

L2MP-basierte Weiterleitung über vPC Peer-Link in Carmel ASIC-basierten Switches (Nexus 5548/5596)

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Vermeidung von Schleifen](#)

[Zugehörige Informationen](#)

Einführung

In vPC-Topologien wird Benutzerdatenverkehr nur für verwaisten Port-Datenverkehr oder überfluteten Datenverkehr (Unicast, Broadcast, Multicast) auf dem Peer-Link angezeigt. Bei diesem Hochwasserdatenverkehr müssen Switches sicherstellen, dass der auf einer der vPC-Bereiche empfangene Hochwasserdatenverkehr nicht auf der anderen vPC-Ebene zurückgesendet wird, sodass Pakete nicht an die Quelle zurückgesendet oder an andere vPCs dupliziert werden.

Bei Carmel-basierten Switches (Nexus 55xx) ist die Implementierung der vPC-Schleifenvermeidung anders als bei einer auf Gatos (Nexus 5010/5020) basierenden Implementierung, bei der ein separates internes MCT-VLAN für überfluteten Datenverkehr über Peer-Links verwendet wird.

Da Carmel-basierte Switches L2MP oder FabricPath unterstützen, entschieden sich die Techniker für eine L2MP-basierte Weiterleitung über den Peer-Link. Bei diesem Modell verfügt der primäre vPC-Switch über eine Switch-ID von 2748(0xabc), während der sekundäre vPC-Switch über eine Switch-ID von 2749(0xabd) verfügt. Die emulierte Switch-ID von 2750(0xabe) wird als Quell-Switch-ID für Frames verwendet, die einen vPC empfangen, aber über den Peer-Link gesendet werden. Alle Ports auf dem primären vPC-Switch sind Mitglieder von FTAG 256, während die Ports auf dem sekundären vPC Mitglieder von FTAG 257 sind. Im primären vPC-Switch sind nur verwaiste Ports FTAG 257-Mitglieder, während im sekundären vPC-Switch verwaiste Ports FTAG 256-Mitglieder sind.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

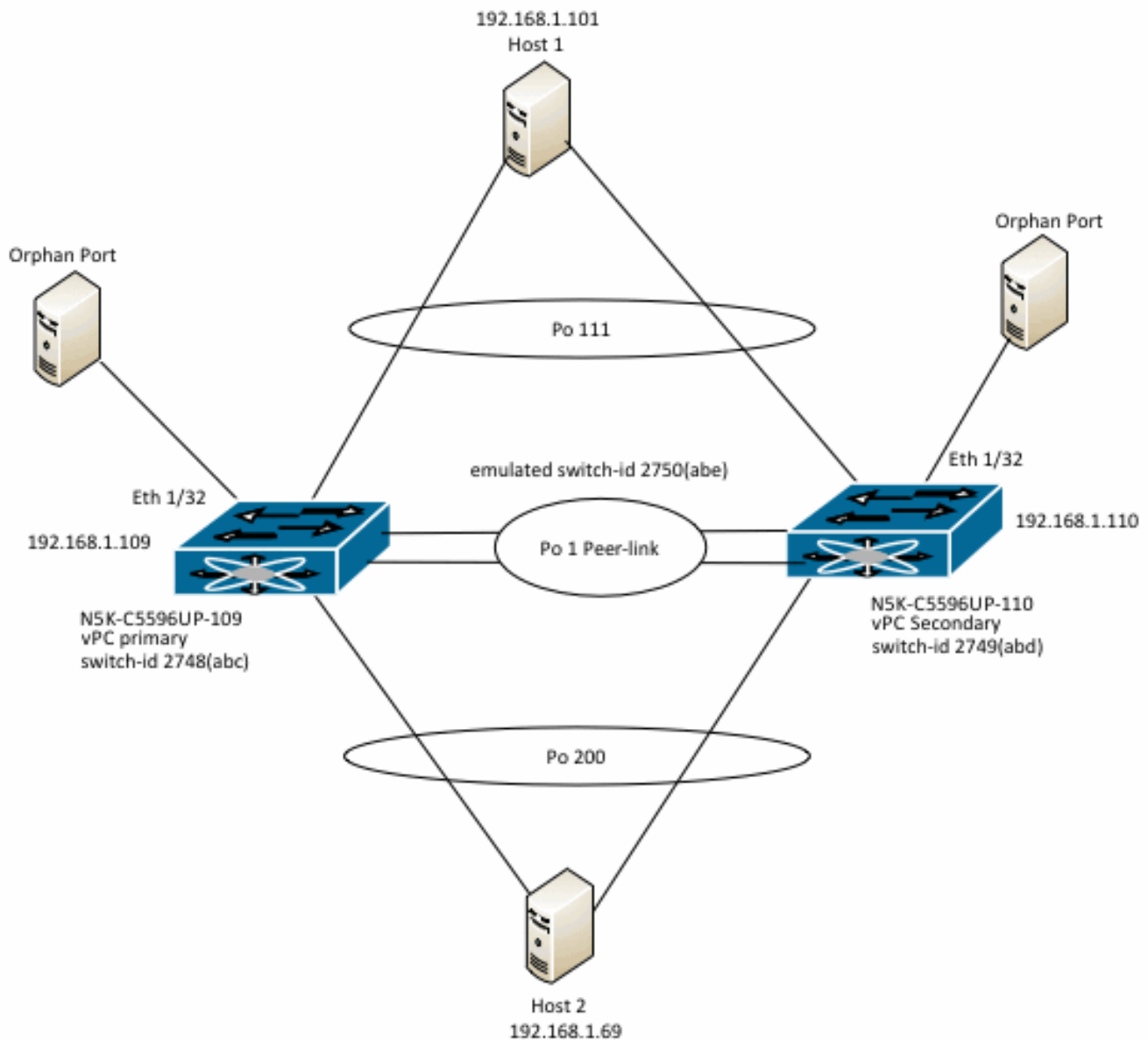
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Vermeidung von Schleifen

