



## TCP/IP Normalization and IP Reassembly Parameters Commands on the Virtual Firewall

---

This module describes the commands necessary to configure TCP/IP normalization and IP reassembly for the VFW application. For information regarding configuring TCP/IP normalization and IP reassembly, refer to the [“Configuring TCP/IP Normalization and IP Reassembly Parameters on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.



### Note

---

The commands described in this module are SanOS (Linux) commands used on the VFW application. Before you can access any of these commands, you must attach from the route processor to the VFW application using the [service firewall attach location](#) command. For more information, see the [“Attaching to the VFW Application”](#) section in *Cisco IOS XR Virtual Firewall Configuration Guide*.

---

# clear conn

To clear a connection that passes through, terminates, or originates with the VFW application, use the **clear conn** command in EXEC mode.

```
clear conn [all | flow {prot_number | icmp | tcp | udp {source_ip | source_port | dest_ip |
dest_port}}]
```

## Syntax Description

<b>all</b>	(Optional) Clears all connections, which includes the connections that go through the VFW application, originate with the VFW application, or terminate with the VFW application.
<b>flow</b>	(Optional) Clears the connection matching the specified flow descriptor.
<i>prot_number</i>	Protocol number of the flow.
<b>icmp</b>	Specifies flow types using ICMP.
<b>tcp</b>	Specifies flow types using TCP.
<b>udp</b>	Specifies flow types using UDP.
<i>source_ip</i>	Source IP address of the flow. Enter an IP address in dotted-decimal notation.
<i>source_port</i>	Source port of the flow.
<i>dest_ip</i>	Destination IP address of the flow. Enter an IP address in dotted-decimal notation.
<i>dest_port</i>	Destination port of the flow.

## Defaults

No default behavior or values

## Command Modes

EXEC

## Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

## Usage Guidelines

This command requires the inspect, NAT, connection, or SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

To clear only the connections that go through the VFW application (flows that pass through the VFW application between the originating network host and the terminating network host), use the **clear conn** command without any keywords. When you do not include any keywords, the connections that terminate or originate with the VFW application are not cleared.

---

**Examples**

The following example shows how to clear the connections:

```
firewall/Admin# clear conn
```

---

**Related Commands**

Command	Description
<a href="#">show conn</a>	Displays the connection statistics.

---

# clear icmp statistics

To clear the Internet Control Message Protocol (ICMP) statistics, use the **clear icmp statistics** command in EXEC mode.

## clear icmp statistics

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values

**Command Modes** EXEC

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

**Usage Guidelines** This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

**Examples** The following example shows how to clear the ICMP statistics:

```
firewall/Admin# clear icmp statistics
```

Related Commands	Command	Description
	<a href="#">show icmp statistics</a>	Displays the Internet Control Message Protocol (ICMP) statistics.

# clear stats

To clear the statistical information stored in the VFW application buffer, use the **clear stats** command in EXEC mode.

```
clear stats {all | connections | http | inspect}
```

Syntax Description		
<b>all</b>	(Optional)	Clears all statistical information in a context.
<b>connections</b>	(Optional)	Clears connection statistical information.
<b>http</b>	(Optional)	Clears HTTP statistical information.
<b>inspect</b>	(Optional)	Clears HTTP inspect statistical information.

**Defaults** No default behavior or values

**Command Modes** EXEC

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

**Usage Guidelines** This command requires the inspect, NAT, connection, or SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

**Examples** The following example shows how to clear the system buffer:

```
firewall/Admin# clear buffer stats
```

Related Commands	Command	Description
	<a href="#">show stats</a>	Displays the statistical information relating to the operation of the VFW application.

# clear tcp statistics

To clear all the TCP connections and normalization statistics, use the **clear tcp statistics** command in EXEC mode.

## clear tcp statistics

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values

**Command Modes** EXEC

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

**Usage Guidelines** This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

**Examples** The following example shows how to clear the TCP statistics:

```
firewall/Admin# clear tcp statistics
```

Related Commands	Command	Description
	<a href="#">show tcp statistics</a>	Displays the Transmission Control Protocol (TCP) statistics.

# clear udp statistics

To clear the User Datagram Protocol (UDP) connection statistics, use the **clear udp statistics** command in EXEC mode.

