



## Monitoring Interfaces

---

ASDM lets you monitor interface statistics as well as interface-related features.

### ARP Table

The ARP Table pane displays the ARP table, including static and dynamic entries. The ARP table includes entries that map a MAC address to an IP address for a given interface. See Configuration > Properties > [ARP Static Table](#) for more information about the ARP table.

#### Fields

- **Interface**—Lists the interface name associated with the mapping.
  - IP Address—Shows the IP address.
  - MAC Address—Shows the MAC address.
  - Proxy ARP—Displays Yes if proxy ARP is enabled on the interface. Displays No if proxy ARP is not enabled on the interface.
  - Clear—Clears the dynamic ARP table entries. Static entries are not cleared.
  - Refresh—Refreshes the table with current information from the security appliance and updates Last Updated date and time.
  - Last Updated—*Display only*

#### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	

### DHCP

The security appliance lets you monitor DHCP status, including the addresses assigned to clients, the lease information for a security appliance interface, and DHCP statistics.

## DHCP Server Table

### Fields

- 
- 
- Lease Expiration—Shows the date that the DHCP lease expires. The lease indicates how long the client can use the assigned IP address. Remaining time is also specified in the number of seconds and is based on the timestamp in the Last Updated display-only field.
- Number of Active Leases—Shows the total number of DHCP leases.
- Refresh—Refreshes the information from the security appliance.
- Last Updated—Shows when the data in the table was last updated.

### Modes

The following table shows the modes in which this feature is available:



## DHCP Client Lease Information

### Fields

- 
- Attribute and Value—Lists the attributes and values of the interface DHCP lease.
  - Temp sub net mask— . The subnet mask assigned to the interface.
  - DHCP lease server— . The DHCP server address.
  - state— . The state of the DHCP lease, as follows:
    - Initial—The initialization state, where the security appliance begins the process of acquiring a lease. This state is also shown when a lease ends or when a lease negotiation fails.
    - Selecting—The security appliance is waiting to receive DHCPOFFER messages from one or more DHCP servers, so it can choose one.
    - Requesting—The security appliance is waiting to hear back from the server to which it sent its request.
    - Purging—The security appliance is removing the lease because of an error.

- Bound—The security appliance has a valid lease and is operating normally.
- Renewing—The security appliance is trying to renew the lease. It regularly sends DHCPREQUEST messages to the current DHCP server, and waits for a reply.
- Rebinding—The security appliance failed to renew the lease with the original server, and now sends DHCPREQUEST messages until it gets a reply from any server or the lease ends.
- Holddown—The security appliance started the process to remove the lease.
- Releasing—The security appliance sends release messages to the server indicating that the IP address is no longer needed.
- Lease— . The length of time, specified by the DHCP server, that the interface can use this IP address.
- Renewal— . The length of time until the interface automatically attempts to renew this lease.
- Rebind— . The length of time until the security appliance attempts to rebind to a DHCP server. Rebinding occurs if the security appliance cannot communicate with the original DHCP server, and 87.5 percent of the lease time has expired. The security appliance then attempts to contact any available DHCP server by broadcasting DHCP requests.
- Next timer fires after— . The number of seconds until the internal timer triggers.
- Retry count— . If the security appliance is attempting to establish a lease, this field shows the number of times the security appliance tried sending a DHCP message. For example, if the security appliance is in the Selecting state, this value shows the number of times the security appliance sent discover messages. If the security appliance is in the Requesting state, this value shows the number of times the security appliance sent request messages.
- Client-ID— . The client ID used in all communication with the server.
- Proxy— . Specifies if this interface is a proxy DHCP client for VPN clients, True or False.
- Hostname— . The client hostname.

The following table shows the modes in which this feature is available:


## DHCP Statistics

The

DHCPACK

DHCPNAK

- Count—Shows the number of times a specific message was processed.
- Direction—Shows if the message type is Sent or Received.
- Total Messages Received—Shows the total number of messages received by the security appliance.
- Total Messages Sent—Shows the total number of messages sent by the security appliance.
- Counter—Shows general statistical DHCP data, including the following:
  - DHCP UDP Unreachable Errors
  - DHCP Other UDP Errors
  - Address Pools
  - Automatic Bindings
  - Expired Bindings
  - Malformed Messages
- Value—Shows the number of each counter item.
- Refresh—Updates the DHCP table listings.
- Last Updated—Shows when the data in the tables was last updated.

**Modes**

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	

# MAC Address Table

**Fields**

- 
-

- 
- 
- 

### Modes

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
—	•	•	•	—

## Dynamic ACLs

identified by the “(dynamic)” keyword in the ACL header.