Für Broadcast-/unbekannte Unicast-/Multicast-Frames, die an den primären vPC-Switch gesendet werden, wird eine FTAG von 256 über die Peer-Verbindung gesendet. Wenn der sekundäre vPC-Switch diesen Frame über die vPC-Peer-Verbindung empfängt, prüft er die FTAG, und seit dem 256 sendet der sekundäre vPC-Switch diesen nur noch an FTAG 256-Mitglieder, die nur verwaiste Ports sind. Für Flutdatenverkehr vom sekundären vPC wird der FTAG 257 gesendet. Wenn der primäre vPC-Switch diesen Frame abrufen, sendet er den empfangenen Flut-Frame nur an Mitglieder des FTAG 257, die nur verwaiste Ports sind. Auf diese Weise implementieren Carmel-basierte Switches die Vermeidung von vPC-Schleifen.

Um die L2MP/FTAG-basierte Weiterleitung von Flood-Frames über Peer-Link zu vertiefen, wird diese Topologie verwendet:



N5K-C5596UP-109 und N5K-C5596UP-100 sind ein vPC-Paar von Nexus 5596-Switches mit NX-OS 5.2(1)N1(2a). N5K-C5596UP-109 ist der primäre vPC-Switch und N5K-C5596UP-110 der sekundäre vPC-Switch. Port-Channel 1 ist der vPC Peer-Link. Die angegebenen IP-Adressen gehören zu Schnittstelle VLAN 1 der Switches. Host 1 und Host 2 sind Cisco Switches, die über vPC in VLAN 1 verbunden sind. Diese werden in diesem Dokument als Host 1 und Host 2 bezeichnet. In VLAN 1 ist auf beiden Switches ein verwaister Port mit Eth1/32 verbunden.

Hier einige Befehlsausgaben der Switches:

```
N5K-C5596UP-109# show vpc
```

```
Legend:
```

```
(*) - local vPC is down, forwarding via vPC peer-link
```

```
vPC domain id           : 2
Peer status              : peer adjacency formed ok
vPC keep-alive status   : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role                 : primary
Number of vPCs configured : 2
Peer Gateway             : Enabled
Peer gateway excluded VLANs : -
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status     : Disabled
```

```
vPC Peer-link status
```

```
-----
id   Port   Status  Active vlans
-----
1    Po1    up      1
```

```
vPC status
```

```
-----
id     Port       Status Consistency Reason           Active vlans
-----
111    Po111        up     success    success                    1
200    Po200        up     success    success                    1
```

```
N5K-C5596UP-109# show platform fwm info l2mp myswid
```

```
switch id
```

```
switch id manager
```

```
-----
vpc role: 0
my primary switch id: 2748 (0xabc)
emu switch id: 2750 (0xabe)
peer switch id: 2749 (0xabd)
```

```
N5K-C5596UP-109# show vpc orphan-ports
```

```
Note:
```

```
-----::Going through port database. Please be patient.::-----
```

```
VLAN           Orphan Ports
-----
1              Eth1/32
```

```
N5K-C5596UP-110# show vpc
```

```
Legend:
```

```
(*) - local vPC is down, forwarding via vPC peer-link
```

```

vPC domain id          : 2
Peer status            : peer adjacency formed ok
vPC keep-alive status  : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role               : secondary
Number of vPCs configured : 2
Peer Gateway           : Enabled
Peer gateway excluded VLANs : -
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status   : Disabled
vPC Peer-link status

```

```

-----
id   Port   Status  Active vlans
--  -
1    Po1    up      1

```

vPC status

```

-----
id     Port      Status Consistency Reason          Active vlans
-----
111    Po111      up     success    success                1
200    Po200      up     success    success                1

```

N5K-C5596UP-110# show platform fwm info l2mp myswid

switch id

```

-----
switch id manager
-----

```

```

vpc role: 1
my primary switch id: 2749 (0xabd)
emu switch id: 2750 (0xabe)
peer switch id: 2748 (0xabc)

```

N5K-C5596UP-110# show vpc orphan-ports

Note:

```

-----::Going through port database. Please be patient.::-----

```

```

VLAN          Orphan Ports
-----

```

```

1             Eth1/32

```

Now lets check on default FTAGs used and its members.

