

Packet truncation

Packet truncation is a software feature that allows a Cisco Nexus 9000 Series switch to shorten packets to a user-defined size as they exit an interface. You can control the Cyclic Redundancy Check (CRC) value of truncated packets, streamline monitoring by truncating packets at the egress port, and save resources.

Packet truncation lets you perform truncation directly on the egress port that connects to your monitoring tool. This approach simplifies your workflow and saves resources.

For more information, see Packet Truncation.

In typical Network Data Broker (NDB) environments, monitoring tools receive traffic using SPAN (Switched Port Analyzer) sessions. When full packet payloads are not required, SPAN truncation is often used. However, this method requires redirecting traffic through additional ports configured with a Port Access Control List (PACL), consuming the port capacity.

The packet truncation feature enables you to truncate packets at the egress port. This optimizes network monitoring traffic, reduces infrastructure costs, and addresses the operational overhead associated with traditional packet capture methods.

Components of packet truncation

Packet truncation includes three main components:

- **Egress Port Level Truncation**

  This function is available on CloudScale switches. Administrators can define a maximum size for packets on a specific egress port. Packets larger than this size are truncated. The configuration is managed using the CLI and is integrated into the Cisco NX-OS Device Management Engine (DME).

- **CRC Stomping Control**

  On the Cisco Nexus switches, packet truncation invalidates the original CRC value. The switch replaces the packet with a bad CRC causing the receiving peer or monitoring tool to discard the packet. This feature provides a CLI command to disable CRC stomping.

- **CRC Check Control (Legacy Hardware)**

  On the Cisco Nexus FX, FX2, and FX3 Series switches, a system-level command is available to disable the CRC check for truncated packets. This allows packets with CRC anomalies after truncation, to be forwarded successfully to monitoring tools.

Configure and manage the egress packet truncation

Use these commands to configure and manage packet truncation at the egress port.

Command	Description
packet-truncation size *size_in_bytes*	Enable packet truncation on an egress interface and set the maximum packet size in bytes.
[**no**] **packet-truncation crc-stomp**	Disable CRC stomping on truncated packets to ensure the peer device receives a valid CRC.The option to enable or disable packet-truncation crc-stomp is not supported on Nexus 9300-FX, FX2, and FX3 platforms.
[**no**] **system packet-truncation crc-check**	Disable the CRC check for truncated packets across the system.

Guidelines and limitations for packet truncation

Follow these guidelines when you use packet truncation.

- The packet truncation feature can be enabled only after enabling feature tap-aggregation feature.
- The **packet-truncation size** command is configurable only under physical interface and port-channel interfaces. It is *not* configurable on the Layer 3 interfaces and SVI interfaces.
- The [**no**] **packet-truncation crc-stomp** is configurable only under physical interface and port-channel interfaces. It is *not* configurable on the Layer 3 interfaces and SVI interfaces.

  It is *not* configurable on Cisco Nexus FX, FX2 and FX3 Series switches.
- The [**no**] **system packet-truncation crc-check** command is configurable at the global level. It allows crc-stomped packets from the previous hop and forwards the packets to next hop.
- Packet truncation is supported on the Cisco Nexus CloudScale switches.

  Packet truncation is *not* supported on these Cisco Nexus switches.
  - Cisco Nexus 9500 Series switches
  - Cisco Nexus SiliconOne switches
- If packet-truncation is configured under interfaces (such as Po and Eth), it can affect the control packets such as LLDP, LACP, STP, and CDP egressing out of those interfaces depending on the size configured. Lower packet-truncation size can corrupt the egress protocol packets, resulting in neighborship formation or ports going to suspended state. Beginning with NX-OS Release 10.6(3)F, a new command executed at the interface or global level allows you to exclude the control packets from being truncated.

- Configure packet truncation at the egress ports task, on page 3
- Configure packet truncation with CRC stomping disabled, on page 3
- Configure packet truncation to exclude control packets, on page 4
- Configure system-wide packet truncation CRC check, on page 6
- Verify packet truncation , on page 7

Configure packet truncation at the egress ports task

Use this procedure to configure an interface to truncate all egress packets to a specific size.

Procedure

Step 1 Enter global configuration mode.

Example:

```
switch# configure terminal
```

Step 2 Specify the interface to configure and enter interface configuration mode.

Example:

```
switch(config)# interface ethernet 1/1
```

Step 3 Enable packet truncation of egress packets to a specific size on the interface.

Example:

```
switch(config)# packet-truncation size 128
```

Step 4 Exit interface configuration mode.

Example:

```
switch(config)# exit
```

Example

This is a sample configuration example to truncate packets to a specific size of 128 bytes.

