5 IP Router Commands

The following chapter contains information on Text-Based IP Routing commands. Topics include:

- Configuring IP Routing parameters
- Viewing IP Routing information

Refer to the command task list below to find the page number for a specific task. If you would like to reference configuration tasks based on traditional UI commands, refer to Appendix A.

view ip mac

Command Usage

Display the IP-to-Mac Address Association Table.

Syntax Options

view ip mac (No additional syntax options are used.)

Corresponding UI Command

ipmac

Screen Output

A screen similar to the following will be displayed:

IP to MAC ADDRESS ASSOCIATION TABLE

IP Address	MAC Address	Slot / Intf
192. 168. 10. 1	0020DA:6DE610	4 / 5
172. 16. 0. 5	0020DA:76D3D0	3 / 2
172. 16. 0. 7	00E029:00D41E	3 / 2
172. 16. 0. 41	0000C0:24FFEC	3 / 2
172. 16. 0. 47	00A0C9:0AA907	3 / 2
172. 16. 0. 28	0020DA:7AE9D3	3 / 2
172. 16. 0. 45	080020:8AE301	3 / 2
172. 16. 0. 60	0020DA:73C3A0	3 / 2
172. 16. 30. 00	0020AF:04BA57	3 / 2
172. 16. 41. 03	0000C0:AD8EE9	3 / 2
172. 16. 50. 12	080020:7B79E1	3 / 2
172. 16. 255. 254	0020DA:6F97E5	3 / 2
*******	0020DA:032273	5 / 1
192. 168. 10. 1	0020DA:7AEA60	3 / 2
198. 206. 182. 222	0020DA:7F48A0	3 / 2

Table Description

IP Address. The IP address learned from ARP messages received on "leaf" ports. A series of asterisks (*******) in this field indicates that the preceding entry is a duplicate to this entry. In the example screen shown above, the address 172.16.255.254 is assigned to two MAC addresses.

MAC Address. The MAC address corresponding to the listed IP address.

Slot/Intf. The slot number and interface number from which the IP and MAC addresses were learned.

view rip filter

Command Usage

Display all existing IP RIP Input and Output filters.

Syntax Options

view rip filter (No additional syntax options are used.)

Corresponding UI Command

ipf

Screen Output

A screen similar to the following will be displayed:

Displaying all filters:

#	Type	Network	Mask	Md	GP:VL (s/p/vc) (Peer ID)
1	RIP OUT	99.0.0.0	255.0.0.0	A	global
2	RIP IN	99.0.0.0	255.0.0.0	B	2:1
3	RIP OUT	All Networks		B	5:1 (3/1/32)
4	RIP IN	All Networks		B	6:1 (P1)

Table Description

#. Indicates the index number assigned to identify this filter.

Type. Indicates the type of filter, either RIP Input (**RIP IN**) or RIP Output (**RIP OUT**).

Network. Indicates the IP address that is to be filtered (entered in dotted-decimal format). An entry of "All Networks" means that all addresses are to be filtered.

Mask. The IP network mask of the network to be filtered (entered in dotted-decimal format). This field is blank if the network entered is "All Networks."

Md. Indicates the filter's mode of operation, either to allow traffic (**A**) or to block traffic (**B**).

GP:VL (s/p/vc) and **(Peer ID).** The first number (**GP**) is the group associated with this entry. The second number (**VL**) is the VLAN associated with this entry. When a filter applies to all interfaces, this field will say "global." If an entry refers to a Frame Relay interface, column headings for slot, port, and virtual circuit (**s/p/vc**) may be displayed when the filter is applied to a particular virtual circuit rather than to the entire VLAN. If an entry refers to a PPP interface, the Peer ID (**Peer ID**) may be displayed when the filter is applied to a particular PPP Peer.

rip filter

Command Usage

Add IP RIP Output or Input filters.