N5K-C5596UP-109# show platform fwm info l2mp ftag all

L2MP FTAG

```

-----
ftag[0x9565b1c] id: 256 (0x100)
Topology ID: 0x111
Ftag flags: 0 (invalid ftag-flags)
Is stale: FALSE
ftag_mask[0x973eca4]
ifindex array:
0x160000c7 0x1600006e 0x1a01f000
0x15010000 0x15020000 0x1600007e
0x16000000

```

```
ifmap[0x88400fc]
ifmap idx 6: ref 1, lu_mcq_allocated 0, lu_mcq 15 (orig 15) 'not pruned'
ifmap idx 6: prune_ifmap 0, prune ref count 0, prune_unvisited 0
ifmap_idx 6: oifls_macg_ref_cnt 0, num_oifls 0
ifmap idx 6: ifs - sup-eth1 sup-eth2 Po200 Pol Pol111 Eth1/32 Po127
rpf: (0x0)
alternate: 0
intf:
Pol (0x16000000)
ftag_ucast_index: 1
ftag_flood_index: 1
ftag_mcast_index: 32
ftag_alt_mcast_index: 48
```

```
-----
ftag[0x9565e3c] id: 257 (0x101)
Topology ID: 0x111
Ftag flags: 0 (invalid ftag-flags)
```

```
Is stale: FALSE
ftag_mask[0x95612b4]
ifindex array:
0x1a01f000 0x15010000 0x15020000
0x16000000
```

```
ifmap[0x883b81c]
ifmap idx 11: ref 1, lu_mcq_allocated 0, lu_mcq 14 (orig 14) 'not pruned'
ifmap idx 11: prune_ifmap 0, prune ref count 0, prune_unvisited 0
ifmap_idx 11: oifls_macg_ref_cnt 0, num_oifls 0
ifmap idx 11: ifs - sup-eth1 sup-eth2 Pol Eth1/32
rpf: (0x0)
alternate: 1
intf:
Pol (0x16000000)
ftag_ucast_index: 0
ftag_flood_index: -1
ftag_mcast_index: 0
ftag_alt_mcast_index: 0
```

```
-----
N5K-C5596UP-109#
```

```
N5K-C5596UP-110# show platform fwm info l2mp ftag all
L2MP FTAG
```

```
-----
ftag[0x956a99c] id: 256 (0x100)
Topology ID: 0x111
Ftag flags: 0 (invalid ftag-flags)
```

```
Is stale: FALSE
ftag_mask[0x98b4764]
ifindex array:
0x16000066 0x1a01f000 0x15010000
0x15020000 0x16000000
```

```
ifmap[0x9635adc]
ifmap idx 4: ref 1, lu_mcq_allocated 0, lu_mcq 15 (orig 15) 'not pruned'
ifmap idx 4: prune_ifmap 0, prune ref count 0, prune_unvisited 0
ifmap_idx 4: oifls_macg_ref_cnt 0, num_oifls 0
ifmap idx 4: ifs - sup-eth1 sup-eth2 Po103 Pol Eth1/32
rpf: (0x0)
alternate: 1
intf:
Pol (0x16000000)
ftag_ucast_index: 1
ftag_flood_index: -1
ftag_mcast_index: 32
ftag_alt_mcast_index: 48
```

```
-----
ftag[0x956acbc] id: 257 (0x101)
```

```

Topology ID: 0x111
Ftag flags: 0 (invalid ftag-flags)
Is stale: FALSE
ftag_mask[0x97359bc]
ifindex array:
0x160000c7 0x16000066 0x1600006e
0x1a01f000 0x15010000 0x15020000
0x1600007e 0x16000000
ifmap[0x95c624c]
ifmap idx 7: ref 1, lu_mcq_allocated 0, lu_mcq 16 (orig 16) 'not pruned'
ifmap idx 7: prune_ifmap 0, prune_ref_count 0, prune_unvisited 0
ifmap_idx 7: oifls_macg_ref_cnt 0, num_oifls 0
ifmap idx 7: ifs - sup-eth1 sup-eth2 Po200 Po103 Po1 Po111 Eth1/32 Po127
rpf: (0x0)
alternate: 0
intf:
Po1 (0x16000000)
ftag_ucast_index: 0
ftag_flood_index: 1
ftag_mcast_index: 32
ftag_alt_mcast_index: 48

```

Test 1: Broadcast-ARP-Datenverkehr über sekundäre vPC-Verbindungen

Eine nicht vorhandene IP 192.168.1.199 wird von Host 1 gepingt (192.168.1.101). Aus diesem Grund sendet Host 1 immer wieder eine Broadcast-ARP-Anfrage mit der Frage "Wer ist 192.168.1.199". Host 1 hasht diesen Broadcast-Datenverkehr an den sekundären vPC-Switch N5K-C5596UP-110, der ihn wiederum an alle Ports in VLAN 1 weiterleitet, einschließlich Po1, dem vPC-Peer-Link.

Ein TX-SPAN von Port-Channel 1 wird erfasst, um die FabricPath-Header dieses ARP-Broadcast anzuzeigen, der ein Frame mit mehreren Zielen in FP-Terminologie ist. Sehen Sie sich den FabricPath-Header dieses Multi-Destination-Frames an.

The screenshot displays a network traffic analysis tool (Wireshark) capturing packets on a Peer-link-switch-110. The packet list shows four ARP requests (No. 1-4) originating from source 192.168.1.101 and destined for Broadcast (ff:ff:ff:ff:ff:ff). The packet details pane for the selected packet (No. 1) shows the Ethernet II header with source MAC address abe.00.0000 and destination MAC address ff:ff:ff:ff:ff:ff. The ARP request details show the sender IP address as 192.168.1.101 and target IP address as 192.168.1.199. The packet bytes pane shows the raw data of the frame.

