

TCP MSS and Clear Dont Fragment

- Feature history for TCP MSS and clear dont fragment, on page 1
- TCP MSS, on page 1
- Restrictions for TCP MSS and clear dont fragment, on page 2
- Configure TCP MSS and clear dont fragment, on page 2
- Verify TCP MSS and dont clear fragment configurations, on page 4

Feature history for TCP MSS and clear dont fragment

Table 1: Feature History

Feature Name	Release Information	Description
Configure TCP MSS	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature adds support for TCP MSS adjustment on Cisco IOS XE Catalyst SD-WAN devices on both directions of the Cisco Catalyst SD-WAN tunnel interface.
Configure Clear Don’t Fragment Option	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature provides the option to clear the Don't Fragment bit in the IPv4 packet header for packets being sent out on a Cisco Catalyst SD-WAN tunnel . When you clear the Don't Fragment configuration, packets larger than the interface MTU are fragmented before being sent.

TCP MSS

A TCP maximum segment size (MSS) is a parameter that

- specifies the largest amount of data, in bytes, that a communications device can receive in a single TCP segment without counting the TCP header or the IP header, and

- is specified as TCP MSS, initially in the TCP SYN packet during the TCP handshake.

TCP MSS for SYN packets

Small MSS values reduce or eliminate IP fragmentation, which results in higher overhead. You can configure the MSS of TCP SYN packets passing through a device. By default, the device dynamically adjusts the MSS based on the interface or tunnel maximum transmission unit (MTU) to ensure that TCP SYN packets are never fragmented. For data sent over an interface, the device calculates the MSS by adding the interface MTU, the IP header length, and the maximum TCP header length.

Restrictions for TCP MSS and clear dont fragment

TCP MSS

- TCP MSS values can be adjusted for Cisco Catalyst SD-WAN tunnel interfaces only.

  From Cisco IOS XE Catalyst SD-WAN Release 17.9.1aand Cisco vManage Release 20.9.1, you can adjust the TCP MSS value for a service VPN or for Network Address Translation (NAT) Direct Internet Access (DIA) use cases. Adjusting the TCP MSS value helps prevent TCP sessions from being dropped.

  For more information on NAT DIA, see the *Cisco Catalyst SD-WAN NAT Configuration Guide*.

- From Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, for an IPv4 SD-WAN tunnel carrying IPv6 traffic, the system uses the IPv6 TCP MSS value. Also, for an IPv6 tunnel carrying IPv4 traffic, the system uses the IPv4 TCP MSS value. This upgrade aligns MSS adjustment with the traffic protocol and tunnel configurations, ensuring accurate and efficient handling of traffic.

Clear dont fragment

- The option **Clear Dont Fragment** is available for Cisco Catalyst SD-WAN tunnel interfaces only.

Configure TCP MSS and clear dont fragment

Use one of these methods to configure TCP MSS and clear dont fragment:

- CLI commands
- Templates

Configure TCP MSS and clear dont fragment using CLI commands

Follow these steps to configure TCP MSS and clear dont fragment using CLI commands:

Procedure

Step 1 Configure an interface type and enter the interface configuration mode.

Example:

```
interface Tunnel 1
```

Step 2 Enable IP processing on an interface without assigning an explicit IP address to the interface.

Example:

```
ip unnumbered GigabitEthernet1
```

Step 3 Configure TCP MSS and clear dont fragment.

- Enable a maximum segment size (MSS) for TCP connections.

Example:

```
ip tcp adjust-mss 1460
```

- Clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface.

Example:

```
ip clear-dont-fragment
```

The following is an example configuration of TCP MSS:

```
Device(config)#interface Tunnel 1
Device(config-if)#ip unnumbered GigabitEthernet1
Device(config-if)#ip tcp adjust-mss 1460
```

The following is an example to configure Clear Dont Fragment option:

```
Device(config)#interface Tunnel 1
Device(config-if)#ip unnumbered GigabitEthernet1
Device(config-if)#ip clear-dont-fragment
```

Configure TCP MSS and clear dont fragment using templates

Follow these steps to configure TCP MSS and clear dont fragment using feature templates.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**.

Note
In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 Create a new CLI add-on feature template or edit one of the following templates. You can use any of the following feature templates to configure TCP MSS and clear dont fragment:

- VPN Ethernet Interface
- VPN Interface DSL IPoE
- VPN Interface DSL PPoA

- VPN Interface DSL PPPoE
- VPN Interface Multilink
- VPN Interface T1/E1
- Cellular Interfaces

Step 4 Click **Tunnel**.

Step 5 Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device to configure TCP MSS in the tunnel TCP MSS. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU so that TCP SYN packets are not fragmented.

- Range: 552 to 1460 bytes
- Default: None

TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, it flows through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set at 40 bytes lower than the minimum path MTU.

Step 6 Click the **Clear-Dont-Fragment** option to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the **Don't Fragment** bit is cleared, packets larger than that interface's MTU are fragmented before being sent.

Clear-Dont-Fragment clears the **Don't Fragment** bit when there is fragmentation needed and the **Don't Fragment** bit is set. For packets that don't require fragmentation, the **Don't Fragment** bit is not affected.

Step 7 Click **Save** or **Update**.

Verify TCP MSS and dont clear fragment configurations

TCP MSS configuration

The following is sample output of the **show platform hardware qfp active feature sdwan datapath session summary** command:

```
Device# show platform hardware qfp active feature sdwan datapath session summary

Src IP          Dst IP          Src Port Dst Port   Encap    Uidb     Bfd Discrim PMTU

------          ------          -------- -------    ------   -------  ----------- -----

10.1.15.25      10.1.14.14      12347    12346      IPSEC    65526    10007       1446

10.1.15.25      10.0.5.21       12347    12357      IPSEC    65526    10009       1446

10.1.15.25      10.0.5.11       12347    12347      IPSEC    65526    10008       1446

10.1.15.25      10.1.16.16      12347    12366      IPSEC    65526    10006       1446
```

Dont fragment configuration

The following is sample output of the **show platform software interface rp active name Tunnel1** command to verify if **Clear-dont-fragment** is enabled or not.

```
Device# show platform software interface rp active name Tunnel1 | include dont
IP Clear-dont-fragment: TRUE
```

The following is sample output of the **show running-config interface Tunnel1** command that displays the running configuration when Clear-dont-fragment is enabled.

```
Device# show running-config interface Tunnel1
Building configuration...

Current configuration : 132 bytes
!
interface Tunnel1
ip unnumbered GigabitEthernet1
ip clear-dont-fragment
tunnel source GigabitEthernet1
tunnel mode sdwan
end
```