Syntax Options

rip filter [*group [vlan]***] [in | out] [block | allow] {all |** *ip-address [ip-mask]***}**

Definitions:
group = a RIP filter will be added only to the specified group
vlan = a RIP filter will be added only to the specified VLAN
in = specifies *input* filter only
out = specifies *output* filter only
block = sets the filter action to *block*
allow = sets the filter action to *allow*
all = specifies that rip filters will be added to all IP networks
ip-address = specifies the IP address of a single rip filter to be added
ip-mask = specifies the IP subnet mask of a single rip filter to be added

Command Defaults:
in | out = both (**in** *and* **out**)
block | allow = **allow**

Command Examples:
rip filter 4 2 in block all
rip filter 77 168.18.140.1
rip filter in allow all
rip filter out block 172.23.9.1 255.255.0.0
rip filter in 172.23.9.1
rip filter all

Corresponding UI Command

ipfilter

Remarks

The IP RIP Filtering feature gives you a means of controlling the operation of the IP RIP protocol. By using IP RIP filters, you can minimize the number of entries that are put into the IP Routing Table as well as improve overall network performance by eliminating unnecessary traffic.

Two types of IP RIP filters are available:

1. **RIP Input** filters control which IP networks are allowed into the switch's IP Routing Table whenever IP RIP updates are received.
2. **RIP Output** filters control the list of IP networks that are included in the RIP Updates sent out by the switch on any interface. Thus, RIP Output filters effectively control which networks the router advertises in the RIP updates it generates.

no rip filter

Command Usage

Delete IP RIP Output or Input filters.

Syntax Options

no rip filter [*group [vlan]***] [in | out] [block | allow] {all |** *ip-address [ip-mask]***}**

Definitions:
group = specifies a group for which a RIP filter is to be deleted
vlan = specifies a VLAN for which a RIP filter is to be deleted
in = only the specified *input* filters will be deleted
out = only the specified *output* filters will be deleted
block = only the specified *block* filters will be deleted
allow = only the specified *allow* filters will be deleted
all = specifies that RIP filters will be deleted for *all* networks
ip-address = specifies the IP address of a single RIP filter to be deleted
ip-mask = specifies the IP subnet mask of a single RIP filter to be deleted

Command Defaults:
in | out = both (**in** *and* **out**)
block | allow = **allow**

Command Examples:
no rip filter 4 2 in block all
no rip filter 77 168.18.140.1
no rip filter in allow all
no rip filter out block 172.23.9.1 255.255.0.0
no rip filter in 172.23.9.1
no rip filter all

Corresponding UI Command

ipfilter

clear ip route

Command Usage

Flush entries from the RIP Routing Table.

Syntax Options

clear ip route {*network [mask]* **| all }**

Definitions:
network = only the routing table entry the corresponding network address will be removed
mask = only the routing table entry the corresponding subnet address will be removed
all = specifies that *all* routing table entries will be removed

Command Examples:
clear ip route all
clear ip route 203.229.229.0
clear ip route 203.229.229.0 255.255.255.0

Corresponding UI Command

ripflush

Remarks

Static and direct routes will not be removed from the Routing Table.

ip route

Command Usage

Add IP static routes to the switch's IP Routing Table.

Syntax Options

ip route <*network-address***> [***mask***] {***next-hop-address*** | ***interface***} [***distance***]**

Definitions:
network-address = the IP address for the host or network to which you are setting up a route (to specify a default route, enter **0.0.0.0**)
mask = the network mask that allows you to mask network and subnetwork bits (e.g., **255.255.0.0**)
next-hop-address = the IP address of the next hop (or *gateway*) router (the next hop address must be a directly-connected network—i.e., it must be on the same network as one of the VLANs)
interface = a network interface for the gateway router (e.g., **3/1**)
distance = an administrative distance (e.g., **2**)

Command Examples:
ip route 0.0.0.0 172.23.9.101
ip route 172.22.0.0 255.255.0.0 172.23.0.253
ip route 1.1.1.1 172.23.140.1 2
ip route 0.0.0.0 3/1

Corresponding UI Command

aisr

Remarks

You might want to add a static route to send traffic to a router other than the one determined by the routing protocols. In order to add a static route, you will need to know the host/net IP address, as well as the gateway IP address (which will be used to route traffic to the external IP address).

no ip route

Command Usage

Remove a *specified* IP static route from the switch's IP Routing Table.

