

Überprüfen Sie mithilfe des Ping-Tests, ob der NCS6K-Paketpfad langsam weitergeleitet wird.

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Überprüfen](#)

[Ähnliche Diskussionen in der Cisco Support Community](#)

Einführung

Der Ping-Pakettest wird häufig zur Behebung von Verbindungsproblemen verwendet. In diesem Dokument wird ein systematischer Ansatz für die Verwendung des Ping-Tests zur Überprüfung des langsameren Weiterleitungspakets des Network Convergence System 6000 (NCS6K) beschrieben.

Voraussetzungen

Anforderungen

Die Leser dieses Dokuments sollten folgende Themen kennen:

- Grundlegendes IP-Routing.
- XR-Betriebssystem.

Verwendete Komponenten

Dieses Dokument wurde für die NCS6K-Plattform erstellt.

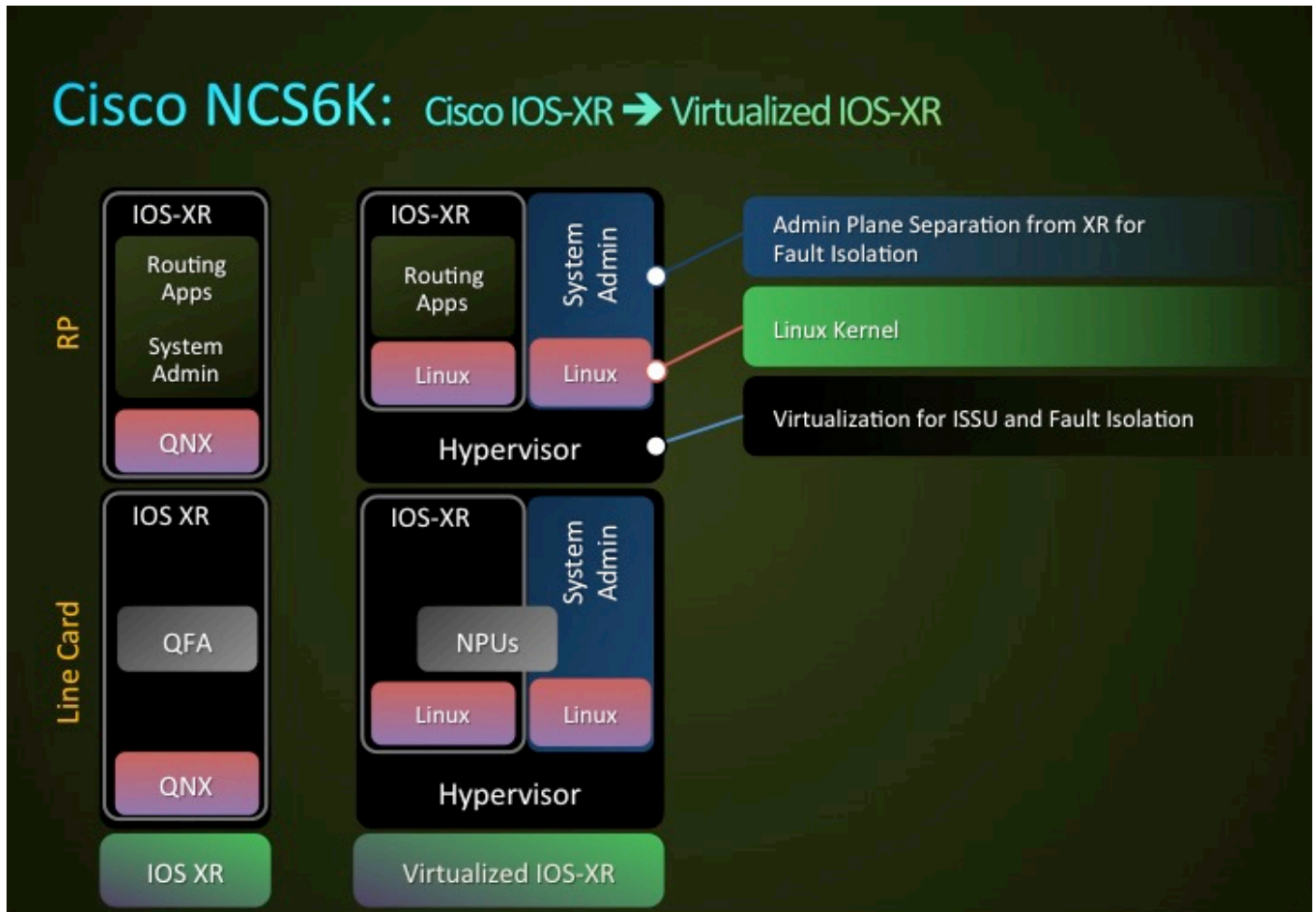
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Zwischen NCS6K und der herkömmlichen IOS-XR-Plattform besteht ein wesentlicher Unterschied: NCS6K verwendet Virtualisierungstechnologie zum Aufbau des Systems. Jeder Knoten, Routing Processor (RP) oder Line Card (LC), kann mehrere virtuelle Systeme (VM) wie System Admin VM, IOS-XR VM1, IOS-XR VM2 usw. ausführen, die zusammen einen voll funktionsfähigen XR-Knoten