## clear udp statistics

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values

**Command Modes** EXEC

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

**Usage Guidelines** This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

**Examples** The following example shows how to clear the UDP statistics:

```
firewall/Admin# clear udp statistics
```

Related Commands	Command	Description
	<a href="#">show udp statistics</a>	Displays the UDP statistics.

# fragment chain

To configure the maximum number of fragments belonging to the same packet that the VFW application accepts for reassembly for an interface, use the **fragment chain** command in the appropriate interface configuration mode. To reset the default value, use the **no** form of this command.

**fragment chain** *number*

**no fragment chain**

## Syntax Description

<i>number</i>	Maximum number of fragments belonging to the same packet. Enter an integer from 1 to 256.
---------------	---

## Defaults

By default, the maximum number of fragments is 24.

## Command Modes

Interface configuration  
Management interface configuration

## Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

## Usage Guidelines

This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

## Examples

The following example shows how to configure a fragment chain limit of 126:

```
firewall/C1(config-if)# fragment chain 126
```

## Related Commands

Command	Description
<a href="#">fragment timeout</a>	Configures a reassembly timeout for an interface.
<a href="#">show fragment</a>	Displays the IP fragmentation and reassembly statistics for all interfaces in the VFW application or the specified interface.

# fragment min-mtu

To configure the minimum fragment size that the VFW application accepts for reassembly for an interface, use the **fragment min-mtu** command in the appropriate interface configuration mode. To reset the default value, use the **no** form of this command.

**fragment min-mtu** *number*

**no fragment min-mtu**

## Syntax Description

<i>number</i>	The minimum fragment size. Enter an integer from 68 to 9216 bytes. The default is 576 bytes.
---------------	--

## Defaults

By default, minimum fragment size is 576 bytes.

## Command Modes

Interface configuration  
Management interface configuration

## Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

## Usage Guidelines

This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

## Examples

The following example shows how to configure a minimum fragment size of 1024:

```
firewall/C1(config-if)# fragment min-mtu 1024
```

## Related Commands

Command	Description
<a href="#">fragment chain</a>	Configures the maximum number of fragments belonging to the same packet that the VFW application accepts for reassembly for an interface.
<a href="#">fragment timeout</a>	Configures a reassembly timeout for an interface.
<a href="#">show fragment</a>	Displays the IP fragmentation and reassembly statistics for all interfaces in the VFW application or the specified interface.

# fragment timeout

To configure a reassembly timeout for an interface, use the **fragment timeout** command in the appropriate interface configuration mode. To reset the default value, use the **no** form of this command.

**fragment timeout** *seconds*

**no fragment timeout**

<b>Syntax Description</b>	<i>seconds</i>	Reassembly timeout in seconds. Enter an integer from 0 to 65535. A value of 0 instructs the VFW application to never time out.
---------------------------	----------------	--

**Defaults** The default reassembly timeout is 10 seconds.

**Command Modes** Interface configuration  
Management interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

**Usage Guidelines** This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

The IP reassembly timeout specifies the period of time after which the VFW application abandons the fragment reassembly process if it does not receive any outstanding fragments for the current fragment chain (fragments belonging to the same packet).

**Examples** The following example shows how to configure an IP reassembly timeout of 750 seconds:

```
firewall/C1(config-if)# fragment timeout 750
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">fragment chain</a>	Configures the maximum number of fragments belonging to the same packet that the VFW application accepts for reassembly for an interface.
	<a href="#">show fragment</a>	Displays the IP fragmentation and reassembly statistics for all interfaces in the VFW application or the specified interface.

# icmp-guard

To enable the Internet Control Message Protocol (ICMP) security checks in the VFW application, use the **icmp-guard** command in the appropriate interface configuration mode. To disable the ICMP security checks, use the **no** form of this command.

**icmp-guard**

**no icmp-guard**

## Syntax Description

This command has no arguments or keywords.

## Defaults

This feature is enabled by default.

## Command Modes

Interface configuration  
Management interface configuration

## Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

## Usage Guidelines

This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

By default, the VFW application provides several ICMP security checks by matching ICMP reply packets with request packets and using mismatched packets to detect attacks. Also, the VFW application forwards ICMP error packets only if a connection record exists pertaining to the flow for which the error packet was received.



### Caution

Disabling the VFW application ICMP security checks may expose your VFW application and your data center to potential security risks. After you enter the **no icmp-guard** command, the VFW application no longer performs NAT translations on the ICMP header and payload in error packets, which potentially can reveal real host IP addresses to attackers.

## Examples

The following example shows how to enable the VFW application ICMP security checks after you have disabled them:

