Risoluzione dei problemi relativi a Nexus Cheat Sheet per principianti

Sommario

Introduzione

In questo documento vengono descritti i diversi strumenti disponibili per la risoluzione dei problemi dei prodotti Nexus che è possibile utilizzare per diagnosticare e risolvere un problema.

Panoramica

Èimportante comprendere quali strumenti sono disponibili e in quale scenario utilizzarli per ottenere il massimo vantaggio. In realtà, a volte un certo strumento non è realizzabile semplicemente perché è progettato per funzionare su qualcos'altro.

In questa tabella vengono compilati i vari strumenti per la risoluzione dei problemi della piattaforma Nexus e le relative funzionalità. Per i dettagli e gli esempi della CLI, fare riferimento alla sezione Nexus Tools.

STRUMENTI	FUNZIONE	CASI DI UTILIZZO DI ESEMPIO	PRO	SVANTAGGI	PERSISTENZA	PIANO EFFETTIVO	COMANDI CLI USATI
Etanalizzatore	Acquisire il traffico destinato alla CPU o provenie	Problemi di lentezza del traffico, latenza e congestione	Eccellente per problemi di lentezza, congestione e latenza	In genere vede solo il traffico del control plane, velocità limitata	N/D	Piano di controllo. Può essere utilizza	interfaccia in ba locale #ethanaly #ethanalyzer loc interface [ID interfaccia] disp filter [WORD] esempio:

	nte dalla CPU					to per il piano dati in alcuni scenari (SPAN-CPU)	#ethanalyzer loc interface Ethern display filter ICM
SPAN	Acquisizione e mirroring di una serie di pacchetti	Non riuscito ping s, pacchetti non in ordine e così via	Eccellente per la perdita intermittente del traffico	Richiede un dispositivo esterno con software sniffer Richiede risorse TCAM	La sessione SPAN deve essere configurata e abilitata/disabilitata	Ctrl + Dati	#monitor sessio #description [NO #source interfac porta] #destinati interface [ID por #no shut
Errore DM	Acquisire il traffico destinato alla o proveniente dalla CPU solo per i dispositivi Broadcom Nexus	Problemi di lentezza del traffico, latenza e congestione	Eccellente per problemi di lentezza, congestione e latenza	Solo per dispositivi Broadcom Nexus. Velocità limitata (CloudScale Nexus 9k non dispone di SPAN-CPU)	N/D	Piano di controllo. Può essere utilizzato per il piano dati in alcuni scenari	Varia in base all piattaforma. Vec Panoramica di E - Cisco
ELAM	Cattura un singolo pacchetto che entra [o esce, se Nexus 7K] dallo switch Nexus	Verificare che il pacchetto raggiunga il Nexus, controllare le decisioni di inoltro, verificare la presenza di modifiche nel pacchetto, verificare l'interfaccia/VLAN del pacchetto e così via	Eccellente per i problemi di flusso e inoltro dei pacchetti. Non intrusivo	Richiede una conoscenza approfondita dell'hardware. Utilizza meccanismi di trigger univoci specifici dell'architettura. Utile solo se si conosce il traffico che si desidera ispezionare	N/D	Ctrl + Dati	# attach module [NUMERO MOD # debug platform internal <>
Nexus 9k Packet Tracer	Rileva percorso del pacchetto	Problemi di connettività e perdita di pacchetti	Fornisce un contatore per le statistiche di flusso utili per la	Impossibile acquisire il traffico ARP. Funziona solo per Nexus 9k	N/D	Dati + Controllo	# test packet-tra src_IP [IP ORIG dst_IP [IP DESTINAZIONE test packet-trace start # test pack

			perdita intermittente /completa. Ideale per schede di linea senza intagli TCAM				tracer stop # tes packet-tracer sh
Traceroute	Rileva percorso del pacchetto rispetto agli hop L3	Ping non riusciti, impossibile raggiungere host/destinazione /Internet e così via	Rileva i vari hop nel percorso per isolare gli errori L3.	Identifica solo dove il limite L3 è interrotto (non identifica il problema stesso)	N/D	Dati + Controllo	# traceroute [IP DESTINAZIONE Gli argomenti includono: porta, numero p origine, interfac vrf, source-inter
Ping	Verifica della connettività tra due punti di una rete	Verifica della raggiungibilità tra i dispositivi	Uno strumento rapido e semplice per verificare la connettività	Identifica solo se l'host è raggiungibile o meno	N/D	Dati + Controllo	# ping [IP DESTINAZIONE Gli argomenti includono: count, dimensio pacchetto, interf di origine, interv multicast, loopb timeout
PACL/RACL/VACL	Acquisire il traffico in entrata/uscita da una determinata porta o VLAN	Perdita di pacchetti intermittente tra gli host, conferma dell'arrivo o dell'uscita dei pacchetti al Nexus e così via	Eccellente per la perdita intermittente del traffico	Richiede risorse TCAM. Per alcuni moduli è richiesta l'intaglio manuale TCAM	Permanente (applicato a running-configurazione)	Dati + Controllo	# ip access-list [NOME ACL] # i access-group [N ACL] # ip acces group [NOME A Gli argomenti includono: deny, fragments allow, remark, s statistics, end, e pop, push, wher
LogFlash	Memorizza i dati cronologici dello switch a livello globale, ad esempio i registri degli account, i file di arresto anomalo del sistema e gli	Riavvio/arresto improvviso del dispositivo, ogni volta che un dispositivo viene ricaricato, i dati di log flash forniscono alcune informazioni utili per l'analisi	Le informazioni vengono conservate al momento del ricaricamento del dispositivo (archiviazione permanente)	Esterno su Nexus 7K = Deve essere installato/integrato sulla piattaforma supervisor per consentire la raccolta di questi registri (I non si applica a 3K/9K poiché logflash è una partizione del dispositivo di storage interno)	Reload-Persistent	Dati + Controllo	# dir flash log:

	eventi, indipendentemente dal ricaricamento del dispositivo						
OBFL	Memorizza i dati cronologici in un modulo specifico, ad esempio informazioni relative a guasti e problemi ambientali	Riavvio/arresto improvviso del dispositivo, ogni volta che un dispositivo viene ricaricato, i dati di log flash forniscono alcune informazioni che possono essere utili	Le informazioni vengono conservate al momento del ricaricamento del dispositivo (archiviazione permanente)	Supporta un numero limitato di operazioni di lettura e scrittura	Reload-Persistent	Dati + Controllo	# show logging onboard module Gli argomenti includono: boot-uptime, ca boot-history, ca first-power-on, counter-stats, d version, endtime environment-his error-stats, exception-log, internal, interru stats, obfl-histor stat-trace, startt status
Event-History	Quando sono necessarie informazioni per un processo specifico attualmente in esecuzione	Ogni processo in nexus ha una propria cronologia di eventi, ad esempio CDP, STP, OSPF, EIGRP, BGP, vPC, LACP e così via	Risoluzione dei problemi relativi a un processo specifico in esecuzione su Nexus	Le informazioni vengono perse quando il dispositivo viene ricaricato (non persistente)	Non persistente	Dati + Controllo	# show [PROCE cronologia even interna [ARGUMENT] Gli argomenti includono: Adiacente, cli, evento, flooding hello, ldp, lsa, m objstore, redistribution, ri segrt, spf, spf-tr statistics, te
Debug	Quando sono necessarie informazioni più granulari in tempo reale/in tempo	Èpossibile eseguire il debug su ogni processo in nexus, ad esempio CDP, STP, OSPF, IGRP, BGP, vPC, LACP e così via	Risoluzione dei problemi relativi a un processo specifico in esecuzione su Nexus in tempo reale per una maggiore	Può influire sulle prestazioni della rete	Non persistente	Dati + Controllo	# processo di de [PROCESS] esempio: # debug ip ospf