♦ Note ♦

To remove *all* IP static routes from the switch's IP Routing Table, use the **no ip route all** command. For more information, refer to page 5-10.

Syntax Options

no ip route <*network-address***> [***mask***] {***next-hop-address***| *interface***} [***distance***]**

Definitions:
network-address = the host or network IP address for the route that is to be removed (e.g., **0.0.0.0**)
mask = the network mask for the route that is to be removed (e.g., **255.255.0.0**)
next-hop-address = the next hop (or *gateway*) router IP address for the route that is to be removed
interface = a network interface for the route that is to be removed (e.g., **3/1**)
distance = an administrative distance for the route that is to be removed (e.g., **2**)

Command Examples:
no ip route 0.0.0.0 172.23.9.101
no ip route 172.22.0.0 255.255.0.0 172.23.0.253
no ip route 1.1.1.1 172.23.140.1 2
no ip route 0.0.0.0 3/1

Corresponding UI Command

risr

no ip route all

Command Usage

Remove *all* IP static routes from the switch's IP Routing Table.

♦ Note ♦

To remove only a *specified* IP static route from the switch's IP Routing Table, use the **no ip route** command. For more information, refer to page 5-9.

Syntax Options

no ip route all (No additional syntax options are used.)

Corresponding UI Command

risr

trace

Command Usage

Find the IP route from the local switch to a specified IP address destination. (This command displays the individual hops to the destinations as well as some timing information.)

Syntax Options

trace <*ip-address***>**

Definitions:
ip-address = IP address for the route you want to trace

Example:
trace 198.23.9.101

Corresponding UI Command

traceroute

Screen Output

A screen similar to the following will be displayed:

```
traceroute to corporate.com (198.206.185.7),30 hops max,40 byte packets
1 branch-wan-gw.CORPORATE.COM (198.206.181.252) 16 ms 0 ms 16 ms
2 10.254.1.253 (10.254.1.253) 98 ms 81 ms 98 ms
3 198.206.185.7 (198.206.185.7) 121 ms 81 ms 98 ms
```

Table Description

Each number listed in this screen display corresponds to an individual hop. The time needed to reach that hop is shown (in milliseconds) after the hop's IP address. The time may be followed by one of the following codes:

- **!** The TTL of the received ICMP message is less than or equal to 1.
- **!H** The host was unreachable.
- **!N** The network was unreachable.
- **!P** The protocol was unreachable.

If the time is replaced by an asterisk (*****), no response was received from the host during the default 3-second timeout period.

view tcp users

Command Usage

View the current TCP connections available in the TCP Connection Table.

Syntax Options

view tcp users (No additional syntax options are used.)

Corresponding UI Command

tcpc

Screen Output

A screen similar to the following will be displayed:

TCP Connection/Listener Table

Local Address/Port			Remote Address/Port			Recv-Q	Send-Q	Conn State
127.0.0.1	/	1090	27.0.0.1	/	1091	0	0	ESTABLISHED
127.0.0.1	/	1091	127.0.0.1	/	1090	0	322	ESTABLISHED
198.206.184.42	/	23	198.206.184.34	/	2057	0	0	ESTABLISHED
0.0.0.0	/	23	0.0.0.0	/	0	0	0	LISTEN
0.0.0.0	/	21	0.0.0.0	/	0	0	0	LISTEN

Table Description

Local Address/Port. The local IP address for this TCP connection/the local port for this TCP connection. (The value 0.0.0.0 is used for a connection in the listen state that is willing to accept connections for any IP interface associated with the node.)

