# TCP Reset Segment Control

The TCP Reset Segment Control feature provides a mechanism to configure if a TCP reset (RST) segment should be sent when a session deletion occurs for half-close, half-open, or idle sessions.



# Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

# Information about TCP Reset Segment Control

## TCP Reset Segment Control

The TCP header contains a flag known as the reset (RST) flag. A TCP segment is sent with the RST flag whenever a segment arrives that does not meet the criteria for a referenced connection. For example, a TCP segment is sent with a RST flag when a connection request is received on the destination port, but no process is listening at that port.

This behavior is defined in RFC 793, Transmission Control Protocol, for host-to-host communication and implemented by various vendors. However, for the network devices that reside on the network between hosts, specific rules have not been defined to determine if the device should send the TCP RST segment to the connection initiator, receiver, or both when sessions (half-open, idle, half-close) are cleared. Some devices send the TCP RST segment to both sender and receiver ports when a session is cleared, while some devices silently remove the session in the session table without sending out any TCP RST segments.

The TCP Reset Segment Control feature provides a mechanism to configure if a TCP RST segment should be sent when a session is cleared for half-close, half-open, or idle sessions.

A half-open session is an unestablished session initiated by a TCP synchronization (SYN) segment but is incomplete as only a TCP three-way handshake occurs and a timer is started.

TCP provides the ability for one end of a connection to terminate its output while still receiving data from the other end of the connection. This TCP state is called the half-close state. A session enters the half-close state when it receives the first TCP FIN segment and starts a timer. If another segment is received before the session timeout occurs, then the timer is restarted.

You can set the timeout value for half-open and half-close sessions by using the **tcp synwait-time** and **tcp finwait-time** commands respectively. The default timeout value is 30 seconds.

An idle session is a TCP session that is active between two devices and no data is transmitted by either of the devices for a prolonged period of time. You can set the timeout value for an idle session by using the **tcp idle-time** command. The default timeout value for idle sessions is 3600 seconds.

Once the timeout occurs on the TCP sessions and the session is cleared, the TCP RST segment is sent and the session will be reset only if the TCP reset segment control is configured on the sessions.

# How to Configure TCP Reset Segment Control

## Configuring TCP Reset for Half-Open Sessions

A half-open session is an unestablished session that is initiated by a TCP synchronization (SYN) segment but has an incomplete three-way handshake. A timer is started as soon as the incomplete three-way handshake occurs. You can set the timer values for a half-open session timeout by using the **tcp synwait-time** command. The default timeout value for these sessions is 30 seconds.

When the timeout occurs and the session is cleared on the half-open TCP session, the TCP reset (RST) segment is sent and the session will be reset only if the TCP reset segment control is configured on the sessions.

If you configure the **tcp half-open reset on** command, the TCP RST segment is sent to both ends of the half-open session when the session is cleared. If you configure the **tcp half-open reset off** command, the TCP RST segment is not transmitted when the session is cleared.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** *parameter-map-name*
4. **tcp synwait-time** *seconds*
5. **tcp half-open reset** {**off** | **on**}
6. **end**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **parameter-map type inspect** *parameter-map-name*<br>**Example:**<br>`Device(config)# parameter-map type inspect pmap-name` | (Optional) Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** keyword and enters parameter-map type inspect configuration mode. |
| **Step 4** | **tcp synwait-time** *seconds*<br>**Example:**<br>`Device(config-profile)# tcp synwait-time 10` | Specifies how long the software will wait for a TCP session to reach the established state before dropping the session. |
| **Step 5** | **tcp half-open reset** {**off** \| **on**}<br>**Example:**<br>`Device(config-profile)# tcp half-open reset on` | Specifies whether the TCP RST segment should be sent when timeout occurs and the session is cleared for a half-open session. |
| **Step 6** | **end**<br>**Example:**<br>`Device(config-profile)# end` | Exits parameter-map type inspect configuration mode and enters privileged EXEC mode. |

# Configuring TCP Reset for Half-Close Sessions

TCP provides the ability for one end of a connection to terminate its output, while still receiving data from the other end of the connection. This TCP state is called the half-close state. A session enters the half-close state when it receives the first TCP finish (FIN) segment and starts a timer. If another segment is received before the session timeout occurs, then the timer is restarted. You can set the timeout value for a half-close session by using the **tcp finwait-time** command. The default timeout value for half-close sessions is 30 seconds.

Once the timeout occurs on the half-close TCP session, the TCP RST segment is sent and the session will be reset only if the TCP reset segment control is configured on the sessions.