- Da der Frame über einen vPC(vPC 111) eingeht, ist die Quell-Switch-ID able.00.000.

- Ziel ist ein Broadcast-MAC FF:FF:FF:FF:FF:FF
- FTAG ist 257.

Wenn dieser Frame in den primären vPC-Switch eingeht, wird der FTAG 257 überprüft. Da nur verwaiste Ports Mitglieder von FTAG 257 sind, wird dieser Broadcast-ARP-Frame nur an Eth 1/32 gesendet.

Test 2: Unbekannter Unicast-Frame kommt in sekundäres vPC-System

Um unbekanntem Unicast-Datenverkehr einzuführen, richtete ich auf Host 1 ein statisches ARP für 192.168.1.99 mit einer statischen MAC von 0001.0002.0003 ein und ping an 192.168.1.99. Die ICMP-Echoanfrage erreicht den Nexus 500-C5596UP-110. Da die Adresse nicht weiß, wo sich der MAC 0001.0002.0003 befindet, wird dieser Frame im VLAN inklusive Peer-Link überflutet.

Ein TX-SPAN von Port-Channel 1 wird erfasst, um die FabricPath-Header dieses unbekanntem Unicast-Flood-Frames zu betrachten, der in FP-Terminologie ein Frame mit mehreren Zielen ist. Sehen Sie sich den FabricPath-Header dieses Multi-Destination-Frames an.

The screenshot shows a network traffic capture in Wireshark. The top part displays a list of four ICMP packets. The selected packet (No. 1) is expanded to show its internal structure:

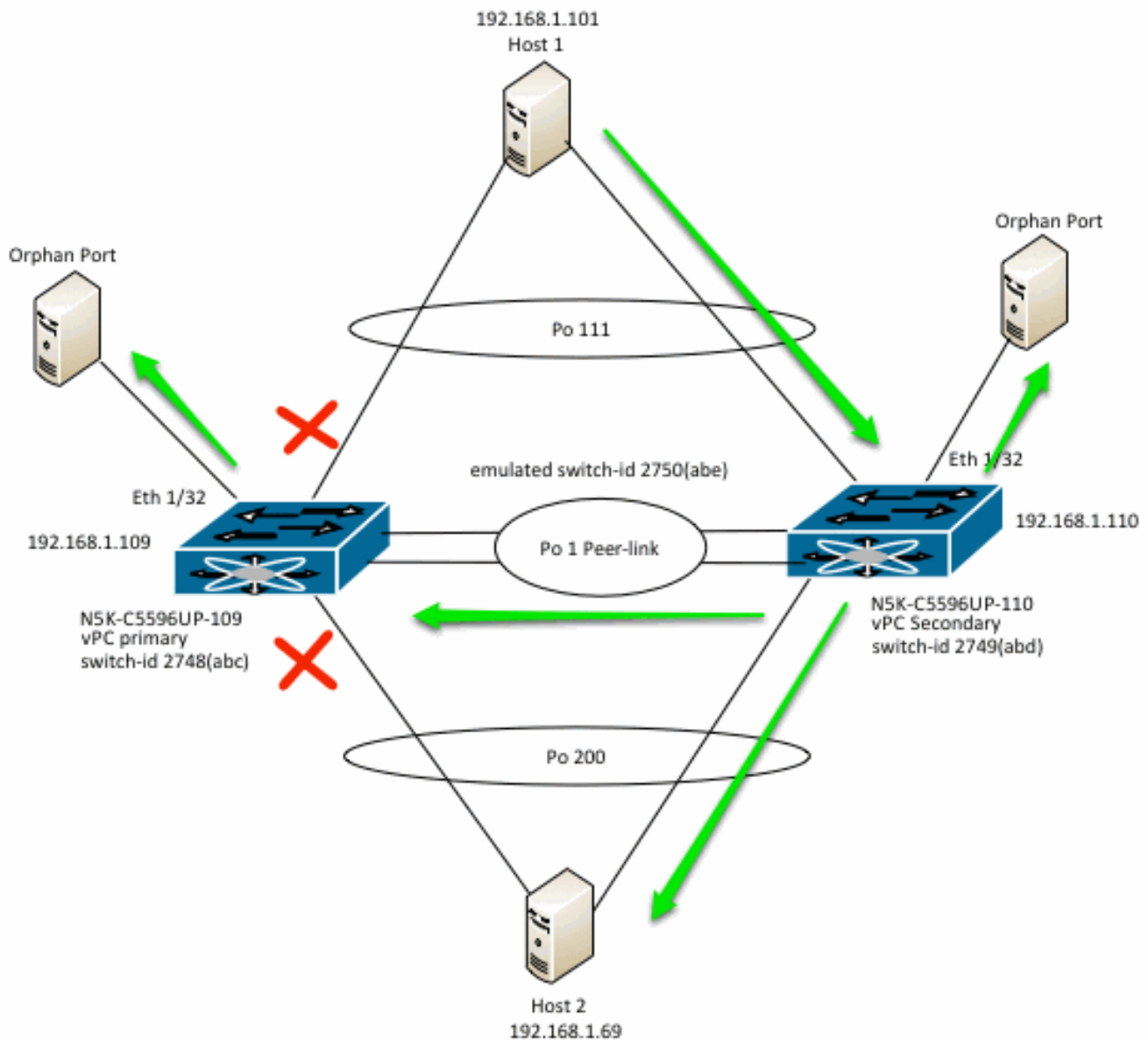
- Frame 1:** 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
- Cisco FabricPath, Src:** abe.00.0000, **Dst:** 01:bb:cc:dd:01:01
- MC Destination:** 01:bb:cc:dd:01:01 (01:bb:cc:dd:01:01)
- Source:** abe.00.0000
 - 0000 00.. 00.. = End Node ID: 0 (0x000000)
 -1. = U/L bit: Locally administered address (this is NOT the factory default)
 -0 = I/G bit: Individual address (unicast)
 -0 = 000/DL Bit: Deliver in order (If DA) or Learn (If SA)
 - 1010 1011 1110 = switch-id: 2750 (0x000abe)
 - sub-switch-id: 0 (0x00)
 - Source LID: 0 (0x0000)
 - 0100 0000 01.. = FTAG: 257
 -10 0000 = TTL: 32
- Ethernet II, Src:** Cisco_0f:b3:01 (54:7f:ee:0f:b3:01), **Dst:** EquipTra_02:00:03 (00:01:00:02:00:03)
- Destination:** EquipTra_02:00:03 (00:01:00:02:00:03)
- Source:** Cisco_0f:b3:01 (54:7f:ee:0f:b3:01)
- 802.1Q Virtual LAN, PRI:** 0, CFI: 0, ID: 1
- Internet Protocol Version 4, Src:** 192.168.1.101, **Dst:** 192.168.1.99

