host, identified by MAC address 00-0e-2e-64-c4-44, sends a DHCP discover packet and is given IP settings with a router IP (172.16.3.254) in the DHCP options part of the packet. MACFF debugging notes that there was previously no router for this host and now there is. Note that the first line of this debugging says “Add Client”, which means that the host is new to MACFF.

```
MACFF_DHCP: Add Client 00-0e-2e-64-c4-44 on VLAN 300.
MACFF_DHCP:    routers: 172.16.3.254
```

▶ DHCP snooping entry times out

The DHCP snooping entry for a host times out, so MACFF deletes the related entry. Note that the first line of this debugging says “Delete Client”.

```
MACFF_DHCP: Delete Client 00-0e-2e-64-c4-44 on VLAN 300.
MACFF_DHCP:    routers: -
```

Backing up DHCP snooping database

The DHCP snooping process checks periodically for changes to the DHCP snooping database and attempts to write any changes to a file. That file is stored in Flash memory. After a reboot, DHCP snooping reads the information from the file and writes it to the database.

In this example, there were no changes to the database during the debugging period.

```
DHCPSN_DB: Timer expired (23:05:00), checking entries...
DHCPSN_DB: Deleted 0 entries (9)
DHCPSN_DB: No change has occured in DB, so no need to update the file
```

You can change the frequency of these backups by using the command:

```
set dhcpsnooping checkinterval=1..3600
```

The interval is in seconds.

Uplink port is not trusted

The uplink ports 49 and 50 on each of the edge switches must be DHCP snooping trusted ports. This is because DHCP snooping will not accept option 82 information inserted by other EANs on an untrusted port.

In this example, port 49 is not trusted.

```
DHCPSN_PROCESS: [0131fe6c] DHCP Snooping pkt for VLAN 200 from port 49
DHCPSN_PROCESS: [0131fe6c] Type: REQUEST
DHCPSN_PROCESS: [0131fe6c] On DHCP Snooping non-trusted port
DHCPSN_PROCESS: [0131fe6c] Discard packet, Option82 RXd on non-trusted port
```

ARP received on untrusted port

This section shows the debugging output from edge switch 1 when it receives an ARP request on an untrusted port. ARP security is enabled.

1. ARP request is received

The switch receives an ARP request on port 15 (vlan300). First, DHCP snooping validates the sender. Once DHCP snooping has identified that the sender is legal, it passes processing to MACFF.

```
DHCPSN_ARP: [01dbf3cc] ARP Received on untrusted port 15 VLAN 300
DHCPSN_ARP: [01dbf3cc] ARP to be passed to MACFF, sender validated
macffControllerProcessArpRequest( arpPktPt=01dbf526, intName=012c8000,
portNum=14 )
macffCounterPortIncrement: portNum=14, counter=0
```

Note that part of the output above refers to portNum=14, although the packet arrived at port 15. This apparent inconsistency is because ports are internally numbered from 0, so the port with external number 15 has an internal number of 14.

2. MACFF checks the ARP requirements

MACFF checks the ARP requirements and sees that the host 172.16.3.202 on port 15 has asked for the MAC address for 172.16.3.254 (the gateway).

```
MACFF_PACKET: Received ARP request on VLAN 300, port 15.
MACFF_PACKET:   00-0e-2e-65-3f-c8/172.16.3.202 -> 00-00-00-00-00-00/
172.16.3.254.
macffCounterPortIncrement: portNum=14, counter=8
macffCounterPortIncrement: portNum=14, counter=6
```

3. MACFF checks for a router mapping for the host

MACFF checks for a router mapping for the host 172.16.3.202. There are three possibilities here: the router could have been set statically, or learnt via DHCP, or not learnt at all.

If the router has been learnt statically or through DHCP, then MACFF puts the router details into the ARP packet and replies, as the following output shows.

```
MACFF_PACKET: Sent ARP reply on VLAN 300, port 15.
MACFF_PACKET:   00-00-cd-11-79-a0/172.16.3.254 -> 00-0e-2e-65-3f-c8/
172.16.3.202.
macffCounterPortIncrement: portNum=14, counter=1
```

If the router has not been learnt—MACFF has no router-to-host mapping for the host—then MACFF drops the packet, as the following output shows.

```
MACFF_ERROR: Client 172.16.3.202 has no routers defined for it.
macffLogGenerate: MT=2, OT=0, IP1=172.16.3.202, IP2=172.16.3.254
macffLogGenerate: IP3=0.0.0.0, eth=00-00-00-00-00-00, desc=
macffLogGenerate: logCount=0
```

ARP received on trusted port

This section shows the debugging output from edge switch 1 when it receives an ARP request on a trusted port. ARP security is enabled.

The following output shows the debugging displayed when an ARP arrives on port 1, which is trusted by the DHCP snooping process. DHCP snooping forwards the packet to all interfaces in the VLAN on which it arrived (vlan100).

```
DHCPSN_ARP: [01507e8c] ARP Received on trusted port 1 VLAN 100
DHCPSN_ARP: [01507e8c] Forwarding ARP at L2 for VLAN 100
DHCPSN_ARP: [01507e8c] Forward ports (except 1)
DHCPSN_ARP: [01507e8c]    Tagged:1-2,15,49-50
DHCPSN_ARP: [01507e8c]  Untagged:None
macffControllerProcessArpRequest( arpPktPt=01507fe6, intName=00648000,
portNum=0 )
macffCounterPortIncrement: portNum=0, counter=0
```

MACFF does very little when an ARP arrives on a trusted port, but has printed some information. The second-last line of the above output shows that the packet arrived on vlan100 (intName=0064xxxx indicates this because hexadecimal 64 is decimal 100) on external port number 1. The last line indicates that a server counter, ARP Resolution Requests, was incremented (see "Counters" on page 33).

