Troubleshoot IP Source Violation when Verizon is the Carrier

Contents

Introduction

This document describes how to troubleshoot IP source violenation which is a frequent issue when Verizon is the carrier.

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of these topics:

- 5G Cellular Network Basics
- Cisco Cellular Gateway 522-E
- Cisco P-5GS6-GL module
- Cisco IOS-XE
- Cisco IOS-CG

Components Used

The information in this document is based on these software and hardware versions:

- Cellular Gateway 522-E with IOS-CG version 17.9.5a.
- IR1101 with IOS-XE version 17.9.5 with a P-5GS6-GL module plugged in.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

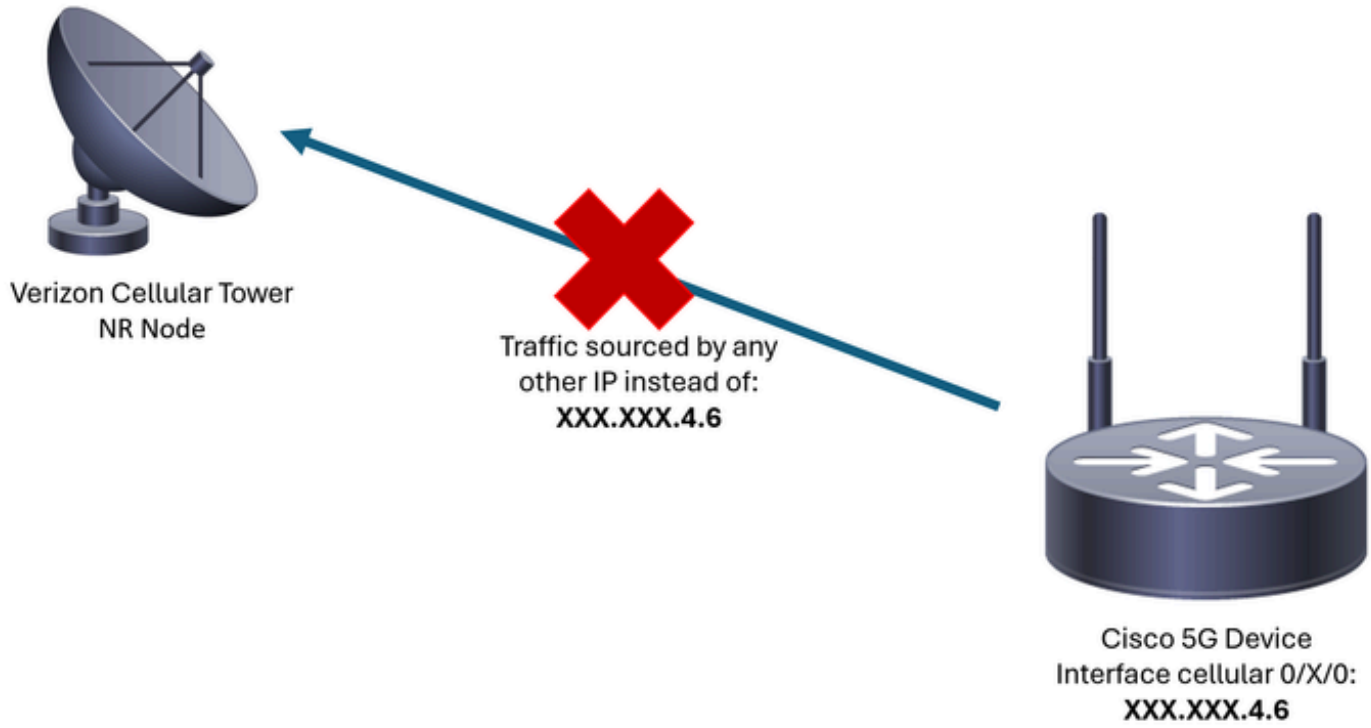
This applies to a P-5GS6-GL module connected to a router in standalone mode, or a CG522-E in standalone or controller mode managed by SD-WAN. This document does not apply to a P-5GS6-GL module connected to a router in SD-WAN since command syntax is different.

Problem

Verizon assigns an IP address specifically to each client/SIM, and they always expect to receive traffic sourced only from that IP.

Source violation occurs when Verizon detects that traffic sent from the client is sourced by a different IP from the one they previously assigned.

For example, if the IP address **XXX.XXX.4.6** was assigned, and Verizon receives traffic from the IP address **XXX.XXX.8.9**, the issue is present:



Every time Verizon receives more than 10 packets from the device with a different IP address, the connection to the cellular network flaps and stops. As a result, a new connection is initiated from the cellular device, and it can get either the same IP address than before or a new one. It depends on the acquired service.