	reale per un processo specifico		granularità				
ORO	Fornisce avvio, runtime e diagnostica su richiesta sui componenti hardware (come moduli I/O e Supervisor)	Testing hardware come USB, Bootflash, OBFL, memoria ASIC, PCIE, loopback delle porte, NVRAM e così via	Èin grado di rilevare guasti nell'hardware e di intraprendere le necessarie azioni correttive solo nella release 6(2)8 e successive	Rileva solo problemi hardware	Non persistente	N/D	# show diagnos content module show diagnostic description mod [#] test all
EEM	Monitoraggio degli eventi nel dispositivo e esecuzione delle azioni necessarie	Qualsiasi attività del dispositivo che richieda un'azione/soluzione alternativa/notifica, come arresto dell'interfaccia, malfunzionamento della ventola, utilizzo della CPU e così via	Supporta gli script Python	Per configurare EEM è necessario disporre dei privilegi di amministratore di rete	Lo script e il trigger EEM risiedono nella configurazione	N/D	Varia, vedere Configurazione Embedded Even Manager

Strumenti Nexus

Per ulteriori informazioni sui vari comandi e sulla relativa sintassi o opzioni, fare riferimento a Cisco Nexus serie 9000 Switch - Riferimenti per i comandi - Cisco.

- **Etanalizzatore**

Ethanalyzer è uno strumento NX-OS progettato per acquisire il traffico della CPU dei pacchetti. Qualsiasi cosa che colpisca la CPU, sia in entrata che in uscita, può essere catturata con questo strumento. È basato sul noto analizzatore di protocollo di rete open source Wireshark. Per ulteriori informazioni su questo strumento, consultare la guida alla risoluzione dei problemi di Ethanalyzer su Nexus 7000 - Cisco

Èimportante notare che in genere, Ethanalyzer cattura tutto il traffico da e verso il supervisore,

ossia, non supporta acquisizioni specifiche dell'interfaccia. Miglioramenti specifici dell'interfaccia sono disponibili per alcune piattaforme nei punti di codice più recenti. Inoltre, Ethanalyzer acquisisce solo il traffico che viene commutato dalla CPU, non dall'hardware. Ad esempio, è possibile acquisire il traffico sull'interfaccia in banda, sull'interfaccia di gestione o su una porta del pannello anteriore (se supportata):

```
Nexus9000_A(config-if-range)# ethanalyzer local interface inband
Capturing on inband
2020-02-18 01:40:55.183177 cc:98:91:fc:55:8b -> 01:80:c2:00:00:00 STP RST. Root =
32768/1/cc:98:91:fc:55:80  Cost = 0  Port = 0x800b
2020-02-18 01:40:55.184031 f8:b7:e2:49:2d:f2 -> 01:80:c2:00:00:0e LLC U, func=UI; SNAP, OUI
0x00000C (Cisco), PID 0x0134
2020-02-18 01:40:55.184096 f8:b7:e2:49:2d:f5 -> 01:80:c2:00:00:0e LLC U, func=UI; SNAP, OUI
0x00000C (Cisco), PID 0x0134
2020-02-18 01:40:55.184147 f8:b7:e2:49:2d:f4 -> 01:80:c2:00:00:0e LLC U, func=UI; SNAP, OUI
0x00000C (Cisco), PID 0x0134
2020-02-18 01:40:55.184190 f8:b7:e2:49:2d:f3 -> 01:80:c2:00:00:0e LLC U, func=UI; SNAP, OUI
0x00000C (Cisco), PID 0x0134
2020-02-18 01:40:55.493543 dc:f7:19:1b:f9:85 -> 01:80:c2:00:00:00 STP RST. Root =
32768/1/dc:f7:19:1b:f9:80  Cost = 0  Port = 0x8005
2020-02-18 01:40:56.365722      0.0.0.0 -> 255.255.255.255 DHCP DHCP Discover - Transaction ID
0xc82a6d3
2020-02-18 01:40:56.469094 f8:b7:e2:49:2d:b4 -> 01:80:c2:00:00:0e LLC U, func=UI; SNAP, OUI
0x00000C (Cisco), PID 0x0134
2020-02-18 01:40:57.202658 cc:98:91:fc:55:8b -> 01:80:c2:00:00:00 STP RST. Root =
32768/1/cc:98:91:fc:55:80  Cost = 0  Port = 0x800b
2020-02-18 01:40:57.367890      0.0.0.0 -> 255.255.255.255 DHCP DHCP Discover - Transaction ID
0xc82a6d3
10 packets captured

Nexus9000_A(config-if-range)# ethanalyzer local interface mgmt
Capturing on mgmt0
2020-02-18 01:53:07.055100 cc:98:91:fc:55:94 -> 01:80:c2:00:00:00 STP RST. Root =
32768/46/84:8a:8d:7d:a2:80  Cost = 4  Port = 0x8014
2020-02-18 01:53:09.061398 cc:98:91:fc:55:94 -> 01:80:c2:00:00:00 STP RST. Root =
32768/46/84:8a:8d:7d:a2:80  Cost = 4  Port = 0x8014
2020-02-18 01:53:11.081596 cc:98:91:fc:55:94 -> 01:80:c2:00:00:00 STP RST. Root =
32768/46/84:8a:8d:7d:a2:80  Cost = 4  Port = 0x8014
2020-02-18 01:53:13.080874 cc:98:91:fc:55:94 -> 01:80:c2:00:00:00 STP RST. Root =
32768/46/84:8a:8d:7d:a2:80  Cost = 4  Port = 0x8014
2020-02-18 01:53:15.087361 cc:98:91:fc:55:94 -> 01:80:c2:00:00:00 STP RST. Root =
32768/46/84:8a:8d:7d:a2:80  Cost = 4  Port = 0x8014
2020-02-18 01:53:17.090164 cc:98:91:fc:55:94 -> 01:80:c2:00:00:00 STP RST. Root =
32768/46/84:8a:8d:7d:a2:80  Cost = 4  Port = 0x8014
2020-02-18 01:53:19.096518 cc:98:91:fc:55:94 -> 01:80:c2:00:00:00 STP RST. Root =
32768/46/84:8a:8d:7d:a2:80  Cost = 4  Port = 0x8014
2020-02-18 01:53:20.391215 00:be:75:5b:d9:00 -> 01:00:0c:cc:cc:cc CDP Device ID:
Nexus9000_A(FDO21512ZES)  Port ID: mgmt0
2020-02-18 01:53:21.119464 cc:98:91:fc:55:94 -> 01:80:c2:00:00:00 STP RST. Root =
32768/46/84:8a:8d:7d:a2:80  Cost = 4  Port = 0x8014
2020-02-18 01:53:23.126011 cc:98:91:fc:55:94 -> 01:80:c2:00:00:00 STP RST. Root =
32768/46/84:8a:8d:7d:a2:80  Cost = 4  Port = 0x8014
10 packets captured

Nexus9000-A# ethanalyzer local interface front-panel eth1/1
Capturing on 'Eth1-1'
1 2022-07-15 19:46:04.698201919 28:ac:9e:ad:5c:b8  01:80:c2:00:00:00 STP 53 RST. Root =
32768/1/28:ac:9e:ad:5c:b7 Cost = 0 Port = 0x8001
2 2022-07-15 19:46:04.698242879 28:ac:9e:ad:5c:b8  01:00:0c:cc:cc:cd STP 64 RST. Root =
32768/1/28:ac:9e:ad:5c:b7 Cost = 0 Port = 0x8001
3 2022-07-15 19:46:04.698314467 28:ac:9e:ad:5c:b8  01:00:0c:cc:cc:cd STP 64 RST. Root =
```

```
32768/10/28:ac:9e:ad:5c:b7 Cost = 0 Port = 0x8001
4 2022-07-15 19:46:04.698386112 28:ac:9e:ad:5c:b8  01:00:0c:cc:cc:cd STP 64 RST. Root =
32768/20/28:ac:9e:ad:5c:b7 Cost = 0 Port = 0x8001
5 2022-07-15 19:46:04.698481274 28:ac:9e:ad:5c:b8  01:00:0c:cc:cc:cd STP 64 RST. Root =
32768/30/28:ac:9e:ad:5c:b7 Cost = 0 Port = 0x8001
6 2022-07-15 19:46:04.698555784 28:ac:9e:ad:5c:b8  01:00:0c:cc:cc:cd STP 64 RST. Root =
32768/40/28:ac:9e:ad:5c:b7 Cost = 0 Port = 0x8001
7 2022-07-15 19:46:04.698627624 28:ac:9e:ad:5c:b8  01:00:0c:cc:cc:cd STP 64 RST. Root =
32768/50/28:ac:9e:ad:5c:b7 Cost = 0 Port = 0x8001
```