bilden. Die folgende Abbildung zeigt ein Beispiel, in dem RP und LC eine IOS-XR-VM ausführen:

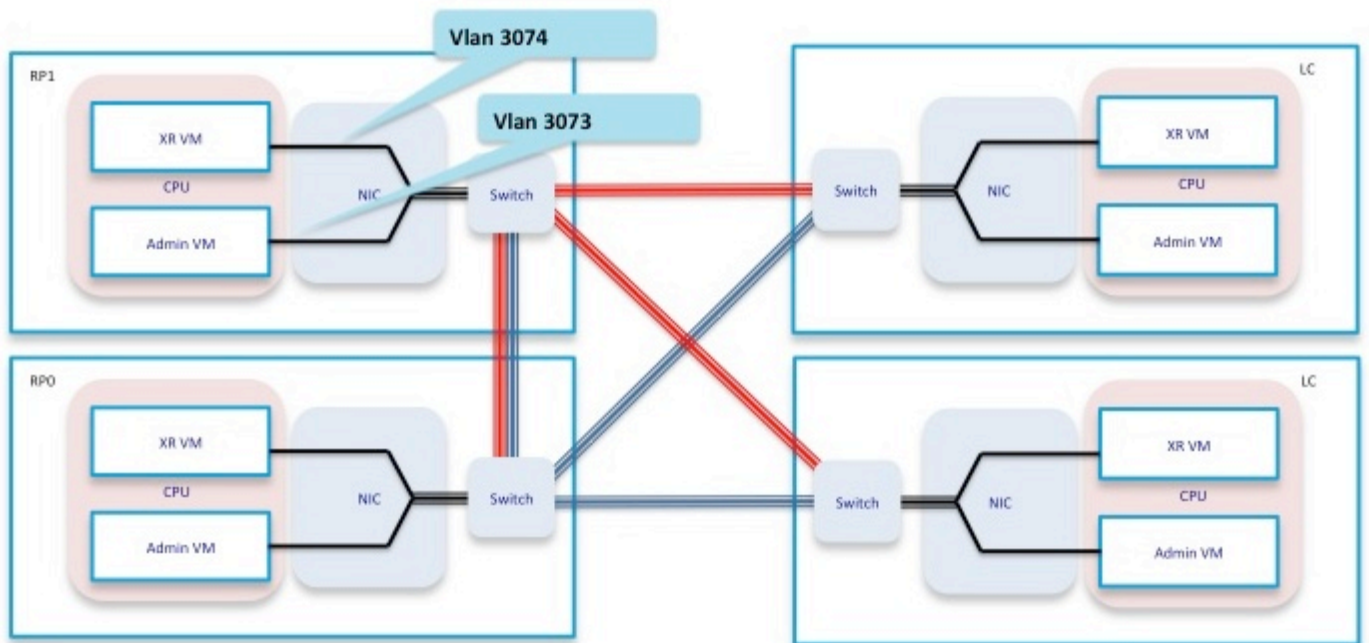
Abbildung 1



RPs und LCs können über ein Ethernet-Steuerungsnetzwerk miteinander verbunden werden. Der Steuerungsebenen-Datenverkehr zwischen RPs und LCs wird durch dieses Kontroll-Ethernet-Netzwerk geleitet. Da es sich um eine Virtualisierungsumgebung handelt, stellen sich Fragen wie die Bereitstellung dieses Pakets an eine bestimmte VM, und wie die Nicantic (NIC) in RP oder LC weiß, dass ein Paket für diese bestimmt ist.

Kurz gesagt: VLANs werden verwendet, um den Datenverkehr verschiedener VMs zu differenzieren. Dieser Prozess wird von der Netzwerkkarte durchgeführt. Abbildung 2 zeigt, wie die Netzwerkkarte VLAN 3074-Datenverkehr an die IOS-XR VM und VLAN 3073-Datenverkehr an die Admin VM übermittelt.