Detect the Issue in a P-5GS6-GL Module Connected to a Router

When the shown disconnect reason is present in the output of the command, source violation is in placed:

<#root>

```
isr#
```

show cellular 0/X/0 call-history

```
                          *
                          *
[Wed May    8  18:46:26   2024]   Session disconnect reason = Regular deactivation (36)

                          *
                          *
```

If the previous output does not give information (due to buffer process), a Netflow packet capture can be taken with these commands:

```
isr#conf t
isr(config)#flow record NETFLOW_MONITOR
isr(config-flow-record)#match ipv4 protocol
isr(config-flow-record)#match ipv4 source address
isr(config-flow-record)#match ipv4 destination address
isr(config-flow-record)#match transport source-port
isr(config-flow-record)#match transport destination-port
isr(config-flow-record)#collect ipv4 source prefix
isr(config-flow-record)#collect ipv4 source mask
isr(config-flow-record)#collect ipv4 destination prefix
isr(config-flow-record)#collect ipv4 destination mask
isr(config-flow-record)#collect interface output
isr(config-flow-record)#exit

isr(config)#flow monitor NETFLOW_MONITOR
isr(config-flow-monitor)#cache timeout active 60
isr(config-flow-monitor)#record NETFLOW_MONITOR
isr(config-flow-monitor)#exit

isr(config)#interface cellular 0/X/0
isr(config-if)#ip flow monitor NETFLOW_MONITOR output
isr(config-if)#exit
```

To see the output of the capture:

<#root>

isr#

show flow monitor NETFLOW_MONITOR cache format table

Verizon assigned IP address to the device can be seen with the command:

<#root>

isr#

show ip interface brief

```
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES NVRAM  administratively down down
FastEthernet0/0/1      unassigned      YES unset  down                  down
FastEthernet0/0/2      unassigned      YES unset  down                  down
FastEthernet0/0/3      unassigned      YES unset  down                  down
FastEthernet0/0/4      unassigned      YES unset  down                  down

Cellular0/1/0          IP_address      YES IPCP   up                    up


Cellular0/1/1          unassigned      YES NVRAM  administratively down down
Async0/2/0             unassigned      YES unset  up                    down
Vlan1                  unassigned      YES unset  up                    down
```

If in the logs of the Netflow capture any traffic, it is reported sourced with a different IP address from the one confirmed in the cellular interface. The source violation is present.

Solution for a P-5GS6-GL Module Connected to a Router

The goal is to ensure that all the traffic is only sent sourced by the IP assigned by Verizon. There are different methods that meet this goal. Their implementation depends on the deployment and network requirements:

- **Option 1: ACL for Outbound Traffic**

- With an Access Control List, you can ensure that traffic sent from the device is only sourced from Verizon IP Address:

```
isr#conf t
isr(config)#ip access-list extended 196
isr(config-ext-nacl)#permit ip host <IP_Assigned_by_Verizon> any
isr(config-ext-nacl)#deny ip any any
isr(config-ext-nacl)#exit

isr(config)#interface cellular 0/X/0
isr(config-if)#ip access-group 196 out
isr(config-if)#end
```

- **Option 2: NAT for Internal Traffic**

- These requirements must be met:
    1. Cellular interface is configured as “ip nat outside”.
    2. LAN interface is configured as “ip nat inside”.
    3. NAT overload (PAT) is implemented so all ports are also translated.
    4. The use of an ACL to define traffic to be NATed.

Configuration example:

<#root>

```
isr#conf t
```

```
isr(config)#interface cellular 0/X/0
isr(config-if)#ip nat outside
isr(config-if)#exit

isr(config)#interface vlan 6
isr(config-if)#ip nat inside
isr(config-if)#exit

isr(config)#access-list 20 permit <IPv4_subnet_to_be_NATed> <wildcard>
isr(config)#ip nat inside source list 20 interface cellular 0/1/0 overload
```

- **Option 3: Implement an IPsec or Any Other Tunnel Configuration**

- This tunnel is done with the Verizon assigned IP address. As all traffic travels inside of it, the external IP address never changes.

- **Option 4: Implement a Route Map**

- If there is router generated traffic, a route map can be implemented so that traffic is sourced correctly. For example, a continues ping to a DNS, to ensures there is “Internet connectivity”, and a route map can be implemented so that traffic is sourced correctly.

This ends the procedure to troubleshoot source violation in a Cisco P-5GS6-GL Module connected to a router.