Questo output mostra alcuni dei messaggi che possono essere acquisiti con Ethanalyzer. Per impostazione predefinita, Ethanalyzer cattura solo 10 pacchetti. Tuttavia, è possibile usare questo comando per richiedere alla CLI di acquisire i pacchetti per un periodo di tempo indefinito. Utilizzare CTRL+C per uscire dalla modalità di cattura.

```
Nexus9000_A(config-if-range)# ethanalyzer local interface inband limit-captured-frames 0
Capturing on inband
2020-02-18 01:43:30.542588 f8:b7:e2:49:2d:f2 -> 01:80:c2:00:00:0e LLC U, func=UI; SNAP, OUI
0x00000C (Cisco), PID 0x0134
2020-02-18 01:43:30.542626 f8:b7:e2:49:2d:f5 -> 01:80:c2:00:00:0e LLC U, func=UI; SNAP, OUI
0x00000C (Cisco), PID 0x0134
2020-02-18 01:43:30.542873 f8:b7:e2:49:2d:f4 -> 01:80:c2:00:00:0e LLC U, func=UI; SNAP, OUI
0x00000C (Cisco), PID 0x0134
2020-02-18 01:43:30.542892 f8:b7:e2:49:2d:f3 -> 01:80:c2:00:00:0e LLC U, func=UI; SNAP, OUI
0x00000C (Cisco), PID 0x0134
2020-02-18 01:43:31.596841 dc:f7:19:1b:f9:85 -> 01:80:c2:00:00:00 STP RST. Root =
32768/1/dc:f7:19:1b:f9:80  Cost = 0  Port = 0x8005
2020-02-18 01:43:31.661089 f8:b7:e2:49:2d:b2 -> 01:80:c2:00:00:0e LLC U, func=UI; SNAP, OUI
0x00000C (Cisco), PID 0x0134
2020-02-18 01:43:31.661114 f8:b7:e2:49:2d:b3 -> 01:80:c2:00:00:0e LLC U, func=UI; SNAP, OUI
0x00000C (Cisco), PID 0x0134
2020-02-18 01:43:31.661324 f8:b7:e2:49:2d:b5 -> 01:80:c2:00:00:0e LLC U, func=UI; SNAP, OUI
0x00000C (Cisco), PID 0x0134
2020-02-18 01:43:31.776638 cc:98:91:fc:55:8b -> 01:80:c2:00:00:00 STP RST. Root =
32768/1/cc:98:91:fc:55:80  Cost = 0  Port = 0x800b
2020-02-18 01:43:33.143814 f8:b7:e2:49:2d:b4 -> 01:80:c2:00:00:0e LLC U, func=UI; SNAP, OUI
0x00000C (Cisco), PID 0x0134
2020-02-18 01:43:33.596810 dc:f7:19:1b:f9:85 -> 01:80:c2:00:00:00 STP RST. Root =
32768/1/dc:f7:19:1b:f9:80  Cost = 0  Port = 0x8005
2020-02-18 01:43:33.784099 cc:98:91:fc:55:8b -> 01:80:c2:00:00:00 STP RST. Root =
32768/1/cc:98:91:fc:55:80  Cost = 0  Port = 0x800b
2020-02-18 01:43:33.872280 f8:b7:e2:49:2d:f2 -> 01:80:c2:00:00:0e LLC U, func=UI; SNAP, OUI
0x00000C (Cisco), PID 0x0134
2020-02-18 01:43:33.872504 f8:b7:e2:49:2d:f5 -> 01:80:c2:00:00:0e LLC U, func=UI; SNAP, OUI
0x00000C (Cisco), PID 0x0134
2020-02-18 01:43:33.872521 f8:b7:e2:49:2d:f4 -> 01:80:c2:00:00:0e LLC U, func=UI; SNAP, OUI
0x00000C (Cisco), PID 0x0134
15 packets captured
```

I filtri possono essere usati con Ethanalyzer per focalizzare l'attenzione su traffico specifico. Con etanalizzatore è possibile utilizzare due tipi di filtri, denominati filtri di acquisizione e filtri di visualizzazione. Un filtro di acquisizione acquisisce solo il traffico che corrisponde ai criteri definiti nel filtro di acquisizione. Un filtro di visualizzazione acquisisce ancora tutto il traffico, ma viene visualizzato solo il traffico che corrisponde ai criteri definiti nel filtro di visualizzazione.

```
Nexus9000_B# ping 10.82.140.106 source 10.82.140.107 vrf management count 2
PING 10.82.140.106 (10.82.140.106) from 10.82.140.107: 56 data bytes
64 bytes from 10.82.140.106: icmp_seq=0 ttl=254 time=0.924 ms
64 bytes from 10.82.140.106: icmp_seq=1 ttl=254 time=0.558 ms

Nexus9000_A(config-if-range)# ethanalyzer local interface mgmt display-filter icmp
```

```
Capturing on mgmt0
2020-02-18 01:58:04.403295 10.82.140.107 -> 10.82.140.106 ICMP Echo (ping) request
2020-02-18 01:58:04.403688 10.82.140.106 -> 10.82.140.107 ICMP Echo (ping) reply
2020-02-18 01:58:04.404122 10.82.140.107 -> 10.82.140.106 ICMP Echo (ping) request
2020-02-18 01:58:04.404328 10.82.140.106 -> 10.82.140.107 ICMP Echo (ping) reply

4 packets captured
```