If you configure the **tcp half-close reset on** command, the TCP RST segment is sent to both ends of the half-open session when timeout occurs and the session is cleared. If you configure the **tcp half-close reset off** command, the TCP RST segment is not transmitted when the session timeout occurs and the session is cleared.

**SUMMARY STEPS**

1. **enable**

2. **configure terminal**
3. **parameter-map type inspect** *parameter-map-name*
4. **tcp finwait-time** *seconds*
5. **tcp half-close reset** {**off** | **on**}
6. **end**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **parameter-map type inspect** *parameter-map-name*<br>**Example:**<br>`Device(config)# parameter-map type inspect pmap-name` | Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** keyword and enters parameter-map type inspect configuration mode. |
| **Step 4** | **tcp finwait-time** *seconds*<br>**Example:**<br>`Device(config-profile)# tcp finwait-time 10` | (Optional) Specifies how long a TCP session will be managed after the firewall detects a FIN-exchange. |
| **Step 5** | **tcp half-close reset** {**off** \| **on**}<br>**Example:**<br>`Device(config-profile)# tcp half-close reset on` | Specifies whether the TCP RST segment should be sent when session deletion occurs on a half-open session. |
| **Step 6** | **end**<br>**Example:**<br>`Device(config-profile)# end` | Exits parameter-map type inspect configuration mode and enters privileged EXEC mode. |

# Configuring TCP Reset for Idle Sessions

An idle session is a TCP session that is active between two devices and no data is transmitted by either device for a prolonged period of time. You can set the timeout value for an idle session by using the **tcp idle-time** command. The default timeout value for idle sessions is 3600 seconds.

Once the timeout occurs on the idle TCP session, the TCP RST segment is sent and the session will be reset if the TCP reset segment control is configured on the session.

If you configure the **tcp idle reset on** command, the TCP RST segment is sent to both ends of the idle session when timeout occurs and the session is cleared. If you configure the **tcp idle reset off** command, the TCP RST segment is not transmitted when the session timeout occurs and the session is cleared.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** *parameter-map-name*
4. **tcp idle-time** *seconds*
5. **tcp idle reset** {**off** | **on**}
6. **end**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **parameter-map type inspect** *parameter-map-name*<br>**Example:**<br>`Device(config)# parameter-map type inspect pmap-name` | Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** keyword and enters parameter-map type inspect configuration mode. |
| **Step 4** | **tcp idle-time** *seconds*<br>**Example:**<br>`Device(config-profile)# tcp idle-time 90` | (Optional) Configures the timeout for TCP sessions. |
| **Step 5** | **tcp idle reset** {**off** \| **on**}<br>**Example:**<br>`Device(config-profile)# tcp idle reset on` | Specifies whether the TCP RST segment should be sent when session deletion occurs on an idle session. |
| **Step 6** | **end**<br>**Example:**<br>`Device(config-profile)# end` | Exits parameter-map type inspect configuration mode and enters privileged EXEC mode. |

# Configuration Examples for TCP Reset Segment Control

## Example: Configuring TCP Reset for Half-Open Sessions

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect pmap-name
Device(config-profile)# tcp synwait-time 10
```

```
Device(config-profile)# tcp half-open reset on
Device(config-profile)# end
```

# Example: Configuring TCP Reset for Half-Close Sessions

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect pmap-name
Device(config-profile)# tcp finwait-time 10
Device(config-profile)# tcp half-close reset on
Device(config-profile)# end
```

# Example: Configuring TCP Reset for Idle Sessions

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect pmap-name
Device(config-profile)# tcp idle-time 90
Device(config-profile)# tcp idle reset on
Device(config-profile)# end
```

# Additional References for TCP Reset Segment Control

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Firewall commands | • Cisco IOS Security Command Reference: Commands A to C<br>• Cisco IOS Security Command Reference: Commands D to L<br>• Cisco IOS Security Command Reference: Commands M to R<br>• Cisco IOS Security Command Reference: Commands S to Z |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| RFC 793 | Transmission Control Protocol |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for TCP Reset Segment Control

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

***Table 1: Feature Information for TCP Reset Segment Control***

| Feature Name | Releases | Feature Information |
|---|---|---|
| TCP Reset Segment Control | Cisco IOS XE Release 3.8S | The TCP Reset Segment Control feature provides a consistent mechanism to configure if the TCP RST bits should be sent out when a session is cleared for half-open, half-close, and idle sessions.<br><br>The following commands were introduced or modified: **tcp idle reset**, **tcp half-close reset**, and **tcp half-open reset**. |