Remote Address/Port. The remote IP address/the remote port number for this TCP connection.

Recv-Q. The number of segments received on this port.

Send-Q. The number of segments sent on this port.

Conn State. Describes the state of the TCP connection, as defined in RFC 973. Possible values are: closed, listen, synSent, synReceived, established, finWait1, finWait2, closeWait, lastAck, closing, timeWait, and delete TCB.

view tcp

Command Usage

View TCP traffic activity and TCP configuration parameters.

Syntax Options

view tcp (No additional syntax options are used.)

Corresponding UI Command

tcps

Screen Output

A screen similar to the following will be displayed:

```
TCP Statistics

Round Trip Algorithm Used          :  RSRE (MIL-STD-1778)
Retransmission Min/Max Timeout     :  300/3000
Max Connections Allowed            :  Unlimited
Active Opens                       :  76
Passive Opens                      :  43
Attempt Fails                      :  0
Established Resets                 :  5
Currently Established              :  3
Total Segments Received            :  1117
Total Segments Sent                :  832
Total Segments Retransmitted       :  0
Total Segments Received w/err      :  0
Total Segments Sent w/RST flag     :  0
```

Table Description

Round Trip Algorithm Used. The algorithm used to determine the Timeout value used for retransmitting unacknowledged octets. The value is: RSRE (MIL-STD-1778).

Retransmission Min/Max Timeout. The minimum/maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.

Max Connections Allowed. The maximum number of connections allowed. Currently, the number is unlimited.

Active Opens. The number of times TCP connections have made a direct transition to the "synSent" state from the "closed" state (refer to RFC 973).

Passive Opens. The number of times TCP connections have made a direct transition to the "synReceived" state from the "listen" state (refer to RFC 973).

Attempt Fails. The number of times TCP connections have made a direct transition to the "closed" state from either the "synSent" state or the "synReceived" state, plus the number of times TCP connections have made a direct transition to the "listen" state from the "synReceived" state.

Established Resets. The number of times TCP connections have made a direct transition to the "closed" state from either the "established" state or the "closeWait" state.

Currently Established. The number of TCP connections for which the current state is either "established" or "closeWait".

Total Segments Received. The total number of segments received, including those received in error. This count includes segments received on currently established connections.

Total Segments Sent. The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.

Total Segments Retransmitted. The number of TCP segments transmitted containing one or more previously transmitted octets.

Total Segments Received w/err. The total number of TCP segments that are in error; for example, bad TCP checksums.

Total Segments Sent w/RST flag. The number of TCP segments containing the RST flag.

view rip

Command Usage

View RIP statistics and errors.

Syntax Options

view rip (No additional syntax options are used.)

Corresponding UI Command

rips

Remarks

This command displays cumulative statistics since the last time the switch was powered on, or since the last reset of the switch was executed.

Screen Output

A screen similar to the following will be displayed:

```
                              RIP Statistics
Rtr (Group ID:VLAN ID 1:1) IP Address 198.206.182.115 RIP Mode silent
In                  4769      Out                 0
Transmit Error      0         Non-zero field      0
Bad Version         0         Bad Metric          0
Bad Family          0         Bad Size            0
Bad Address         0         Bad Command         0
```

Table Description

In/Out. The total number of RIP packets received and transmitted on a per-virtual-LAN basis.

Transmit Error. The total number of RIP packets that were unable to be sent.

Bad Version. The total number of RIP messages delivered to the switch that were not version 1.

Bad Family. The number of packets received on this VLAN whose family ID was not of the Internet family.

Bad Address. The number of received packets whose IP address was not a Class A, B, or C.

Non-zero Field. The number of received packets whose mandated "must-be-zero" fields were not zero.

Bad Metric. The number of received packets with a routing entry's metric that was out of range.

Bad Size. The number of received packets that were not compatible with the expected size.

Bad Command. The number of received packets whose command field was not a "request" or "response."

view udp users

Command Usage

Display the UDP Listener Table.