Inoltre, è possibile acquisire i pacchetti con l'opzione detail e visualizzarli nel terminale, come su Wireshark. Ciò consente di visualizzare le informazioni complete dell'intestazione in base al risultato del dissettore di pacchetti. Ad esempio, se un frame è crittografato, non sarà possibile visualizzare il payload crittografato. Vedere questo esempio:

```
Nexus9000_A(config-if-range)# ethanalyzer local interface mgmt display-filter icmp detail
Capturing on mgmt0
Frame 2 (98 bytes on wire, 98 bytes captured)
    Arrival Time: Feb 18, 2020 02:02:17.569801000
    [Time delta from previous captured frame: 0.075295000 seconds]
    [Time delta from previous displayed frame: 0.075295000 seconds]
    [Time since reference or first frame: 0.075295000 seconds]
    Frame Number: 2
    Frame Length: 98 bytes
    Capture Length: 98 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:icmp:data]
Ethernet II, Src: 00:be:75:5b:de:00 (00:be:75:5b:de:00), Dst: 00:be:75:5b:d9:00
(00:be:75:5b:d9:00)
    Destination: 00:be:75:5b:d9:00 (00:be:75:5b:d9:00)
        Address: 00:be:75:5b:d9:00 (00:be:75:5b:d9:00)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
>>>>>>>Output Clipped
```

Con Ethanalyzer è possibile:

- Scrivere l'output (un file PCAP) nel nome file specificato su vari file system di destinazione: bootflash, logflash, USB, ecc. Èquindi possibile trasferire il file salvato all'esterno del dispositivo e visualizzarlo in Wireshark, in base alle esigenze.
- Leggere un file da bootflash e visualizzarlo sul terminale. Proprio come quando si legge direttamente dall'interfaccia della CPU, è possibile visualizzare le informazioni complete sul pacchetto usando la parola chiave detail.

Vedere gli esempi per le diverse origini di interfaccia e opzioni di output:

```
Nexus9000_A# ethanalyzer local interface mgmt capture-filter "host 10.82.140.107" write
bootflash:TEST.PCAP
Capturing on mgmt0
10
Nexus9000_A# dir bootflash:
       4096    Feb 11 02:59:04 2020  .rpmstore/
       4096    Feb 12 02:57:36 2020  .swtam/
       2783    Feb 17 21:59:49 2020  09b0b204-a292-4f77-b479-1ca1c4359d6f.config
       1738    Feb 17 21:53:50 2020  20200217_215345_poap_4168_init.log
       7169    Mar 01 04:41:55 2019  686114680.bin
       4411    Nov 15 15:07:17 2018  EBC-SC02-M2_303_running_config.txt
   13562165    Oct 26 06:15:35 2019  GBGBLD4SL01DRE0001-CZ07-
        590    Jan 10 14:21:08 2019  MDS20190110082155835.lic
       1164    Feb 18 02:18:15 2020  TEST.PCAP
>>>>>>>Output Clipped
```

```
Nexus9000_A# copy bootflash: ftp:
Enter source filename: TEST.PCAP
Enter vrf (If no input, current vrf 'default' is considered): management
Enter hostname for the ftp server: 10.122.153.158
Enter username: calo
Password:
***** Transfer of file Completed Successfully *****
Copy complete, now saving to disk (please wait)...
Copy complete.

Nexus9000_A# ethanalyzer local read bootflash:TEST.PCAP
2020-02-18 02:18:03.140167 10.82.140.107 -> 10.82.140.106 ICMP Echo (ping) request
2020-02-18 02:18:03.140563 10.82.140.106 -> 10.82.140.107 ICMP Echo (ping) reply
2020-02-18 02:18:15.663901 10.82.140.107 -> 10.82.140.106 ICMP Echo (ping) request
2020-02-18 02:18:15.664303 10.82.140.106 -> 10.82.140.107 ICMP Echo (ping) reply
2020-02-18 02:18:15.664763 10.82.140.107 -> 10.82.140.106 ICMP Echo (ping) request
2020-02-18 02:18:15.664975 10.82.140.106 -> 10.82.140.107 ICMP Echo (ping) reply
2020-02-18 02:18:15.665338 10.82.140.107 -> 10.82.140.106 ICMP Echo (ping) request
2020-02-18 02:18:15.665536 10.82.140.106 -> 10.82.140.107 ICMP Echo (ping) reply
2020-02-18 02:18:15.665864 10.82.140.107 -> 10.82.140.106 ICMP Echo (ping) request
2020-02-18 02:18:15.666066 10.82.140.106 -> 10.82.140.107 ICMP Echo (ping) reply

RTP-SUG-BGW-1# ethanalyzer local interface front-panel eth1-1 write bootflash:e1-1.pcap
Capturing on 'Eth1-1'
10

RTP-SUG-BGW-1# ethanalyzer local read bootflash:e1-1.pcap detail
Frame 1: 53 bytes on wire (424 bits), 53 bytes captured (424 bits) on interface Eth1-1, id 0
    Interface id: 0 (Eth1-1)
        Interface name: Eth1-1
    Encapsulation type: Ethernet (1)
    Arrival Time: Jul 15, 2022 19:59:50.696219656 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1657915190.696219656 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 53 bytes (424 bits)
    Capture Length: 53 bytes (424 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:llc:stp]
```

- SPAN

SPAN è l'acronimo di SwitchPort Analyzer e viene usato per acquisire tutto il traffico proveniente da un'interfaccia ed eseguirne il mirroring su una porta di destinazione. La porta di destinazione in genere si connette a uno strumento di analisi della rete (ad esempio un PC con Wireshark) che consente di analizzare il traffico che attraversa queste porte. È possibile eseguire lo SPAN del traffico proveniente da una o più porte e VLAN.

Le sessioni SPAN includono una porta di origine e una porta di destinazione. Una porta di origine può essere una porta Ethernet (senza sottointerfacce), canali di porta, interfacce in banda del Supervisor e non può essere una porta di destinazione contemporaneamente. Inoltre, per alcuni dispositivi come la piattaforma 9300 e 9500, sono supportate anche le porte FEX (Fabric Extender). Una porta di destinazione può essere una porta Ethernet (accesso o trunk), un canale porta (accesso o trunk) e per alcuni dispositivi come le porte uplink 9300 sono supportate anche quando le porte FEX non sono supportate come destinazione.

