Configuring ARP

SYSTEM ADMINISTRATOR GUIDE

Copyright

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

SmartEdge	is a registered trademark of Telefonaktiebolaget LM Ericsson.

Contents

1 Overview

This document provides an overview of the Address Resolution Protocol (ARP) features supported by the SmartEdge router and describes the tasks used to configure, monitor, and administer ARP. This document also provides ARP configuration examples.

This document applies to both the Ericsson SmartEdge® and SM family routers. However, the software that applies to the SM family of systems is a subset of the SmartEdge OS; some of the functionality described in this document may not apply to SM family routers.

For information specific to the SM family chassis, including line cards, refer to the SM family chassis documentation.

For specific information about the differences between the SmartEdge and SM family routers, refer to the Technical Product Description *SM Family of Systems* (part number 5/221 02-CRA 119 1170/1) in the `Product Overview` folder of this Customer Product Information library.

The SmartEdge router supports RFC 826, `An Ethernet Address Resolution Protocol`, also called `Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware`. In addition, the SmartEdge router supports the following features:

- A configurable ARP entry age timer

- The option to enable automatic deletion of dynamic ARP entries (as opposed to automatic refresh of the ARP table)

- The static IP ARP entry mapping of a unicast IP address to a multicast medium access control (MAC) address

2 Configuration and Operations Tasks

Note: In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the *Command List*.

2.1 Enable ARP

To enable ARP, perform the task described in Table 1.

Table 1   Enable ARP

Task	Root Command	Notes
Enable ARP.	*ip arp secured-arp*	Enter this command in interface configuration mode. By default, ARP is already enabled. Use the **no** form of this command to disable ARP.

2.2 Enable Secured ARP (Optional)

To enable secured ARP, perform the task described in Table 2. You can enable either secured ARP or proxy ARP on an interface.

Table 2   Enable Secured ARP (Optional)

Task	Root Command	Notes
Enable secured ARP.	*ip arp secured-arp*	Enter this command in interface configuration mode. ARP must be enabled before you can enable secured ARP.

2.3 Enable Proxy ARP (Optional)

To enable proxy ARP, perform the task described in Table 3. You can enable either secured ARP or proxy ARP on an interface.

Table 3   Enable Proxy ARP (Optional)

Task	Root Command	Notes
Enable proxy ARP.	*ip arp proxy-arp*	Enter this command in interface configuration mode. ARP must be enabled before you can enable proxy ARP.

2.4   Configure Static Entries in the ARP Table (Optional)

To configure static entries in the ARP table, perform the appropriate task described in Table 4. If you use both commands to specify the same IP address and MAC address, the most recently updated command takes precedence.

Table 4   Configure Static Entries in the ARP Table (Optional)

Task	Root Command	Notes
Configure an entry in the ARP table for a subscriber whose host cannot (or is not configured to) respond to ARP requests.	*ip subscriber arp*	Enter this command in subscriber configuration mode.
Configure an entry in the ARP table.	*ip arp*	Enter this command in context configuration mode.

2.5   Configure the Automatic Deletion of ARP Entries (Optional)

To configure the automatic deletion of ARP table entries, perform the tasks described in Table 5; enter all commands in interface configuration mode.

Table 5   Configure the Automatic Deletion of ARP Entries

Task	Root Command	Notes
Configure the automatic deletion of ARP entries.	*ip arp delete-expired*	
Modify the length of time entries remain in the ARP table before being automatically deleted.	*ip arp timeout*	Optional. When you enable the **ip arp delete-expired** command, entries are deleted after 60 minutes by default.

2.6   Set a Maximum Number of Incomplete ARP Entries (Optional)

When requesting the MAC address that corresponds to a particular IP address for a subscriber circuit, the SmartEdge system creates an incomplete entry in the ARP table and sends an ARP request packet. On reply, the entry is updated and completed. By default, the maximum number of incomplete entries that are allowed in the ARP table is 4,294,967,295.

To set a maximum allowable number of incomplete entries, perform the task described in Table 6.

Table 6   Set a Maximum Number of Incomplete ARP Entries (Optional)

Task	Root Command	Notes
Set a maximum allowable number of incomplete ARP entries.	*ip arp maximum incomplete-entries*	Enter this command in context configuration mode.

2.7   Configure an ARP Policy to Prevent DoS Attacks

To configure a subscriber circuit or port to prevent denial of service (DoS) attacks, perform the tasks described in Table 7.