Abbildung 2

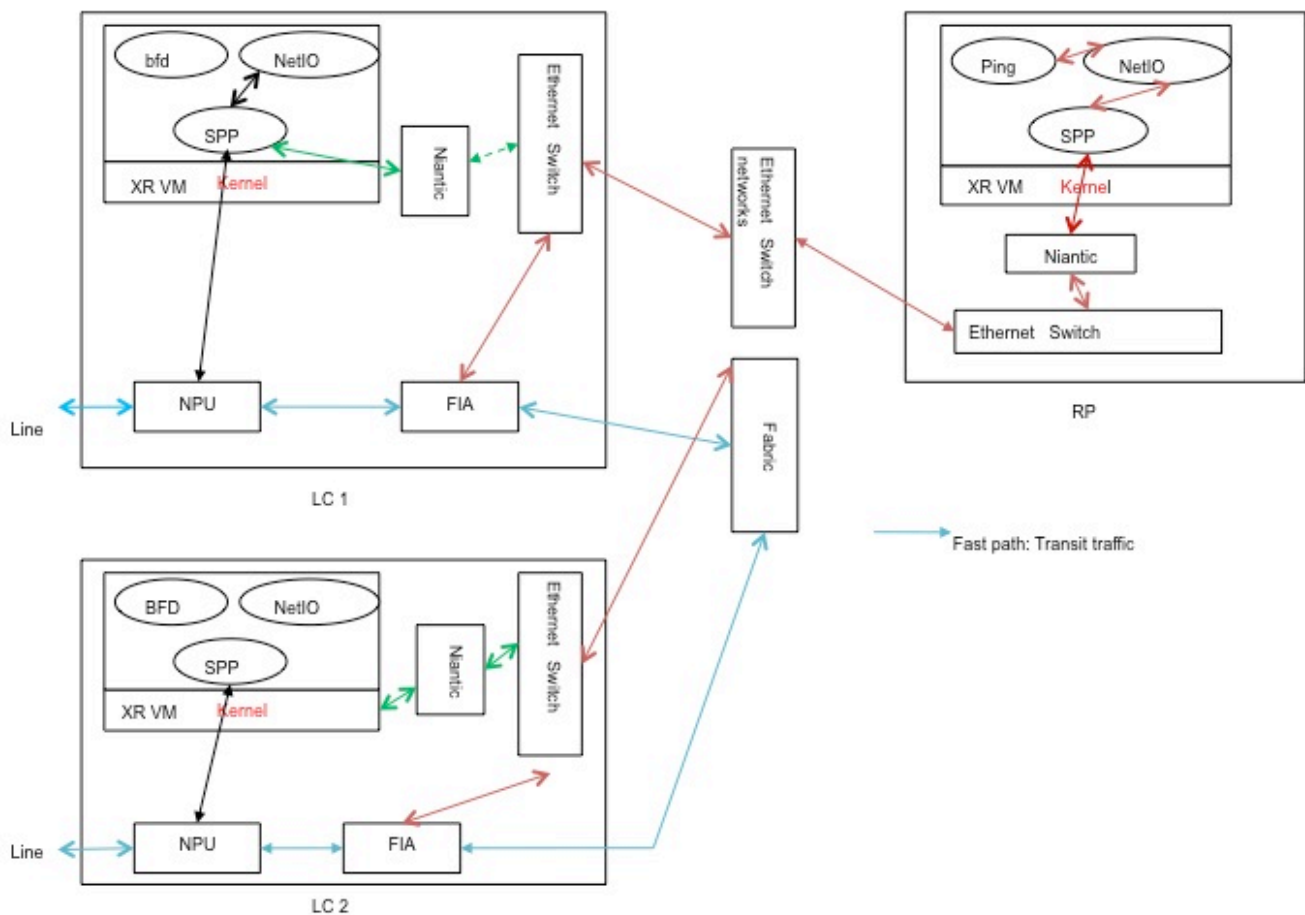


Wenn Sie diese Weiterleitungskomponente zusammenfassen, erhalten Sie einen vereinfachten Weiterleitungspfad für das Ping-Testszenario, wie in Abbildung 3 gezeigt.

