



## 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.* Shows the date and time the display was updated.

#### 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

The DHCP Server Table lists the IP addresses assigned to DHCP clients.

### Fields

- IP Address—Shows the IP address assigned to the client.
- Client-ID—Shows the client MAC address or ID.
- 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:

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

## DHCP Client Lease Information

If you obtain the security appliance interface IP address from a DHCP server, the DHCP Client Lease Information panel shows information about the DHCP lease.

### Fields

- Select an interface—Lists the security appliance interfaces. Choose the interface for which you want to view the DHCP lease. If an interface has multiple DHCP leases, then choose the interface and IP address pair you want to view.
- Attribute and Value—Lists the attributes and values of the interface DHCP lease.
  - Temp IP addr—*Display only*. The IP address assigned to the interface.
  - Temp sub net mask—*Display only*. The subnet mask assigned to the interface.
  - DHCP lease server—*Display only*. The DHCP server address.
  - state—*Display only*. 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**—*Display only*. The length of time, specified by the DHCP server, that the interface can use this IP address.
- **Renewal**—*Display only*. The length of time until the interface automatically attempts to renew this lease.
- **Rebind**—*Display only*. 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**—*Display only*. The number of seconds until the internal timer triggers.
- **Retry count**—*Display only*. 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**—*Display only*. The client ID used in all communication with the server.
- **Proxy**—*Display only*. Specifies if this interface is a proxy DHCP client for VPN clients, True or False.
- **Hostname**—*Display only*. The client hostname.

### Modes

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

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

## DHCP Statistics

The DHCP Statistics pane shows statistics for the DHCP server feature.

### Fields

- **Message Type**—Lists the DHCP message types sent or received:
  - BOOTREQUEST
  - DHCPDISCOVER

- DHCPREQUEST
- DHCPDECLINE
- DHCPRELEASE
- DHCPINFORM
- BOOTREPLY
- DHCPOFFER
- 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

The MAC Address Table pane shows the static and dynamic MAC address entries. See Configuration > Properties > Bridging > [MAC Address Table](#) for more information about the MAC address table and adding static entries.

### Fields

- Interface—Shows the interface name associated with the entry.
- MAC Address—Shows the MAC address.

- Type—Shows if the entry is static or dynamic.
- Age—Shows the age of the entry, in minutes. To set the timeout, see [MAC Address Table](#).
- Refresh—Refreshes the table with current information from the security appliance.

### Modes

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

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

## Dynamic ACLs

The Dynamic ACLs pane shows a table of the Dynamic ACLs, which are functionally identical to the user-configured ACLs except that they are created, activated and deleted automatically by the security appliance. These ACLs do not show up in the configuration and are only visible in this table. They are 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.

### Fields

- 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.

### Modes

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

- Available Graphs for—Lists the types of statistics available for monitoring. You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.
  - Byte Counts—Shows the number of bytes input and output on the interface.
  - Packet Counts—Shows the number of packets input and output on the interface.
  - Packet Rates—Shows the rate of packets input and output on the interface.
  - Bit Rates—Shows the bit rate for the input and output of the interface.
  - Drop Packet Count—Shows the number of packets dropped on the interface.

These additional statistics display for physical interfaces:

- Buffer Resources—Shows the following statistics:
  - Overruns—The number of times that the security appliance was incapable of handing received data to a hardware buffer because the input rate exceeded the security appliance capability to handle the data.
  - Underruns—The number of times that the transmitter ran faster than the security appliance could handle.
  - No Buffer—The number of received packets discarded because there was no buffer space in the main system. Compare this with the ignored count. Broadcast storms on Ethernet networks are often responsible for no input buffer events.
- Packet Errors—Shows the following statistics:
  - CRC—The number of Cyclical Redundancy Check errors. When a station sends a frame, it appends a CRC to the end of the frame. This CRC is generated from an algorithm based on the data in the frame. If the frame is altered between the source and destination, the security appliance notes that the CRC does not match. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
  - Frame—The number of frame errors. Bad frames include packets with an incorrect length or bad frame checksums. This error is usually the result of collisions or a malfunctioning Ethernet device.
  - Input Errors—The number of total input errors, including the other types listed here. Other input-related errors can also cause the input error count to increase, and some datagrams might 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.

### Modes

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

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

## Graph/Table

The Graph window shows a graph for the selected statistics. The Graph window can show up to four graphs and tables at a time. By default, the graph or table displays the real-time statistics. If you enable [History Metrics, page 10-6](#), you can view statistics for past time periods.

### Fields

- View—Sets the time period for the graph or table. To view any time period other than real-time, enable [History Metrics, page 10-6](#). The data is updated according to the specification of the following options:
  - 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.
- Bookmark—Opens a browser window with a single link for all graphs and tables on the Graphs window, as well as individual links for each graph or table. You can then copy these URLs as bookmarks in your browser. ASDM does not have to be running when you open the URL for a graph; the browser launches ASDM and then displays the graph.

### Modes

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

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

## PPPoE Client

The PPPoE Client Lease Information pane displays information about current PPPoE connections.

**Fields**

Select a PPPoE interface—Select an interface that you want to view PPPoE client lease information.

Refresh—loads the latest PPPoE connection information from the security appliance for display.

## interface connection

The *interface* connection node in the Monitoring > Interfaces tree only appears if static route tracking is configured. If you have several routes tracked, there will be a node for each interface that contains a tracked route.

See the following for more information about the route tracking information available:

- [Track Status for, page 44-9](#)
- [Monitoring Statistics for, page 44-9](#)

## Track Status for

The Track Status for pane displays information about the the tracked object.

**Fields**

- Tracked Route—*Display only*. Displays the route associated with the tracking process.
- Route Statistics—*Display only*. Displays the reachability of the object, when the last change in reachability occurred, the operation return code, and the process that is performing the tracking.

**Modes**

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

## Monitoring Statistics for

The Monitoring Statics for pane displays statistics for the SLA monitoring process.

**Fields**

- SLA Monitor ID—*Display only*. Displays the ID of the SLA monitoring process.
- SLA statistics—*Display only*. Displays SLA monitoring statistics, such as the last time the process was modified, the number of operations attempted, the number of operations skipped, and so on.

**Modes**

Firewall Mode		Security Context		
<b>Routed</b>	<b>Transparent</b>	<b>Single</b>	<b>Multiple</b>	
			<b>Context</b>	<b>System</b>
•	—	•	—	—