Èpossibile configurare più sessioni SPAN in entrata/uscita/entrambe. Esiste un limite al numero totale di sessioni SPAN che un singolo dispositivo può supportare. Ad esempio, un Nexus 9000 può supportare fino a 32 sessioni, mentre un Nexus 7000 ne può supportare solo 16. È possibile controllare questa condizione dalla CLI o fare riferimento alle guide alla configurazione SPAN per il prodotto in uso.

Si noti che per ogni versione di NX-OS e per il tipo di prodotto, i tipi di interfacce e le funzionalità supportate sono diversi. Fare riferimento alle linee guida e alle limitazioni di configurazione più recenti per il prodotto e la versione in uso. Di seguito sono riportati i collegamenti per Nexus 9000 e Nexus 7000 rispettivamente:

Guida alla configurazione di Cisco Nexus serie 9000 NX-OS System Management, versione 9.3(x) - Configurazione dello SPAN [Switch Cisco Nexus serie 9000] - Cisco

Cisco Nexus serie 7000 NX-OS System Management Configuration Guide - Configuring SPAN [Cisco Nexus serie 7000 Switch] - Cisco

Esistono vari tipi di sessioni SPAN. Di seguito sono elencati alcuni dei tipi più comuni:

- SPAN locale: tipo di sessione SPAN in cui l'host di origine e quello di destinazione sono locali per lo switch. In altre parole, tutta la configurazione richiesta per impostare la sessione SPAN viene applicata a un singolo switch, lo stesso switch su cui risiedono le porte host di origine e di destinazione.
- RSPAN (Remote SPAN): tipo di sessione SPAN in cui l'host di origine e di destinazione non sono locali per lo switch. In altre parole, è possibile configurare le sessioni RSPAN di origine su uno switch e le sessioni RSPAN di destinazione sullo switch di destinazione ed estendere la connettività con la VLAN RSPAN.

Nota: RSPAN non è supportato su Nexus

- ERSPAN (Extended Remote SPAN): Lo switch incapsula il frame copiato con un'intestazione tunnel GRE (Generic Routing Encapsulation) e instrada il pacchetto alla destinazione configurata. Le sessioni di origine e di destinazione devono essere configurate sugli switch di incapsulamento e decapsulamento (due dispositivi diversi). Questo permette di estendere il traffico su una rete di layer 3.
- SPAN-to-CPU: nome assegnato a un tipo speciale di sessione SPAN in cui la porta di destinazione è il supervisore o la CPU. È una forma di sessione SPAN locale e può essere utilizzata nei casi in cui non è possibile utilizzare una sessione SPAN standard. Alcuni dei motivi più comuni sono: nessuna porta di destinazione SPAN disponibile o appropriata, sito non accessibile o non gestito, nessun dispositivo disponibile in grado di connettersi alla porta di destinazione SPAN e così via. Per ulteriori informazioni, fare riferimento a questo collegamento Cisco Nexus 9000 Cloud Scale ASIC NX-OS SPAN-to-CPU Procedure. È importante ricordare che la velocità della CPU SPAN-to è limitata dal CoPP (Control Plane Policing), quindi sniffing una o più interfacce di origine che superano il policer possono causare interruzioni per la sessione SPAN-CPU. In questo caso, i dati non riflettono al 100% ciò che è presente sul cavo, quindi SPAN alla CPU non è sempre appropriato per la risoluzione di scenari con alta velocità di dati e/o perdita intermittente. Dopo aver configurato una sessione SPAN su CPU e averla abilitata a livello amministrativo, è necessario eseguire Ethanalyzer per verificare il traffico inviato alla CPU per eseguire l'analisi di conseguenza.

Questo è un esempio di come è possibile configurare una semplice sessione SPAN locale su uno switch Nexus 9000:

```
Nexus9000_A(config-monitor)# monitor session ?

*** No matching command found in current mode, matching in (config) mode ***
  <1-32>
  all     All sessions

Nexus9000_A(config)# monitor session 10
Nexus9000_A(config-monitor)#?
  description  Session description (max 32 characters)
  destination  Destination configuration
  filter       Filter configuration
  mtu          Set the MTU size for SPAN packets
  no           Negate a command or set its defaults
  show         Show running system information
  shut         Shut a monitor session
  source       Source configuration
  end          Go to exec mode
  exit         Exit from command interpreter
  pop          Pop mode from stack or restore from name
  push         Push current mode to stack or save it under name
  where        Shows the cli context you are in

Nexus9000_A(config-monitor)# description Monitor_Port_e1/1
Nexus9000_A(config-monitor)# source interface ethernet 1/1
Nexus9000_A(config-monitor)# destination interface ethernet 1/10
Nexus9000_A(config-monitor)# no shut
```

L'esempio mostra la configurazione di una sessione SPAN-CPU che è stata attivata e quindi l'uso di Ethanalyzer per acquisire il traffico:

```
N9000-A#show run monitor

monitor session 1
source interface Ethernet1/7 rx
destination interface sup-eth0 << this is what sends the traffic to CPU
no shut

RTP-SUG-BGW-1# ethanalyzer local interface inband mirror limit-c 0
Capturing on 'ps-inb'
2020-02-18 02:18:03.140167 10.82.140.107 -> 10.82.140.106 ICMP Echo (ping) request
2020-02-18 02:18:15.663901 10.82.140.107 -> 10.82.140.106 ICMP Echo (ping) request
```

- Dmirror

Dmirror è un tipo di sessione SPAN-TO-CPU per piattaforme Nexus basate su Broadcom. Il concetto è lo stesso di SPAN-CPU e la velocità è limitata a 50 pps (pacchetti al secondo). La funzione è stata implementata per eseguire il debug del percorso dati interno con la CLI di bcm-shell. A causa delle limitazioni associate, non esiste una CLI di NX-OS che consenta agli utenti di configurare le sessioni SPAN per l'Sup in quanto può influire sul traffico di controllo e utilizzare le classi CoPP.

- ELAM

ELAM è l'acronimo di Embedded Logic Analyzer Module. Consente di esaminare l'ASIC e determinare le decisioni di inoltro da adottare per un SINGOLO pacchetto. Con ELAM è quindi possibile identificare se il pacchetto raggiunge il motore di inoltro e su quali porte/VLAN devono essere inviate le informazioni. È inoltre possibile verificare la struttura dei pacchetti L2 - L4 e controllare se sono state apportate modifiche al pacchetto.