Beim Durchführen eines Ping-Tests vom RP nehmen Pakete den folgenden Weiterleitungspfad innerhalb der Box:

RP_PING \longleftrightarrow RP_NETIO \longleftrightarrow RP_SPP \longleftrightarrow RP_Linux_Kernel_Socket \longleftrightarrow Switch \longleftrightarrow
 LC_FIA \longleftrightarrow LC_NPU (Include PSE, PLIM_ASIC) \longleftrightarrow Line

Abbildung 3



Überprüfen

Für den Rest des Dokuments wird als Beispiel ein Szenario verwendet, in dem ein Ping vom RP initiiert wird. Der Ping-Befehl wird an einen direkt verbundenen Host auf Te0/0/0/2/0 initiiert. Die folgenden Schritte zeigen einen schrittweisen Ansatz für die Überprüfung des Ping-Paketes.

```
RP/0/RP0/CPU0:NCS6k-Deploy#show ip interface brief
```

Interface	IP-Address	Status	Protocol
Bundle-Ether671	10.67.2.2	Up	Up
Bundle-Ether672	10.67.3.2	Down	Down
Loopback0	10.17.17.17	Up	Up
MgmtEth0/RP0/CPU0/0	10.7.54.11	Up	Up
TenGigE0/0/0/2/0	10.67.1.2	Up	Up
TenGigE0/0/0/2/1	unassigned	Up	Up
TenGigE0/0/0/2/2	unassigned	Up	Up
TenGigE0/0/0/2/3	unassigned	Up	Up
TenGigE0/0/0/2/4	unassigned	Up	Up
TenGigE0/0/0/2/5	unassigned	Down	Down

[snip]

```
RP/0/RP0/CPU0:NCS6k-Deploy#show run interface Ten 0/0/0/2/0
interface TenGigE0/0/0/2/0
  ipv4 address 10.67.1.2 255.255.255.252
  load-interval 30
```

```
RP/0/RP0/CPU0:NCS6k-Deploy#ping 10.67.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.67.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/7 ms
```

1. Der Zähler "show IPv4 traffic" (IPv4-Datenverkehr anzeigen) auf dem RP-Knoten zeigt an, wie viele ICMP-Echos (Internet Control Message Protocol) gesendet wurden und wie viele ICMP-Antworten zurückgegeben wurden.

```
RP/0/RP0/CPU0:NCS6k-Deploy#show ipv4 traffic
```

```
IP statistics:
  Rcvd: 1495334 total, 80112 local destination
        0 format errors, 0 bad hop count
        23 unknown protocol, 0 not a gateway
        0 security failures, 0 bad source, 0 bad header
        133207 with options, 0 bad, 0 unknown
  Opts: 0 end, 0 nop, 0 basic security, 0 extended security
        0 strict source rt, 0 loose source rt, 0 record rt
        0 stream ID, 0 timestamp, 133207 alert, 0 cipso
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble, 0 fragments received
        0 fragmented, 0 fragment count, 0 fragment max drop
  Bcast: 0 sent, 0 received
  Mcast: 1361652 sent, 1376283 received
        Drop: 0 encapsulation failed, 237 no route, 0 too big
  Sent: 1437435 total
```

ICMP statistics:

```
  Sent: 0 admin unreachable, 63 network unreachable
        8 host unreachable, 0 protocol unreachable
        16 port unreachable, 0 fragment unreachable
        0 time to live exceeded, 0 reassembly ttl exceeded
        24 echo request, 30024 echo reply
        0 mask request, 0 mask reply
        0 parameter error, 0 redirects
        30131 total
  Rcvd: 0 admin unreachable, 21 network unreachable
        0 host unreachable, 0 protocol unreachable
        0 port unreachable, 0 fragment unreachable
        0 time to live exceeded, 0 reassembly ttl exceeded
        30024 echo request, 15 echo reply
        0 mask request, 0 mask reply
        0 redirect, 0 parameter error
        0 source quench, 0 timestamp, 0 timestamp reply
        0 router advertisement, 0 router solicitation
        30063 total, 0 checksum errors, 0 unknown
```

2. Aktivieren Sie die Komponente Network Input Output (NETIO). Der nächste Schritt besteht in der Überprüfung des RP FINT NETIO Kettenzählers. Sie müssen den "OUT"-Zähler des IPv4-Knotens in der Netzwerkkette sehen. Wenn sie erhöht wird, bedeutet dies, dass Pakete die NETIO-Komponente erreicht haben und von der NETIO-Komponente ausgesendet werden.