The bottom part of the image shows the raw packet data in hexadecimal and ASCII format.

- Da der Frame über einen vPC(vPC 11) eingeht, ist die Quell-Switch-ID abzurufen.00.000
- Das Ziel ist eine Multicast-MAC-Adresse 01:bb:cc:dd:01:01
- FTAG ist 257.

Wenn dieser Frame in den primären vPC-Switch eingeht, wird der FTAG 257 überprüft. Da nur verwaiste Ports Mitglieder von FTAG 257 sind, wird dieser primäre vPC-Switch diesen Frame nur an den verwaisten Port Eth 1/32 überfluten.

Aufgrund des obigen Mechanismus ist der folgende Fluss für den überfluteten Datenverkehr, der an den sekundären vPC-Switch geleitet wird.

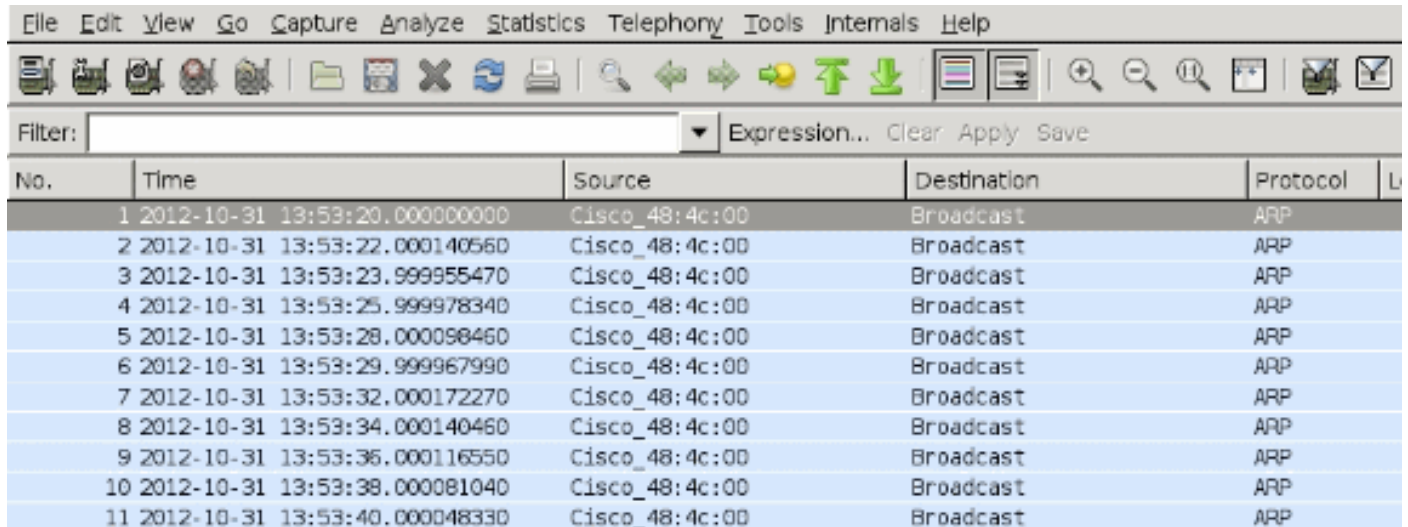


