

當Verizon是業者時，排除IP源違規故障

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[問題](#)

[在連線到路由器的P-5GS6-GL模組中檢測問題](#)

[連線到路由器的P-5GS6-GL模組的解決方案](#)

[選項1：用於出站流量的ACL](#)

[選項2：用於內部流量的NAT](#)

[選項3：實施IPsec或任何其它隧道配置](#)

[選項4：實施路由對映](#)

[CG522-E中的IP源違規](#)

簡介

本文檔介紹如何對Verizon作為業者時經常出現的IP源違規進行故障排除。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- 5G蜂窩網路基礎知識
- 思科行動閘道522-E
- 思科P-5GS6-GL模組
- Cisco IOS-XE
- Cisco IOS-CG

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 蜂窩網關522-E，帶IOS-CG版本17.9.5a。
- IR1101，帶IOS-XE 17.9.5版，並插入P-5GS6-GL模組。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

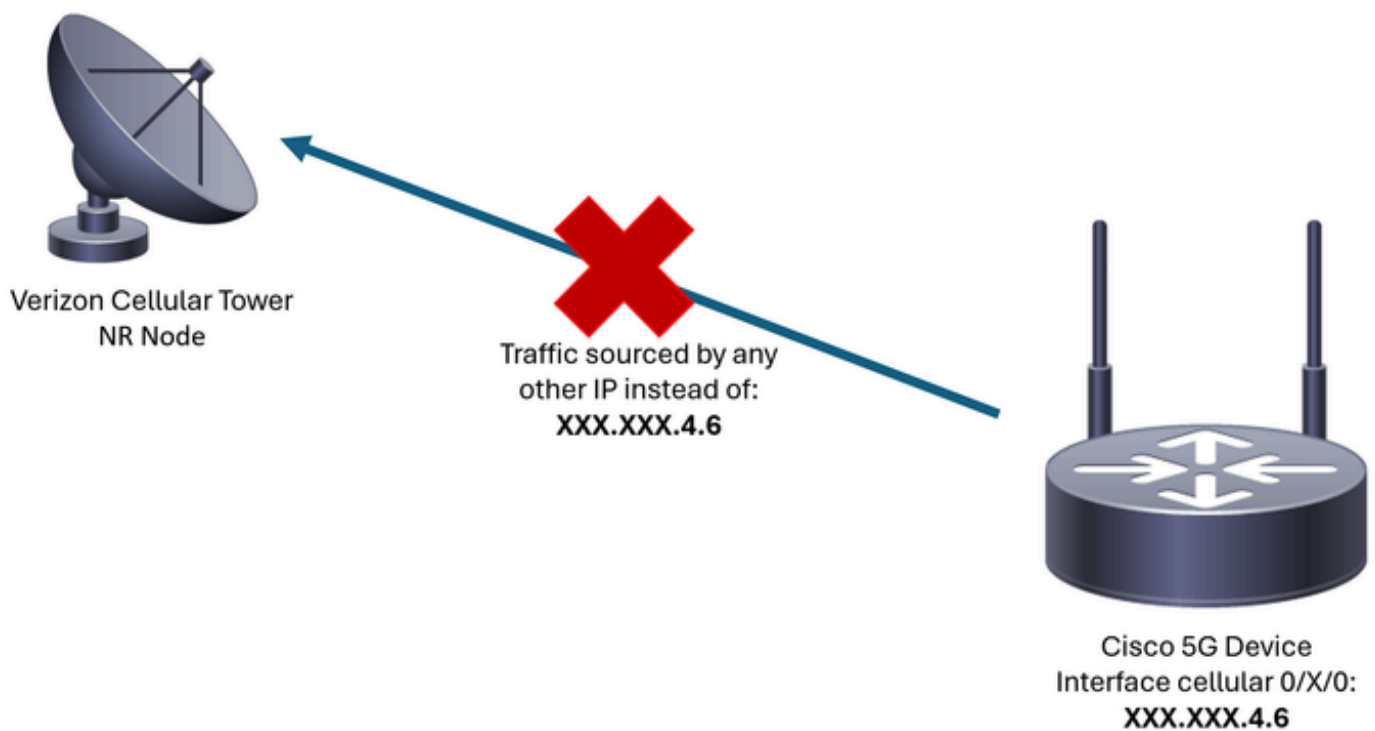
這適用於在獨立模式下連線到路由器的P-5GS6-GL模組，或者在SD-WAN管理的獨立或控制器模式下連線到路由器的CG522-E。本文檔不適用於連線到SD-WAN中路由器的P-5GS6-GL模組，因為命令語法不同。

問題

Verizon會特別為每個客戶端/SIM分配一個IP地址，並且它們總是期望只接收來自該IP的流量。

當Verizon檢測到來自客戶端的流量來自與之前分配的不同IP時，就會發生源違規。

例如，如果分配了IP地址XXX.XXX.4.6，則Verizon收到來自IP地址XXX.XXX.8.9的流量，則問題存在：



每當Verizon收到來自具有不同IP地址的裝置的10個以上的資料包時，與蜂窩網路的連線就會抖動並停止。結果，從蜂窩裝置發起新的連線，並且它可以獲得與以前相同的IP地址或新的IP地址。這取決於所獲得服務。

在連線到路由器的P-5GS6-GL模組中檢測問題

當顯示的斷開原因出現在命令的輸出中時，將放置源違規：

```
<#root>
```

```
isr#
```

```
show cellular 0/X/0 call-history
```

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

如果先前的輸出沒有提供資訊（由於緩衝區進程），則可以使用以下命令進行Netflow資料包捕獲：

```
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
```