Èimportante capire che l'architettura ELAM dipende da essa e la procedura per acquisire un

pacchetto varia da piattaforma a piattaforma in base all'architettura interna. È necessario conoscere le mappature ASIC dell'hardware per applicare correttamente lo strumento. Per Nexus 7000, vengono prese due acquisizioni per un singolo pacchetto, una prima che la decisione venga presa **Data BUS (DBUS**) e l'altra dopo che la decisione è stata presa **Result BUS (RBUS)**. Quando si visualizzano le informazioni DBUS, è possibile visualizzare il percorso/la destinazione del pacchetto e le informazioni sul layer 2-4. I risultati nel RBUS possono mostrare dove il pacchetto viene inoltrato e se il frame è stato alterato. È necessario configurare i trigger per DBUS e RBUS, verificare che siano pronti e quindi provare a acquisire il pacchetto in tempo reale. Le procedure per le varie schede di linea sono le seguenti:

Per maggiori informazioni sulle varie procedure ELAM, fare riferimento ai link riportati nella tabella:

PANORAMICA DI ELAM	Panoramica di ELAM - Cisco
Nexus 7K F1 Module	Nexus 7000 F1 Module ELAM Procedure - Cisco
Nexus 7K F2 Module	Nexus 7000 F2 Module ELAM Procedure - Cisco
Nexus 7K F3 Module	F3- Esempio ELAM
Nexus 7K M Module	Nexus 7000 serie M Module ELAM Procedure - Cisco
Nexus 7K M1/M2 e F2 Module	Nexus 7K ELAM per M1/M2 e F2 ed etanalizzatore
Nexus 7K M3 Module	Procedura ELAM del modulo Nexus 7000 M3 - Cisco

ELAM per Nexus 7000 - M1/M2 (piattaforma Eureka)

- Controllare il numero del modulo con il comando **show module**.
- Collegare al modulo con **attach module x**, dove x è il numero del modulo.
- Controllare la mappatura ASIC interna con il comando **show hardware internal dev-port-map** e controllare L2LKP e L3LKP.

```
Nexus7000(config)#show module
Mod  Ports  Module-Type                        Model              Status
---  -----  ---------------------------------- ------------------ ----------
1    0      Supervisor Module-2                N7K-SUP2E          active *
2    0      Supervisor Module-2                N7K-SUP2E          ha-standby
3    48     1/10 Gbps Ethernet Module          N7K-F248XP-25E     ok
4    24     10 Gbps Ethernet Module            N7K-M224XP-23L     ok


Nexus7000(config)# attach module 4
Attaching to module 4 ...
To exit type 'exit', to abort type '$.'
Last login: Fri Feb 14 18:10:21 UTC 2020 from 127.1.1.1 on pts/0

module-4# show hardware internal dev-port-map
--------------------------------------------------------------
CARD_TYPE:       24 port 10G
>Front Panel ports:24
--------------------------------------------------------------
 Device name             Dev role              Abbr num_inst:
--------------------------------------------------------------
```

```
> Skytrain               DEV_QUEUEING          QUEUE  4
> Valkyrie               DEV_REWRITE           RWR_0  4
> Eureka                 DEV_LAYER_2_LOOKUP    L2LKP  2
> Lamira                 DEV_LAYER_3_LOOKUP    L3LKP  2
> Garuda                 DEV_ETHERNET_MAC      MAC_0  2
> EDC                    DEV_PHY               PHYS   6
> Sacramento Xbar ASIC   DEV_SWITCH_FABRIC     SWICHF 1
+-------------------------------------------------------------------------+
+----------------+++FRONT PANEL PORT TO ASIC INSTANCE MAP+++------------+
+-------------------------------------------------------------------------+
FP port |  PHYS | SECUR | MAC_0 | RWR_0 | L2LKP | L3LKP | QUEUE |SWICHF
   1       0       0       0       0,1     0       0       0,1     0
   2       0       0       0       0,1     0       0       0,1     0
   3       0       0       0       0,1     0       0       0,1     0
   4       0       0       0       0,1     0       0       0,1     0
   5       1       0       0       0,1     0       0       0,1     0
   6       1       0       0       0,1     0       0       0,1     0
   7       1       0       0       0,1     0       0       0,1     0
   8       1       0       0       0,1     0       0       0,1     0
   9       2       0       0       0,1     0       0       0,1     0
   10      2       0       0       0,1     0       0       0,1     0
   11      2       0       0       0,1     0       0       0,1     0
   12      2       0       0       0,1     0       0       0,1     0
   13      3       1       1       2,3     1       1       2,3     0
   14      3       1       1       2,3     1       1       2,3     0
   15      3       1       1       2,3     1       1       2,3     0
   16      3       1       1       2,3     1       1       2,3     0
   17      4       1       1       2,3     1       1       2,3     0
   18      4       1       1       2,3     1       1       2,3     0
   19      4       1       1       2,3     1       1       2,3     0
   20      4       1       1       2,3     1       1       2,3     0
   21      5       1       1       2,3     1       1       2,3     0
   22      5       1       1       2,3     1       1       2,3     0
   23      5       1       1       2,3     1       1       2,3     0
   24      5       1       1       2,3     1       1       2,3     0
+-------------------------------------------------------------------------+
+-------------------------------------------------------------------------+
```

- Per prima cosa, si acquisisce il pacchetto in L2 e si verifica se la decisione di inoltro è giusta. A tale scopo, esaminare la colonna Mapping L2LKP e identificare il numero di istanza ASIC corrispondente alla porta.
- Quindi eseguire ELAM su questa istanza con il comando **elam asic eureka instance x**dove x è il numero dell'istanza ASIC e configura i trigger per DBUS e RBUS. Verificare lo stato dei trigger con lo **stato** del comando e verificare che i trigger siano stati configurati.

```
module-4(eureka-elam)# trigger dbus dbi ingress ipv4 if source-ipv4-address 192.0.2.2
destination-ipv4-address 192.0.2.4 rbi-corelate
module-4(eureka-elam)# trigger rbus rbi pb1 ip if cap2 1

module-4(eureka-elam)# status

Slot: 4, Instance: 1
EU-DBUS: Configured
trigger dbus dbi ingress ipv4 if source-ipv4-address 192.168.10.1
EU-RBUS: Configured
trigger rbus rbi pb1 ip if cap2 1
```

- Attivare i trigger con il comando **start** e verificare che lo stato dei trigger con **lo stato** del comando confermi che i trigger sono armati.

```
module-4(eureka-elam)# start
module-4(eureka-elam)# status

Slot: 4, Instance: 1 EU-DBUS: Armed <<<<<<<<<<
trigger dbus dbi ingress ipv4 if source-ipv4-address 192.168.10.1
EU-RBUS: Armed <<<<<<<<<<
trigger rbus rbi pb1 ip if cap2 1
```

- Una volta che lo stato indica che i trigger sono armati, sono pronti per l'acquisizione. A questo punto, è necessario inviare il traffico attraverso e controllare nuovamente lo stato per verificare se i trigger sono stati effettivamente attivati.

```
module-4(eureka-elam)# status

Slot: 4, Instance: 1
EU-DBUS: Triggered    <<<<<<<<<<trigger dbus dbi ingress ipv4 if source-ipv4-address
192.168.10.1 EU-RBUS: Triggered <<<<<<<<<<
trigger rbus rbi pb1 ip if cap2 1
```

- Una volta attivato, controllare il numero di sequenza del pacchetto per rbus e dbus per verificare che entrambi abbiano acquisito lo stesso pacchetto. A tal fine, è possibile usare il comando **show dbus | seq. mostra rbus | i seq**. Se il numero di sequenza corrisponde, è possibile visualizzare il contenuto di dbus e rbus. In caso contrario, rieseguire l'acquisizione fino a quando non è possibile acquisire lo stesso pacchetto.