Check initial NETIO counter value.

```
RP/0/RP0/CPU0:NCS6k-Deploy#sh netio chains FINT loc 0/rp0/cpu0 | in Stats
<Protocol number> (name) Stats
<6> (fint_n2n) Stats IN: 0 pkts, 0 bytes; OUT: 0 pkts, 0 bytes
<10> (clns) Stats IN: 0 pkts, 0 bytes; OUT: 0 pkts, 0 bytes
```

```

<12> (ipv4)   Stats IN: 2788 pkts, 115373 bytes; OUT: 2816 pkts, 117933 bytes
<13> (mpls)   Stats IN: 16482 pkts, 2467508 bytes; OUT: 0 pkts, 0 bytes
<18> (lpts)   Stats IN: 47234 pkts, 10381065 bytes; OUT: 0 pkts, 0 bytes
<19> (ipv6)   Stats IN: 0 pkts, 0 bytes; OUT: 0 pkts, 0 bytes
<30> (ipv4_preroute) Stats IN: 0 pkts, 0 bytes; OUT: 0 pkts, 0 bytes
<32> (ipv6_preroute) Stats IN: 0 pkts, 0 bytes; OUT: 0 pkts, 0 bytes
<34> (fint_proto_tp) Stats IN: 0 pkts, 0 bytes; OUT: 0 pkts, 0 bytes
<36> (l2transport) Stats IN: 0 pkts, 0 bytes; OUT: 0 pkts, 0 bytes

```

Initiate 10 ping packets.

```

RP/0/RP0/CPU0:NCS6k-Deploy#ping 10.67.1.1 coun 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 10.67.1.1, timeout is 2 seconds:
!!!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 4/7/8 ms

```

Check NETIO counter again. You would see increment of 10 packets.

```

RP/0/RP0/CPU0:NCS6k-Deploy#sh netio chains FINT loc 0/rp0/cpu0 | in Stats
<Protocol number> (name) Stats
<6> (fint_n2n)   Stats IN: 0 pkts, 0 bytes; OUT: 0 pkts, 0 bytes
<10> (clns)     Stats IN: 0 pkts, 0 bytes; OUT: 0 pkts, 0 bytes
<12> (ipv4)     Stats IN: 2788 pkts, 115373 bytes; OUT: 2826 pkts, 118933 bytes
<13> (mpls)     Stats IN: 16482 pkts, 2467508 bytes; OUT: 0 pkts, 0 bytes
<18> (lpts)     Stats IN: 47234 pkts, 10381065 bytes; OUT: 0 pkts, 0 bytes
<19> (ipv6)     Stats IN: 0 pkts, 0 bytes; OUT: 0 pkts, 0 bytes
<30> (ipv4_preroute) Stats IN: 0 pkts, 0 bytes; OUT: 0 pkts, 0 bytes
<32> (ipv6_preroute) Stats IN: 0 pkts, 0 bytes; OUT: 0 pkts, 0 bytes
<34> (fint_proto_tp) Stats IN: 0 pkts, 0 bytes; OUT: 0 pkts, 0 bytes
<36> (l2transport) Stats IN: 0 pkts, 0 bytes; OUT: 0 pkts, 0 bytes

```

Sie können auch den KornShell (ksh) Befehl "show_netio_fwder_stats -g" verwenden, um zu überprüfen, ob Inject/Plot Zählerinkremente erhöht werden oder nicht. **Hinweis:** In der Produktionsumgebung kann es zu anderem Hintergrunddatenverkehr kommen, der es schwierig macht zu überprüfen, ob Ping-Pakete diese Komponente erreicht haben oder nicht. Als Problemumgehung können Sie eine große Anzahl von Paketen mit Timeout 0 verwenden: "ping x.x.x.x count 1000 time 0" und prüfen, ob der Zähler plötzlich inkrementiert oder einen Spitzenwert hat.

Check initial counter value.

```

RP/0/RP0/CPU0:NCS6k-Deploy#run show_netio_fwder_stats -g
RECEIVE STATISTICS SUMMARY:
rx_pkts: 2224455
punt_pkts: 2224447
ingress_total_drops: 8
TRANSMIT STATISTICS SUMMARY:
inject_pkts: 2077319
tx_pkts: 2058041
egress_total_drops: 2
RECEIVE STATISTICS DETAILS:
Rx Pkt type stats:
  lpts_pkts: 2220753
Rx Listener tag stats:
  ipv4: 1116092
  ipv6: 658627
  clns: 112549
  ipv4_l: 286252
  raw4: 23
  raw6: 43984
  ospf_mc4: 45
  ospf_mc6: 2

```

```
udp4: 7
tcp4: 405
isis: 2767
Rx Punt reason stats:
  IFIB: 2220753
Rx Drop stats:
  null_fint_ifh_drops: 8
  ingress_total_drops: 8
TRANSMIT STATISTICS DETAILS:
Tx Pkt type stats:
  ipv4: 2852
  mpls: 42647
  osi: 78760
  ipv4_preroute: 1339401
  ipv6_preroute: 613659
Tx Protocol Id stats:
  clns: 78760
  ipv4: 2852
  mpls: 42647
  ipv4_preroute: 1339401
  ipv6_preroute: 613659
Tx Drop stats:
  invalid_queue_drops: 2
  hdr_init_drops: 2
  egress_total_drops: 2
```

