NCCS 3GPP IP Specification Compliance for Interfaces

Table 1: Feature History Table

Feature Name	Release Information	Feature Description
NCCS 3GPP IP Specification Compliance for Interfaces	Cisco IOS XE 17.15.2	The router adheres to and complies with the IP specification guidelines as outlined by the National Centre for Communication Security (NCCS) certification, which is based on the 3rd Generation Partnership Project (3GPP) standards. This compliance ensures that the router meets rigorous security and performance benchmarks, providing users with a reliable and secure networking solution that aligns with industry best practices and regulatory requirements.

The router adheres to and complies with the IP specification guidelines as outlined by the National Centre for Communication Security (NCCS) certification, which is based on the 3rd Generation Partnership Project (3GPP) standards.

IP Specific Requirements for NCCS 3GPP IP Specification Compliance

The router complies with three IP-specific requirements to adhere to the NCCS 3GPP IP specification compliance standards. By default, IP forwarding, proxy Address Resolution Protocol (ARP), and Internet

Control Message Protocol (ICMP) broadcast or directed broadcast are enabled. To meet the NCCS requirements, these three features must be disabled on the router interfaces. This ensures the router aligns with the security and operational guidelines set forth by the NCCS 3GPP standards, enhancing the overall security and reliability of the network.

Restrictions for NCCS 3GPP IP Requirements

• For control plane-generated IPv6 BDI traffic, enabling the **platform** CLI commands that modify hardware fields can impact other Layer 2 protocols, leading to network instability. Due to this inherent hardware limitation, it is recommended not to enable these **platform** CLI commands for such traffic scenarios to ensure network stability and optimal performance.

How to Configure NCCS 3GPP IP Requirements on Router

To configure NCCS 3GPP IP requirements on the router, ensure that you disable the following features on the router:

• IP forwarding

• Proxy ARP

• ICMP Broadcast

Disabling IP Forwarding

To disable IP forwarding, execute the following command:

```
platform ip-forwarding disable
```

This command ensures that IP forwarding is halted, enhancing network control and security by preventing the forwarding of packets.

Disabling Proxy ARP

NCCS requirements state that the router should not act as a proxy for ARP. You can disable this functionality globally or on a specific interface to ensure the router does not send ARP responses.

Scenario Explanation

Consider the following scenario: In a router, host 1 is connected to subnet A on interface A, and host 2 is connected to subnet B on interface B. When host 1 broadcasts an ARP request on subnet A to discover the MAC address of host 2 on subnet B, the ARP request reaches all nodes in subnet A, including interface A of the router, but it does not reach host 2. The network product should receive this packet but should not send an ARP reply to host 1. This requirement is achieved by configuring existing PI commands to disable ARP either globally or at the interface level.

To disable ARP globally on the router, execute the following PI command:

```
ip arp proxy disable
```

To disable ARP on a specific interface, execute the following PI command:

```
interface <interface-name>
no ip proxy-arp
```

These configurations ensure that the router adheres to NCCS requirements by not acting as an ARP proxy.

Disabling ICMP Broadcast

ICMP broadcast and ICMP directed broadcast are used for ICMP type echo and timestamp messages. When a router receives an ICMP broadcast packet, it typically sends an ICMP reply. However, NCCS requirements state that the router should not respond to directed broadcast packets. To comply with this requirement, you can disable ICMP broadcast functionality.

To disable ICMP broadcast on the router, execute the following command:

```
platform icmp-broadcast disable
```

When you execute this command, the ICMP broadcast request packets are identified and dropped, ensuring that the router does not respond to these packets. This enhances network security and compliance with NCCS requirements by preventing the router from responding to potentially malicious ICMP broadcast requests.