When you choose an ACL in this table, the contents of the ACL is shown in the bottom text field.

ACL—Shows the name of the dynamic ACL.

Element Count—Shows the number of elements in the ACL

Hit Count—Shows the total hit count for all of the elements in the ACL.

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Interface Graphs

The Interface Graphs pane lets you view interface statistics in graph or table form. If an interface is shared among contexts, the security appliance shows only statistics for the current context. The number of statistics shown for a subinterface is a subset of the number of statistics shown for a physical interface.

**Fields**

- 

have more than one error; therefore, this sum might exceed the number of errors listed for the other types.

**Runts**—The number of packets that are discarded because they are smaller than the minimum packet size, which is 64 bytes. Runts are usually caused by collisions. They might also be caused by poor wiring and electrical interference.

**Giants**—The number of packets that are discarded because they exceed the maximum packet size. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.

**Deferred**—For FastEthernet interfaces only. The number of frames that were deferred before transmission due to activity on the link.

**Miscellaneous**—Shows statistics for received broadcasts.

**Collision Counts**—For FastEthernet interfaces only. Shows the following statistics:

**Output Errors**—The number of frames not transmitted because the configured maximum number of collisions was exceeded. This counter should only increment during heavy network traffic.

**Collisions**—The number of messages retransmitted due to an Ethernet collision (single and multiple collisions). This usually occurs on an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once by the output packets.

**Late Collisions**—The number of frames that were not transmitted because a collision occurred outside the normal collision window. A late collision is a collision that is detected late in the transmission of the packet. Normally, these should never happen. When two Ethernet hosts try to talk at once, they should collide early in the packet and both back off, or the second host should see that the first one is talking and wait. If you get a late collision, a device is jumping in and trying to send the packet on the Ethernet while the security appliance is partly finished sending the packet. The security appliance does not resend the packet, because it may have freed the buffers that held the first part of the packet. This is not a real problem because networking protocols are designed to cope with collisions by resending packets. However, late collisions indicate a problem exists in your network. Common problems are large repeated networks and Ethernet networks running beyond the specification.

**Input Queue**—Shows the number of packets in the input queue, the current and the maximum, including the following statistics:

**Hardware Input Queue**—The number of packets in the hardware queue.

**Software Input Queue**—The number of packets in the software queue.

**Output Queue**—Shows the number of packets in the output queue, the current and the maximum, including the following statistics:

**Hardware Output Queue**—The number of packets in the hardware queue.

**Software Output Queue**—The number of packets in the software queue.

**Drop Packet Queue**—Shows the number of packets dropped.

**Add**—Adds the selected statistic type to the selected graph window.

**Remove**—Removes the selected statistic type from the selected graph window. This button name changes to Delete if the item you are removing was added from another panel, and is not being returned to the Available Graphs pane.

**Show Graphs**—Shows the graph window name to which you want to add a statistic type. If you have a graph window already open, a new graph window is listed by default. If you want to add a statistic type to an already open graph, choose the open graph window name. The statistics already included on the graph are shown in the Selected Graphs pane, to which you can add additional types. Graph windows are named for ASDM followed by the interface IP address and the name “Graph”. Subsequent graphs are named “Graph (2)” and so on.

**Selected Graphs**—Shows the statistic types you want to show in the selected graph window. You can include up to four types.

**Show Graphs**—Shows the graph window or updates the graph with additional statistic types if added.

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	

## Graph/Table

### Fields

- 

Real-time, data every 10 sec

Last 10 minutes, data every 10 sec

Last 60 minutes, data every 1 min

Last 12 hours, data every 12 min

Last 5 days, data every 2 hours

- Export—Exports the graph in comma-separated value format. If there is more than one graph or table on the Graph window, the Export Graph Data dialog box appears. Choose one or more of the graphs and tables listed by checking the box next to the name.
- Print—Prints the graph or table. If there is more than one graph or table on the Graph window, the Print Graph dialog box appears. Choose the graph or table you want to print from the Graph/Table Name list.

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	

## PPPoE Client

### Fields

# *interface*

*interface*

, page 41-9

Monitoring Statistics for, page 41-9

## Track Status for

### Fields

- 
- 

### Modes

Firewall Mode		Security Context		
			Multiple	
Routed	Transparent	Single	Context	System
•		•		

## Monitoring Statistics for

### Fields

- 
- 

### Modes

Firewall Mode		Security Context		
			Multiple	
Routed	Transparent	Single	Context	System
•		•		