  Nota: Per una maggiore precisione, eseguire sempre ELAM più volte per confermare i problemi di inoltro.

- Èpossibile visualizzare il contenuto di rbus e dbus con i comandi **show dbus** e **show rbus**. L'elemento importante nell'acquisizione è il numero di sequenza e l'indice di origine/destinazione. Dbus mostra l'indice dell'origine che indica la porta su cui ha ricevuto il pacchetto. Rbus mostra l'indice di destinazione della porta a cui il pacchetto viene inoltrato. Inoltre, è possibile esaminare gli indirizzi IP/MAC di origine e di destinazione e le informazioni sulla VLAN.
- Con l'indice di origine e di destinazione (noto anche come indice LTL), è possibile controllare la porta del pannello anteriore associata con il comando **show system internal pixm info ltl #**.

ELAM per Nexus 7000 - M1/M2 (Piattaforma Lamira)

La procedura è la stessa anche per la piattaforma Lamira, tuttavia vi sono alcune differenze:

- Si esegue ELAM con la parola chiave Lamira **elam asic lamira instance x**.
- I comandi per attivare l'ELAM sono:

```
module-4(lamira-elam)#trigger dbus ipv4 if source-ipv4-address 192.0.2.2 destination-ipv4-
address 192.0.2.4
module-4(lamira-elam)# trigger rbus
```

- Per controllare lo stato, usare il comando **status** e verificare che sia Armata prima di inviare il traffico e che sia attivata dopo la cattura.
- Potete quindi interpretare le uscite di dbus e mostrare bus in modo simile a quello mostrato per Eureka.

ELAM per Nexus 7000 - F2/F2E (piattaforma Clipper)

Anche in questo caso, la procedura è simile, solo i trigger sono diversi. Le poche differenze sono le seguenti:

- Eseguite ELAM con la parola chiave Clipper **elam asic clipper instance x** e specificate la modalità Layer 2 o Layer 3.

```
module-4# elam asic  clipper instance 1
module-4(clipper-elam)#
```

- I comandi per attivare la funzione ELAM sono i seguenti:

```
module-4(clipper-l2-elam)# trigger dbus ipv4 ingress if source-ipv4-address 192.0.2.3
destination-ipv4-address 192.0.2.2
module-4(clipper-l2-elam)# trigger rbus ingress if trig
```

- Per controllare lo stato, usare il comando **status** e verificare che sia Armata prima di inviare il traffico e che sia attivata dopo la cattura.
- Potete quindi interpretare le uscite di dbus e mostrare bus in modo simile a quello mostrato per Eureka.

ELAM per Nexus 7000 - F3 (piattaforma Flanker)

Anche in questo caso, la procedura è simile, solo i trigger sono diversi. Le poche differenze sono le seguenti:

- Eseguite ELAM con la parola chiave Flanker **elam asic flanker instance x** e specificate la modalità Layer 2 o Layer 3.

```
module-4# elam asic flanker instance 1
module-4(flanker-elam)#
```

- I comandi per attivare la funzione ELAM sono i seguenti:

```
module-9(fln-l2-elam)# trigger dbus ipv4 if destination-ipv4-address 10.1.1.2
module-9(fln-l2-elam)# trigger rbus ingress if trig
```

- Per controllare lo stato, usare il comando **status** e verificare che sia Armata prima di inviare il traffico e che sia attivata dopo la cattura.
- Potete quindi interpretare le uscite di dbus e rbus in modo simile a quello mostrato per Eureka.

ELAM per Nexus 9000 (piattaforma Tahoe)

In Nexus 9000, la procedura è leggermente diversa da Nexus 7000. Per Nexus 9000, fare riferimento al collegamento Nexus 9000 Cloud Scale ASIC (Tahoe) NX-OS ELAM - Cisco

- Verificare innanzitutto la mappatura dell'interfaccia con il comando **show hardware internal tah interface #**. Le informazioni più importanti in questo output sono **ASIC #, Slice # e source ID (srcid) #.**
- Inoltre, è possibile controllare queste informazioni con il comando **show system internal ethpm info interface # | i i src**. Oltre ai valori elencati in precedenza, l'elemento importante sono i valori dpid e dmod.
- Controllare il numero del modulo con il comando **show module**.
- Collegare al modulo con **attach module x**, dove x è il numero del modulo.
- Eseguire ELAM sul modulo con il comando **module-1# debug platform internal tah elam asic #**
- Configurare il trigger interno o esterno in base al tipo di traffico che si desidera acquisire (L2, L3, traffico incapsulato, ad esempio GRE o VXLAN, e così via):

```
Nexus9000(config)# attach module 1
module-1# debug platform internal tah elam asic 0
module-1(TAH-elam)# trigger init asic # slice # lu-a2d 1 in-select 6 out-select 0 use-src-id #
module-1(TAH-elam-insel6)# reset
module-1(TAH-elam-insel6)# set outer ipv4 dst_ip 192.0.2.1 src_ip 192.0.2.2
```

- Una volta impostati i trigger, avviare ELAM con il comando **start**, inviare il traffico e visualizzare l'output con il comando **report**. L'output del report mostra le interfacce in uscita e in entrata con l'ID vlan, l'indirizzo IP/MAC di origine e destinazione.

```
SUGARBOWL ELAM REPORT SUMMARY
slot - 1, asic - 1, slice - 1
============================


Incoming Interface: Eth1/49
Src Idx : 0xd, Src BD : 10
Outgoing Interface Info: dmod 1, dpid 14
Dst Idx : 0x602, Dst BD : 10

Packet Type: IPv4
Dst MAC address: CC:46:D6:6E:28:DB
Src MAC address: 00:FE:C8:0E:27:15
.1q Tag0 VLAN: 10,  cos = 0x0
Dst IPv4 address: 192.0.2.1
Src IPv4 address: 192.0.2.2

Ver     =  4, DSCP    =    0, Don't Fragment = 0 Proto   =  1, TTL     =   64, More Fragments =
0 Hdr len = 20, Pkt len =   84, Checksum       = 0x667f
```

ELAM per Nexus 9000 (piattaforma NorthStar)

La procedura per la piattaforma NorthStar è la stessa di quella di Tahoe, l'unica differenza è che viene usata la parola chiave **ns** invece di **thh** quando si entra in modalità ELAM:

```
module-1#debug platform internal ns elam asic 0
```

- ## Packet Tracer N9K

Lo strumento Nexus 9000 packet tracer può essere utilizzato per tenere traccia del percorso del pacchetto e, grazie ai contatori integrati per le statistiche di flusso, lo rende uno strumento prezioso per scenari di perdita di traffico intermittente/completa. Sarebbe molto utile quando le risorse TCAM sono limitate o non sono disponibili per eseguire altri strumenti. Inoltre, questo

strumento non è in grado di catturare il traffico ARP e non visualizza i dettagli del contenuto dei pacchetti, ad esempio Wireshark.