Table 7   Configure a Subscriber Circuit or Circuits or Port to Prevent DoS ARP Attacks

Task	Root Command	Notes
Enter protocol-rate-limit policy configuration mode	*qos policy protocol-rate-limit (global)*	Enter this command in global configuration mode.
Create a rate limit and burst threshold for incoming ARP packets.	*arp rate*	Enter this command in protocol-rate-limit policy configuration mode.
To configure a port for prevention of DoS ARP attacks, enter the port configuration mode.	*port*	Enter this command in global configuration mode.
Apply the ARP policy to the port.	*qos policy protocol-rate-limit*	Enter this command in port configuration mode.
To configure a subscriber circuit or circuits for prevention of DoS ARP attacks, enter the configuration mode for the default subscriber profile, a named subscriber profile, or an individual subscriber record.	*subscriber*	Enter this command in context configuration mode.
Apply the ARP policy to subscriber profile or individual subscriber record.	*qos policy protocol-rate-limit*	Enter this command in subscriber configuration mode.
To configure a 802.1Q PVC for prevention of DoS ARP, enter dot1q PVC configuration mode.	*port encapsulation dot1q*	Enter the **encapsulation** command with the **dot1q** keyword.

Table 7   Configure a Subscriber Circuit or Circuits or Port to Prevent DoS ARP Attacks

Task	Root Command	Notes
Apply the ARP policy to the 802.1Q PVC.	*qos policy protocol-rate-limit*	Enter this command in dot1q PVC configuration mode.
To configure an access link group or aggregated 802.1Q pseudocircuit in an access link group for prevention of DoS ARP, enter the access link group configuration mode or link PVC configuration mode within the link group.	*link-group(Global, DS-1, E1, Port Configuration modes)* *encapsulation dot1q*	Enter the link-group command with the `access` keyword. Enter the `encapsulation` command with the `dot1q` keyword.
Apply the ARP policy to access link group or aggregated 802.1Q pseudocircuit.	*qos policy protocol-rate-limit*	Enter this command in access link-group configuration mode or aggregated link PVC configuration mode.

2.8   Operations Tasks

Note: In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the *Command List*.

To monitor, troubleshoot, and administer ARP features, perform the ARP operations tasks described in Table 8. Enter the `clear` and `debug` commands in exec mode; enter the `show` commands in any mode.

Table 8   ARP Operations Tasks

Task	Root Command
Clear all entries from the ARP table.	*clear arp-cache*
Clear information for cross-connections between ATM PVCs and 802.1Q PVCs from the ARP table.	*clear arp-cache interworking*
Clear traffic statistics from the ARP table.	*clear arp-cache statistics*
Enable the generation of ARP debug messages for the current context.	*debug arp*
Display ARP information for the controller card.	*show arp-cache*

Table 8   ARP Operations Tasks

Task	Root Command
Display ARP information for both the Berkeley Standard Distribution (BSD) and the controller card for the current context.	*show arp-cache all*
Display ARP information for both the BSD and the controller card for all contexts.	*show arp-cache all-context*
Display ARP information for cross-connections between ATM PVCs and 802.1Q PVCs.	*show arp-cache interworking*
Display ARP statistics.	*show arp-cache statistics*
Display summary information about the ARP table.	*show arp-cache summary*
Display ARP information for the controller card.	*show arp-cache xcrp*
Display ARP commands for the current configuration.	*show configuration arp*
Display inverse ARP counters.	*show inverse-arp counters*
Display secured ARP information.	*show secured-arp*

31/1543-CRA 119 1170/1-V1 Uen G | 2011-10-30

3 Configuration Examples

The following example enables secured ARP on the interface, **intf-1:**

```
[local]Redback(config-ctx)#interface intf-1

[local]Redback(config-if)#ip arp secured-arp
```

The following example creates a static entry in the ARP table for IP address, **31.22.213.124**, and associates the IP address with the MAC address, **43:3:23:32:12:82**. After 4 minutes (**240** seconds), any ARP entry associated with the **intf-2** interface is deleted from the ARP table:

```
[local]Redback(config-ctx)#ip arp 31.22.213.124 43:32:23:32:12:82

[local]Redback(config-ctx)#interface intf-2

[local]Redback(config-if)#ip arp delete-expired

[local]Redback(config-if)#ip arp timeout 240
```