要檢視捕獲的輸出，請執行以下操作：

```
<#root>
isr#
show flow monitor NETFLOW_MONITOR cache format table
```

可使用以下命令檢視Verizon為裝置分配的IP地址：

```
<#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

如果在Netflow的日誌中捕獲任何流量，則報告其來源與蜂窩介面中確認的IP地址不同。存在來源違規。

連線到路由器的P-5GS6-GL模組的解決方案

目標是確保所有流量僅透過Verizon分配的IP傳送。有多種方法可以達到這個目標。其實施取決於部署和網路要求：

- 選項1：用於出站流量的ACL
- 使用訪問控制清單，您可以確保從裝置傳送的流量僅源自Verizon IP地址：

```

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

```

- 選項2：用於內部流量的NAT
- 必須滿足以下要求：
 1. 蜂窩介面配置為「ip nat outside」。
 2. LAN介面配置為「ip nat inside」。
 3. 實施NAT過載(PAT)後，所有埠也會被轉換。
 4. 使用ACL定義要進行NAT轉換的流量。

組態範例:

<#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
```

- 選項3：實施IPsec或任何其它隧道配置
- 此隧道使用Verizon分配的IP地址完成。當所有流量都流經內部時，外部IP地址從不改變。
- 選項4：實施路由對映
- 如果有路由器生成的流量，則可以實施路由對映，以便正確確定流量的來源。例如，繼續對DNS執行ping操作，以確儲存在「Internet連線」，並且可以實施路由對映，以便正確分配流量。

對連線到路由器的Cisco P-5GS6-GL模組中的源違規進行故障排除的過程到此結束。

CG522-E中的IP源違規

預設情況下，在這些裝置的代碼中會啟用用於消除此問題的功能。

確認裝置顯示以下輸出：

```
<#root>
```

```
CellularGateway#
```

```
show cellular 1 drop-stats
```

```
Ip Source Violation details:
```

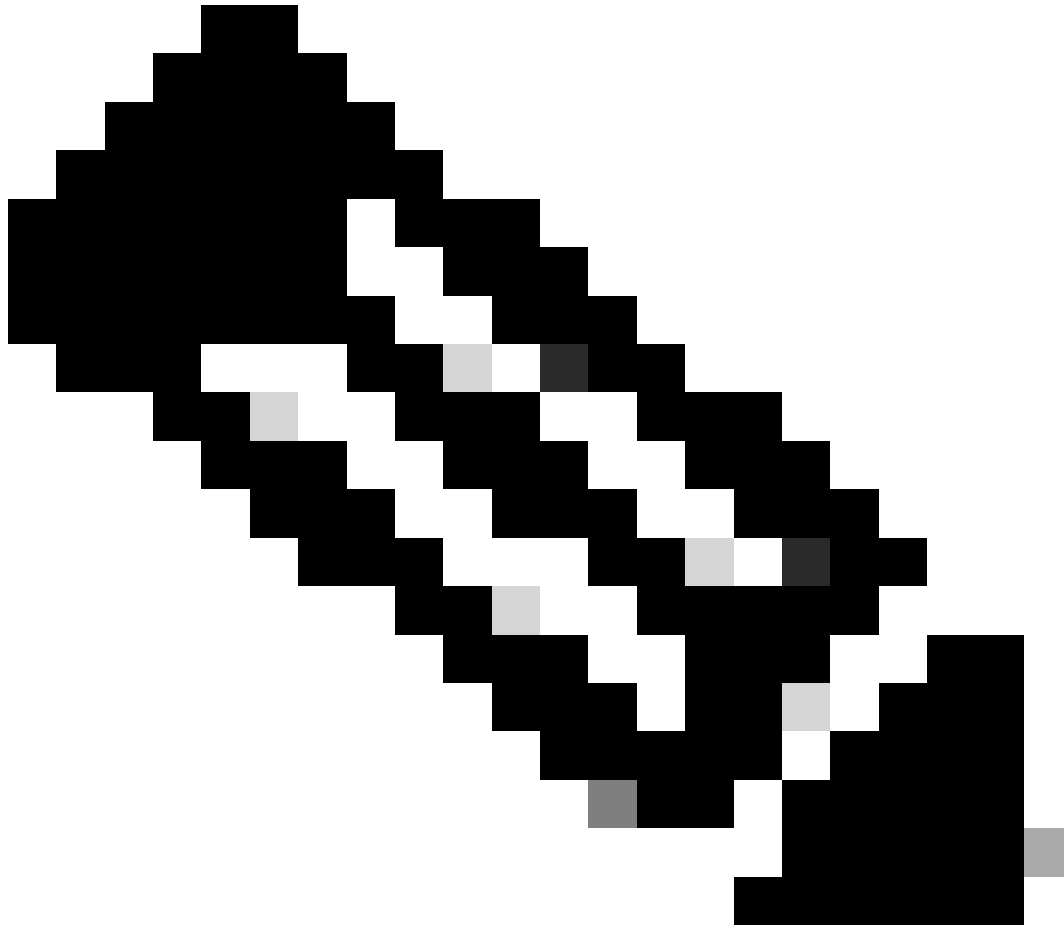
```
Ipv4 Action = Drop
```

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

```
Ipv6 Action = Drop
```

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

Ipv4/Ipv6操作的狀態必須為丟棄。這表示已啟用此功能。



註：如果輸出顯示Permit，則此功能被停用。

使用這些指令可重新啟動功能：

```
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
```

這將結束對Cisco CG522-E中的源違規進行故障排除的過程。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。