Test 3: Übertragung von ARP-Datenverkehr über vPC Primary

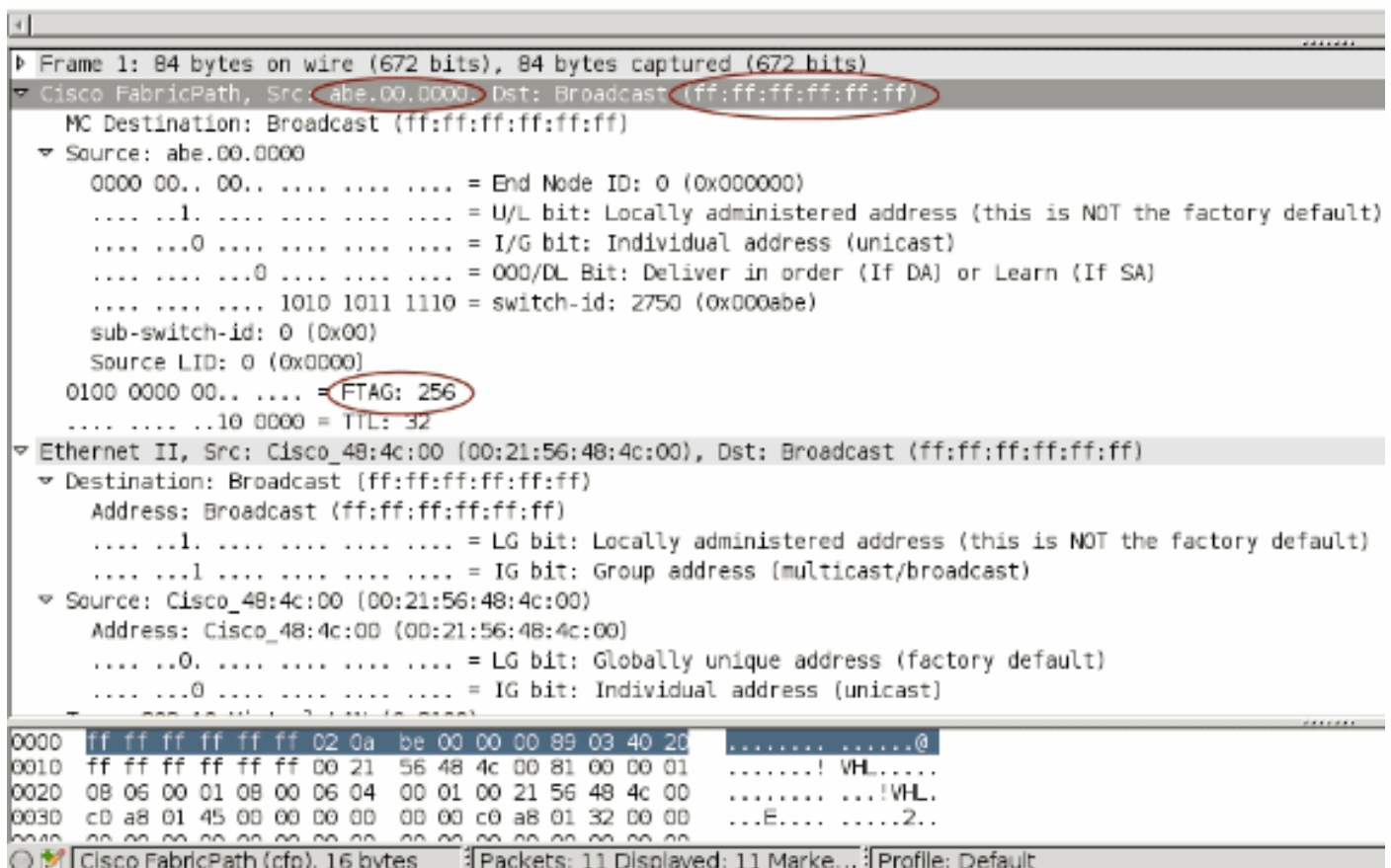
Eine nicht vorhandene IP 192.168.1.200 wird von Host 2 gepingt (192.168.1.69). Aus diesem Grund sendet Host 2 immer wieder eine Broadcast-ARP-Anfrage mit der Frage "Wer ist 192.168.1.200". Host 2 hash diesen Broadcast-Datenverkehr an den vPC Primary Switch N5K-C5596UP-109, der ihn wiederum an alle Ports in VLAN 1 überflutet, einschließlich Po1, dem vPC

Peer-Link.

Ein TX-SPAN von Port-Channel 1 wird erfasst, um die FabricPath-Header dieses ARP-Broadcast anzuzeigen, der ein Frame mit mehreren Zielen in FP-Terminologie ist. Sehen Sie sich den FabricPath-Header dieses Multi-Destination-Frames an.