Initiate 10 ping packets.

```
RP/0/RP0/CPU0:NCS6k-Deploy#ping 10.67.1.1 coun 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 10.67.1.1, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 3/4/7 ms
```

Check counter again to check to se increment of 10 packets.

```
RP/0/RP0/CPU0:NCS6k-Deploy#run show netio fwder_stats -g
RECEIVE STATISTICS SUMMARY:
rx_pkts: 2224465
punt_pkts: 2224457
ingress_total_drops: 8
TRANSMIT STATISTICS SUMMARY:
inject_pkts: 2077332
tx_pkts: 2058051
egress_total_drops: 2
RECEIVE STATISTICS DETAILS:
Rx Pkt type stats:
  lpts_pkts: 2220763
Rx Listener tag stats:
  ipv4: 1116102
  ipv6: 658627
  clns: 112549
  ipv4_l: 286252
  raw4: 23
  raw6: 43984
  ospf_mc4: 45
  ospf_mc6: 2
  udp4: 7
  tcp4: 405
  isis: 2767
Rx Punt reason stats:
  IFIB: 2220763
Rx Drop stats:
  null_fint_ifh_drops: 8
  ingress_total_drops: 8
```



```

4E:41:50:00:10:01 inet addr:172.0.16.1 Bcast:172.255.255.255 Mask:255.0.0.0 inet6 addr:
fe80::4c41:50ff:fe00:1001/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:9700 Metric:1 RX
packets:402491385 errors:0 dropped:0 overruns:0 frame:0 TX packets:350389778 errors:0
dropped:6 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:100599198478 (93.6 GiB)
TX bytes:96834116492 (90.1 GiB) lo Link encap:Local Loopback inet addr:127.0.0.1
Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUNNING MTU:16436 Metric:1 RX
packets:1029861486 errors:0 dropped:0 overruns:0 frame:0 TX packets:1029861486 errors:0
dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:201624257033 (187.7 GiB)
TX bytes:201624257033 (187.7 GiB)

```

eth-vf1.514 wird für die Kommunikation mit der Mgmtether-Schnittstelle verwendet, die IPv4-Adresse wird jedoch nicht angezeigt. Die Mgmtherschnittstelle in XR VM basiert auf dem IP-Stack von IOS-XR anstelle des IP-Stacks in Linux. Für die Kommunikation mit Admin VM wird **ether-vf1.3073** verwendet. **ether-vf1.3074** wird für den Datenverkehr auf Kontrollebene mit XR VM verwendet. Das Ping-Testpaket durchläuft diese Subschnittstelle (mithilfe des Linux-Netzwerkprotokoll-Stacks). Tcpcdump in Verbindung mit Linux hat viele Optionen, um interessanten Datenverkehr auszulagern. Darüber hinaus können Sie mit tcpcdump-Tools den SDR-Verkehr (Secure Domain Router) auf Kontrollebene (VLAN 3074) ausspucken oder anderen Datenverkehr wie IPC-Kommunikation (Inter Process Communication) in VLAN 3073 aussparen.

```
xr-vm_node0_RP0_CPU0:/]$ tcpcdump -i eth-vf1.3074 -XX -vv
```

```

tcpcdump: listening on eth-vf1.3074, link-type EN10MB (Ethernet), capture size 65535 bytes
01:49:21.798386 IP (tos 0x6,ECT(0), ttl 1, id 0, offset 0, flags [DF], proto UDP (17),
length 340)