Syntax Options

view udp users (No additional syntax options are used.)

Corresponding UI Command

udpl

Remarks

This table contains information about the switch's UDP end-points on which a local application is currently accepting datagrams. The UDP Listener Table shows the local IP addresses for each UDP listener and the local port number for this listener. An IP address of zero (0.0.0.0) indicates that it is listening on all interfaces.

Screen Output

A screen similar to the following will be displayed:

UDP Listener Table

Local Address/Port			Recv-Q	Send-Q
0.0.0.0	/	162	0	0
0.0.0.0	/	161	0	0
0.0.0.0	/	520	0	0
0.0.0.0	/	1024	0	0

Table Description

Local Address/Port. The local IP address, and the local port number, for this UDP connection. In the case of a connection in the listen state, which is willing to accept connections for any IP interface associated with the node, the value 0.0.0.0 is used.

Recv-Q and **Send-Q.** For the SNMP Traps (port 162) this is the number transmitted (there is no receive).

For the SNMP Requests (port 161) this is the number of Request PDUs sent and the number of Response PDUs received.

For RIP (port 520) this is the number of packets received and transmitted.

view udp

Command Usage

View a listing of UDP statistics and errors.

Syntax Options

view udp (No additional syntax options are used.)

Corresponding UI Command

udps

Remarks

The **view udp** command displays cumulative statistics since the last time the switch was powered on or since the last reset of the switch was executed.

Screen Output

A screen similar to the following will be displayed:

```
Total UDP datagrams received                          :    831
Total UDP datagrams transmitted                       :     22
Total Datagrams received w/unknown applications       :      0
Total UDP datagrams w/other Errors                    :      0
```

Table Description

Total UDP datagrams received. The total number of UDP datagrams delivered to UDP applications.

Total UDP datagrams transmitted. The total number of UDP datagrams sent from this switch.

Total UDP datagrams received w/unknown applications. The total number of datagrams for which there was no application at the destination.

Total UDP datagrams w/other Errors. The total number of UDP datagrams that could not be delivered for reasons other than lack of application at the destination.

view icmp

Command Usage

View ICMP activity.

Syntax Options

view icmp (No additional syntax options are used.)

Corresponding UI Command

icmps

Screen Output

A screen similar to the following will be displayed:

ICMP Statistics

	In	Out
Total ICMP Messages	1	1
Redirect Messages	0	0
Echo Messages	1	0
Echo Reply Messages	0	1
Time Stamp Messages	0	0
Time Stamp Reply Messages	0	0
Address Mask Messages	0	0
Address Mask Reply Messages	0	0

ICMP Errors

	In	Out
Errors	0	0
Destination Unreachable Msgs	0	0
Time Exceeded Msgs	0	0
Parameter Problems	0	0
Source Quenches	0	0

Table Description

Total ICMP Messages. The total number of ICMP messages which this switch received or attempted to send out.

Redirect Messages. The number of ICMP Redirect messages sent/received by this switch.

Echo Messages. The number of ICMP Echo messages sent/received by this switch to see if a destination is active and reachable.

Echo Reply Messages. The number of ICMP Echo Reply messages received by this switch.

Time Stamp Messages. The number of Time Stamp Request messages sent/received by this switch requesting/receiving a reply with timestamp.

Time Stamp Reply Messages. The number of Time Stamp Reply messages sent/received by this switch.

Address Mask Messages. The number of Address Mask Reply messages that were sent/received by this switch in an attempt to determine the subnet mask for a network.

Address Mask Reply Messages. The number of Address Mask Reply messages that were sent/received by this switch.

Errors. The number of ICMP messages this switch sent/received but was unable to process because something was wrong (for example, a checksum failure).

Destination Unreachable Msgs. The number of ICMP "destination unreachable" messages that were sent/received. These occur when the gateway is unable to route a datagram to its destination.