Static server added to MACFF configuration

This section shows the debugging output for vlan200 when a static entry for a server is added on edge switch 1, but the server does not exist.

1. Server entry is added

The static server entry is added to the MACFF configuration, by using the command:

```
add macff server interface=vlan200 ip=172.16.2.250
```

MACFF generates an ARP request, to find the server's MAC address.

```
MACFF_SERVER: Add static server 172.16.2.250 on VLAN 200.
macffControllerServerCheckArp: serverPt=00d864dc, log=1
macffControllerCheckArp( serverPt=00d864dc, IP=172.16.2.250, genLog=1 )
MACFF_ARP: Checking server 172.16.2.250 on VLAN 200.
macffCounterServerIncrement: counter=0
MACFF_ARP:   ARP not found, generating ARP request.
macffCounterServerIncrement: counter=4
```

2. The ARP request is unsuccessful

The server does not exist, so the ARP fails.

```
macffMainServerArpCallback( userPt=01ca7c3c )
macffMainArpCallback( userPt=01ca7c3c )
macffMainCheckArpReceived( userPt=01ca7c3c )
MACFF_ARP: ARP request for server 172.16.2.250 on VLAN 200 ### failed ###.
macffCounterServerIncrement: counter=2
macffLogGenerate: MT=0, OT=0, IP1=172.16.2.250, IP2=0.0.0.0
macffLogGenerate: IP3=0.0.0.0, eth=00-00-00-00-00-00, desc=Video
macffLogGenerate: logCount=0
```

3. Server entry is deleted

The static server entry is then manually deleted, by using the command:

```
del macff server interface=vlan200 ip=172.16.2.250
```

```
MACFF_SERVER: Delete static server 172.16.2.250 on VLAN 200.
macffLogGenerate: MT=1, OT=0, IP1=172.16.2.250, IP2=0.0.0.0
macffLogGenerate: IP3=0.0.0.0, eth=00-00-00-00-00-00, desc=Video
macffLogGenerate: logCount=0

MACFF_SERVER: Server 172.16.2.250 on VLAN 200 removed from database.
macffCounterServerIncrement: counter=5
```

Events for other VLANs

When you have debugging enabled for one VLAN and an event occurs on another VLAN, you see some information about the event. This section shows two examples of this. In both cases, debugging is enabled for vlan300 and the event occurs on vlan200.

ARP received on untrusted port

The following output shows that the switch received an ARP on an untrusted port in vlan200 and MACFF discarded the packet because there was no host-to-router mapping. This is the same as the example in "ARP received on untrusted port" on page 41, except that the VLAN is different.

```
DHCPSN_ARP: [01da9e8c] ARP Received on untrusted port 15 VLAN 200
DHCPSN_ARP: [01da9e8c] ARP to be passed to MACFF, sender validated
macffControllerProcessArpRequest( arpPktPt=01da9fe6, intName=00c88000,
portNum=14 )
macffCounterPortIncrement: portNum=14, counter=0
macffCounterPortIncrement: portNum=14, counter=8
macffCounterPortIncrement: portNum=14, counter=6
macffLogGenerate: MT=2, OT=0, IP1=172.16.2.200, IP2=172.16.2.254
macffLogGenerate: IP3=0.0.0.0, eth=00-00-00-00-00-00, desc=
macffLogGenerate: logCount=0
```

It is possible to tell what has happened by checking the counter entries in the above output, which shows that counters 6 and 8 are incremented. In the ARP Counters section of output of the command **show macff counter,** counter 6 is the "Src : No Routers" counter and counter 8 is the "Dest: No DHCPSN Entry" counter.

If debugging was enabled on vlan200 instead of vlan300, this debugging would include a MACFF_ERROR statement which would make the error clear.

Periodic event occurs

This example shows MACFF performing a periodic check on its server and router entries for vlan300.

When debugging is enabled on vlan200, the output looks like the following figure.

```
Manager Edge Switch 1> macffControllerTimerCallback( timerId=00000000 )
macffControllerTimerCheckArp( serverPt=00cfdbfc )
macffControllerCheckArp( serverPt=, IP=0.0.0.0        , genLog=0 )
macffCounterServerIncrement: counter=3
```

When debugging is enabled on vlan300, the output looks like the following figure.

```
Manager Edge Switch 1> macffControllerTimerCallback( timerId=00000000 )
macffControllerTimerCheckArp( serverPt=00cfdf20 )
macffControllerCheckArp( serverPt=, IP=0.0.0.0        , genLog=0 )
MACFF_ARP: Checking server 172.16.3.254 on VLAN 300.
macffCounterServerIncrement: counter=3
MACFF_ARP:   ARP found: 00-00-cd-11-79-a0, port 1.
```

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

Connecting The IP World

Allied Telesis