```

```

172.0.16.1.10150 > 239.255.0.4.10150: [bad udp cksum ab2a!] UDP, length 312
0x0000: 0100 5e7f 0004 4e41 5000 1001 0800 4506  ..^...NAP.....E.
0x0010: 0154 0000 4000 0111 cc8e ac00 1001 efff  .T...@.....
0x0020: 0004 27a6 27a6 0140 ad56 abcd abcd 0000  ..'..'@.V.....
0x0030: 0000 0280 f502 0000 0000 0000 0000 0000  .....
0x0040: 0000 0000 0000 7856 3412 0128 0204 0000  .....xV4..(....
0x0050: 0000 5508 0100 0100 0000 3c25 2600 0000  ..U.....=&...
0x0060: 0000 d007 0000 0000 0000 ffff 0000 0000  .....
0x0070: 0000 0000 0000 0000 0000 0000 0000 0000  .....
0x0080: 0000 0000 0000 4800 0000 0200 0000 0000  .....H.....
0x0090: 0000 8800 0000 0000 0000 0000 0000 0000  .....
0x00a0: 0000 0100 0000 0000 0000 0000 0000 0000  .....
0x00b0: 0000 0000 0000 c2ca 0031 0000 0000 0000  .....1.....
0x00c0: 0000 0000 0000 0000 0000 5508 0000 6510  .....U...e.
0x00d0: 0000 ed53 4c00 0000 0000 0000 0000 0000  ...SL.....
0x00e0: 0000 0000 0000 0000 0000 0000 0000 6264  .....bd
0x00f0: 7863 0000 0000 0000 0000 0000 0000 0000  xc.....
0x0100: 0000 0000 0000 0000 0000 0000 0000 0000  .....
0x0110: 0000 0100 0000 0000 0000 0000 0000 30ff  .....0.
0x0120: 0002 0000 0000 0000 0000 0000 0000 0000  .....
0x0130: 0000 0000 0000 0000 0000 0000 0000 0000  .....
0x0140: 0000 0000 0000 0000 0000 0c00 0000 0000  .....
0x0150: 0000 0000 0000 0000 0000 0000 0000 0000  .....
0x0160: 0000 ..

```

```

01:49:21.799167 IP (tos 0x6,ECT(0), ttl 64, id 0, offset 0, flags [DF], proto UDP (17),
length 380)

```

```

172.0.0.1.8197 > 172.0.16.1.8197: [udp sum ok] UDP, length 352
0x0000: 4e41 5000 1001 4e41 5000 0001 0800 4506  NAP...NAP.....E.
0x0010: 017c 0000 4000 4011 d168 ac00 0001 ac00  .|...@.
0x0040: 0000 0000 0000 7856 3412 0128 0204 0000  .....xV4..(....
0x0050: 0000 5508 0100 0100 0000 3d25 2600 0000  ..U.....=%&...
0x0060: 0000 d007 0000 0000 0000 ffff 0000 0000  .....
0x0070: 0000 0000 0000 0000 0000 0000 0000 0000  .....
0x0080: 0000 0000 0000 4800 0000 0200 0000 0000  .....H.....
0x0090: 0000 8800 0000 0000 0000 0000 0000 0000  .....
0x00a0: 0000 0100 0000 0000 0000 0000 0000 0000  .....
0x00b0: 0000 0000 0000 c2ca 0031 0000 0000 0000  .....1.....

```

```

0x00c0: 0000 0000 0000 0000 0000 5508 0000 6510 .....U....
0x00d0: 0000 ee53 4c00 0000 0000 0000 0000 0000 ...SL.....
0x00e0: 0000 0000 0000 0000 0000 0000 0000 6264 .....bd
0x00f0: 7863 0000 0000 0000 0000 0000 0000 0000 xc.....
0x0100: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0110: 0000 0100 0000 0000 0000 0000 0000 30ff .....0.
0x0120: 0002 0000 0000 0000 0000 0000 0000 0000 .....
0x0130: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0140: 0000 0000 0000 0000 0000 0c04 0000 0000 .....
0x0150: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0160: 0000 ..
01:49:21.802982 IP (tos 0x6,ECT(0), ttl 64, id 0, offset 0, flags [DF], proto UDP (17),
length 380)

```

```
172.0.0.1.8197 > 172.0.16.1.8197: [udp sum ok] UDP, length 352
```

```

0x0000: 4e41 5000 1001 4e41 5000 0001 0800 4506 NAP...NAP....E.
0x0010: 017c 0000 4000 4011 d168 ac00 0001 ac00 .|..@.@..h.....
0x0020: 1001 2005 2005 0168 672f abcd abcd 0000 .....hg/.....
0x0030: 0000 3c80 f502 0000 0000 0000 0000 0000 ..<.....
0x0040: 0000 0000 0000 7856 3412 0411 0008 0000 .....xV4.....
0x0050: 0000 5508 0000 0100 0000 3d25 2600 0000 ..U.....=%&...
0x0060: 0000 d007 0100 0000 0000 ffff 0000 0000

```

[snip]

Hinweis: Da es sich um ein VM-Szenario handelt, kann der an VM gesendete Datenverkehr mit der VM-Schnittstellenadresse im äußeren Header gekapselt werden, sodass dieser Datenverkehr die VM-Schnittstelle erreichen kann.

Das oben angegebene Paket-Dump wurde tatsächlich mit dem UDP-Paket-Header mit der Quell-/Ziel-172.0.16.1 gekapselt. Dies ist die eth-vf1.3074 ip-Adresse in IOS-XR VM.