Time Exceeded Msgs. The number of "time exceeded" messages that were sent/received. These occur when a packet is dropped because the Time-to-Live counter reaches zero. When a large number of these messages are encountered this is a symptom that packets are looping, that congestion is severe, or that the Time-to-Live counter is set too low. These messages also occur when all the fragments trying to be reassembled don't arrive before the reassembly timer expires.

Parameter Problems. The number of messages sent/received which indicate that an illegal value has been detected in a header field. These messages can indicate a problem in the sending host's IP software or possibly in the gateway's software.

Source Quenches. The number of messages sent/received which tell a host that is sending too many packets. A host should attempt to reduce its transmissions upon receiving these messages.

view ip route

Command Usage

View the IP Routing Table.

Syntax Options

view ip route (No additional syntax options are used.)

Corresponding UI Command

ipr

Screen Output

A screen similar to the following will be displayed:

IP ROUTING TABLE

Network	Mask	Gateway	Metric	Group VLAN Id: Id
0.0.0.0	255.0.0.0	198.206.184.254	1	STATIC
10.0.0.0	255.0.0.0	10.0.0.1	1	6:1
11.0.0.0	255.0.0.0	11.0.0.1	1	5:1
90.0.0.0	255.0.0.0	90.0.0.3	1	4:1
127.0.0.0	255.0.0.0	127.0.0.1	0	LOOPBACK
127.0.0.1	255.255.255.255	127.0.0.1	0	LOOPBACK
196.196.7.0	255.255.255.0	196.196.7.42	1	3:1
198.206.184.0	255.255.255.0	198.206.184.42	1	1:1
203.229.229.0	255.255.255.0	203.229.229.250	1	2:1

Table Description

Network. The destination network IP address.

Mask. The IP subnet mask.

Gateway. The network address of the gateway (the router from which this address was learned).

Metric. The metric associated with this network. Generally, this is a RIP "hop" count, or the number of hops the network is away from this router.

Group ID. The group number from which this IP address was learned.

VLAN ID. The VLAN number from which this IP address was learned.

view ip traffic

Command Usage

View IP datagram traffic and errors.

Syntax Options

view ip traffic (No additional syntax options are used.)

Corresponding UI Command

ips

Remarks

The **view ip traffic** command displays *cumulative* IP statistics and errors. The statistics show the cumulative totals since the last time the switch was powered on or since the last reset of the switch was executed.

Screen Output

A screen similar to the following will be displayed:

```
 IP Statistics and Errors

Default Time to Live                    32
Reassembly Timeout (seconds)            1

Total Datagrams Recvd/Forwarded         77972 / 58177
HRE Datagrams Forwarded                 0
PDUs Requested for Transmit             4294931545
PDUs Needing Reassembly                 0
PDUs Successfully Reassembled           0
PDUs Needing Fragmentation              0
Fragments created                       0

   IP Errors (Discards due to the following problems)
Header errors                           0
Address errors                          45994
Unknown/Unsupported Protocol            0
Local discards inbound/outbound         0 / 0
Unknown Route                           45994
Reassembly Failures                     0
Fragmentation Failures                  0
```

Table Description

Default Time to Live. The default time, in seconds, assigned to each outgoing IP datagram before it is discarded as expired.

Reassembly Timeout (seconds). The time, in seconds, to wait for all fragments to arrive before discarding datagrams.

Total Datagrams Recvd/Forwarded. The total number of input IP datagrams received, including those received in error.

HRE Datagrams Forwarded. The total number of IP datagrams forwarded by the HRE (Hardware Routing Engine).

PDUs Requested for Transmit. The total number of IP datagrams which transmit local IP user-protocols (including ICMP) supplied to IP in requests for transmission, not including forwarded datagrams.

PDUs Needing Reassembly. The number of IP datagram fragments that needed to be reassembled by this switch.

PDUs Successfully Reassembled. The number of IP datagrams successfully reassembled by this switch.