IP Source Violation in a CG522-E

By default, a feature to eliminate this issue is activated in the code of these devices.

Corroborate that the device shows this output:

<#root>

```
CellularGateway#
```

show cellular 1 drop-stats

```
Ip Source Violation details:
```

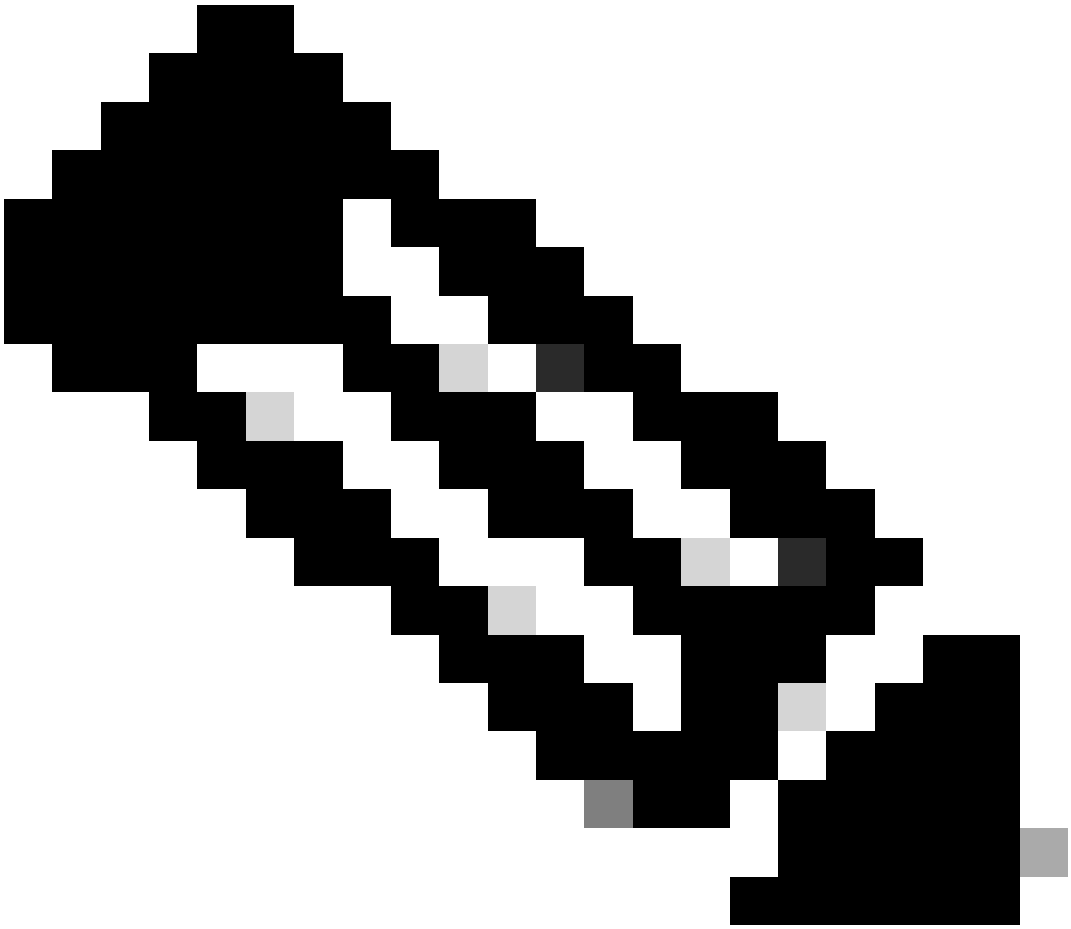
Ipv4 Action = Drop

```
  Ipv4 Packets Drop = 0
  Ipv4 Bytes Drop   = 0
```

Ipv6 Action = Drop

```
  Ipv6 Packets Drop = 0
  Ipv6 Bytes Drop   = 0
```

The state of **Ipv4/Ipv6 Action** must be **Drop**. It means the feature is enabled.



Note: If the output says **Permit**, the feature is disabled.

With these commands, the feature can be re-activated:

```
CellularGateway#conf t
CellularGateway(config)# controller cellular 1
CellularGateway(config-cellular-1)# no ip-source-violation-action ipv4-permit
CellularGateway(config-cellular-1)# no ip-source-violation-action ipv6-permit
CellularGateway(config-cellular-1)# commit
Commit complete.
CellularGateway(config-cellular-1)# end
```

This ends the procedure to troubleshoot source violation in a Cisco CG522-E.