No.	Time	Source	Destination	Protocol
1	2012-10-31 13:53:20.000000000	Cisco_48:4c:00	Broadcast	ARP
2	2012-10-31 13:53:22.000140560	Cisco_48:4c:00	Broadcast	ARP
3	2012-10-31 13:53:23.999955470	Cisco_48:4c:00	Broadcast	ARP
4	2012-10-31 13:53:25.999978340	Cisco_48:4c:00	Broadcast	ARP
5	2012-10-31 13:53:28.000098460	Cisco_48:4c:00	Broadcast	ARP
6	2012-10-31 13:53:29.999967990	Cisco_48:4c:00	Broadcast	ARP
7	2012-10-31 13:53:32.000172270	Cisco_48:4c:00	Broadcast	ARP
8	2012-10-31 13:53:34.000140460	Cisco_48:4c:00	Broadcast	ARP
9	2012-10-31 13:53:36.000116550	Cisco_48:4c:00	Broadcast	ARP
10	2012-10-31 13:53:38.000081040	Cisco_48:4c:00	Broadcast	ARP
11	2012-10-31 13:53:40.000048330	Cisco_48:4c:00	Broadcast	ARP



```
Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
Cisco FabricPath, Src: abe.00.0000, Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  MC Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: abe.00.0000
    0000 00.. 00.. .... = End Node ID: 0 (0x000000)
    .... ..1. .... = U/L bit: Locally administered address (this is NOT the factory default)
    .... ...0 .... = I/G bit: Individual address (unicast)
    .... ....0 .... = 000/DL Bit: Deliver in order (If DA) or Learn (If SA)
    .... .... 1010 1011 1110 = switch-id: 2750 (0x000abe)
    sub-switch-id: 0 (0x00)
    Source LID: 0 (0x0000)
    0100 0000 00.. .... = FTAG: 256
    .... .... ..10 0000 = TTL: 32
Ethernet II, Src: Cisco_48:4c:00 (00:21:56:48:4c:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Address: Broadcast (ff:ff:ff:ff:ff:ff)
    .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
    .... ...1 .... = IG bit: Group address (multicast/broadcast)
  Source: Cisco_48:4c:00 (00:21:56:48:4c:00)
  Address: Cisco_48:4c:00 (00:21:56:48:4c:00)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ...0 .... = IG bit: Individual address (unicast)
```

0000 ff ff ff ff ff ff 02 0a be 00 00 00 89 03 40 20@

0010 ff ff ff ff ff ff 00 21 56 48 4c 00 81 00 00 01!VH.....

0020 08 06 00 01 08 00 06 04 00 01 00 21 56 48 4c 00!VH.....

0030 c0 a8 01 45 00 00 00 00 00 00 c0 a8 01 32 00 00 ...E.....2..

Cisco FabricPath (cfp), 16 bytes | Packets: 11 Displayed: 11 Marke... | Profile: Default

- Da der Frame über einen vPC(vPC 200) eingeht, ist die Quell-Switch-ID abrufbar.00.000
- Ziel ist ein Broadcast-MAC FF:FF:FF:FF:FF:FF
- FTAG ist 256.

Wenn dieser Frame in den sekundären vPC-Switch eingeht, wird der FTAG 256 überprüft. Da nur verwaiste Ports Mitglieder des FTAG 256 sind, wird dieser Broadcast-ARP-Frame nur an Eth 1/32 gesendet.

Test 4: Unbekannter Unicast-Frame kommt in vPC Primary

Um unbekanntem Unicast-Datenverkehr einzuführen, wird auf Host 2 ein statisches ARP für den 192.168.1.200 mit einer statischen MAC-Adresse von 0003.0004.0005 und 192.168.1.200 eingerichtet. Die ICMP-Echoanfrage hackt auf den primären vPC N5K-C5596UP-109 und weil sie nicht weiß, wo sich MAC 0003.0004.0005 befindet, überflutet sie diesen Frame im VLAN, einschließlich Peer-Link. Ein TX-SPAN von Port-Channel 1 wird erfasst, um die FabricPath-Header dieses unbekanntem Unicast-Flood-Frames zu betrachten, der in FP-Terminologie ein Frame mit mehreren Zielen ist. Sehen Sie sich den FabricPath-Header dieses Multi-Destination-Frames an.