PDUs Needing Fragmentation. The number of IP datagrams requiring fragmentation by this switch.

Fragments created. The number of IP datagram fragments that have been generated as a result of fragmentation by this switch.

Header errors. The number of input IP datagrams discarded due to errors in their IP header, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discarded in processing their IP options, etc.

Address errors. The number of input IP datagrams discarded because the IP header destination field contained an invalid address.

Unknown/Unsupported Protocol. The number of local addresses, unsupported protocols, datagrams received successfully but discarded because of an unknown or unsupported protocol.

Local discards inbound/outbound. The number of packets discarded, both inbound and outbound, though they had no errors to prevent their being transmitted (lack of buffer space, etc.).

Unknown Route. The number of packets received and discarded by IP because IP was unable to route them.

Reassembly Failures. The number of failures detected by the IP reassembly algorithm for all reasons (timed out, error, etc.) This value is not necessarily a count of the discarded fragments.

Fragmentation Failures. The number of IP datagrams discarded because they needed to be fragmented but could not be. This situation could happen when a large packet has the “Don’t Fragment” flag set.

arp

Command Usage

Manually add an IP address entry and other information to the ARP Table.

Syntax Options

arp <*ip-address***> <***hardware-address***> [alias | proxy] [permanent] [trailer]**

Definitions:
ip-address = the IP address you want to add (e.g., **172.23.9.101**)
hardware-address = the corresponding hardware address (i.e., physical data link MAC address) you want to add (e.g., **00:05:02:c0:7f:11**)
alias = specifies that the router should act as a proxy for the corresponding address
proxy = same as **alias**
permanent = specifies that the entry is permanent (i.e., it will not be flushed when the **clear arp-cache** command is executed)
trailer = specifies that trailer encapsulation will be enabled for the ARP table entry

Command Examples:
arp 172.23.8.5 00:20:DA:99:96:55
arp 1.1.1.1 00:90:27:17:F7:EB alias
arp 168.18.140.5 00:90:27:17:F7:EB proxy
arp 0.0.0.0 00:90:27:EB:F7:13 permanent
arp 172.18.140.1 00:20:DA:17:F7:DA trailer
arp 168.1.5.5 00:90:FE:13:27:EB permanent trailer

Corresponding UI Command

xlat

Remarks

The *proxy* or *alias* tag allows the switch to answer all ARP requests directed at the hosts on a subnetwork. As the "proxy" for these hosts, the switch responds with its own MAC address whenever ARP requests come in for any of the hosts on the subnetwork. (Proxy entries will be denoted as **published** in the ARP Table.)

The *permanent* tag indicates that you do not want the entry to be removed by the **clear arp-cache** command. Note that all ARP Table entries, whether they are permanent or temporary, survive across switch reboots. As a result, you must use the **no arp** command when you want to remove permanent entries from the ARP Table.

no arp

Command Usage

Manually remove a *specified* IP address entry from the ARP Table.

Syntax Options

no arp <*ip-address***> <***hardware-address***>**

Definitions:
ip-address = specifies the IP address for the ARP Table entry that is to be removed (e.g., **172.23.9.101**)
hardware-address = specifies a hardware address (i.e., physical data link MAC address) for the ARP Table entry that is to be removed (e.g., **00:05:02:c0:7f:11**)

Command Examples:
no arp 172.23.9.101 00:05:02:c0:7f:11

Corresponding UI Command

xlat

Remarks

The **no arp** command can be used to remove permanent ARP entries.

To remove *all* non-permanent entries from the ARP Table, refer to the **clear arp-cache** command on page 5-25.

clear arp-cache

Command Usage

Remove all non-permanent IP address entries from the ARP Table.

♦ Note ♦

If you want to remove a permanent ARP Table entry, you must use the **no arp** command.

Syntax Options

clear arp-cache (No additional syntax options are used.)

Corresponding UI Command

xlat

view arp

Command Usage

View ARP Table information.