```
firewall/Admin(config)# interface xyz
firewall/Admin(config-if)# icmp-guard
```

■ icmp-guard

Related Commands	Command	Description
	<a href="#">normalization</a>	Enables the ICMP security checks in the VFW application.

# ip df

To configure how the VFW application handles an IP packet that has its Don't Fragment (DF) bit set on an interface, use the **ip df** command in interface configuration mode. To instruct the VFW application to ignore the DF bit, use the **no** form of this command.

```
ip df {clear | allow}
```

```
no ip df
```

## Syntax Description

<b>clear</b>	Clears the DF bit and permits the packet. If the packet is larger than the next-hop MTU, the VFW application fragments the packet.
<b>allow</b>	(Default) Permits the packet with the DF bit set. If the packet is larger than the next-hop MTU, the VFW application discards the packet and sends an ICMP unreachable message to the source host.

## Defaults

No default behavior or values

## Command Modes

Interface configuration

## Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

## Usage Guidelines

This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Occasionally, a VFW application may receive a packet that has its Don't Fragment (DF) bit set in the IP header. This flag tells network routers and the VFW application not to fragment the packet and to forward it in its entirety.

## Examples

The following example shows how to clear the DF bit and permit the packet:

```
firewall/Admin(config-if)# ip df clear
```

## Related Commands

This command has no related commands.

# ip options

To configure how the VFW application handles IP options and to perform specific actions when an IP option is set in a packet for an interface, use the **ip-options** command in interface configuration mode. To instruct the VFW application to ignore the IP option, use the **no** form of this command.

**ip options** { **clear** | **clear-invalid** | **allow** | **drop** }

**no ip options**

## Syntax Description

<b>allow</b>	Allows the packet with the IP options set.
<b>clear</b>	Clears the specified option from the packet and allows the packet.
<b>clear-invalid</b>	(Default) Clears all IP options from the packet if the VFW application encounters one or more invalid or unsupported IP options and allows the packet.
<b>drop</b>	Causes the VFW application to discard the packet.

## Defaults

No default behavior or values

## Command Modes

Interface configuration

## Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

## Usage Guidelines

This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

## Examples

The following example shows how to allow packets with IP options set:

```
firewall/Admin(config-if)# ip options allow
```

The following example shows how to reset the VFW application behavior to the default of clearing all IP options if the module encounters one or more invalid or unsupported IP options:

```
firewall/Admin(config-if)# no ip options
```

## Related Commands

This command has no related commands.

# ip ttl

To set the packet time-to-live (TTL) hops in the IP header on an interface, use the **ip ttl** command in interface configuration mode. To reset the default behavior, use the **no** form of this command.

**ip ttl minimum** *number*

**no ip ttl minimum**

## Syntax Description

<i>number</i>	Minimum number of hops that a packet can take to reach its destination. Enter an integer from 1 to 255 seconds.
---------------	---

## Defaults

The default behavior of the VFW application is to not rewrite the TTL value of a packet.

## Command Modes

Interface configuration mode  
Admin and user contexts

## Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

## Usage Guidelines

This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Each router along the packet’s path decrements the TTL by one. If the packet’s TTL equals 0 before the packet reaches its destination, the packet is discarded.

If the TTL value of the incoming packet is lower than the configured value, the VFW application rewrites the TTL with the configured value. Otherwise, the VFW application transmits the packet with its TTL unchanged or discards the packet if the TTL equals zero.

## Examples

The following example shows how to set the TTL hops to 15:

```
firewall/Admin(config-if)# ip ttl minimum 15
```

## Related Commands

This command has no related commands.

# normalization

To enable TCP normalization, use the **normalization** command in interface configuration mode. To disable TCP normalization, use the **no** form of this command.

**normalization**

**no normalization**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Normalization is enabled by default.

**Command Modes** Interface configuration

## Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

## Usage Guidelines

This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

By default, TCP normalization is enabled.



### Caution

Disabling TCP normalization may expose your VFW application and your data center to potential security risks. TCP normalization helps protect the VFW application and the data center from attackers by enforcing strict security policies that are designed to examine traffic for malformed or malicious segments.

To operate your VFW application for load balancing only, disable TCP normalization by entering the **no normalization** command. You must also disable the VFW application ICMP security checks using the **no icmp-guard** command.

## Examples

The following example shows how to enable TCP normalization after you have disabled it:

```
firewall/Admin(config)# interface xyz
firewall/Admin(config-if)# normalization
```

Related Commands	Command	Description
	<a href="#">icmp-guard</a>	Enables the ICMP security checks in the VFW application.

# show conn

To display the connection statistics, use the **show conn** command in EXEC mode.