Hinweis: Die dabei verwendeten Aufzeichnungen sollen den Ansatz demonstrieren und verfügen nicht über ICMP-Datenverkehr (Internet Control Message Protocol).

5. Überprüfen der FIA-Komponente auf der Linecard.

Check initial counter value.

```
RP/0/RP0/CPU0:NCS6k-Deploy#sh controllers fia statistics instance 1 loc 0/0/cpu0
```

```
FIA Statistics Rack: 0, Slot: 0, Asic instance: 1
```

```
FIA Rx (To Fabric) Statistics.
```

```
----- Input Pkt counters
Pkts Bytes Rx pkts from pse : 250 53000 Rx pkts from switch : 993528 349564509 bcast pkts
from switch : 0 mcast pkts from switch : 993278 ucast pkts from switch :
```

250

```

Rx pkts enqueued(IQM)           :                500           86500
Rx pkts dequeued(IQM)           :                500           86500
Rx pkts sent to fabric           :                500

```

Cell counters:

```

Data cells sent to fabric        :                500           86500
Control cells sent to fabric     :           183039783411

```

Drop counters:

```

Rx burst error drops(NBI)       :                0
Rx error drops(Switch)          :                0
Rx error drops(pse)             :                0
Rx pkt discard drops(IQM)       :           993277           334570329
Pkt crc error drops(FDT)        :                0
Unreachable dest cell drops     :                0
Internal Error Count            :           41984110
Internal Drop Count             :                0

```

```
FIA Tx (From Fabric) Statistics
```

```
----- Cell counters:
```



```
Packet EOP Abort Drop      : 0          Bytes EOP Abort Drop      : 0
Packet Policy Deny         : 0          Bytes Policy Deny         : 0
```

Rx Packet Drop Details

=====

```
Unknown Dest MAC Pkts      : 0
Unknown E-Type Pkts        : 0
Unknown Encap Pkts         : 0          Unknown Encap Bytes       : 0
Unknown VLAN Pkts          : 0          Unknown VLAN Bytes        : 0
L2 Subif VLAN Deny Pkts    : 0          L2 Subif VLAN Deny Bytes : 0
```

Rx Accepted Packet Details

=====

```
Packet HPQ CTL Sent        : 6          Bytes HPQ CTL Sent        : 384
Packet HPQ HP Sent         : 0          Bytes HPQ HP Sent         : 0
Packet LPQ LP1 Sent        : 0          Bytes LPQ LP1 Sent        : 0
Packet LPQ LP2 Sent        : 0          Bytes LPQ LP2 Sent        : 0
```

8. Aktivieren Sie die Zähler für die Benutzeroberfläche anzuzeigen. Es ist empfehlenswert, dies im ersten Schritt zu überprüfen, aber in der Paketflusssequenz ist dies der letzte Schritt. Es hilft dabei herauszufinden, ob das Paket an die Leitung gesendet wurde und ob das Paket von der Leitung zurückgesendet wurde. Es kann helfen, das Problem einzugrenzen, ob es sich innerhalb oder außerhalb dieser Box befindet.

Check initial counter values.

```
RP/0/RP0/CPU0:NCS6k-Deploy#show inter ten 0/0/0/2/0
TenGigE0/0/0/2/0 is up, line protocol is up
  Interface state transitions: 1
  Hardware is TenGigE, address is e051.2a0f.8c29 (bia e051.2a0f.8c29)
  Description: Connected to 0/7/0/1 - CRS-F
  Internet address is 10.67.1.2/30
  MTU 1514 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
    reliability 0/255, txload 0/255, rxload 0/255
  Encapsulation ARPA,
  Full-duplex, 10000Mb/s, SR, link type is force-up
  output flow control is off, input flow control is off
  loopback not set,
  ARP type ARPA, ARP timeout 04:00:00
  Last input 00:14:22, output 00:14:22
  Last clearing of "show interface" counters 22:08:42
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
    3256 packets input, 370860 bytes, 0 total input drops
    0 drops for unrecognized upper-level protocol
  Received 0 broadcast packets, 0 multicast packets
    0 runts, 0 giants, 0 throttles, 0 parity
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    3256 packets output, 370860 bytes, 0 total output drops
  Output 0 broadcast packets, 0 multicast packets
  0 output errors, 0 underruns, 0 applique, 0 resets
  0 output buffer failures, 0 output buffers swapped out
  0 carrier transitions
```

Initiate 1000 ping packets.

```
RP/0/RP0/CPU0:NCS6k-Deploy#ping 10.67.1.1 cou 1000
Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 10.67.1.1, timeout is 2 seconds:
```