Syntax Options

view arp [*ip-address* **|** *hardware-address***]**

Definitions:
ip-address = corresponding hardware address information for the specified IP address will be displayed
hardware-address = the corresponding IP address for the specified hardware address (i.e., physical data link MAC address) will be displayed

♦ Syntax Note ♦
If you do not specify an IP or hardware address in the command line, ARP information for *all* addresses will be displayed.

Command Examples:
view arp
view arp 172.23.9.101
view arp 00:05:02:c0:7f:11

Corresponding UI Command

xlat

Screen Output

If additional syntax options (hardware or IP address) are entered in the command line, information for only the specified address will be displayed. For example:

```
Corresponding MAC address : 00:20:da:6a:98:40
```

If *no* additional syntax options are entered in the command line, the entire ARP Table will be displayed. For example:

```
 Address Translation Table

  IP Address          at      Physical Address
---------------------         -------------------------
90.0.0.1              at      3/1, dlci=32
198.206.184.34        at      00:05:02:c0:7f:11
198.206.184.254       at      00:20:da:6a:98:40 permanent published trailers
```

Table Description

IP Address. The IP address, in dotted-decimal format, of a specific host or other device.

Physical Address. The MAC address, in hexadecimal format, of the specific host or other device that corresponds to the IP address in the left-hand column. The term **permanent** indicates that the entry is a permanent ARP entry. The term **published** indicates that the router acts as a proxy for the corresponding address. The term **trailers** indicates that trailer encapsulation is enabled.

ip domain-lookup

Command Usage

Enable DNS Resolver function.

Syntax Options

ip domain-lookup (No additional syntax options are used.)

Corresponding UI Command

res

no ip domain-lookup

Command Usage

Disable DNS Resolver function.

Syntax Options

no ip domain-lookup (No additional syntax options are used.)

Corresponding UI Command

res

ip domain-name

Command Usage

Assign a DNS Resolver domain name.

Syntax Options

ip domain-name <*name-string***>**

Definitions:
name-string = user-defined Resolver domain name (e.g., **alcatel.com**)

Command Examples:
ip domain-name alcatel.com

Corresponding UI Command

res

no ip domain-name

Command Usage

Clear a DNS Resolver domain name.

Syntax Options

no ip domain-name <*name-string***>**

Definitions:
name-string = user-defined Resolver domain name to be cleared (e.g., **alcatel.com**)

Command Examples:
no ip domain-name alcatel.com

Corresponding UI Command

res

Remarks

You must first disable the DNS Resolver function using the **no ip domain-lookup** command before clearing a DNS Resolver domain name.

ip name-server

Command Usage

Assign a DNS Resolver server address.

Syntax Options

ip name-server <*ip-address***> [first | last]**

Definitions:
ip-address = IP address to be used as a DNS Resolver server address
first = the specified IP address will be placed *first* in the Resolver server address list
last = the specified IP address will be placed *last* in the Resolver server address list

Command Example:
ip name-server 172.23.9.101
ip name-server 1.1.1.1 first
ip name-server 192.168.10.1 last

Corresponding UI Command

res

no ip name-server

Command Usage

Remove a DNS Resolver server address.

Syntax Options

no ip name-server <*ip-address***>**

Definitions:
ip-address = the DNS Resolver server address to be removed

Command Examples:
no ip name-server 172.23.9.101

Corresponding UI Command

res

Remarks

You must first disable the DNS Resolver function using the **no ip domain-lookup** command before clearing a DNS Resolver domain name.

view dns

Command Usage

View current DNS Resolver information.

Syntax Options

view dns (No additional syntax options are used.)

Corresponding UI Command

res

Screen Output

A screen similar to the following will be displayed:

```
                    DNS Resolver Configuration

1) Resolver Enabled      : Yes
2) Domain                : UNSET
3) Server Address 1      : UNSET
4) Server Address 2      : UNSET
5) Server Address 3      : UNSET
```