```
show conn {address ip_address1 [ip_address2] netmask mask} | count | detail | {port number1
[number2]} | {protocol {tcp | udp}}
```

Syntax Description		
<b>address</b> <i>ip_address1</i> [ <i>ip_address2</i> ]	Displays connection statistics for a single source or destination IP address or, optionally, for a range of source or destination IP addresses. To specify a range of IP addresses, enter an IP address for the lower limit of the range and a second IP address for the upper limit of the range. Enter one or two IP addresses in dotted-decimal notation.	
<b>count</b>	Displays the total current connections to the VFW application.	
<b>detail</b>	Displays detailed connection information.	
<b>netmask</b> <i>mask</i>	Specifies the network mask for the IP address or range of IP addresses you specify. Enter a network mask in dotted-decimal notation.	
<b>port</b> <i>number1</i> [ <i>number2</i> ]	Displays connection statistics for a single source or destination port or, optionally, for a range of source or destination ports.	
<b>protocol</b> { <b>tcp</b>   <b>udp</b> }	Displays connection statistics for TCP or UDP.	

**Defaults** No default behavior or values

**Command Modes** EXEC

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

**Usage Guidelines** This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

**Examples** The following example shows how to display connection statistics for a range of IP addresses:

```
firewall/Admin# show conn address 192.168.12.15 192.168.12.35 netmask 255.255.255.0
```

Related Commands	Command	Description
	<a href="#">clear conn</a>	Clears a connection that passes through, terminates, or originates with the VFW application.

# show fragment

To display the IP fragmentation and reassembly statistics for all interfaces in the VFW application or the specified interface, use the **show fragment** command in EXEC mode.

**show fragment** [**interface** *interface\_name*]

<b>Syntax Description</b>	<b>interface</b> (Optional) Specifies an existing interface. <i>interface_name</i>
---------------------------	---

**Defaults** No default behavior or values

**Command Modes** EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

**Usage Guidelines** This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

If you omit the **interface** *interface\_name* optional keyword and argument, you can display statistics for all interfaces in the VFW application.

**Examples** The following example shows how to display the IP fragmentation and reassembly statistics for interface xyz:

```
firewall/Admin# show fragment interface xyz
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show interface</a>	Displays the interface information.

# show icmp statistics

To display the Internet Control Message Protocol (ICMP) statistics, use the **show icmp statistics** command in EXEC mode.

**show icmp statistics**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values

**Command Modes** EXEC

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

**Usage Guidelines** This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Use the **clear icmp-statistics** command to clear the ICMP statistics.

**Examples** The following example shows how to display ICMP statistics:

```
firewall/Admin# show icmp statistics
```

Related Commands	Command	Description
	<a href="#">clear icmp statistics</a>	Clears the Internet Control Message Protocol (ICMP) statistics.

# show tcp statistics

To display the Transmission Control Protocol (TCP) statistics, use the **show tcp statistics** command in EXEC mode.

**show tcp statistics**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values

**Command Modes** EXEC

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

**Usage Guidelines** This command requires the connection feature in your user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

**Examples** The following example shows how to display TCP statistics:

```
firewall/Admin# show tcp statistics
```

Related Commands	Command	Description
	<a href="#">clear tcp statistics</a>	Clears all the TCP connections and normalization statistics.

# show udp statistics

To display the User Datagram Protocol (UDP) statistics, use the **show udp statistics** command in EXEC mode.

**show udp statistics**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values

**Command Modes** EXEC

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

**Usage Guidelines** This command requires the connection feature in your user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

**Examples** The following example shows how to display UDP statistics:

```
firewall/Admin# show udp statistics
```

Related Commands	Command	Description
	<a href="#">clear udp statistics</a>	Clears the User Datagram Protocol (UDP) connection statistics.

■ show udp statistics