No.	Time	Source	Destination	Protocol
1	2012-11-01 11:52:09.494715320	192.168.1.69	192.168.1.200	ICMP
2	2012-11-01 11:52:11.494739360	192.168.1.69	192.168.1.200	ICMP

```

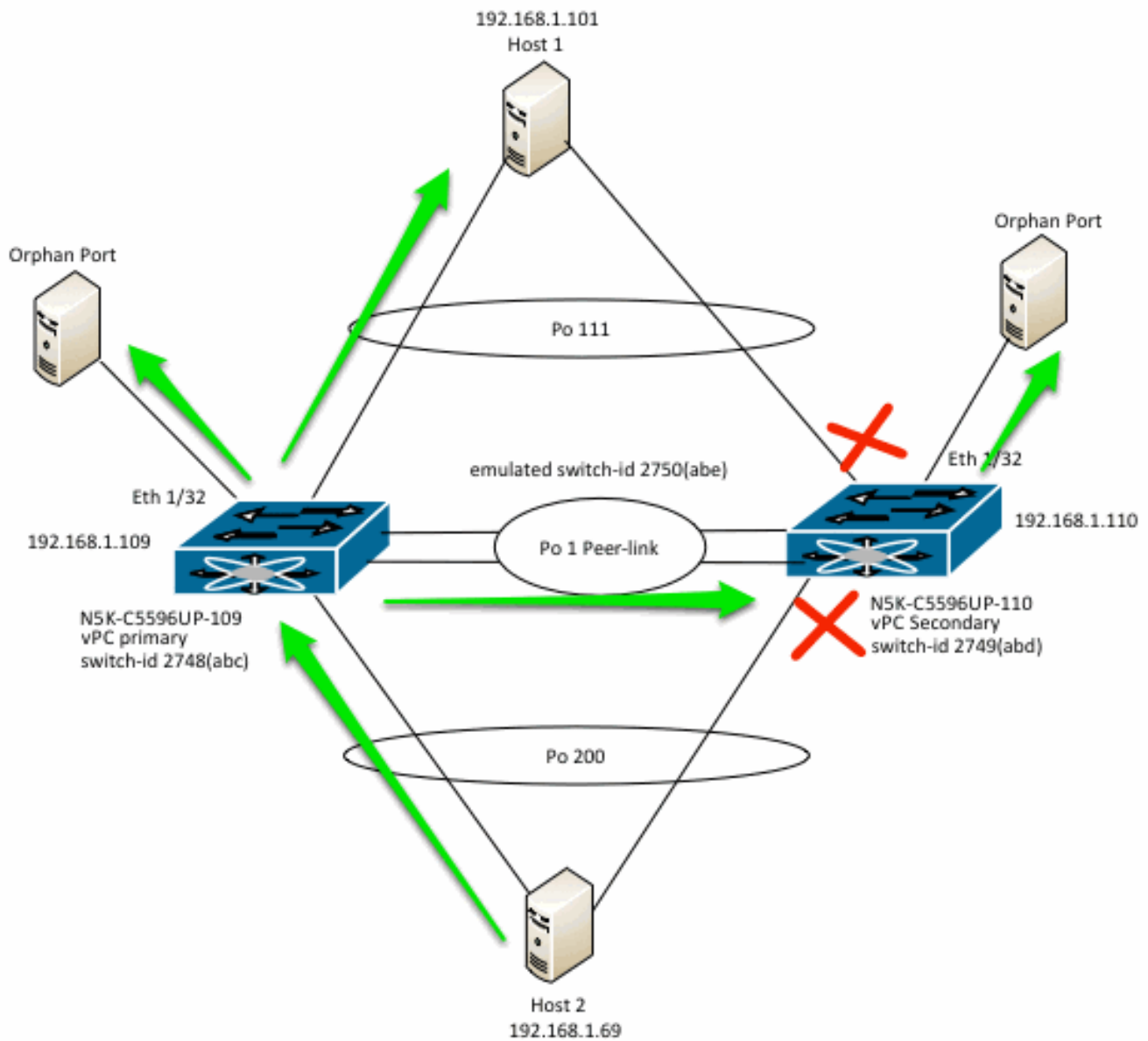
Frame 1: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
Cisco FabricPath, Src: abe.00.0000, Dst: 01:bb:cc:dd:01:01 (01:bb:cc:dd:01:01)
  MC Destination: 01:bb:cc:dd:01:01 (01:bb:cc:dd:01:01)
  Source: abe.00.0000
    0000 00.. 00.. .... = End Node ID: 0 (0x000000)
    .... ..1. .... = U/L bit: Locally administered address (this is NOT the factory default)
    .... ...0 .... = I/G bit: Individual address (unicast)
    .... ....0 .... = 000/DL Bit: Deliver in order (If DA) or Learn (If SA)
    .... .... 1010 1011 1110 = switch-id: 2750 (0x000abe)
    sub-switch-id: 0 (0x00)
    Source LID: 0 (0x0000)
    0100 0000 00.. .... FTAG: 256
    .... .... ..10 0000 = TTL: 32
Ethernet II, Src: Cisco_48:4c:00 (00:21:56:48:4c:00), Dst: Barracud_04:00:05 (00:03:00:04:00:05)
  Destination: Barracud_04:00:05 (00:03:00:04:00:05)
    Address: Barracud_04:00:05 (00:03:00:04:00:05)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ...0 .... = IG bit: Individual address (unicast)
  Source: Cisco_48:4c:00 (00:21:56:48:4c:00)
    Address: Cisco_48:4c:00 (00:21:56:48:4c:00)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ...0 .... = IG bit: Individual address (unicast)
  Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 1
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = CFI: Canonical (0)
  .... 0000 0000 0001 = ID: 1
  Type: IP (0x0800)
  Trailer: 42b8cb0e
Internet Protocol Version 4, Src: 192.168.1.69 (192.168.1.69), Dst: 192.168.1.200 (192.168.1.200)
  Version: 4
0000 01 bb cc dd 01 01 02 0a be 00 00 00 89 03 40 20 .....@
0010 00 03 00 04 00 05 00 21 56 48 4c 00 81 00 00 01 .....! VHL.....
0020 08 00 45 00 00 64 52 56 00 00 ff 01 e4 e4 c0 a8 ..E..dRV .....
0030 01 45 c0 a8 01 c8 08 00 ec 58 00 1d 01 fe 00 00 .E..... .X.....
0040 00 00 04 5e 03 7e eb ed eb ed eb ed eb ed eb ed 7b1
Cisco FabricPath (cfp), 16 bytes | Packets: ... | Profile: Default
  
```

- Da der Frame über einen vPC(vPC 200) geht, ist die Quell-Switch-ID abrufbar.00.000

- Das Ziel ist eine Multicast-MAC 01:bb:cc:dd:01:01, die für unbekannte Unicast-Flooding verwendet wird.
- FTAG ist 256.

Wenn dieser Frame in den sekundären vPC-Switch eingeht, wird der FTAG 257 überprüft. Da nur verwaiste Ports Mitglieder von FTAG 256 sind, wird dieser primäre vPC-Switch diesen Frame nur an den verwaisten Port Eth 1/32 überfluten.

Aufgrund des obigen Mechanismus ist der folgende Fluss für den überfluteten Datenverkehr, der in den primären vPC-Switch eingeht.



Zugehörige Informationen

- [Technischer Support und Dokumentation - Cisco Systems](#)