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# packet-truncation size 128
switch(config-if)# end
```

Configure packet truncation with CRC stomping disabled

Use this procedure to disable CRC stomping on Cisco Nexus GX, GX2, and HX Series switches.



Note If the Cisco Nexus GX, GX2, and HX Series switches receives a truncated packet with a bad CRC from the previous hop, the packet must be further truncated on this switch to a smaller size to utilize the functionality of this command and avoid CRC stomping.

Procedure

Step 1 Enter global configuration mode.

Example:

```
switch# configure terminal
```

Step 2 Specify the interface to configure and enter interface configuration mode.

Example:

```
switch(config)# interface ethernet 1/1
```

Step 3 Enable packet truncation of egress packets to a specific size on the interface.

Example:

```
switch(config)# packet-truncation size 128
```

Step 4 Disable CRC stomping to ensure truncated packets are sent with a valid CRC.

Example:

```
switch(config)# no packet-truncation crc-stomp
```

Step 5 Exit interface configuration mode.

Example:

```
switch(config)# exit
```

Example

The example shows how to configure Ethernet interface 1/2 to truncate all egress packets to 256 bytes and ensures they are sent with a valid CRC.

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# packet-truncation size 256
switch(config-if)# no packet-truncation crc-stomp
switch(config-if)# end
```

Configure packet truncation to exclude control packets

In earlier releases, including 10.6(1)F and 10.6(2)F, packet truncation on interfaces such as PO and Ethernet can corrupt control packets (LLDP, LACP, STP, CDP) if set too low, caused neighborship or port issues. However, from NX-OS Release 10.6(3)F you can exclude control packets from truncation either at the system level or at the interface level.

Configure packet truncation to exclude control packets at system level

Use this procedure to exclude control truncated packets at system level.

Procedure

Step 1 Use the **configure terminal** command to enter the global configuration mode.

Example:

```
switch# configure terminal
```

Step 2 Use the **system packet-truncation exclude control-packets** command to enable the exclusion of control packets from packet truncation. This prevents essential control packets from being truncated while still applying truncation to data packets.

Example:

```
switch(config)# system packet-truncation exclude control-packets
```

Step 3 Use the **exit** command to exit the global configuration mode.

Example:

```
switch(config)# exit
```

This is a sample configuration example to exclude control packets from being truncated.

```
switch# configure terminal
switch(config)# system packet-truncation exclude control-packets
switch(config)# exit
```

Configure packet truncation to exclude control packets on an interface

Use this procedure to configure an interface to exclude control truncated packets.

Procedure

Step 1 Use the **configure terminal** command to enter the global configuration mode.

Example:

```
switch# configure terminal
```

Step 2 Use the **interface ethernet slot/port** command to specify the interface to configure and enter interface configuration mode.

Example:

```
switch(config)# interface ethernet 1/1
```

Step 3 Enable packet truncation of egress packets to a specific size on the interface. It is mandatory to enable packet truncation size before enabling exclude control packets under an interface.

Example:

```
switch(config-if)# packet-truncation size 128
```

Step 4 Enable exclusion of control packets from packet truncation. This prevents essential control packets from being truncated while still applying truncation to data packets.

Example:

```
switch(config-if)# packet-truncation exclude control-packets
```

Step 5 Exit interface configuration mode.

Example:

```
switch(config-if)# exit
```

This is a sample configuration example to exclude control packets from being truncated.

```
switch(config)# interface ethernet 1/1
switch(config-if)# packet-truncation size 128
switch(config-if)# packet-truncation exclude control-packets
switch(config-if)# exit
```

Configure system-wide packet truncation CRC check

Use this task to enable system-wide CRC check and to configure packet truncation for egress ports.

Procedure

Step 1 Enter global configuration mode.

Example:

```
switch# configure terminal
```

Step 2 Disable the system-wide CRC check for truncated packets. This global command accepts all ingress packets with CRC errors instead of dropping it.

Example:

```
switch(config)# no system packet-truncation crc-check
```

Step 3 Specify the interface to configure and enter interface configuration mode.

Example:

```
switch(config)# interface ethernet 1/1
```

Step 4 Configure the interface to truncate all egress packets to 128 bytes.

Example:

```
switch(config)# packet-truncation size 128
```

Step 5 Exit interface configuration mode.

Example:

```
switch(config)# exit
```

Example

The example shows how to disable the system-wide CRC check and configure the Ethernet interface 1/3 to truncate all egress packets to 128 bytes:

```
switch# configure terminal
switch(config)# no system packet-truncation crc-check
switch(config)# interface ethernet 1/3
switch(config-if)# packet-truncation size 128
switch(config-if)# end
```

Verify packet truncation

To verify packet truncation settings on Cisco Nexus 9000 switches, use these commands and review the outputs.

Interface verification

Use the **show running-config interface** command to verify packet truncation settings on a specific interface:

```
Switch# show running-config interface ethernet 1/2
...
interface Ethernet1/2
packet-truncation size 256
no packet-truncation crc-stomp
```

This command displays the packet truncation size and indicates if CRC stomp is disabled for the selected interface.

System verification

Use the **show running-config** command to check global packet truncation CRC settings on the Cisco Nexus 9000 FX, FX2 and FX3 Series switches:

```
Switch# show running-config | include crc-check
no system packet-truncation crc-check
```

This command disables the system level check for bad CRC packets and forwards it to networking monitoring tool for analysis.