Per configurare Packet Tracer, utilizzare i seguenti comandi:

```
N9K-9508#test packet-tracer src_ip



              <==== provide your src and dst ip
N9K-9508# test packet-tracer start                                  <==== Start packet tracer
N9K-9508# test packet-tracer stop                                   <==== Stop packet tracer
N9K-9508# test packet-tracer show                                   <==== Check for packet
matches
```

Per maggiori informazioni, fare riferimento al link Nexus 9000: Spiegazione dello strumento Packet Tracer - Cisco

- ## Traceroute e ping

Questi comandi sono i due più utili che consentono di identificare rapidamente i problemi di connettività.

Il ping utilizza il protocollo Internet Control Message Protocol (ICMP) per inviare messaggi echo ICMP alla destinazione specifica e attende le risposte echo ICMP dalla destinazione. Se il percorso tra l'host funziona correttamente senza problemi, è possibile visualizzare le risposte e i ping completati. Per impostazione predefinita, il comando ping invia messaggi echo ICMP 5 volte (dimensioni uguali in entrambe le direzioni) e se tutto funziona correttamente, è possibile visualizzare 5 risposte echo ICMP. A volte, la richiesta echo iniziale ha esito negativo quando gli switch apprendono l'indirizzo MAC durante la richiesta ARP (Address Resolution Protocol). Se il ping viene eseguito nuovamente subito dopo, non vi è alcuna perdita iniziale. Inoltre, è possibile impostare il numero di ping, le dimensioni del pacchetto, l'origine, l'interfaccia della sorgente e gli intervalli di timeout con queste parole chiave:

```
F241.04.25-N9K-C93180-1# ping 10.82.139.39 vrf management
PING 10.82.139.39 (10.82.139.39): 56 data bytes
36 bytes from 10.82.139.38: Destination Host Unreachable
Request 0 timed out
64 bytes from 10.82.139.39: icmp_seq=1 ttl=254 time=23.714 ms
64 bytes from 10.82.139.39: icmp_seq=2 ttl=254 time=0.622 ms
64 bytes from 10.82.139.39: icmp_seq=3 ttl=254 time=0.55 ms
64 bytes from 10.82.139.39: icmp_seq=4 ttl=254 time=0.598 ms
```

```
F241.04.25-N9K-C93180-1# ping 10.82.139.39 ?
  <CR>
  count             Number of pings to send
  df-bit            Enable do not fragment bit in IP header
  interval          Wait interval seconds between sending each packet
  packet-size       Packet size to send
  source            Source IP address to use
  source-interface  Select source interface
  timeout           Specify timeout interval
  vrf               Display per-VRF information
```

Il comando traceroute viene usato per identificare gli hop usati da un pacchetto prima di raggiungere la destinazione. Si tratta di uno strumento molto importante perché aiuta a identificare il limite L3 in cui si verifica il guasto. È possibile usare anche l'interfaccia port, source e source con

queste parole chiave:

```
F241.04.25-N9K-C93180-1# traceroute 10.82.139.39 ?
  <CR>
  port              Set destination port
  source            Set source address in IP header
  source-interface  Select source interface
  vrf               Display per-VRF information
```

```
Nexus_1(config)# traceroute 192.0.2.1
traceroute to 192.0.2.1 (192.0.2.1), 30 hops max, 40 byte packets
 1 198.51.100.3 (198.51.100.3)  1.017 ms  0.655 ms  0.648 ms
 2 203.0.113.2 (203.0.113.2)  0.826 ms  0.898 ms  0.82 ms
 3 192.0.2.1 (192.0.2.1)  0.962 ms  0.765 ms  0.776 ms
```

- **PACL/RACL/VACL**

ACL è l'acronimo di Access Control List (ACL). Si tratta di uno strumento importante che consente di filtrare il traffico in base a un criterio definito. Dopo aver inserito le voci nell'ACL per i criteri di corrispondenza, è possibile applicarlo per acquisire il traffico in entrata o in uscita. Un aspetto importante dell'ACL è la sua capacità di fornire contatori per le statistiche di flusso. I termini PACL/RACL/VACL si riferiscono a diverse implementazioni di questi ACL e consentono di usare gli ACL come un potente strumento di risoluzione dei problemi, in particolare per la perdita intermittente del traffico. Questi termini sono descritti brevemente qui:

- PACL è l'acronimo di Port Access Control List (elenco di controllo di accesso alla porta): Quando si applica un elenco degli accessi a una porta/interfaccia L2, tale elenco degli accessi viene definito PACL.
- RACL è l'acronimo di Router Access Control List (elenco di controllo di accesso router): Quando si applica un elenco degli accessi a una porta/interfaccia con routing L3, tale elenco degli accessi è noto come RACL.
- VACL è l'acronimo di VLAN Access Control List (elenco di controllo di accesso VLAN): È possibile configurare i VACL in modo che vengano applicati a tutti i pacchetti indirizzati in una VLAN o in uscita da una VLAN o che sono collegati tramite bridge all'interno di una VLAN. I VACL sono destinati esclusivamente ai filtri dei pacchetti di sicurezza e al reindirizzamento del traffico a interfacce fisiche specifiche. I VACL non sono definiti dalla direzione (in entrata o in uscita).

In questa tabella viene mostrato un confronto tra le versioni degli ACL.

TIPO DI ACL	PACL	RACL	VACL
FUNZIONE	Filtra il traffico ricevuto su un'interfaccia L2.	Filtra il traffico ricevuto su un'interfaccia L3	Filtrare il traffico vLAN
APPLICATO IL	- interfacce/porte L2. - Interfacce canale porta L2. - Se applicato a una porta trunk, l'ACL filtra il traffico su tutte le VLAN consentite su tale porta trunk.	- Interfacce VLAN. - Interfacce fisiche L3. - sottointerfacce L3. - Interfacce canale porta L3. - Interfacce di gestione.	Dopo aver abilitato l'ACL, questo viene applicato a t le porte della VLAN (inclu porte trunk).
DIREZIONE APPLICATA	Solo in entrata.	In entrata o In uscita	-

Di seguito è riportato un esempio di come è possibile configurare un elenco degli accessi. Per ulteriori informazioni, fare riferimento alla guida alla configurazione della protezione di Cisco

[Nexus serie 9000 NX-OS, versione 9.3(x) - Configurazione degli ACL IP [Switch Cisco Nexus serie 9000] - Cisco]

```
Nexus93180(config)# ip access-list




Nexus93180(config-acl)# ?
  <1-4294967295>  Sequence number
  deny            Specify packets to reject
  fragments       Optimize fragments rule installation
  no              Negate a command or set its defaults
  permit          Specify packets to forward
  remark          Access list entry comment
  show            Show running system information
  statistics      Enable per-entry statistics for the ACL
  end             Go to exec mode
  exit            Exit from command interpreter
  pop             Pop mode from stack or restore from name
  push            Push current mode to stack or save it under name
  where           Shows the cli context you are in

Nexus93180(config)# int e1/1

Nexus93180(config-if)# ip port access-group



         >>>>>> When you configure ACL like this, it is PACL.
in  Inbound packets
Nexus93180(config-if)# ip access-group



              >>>>>> When you configure ACL like this, it is RACL.
  in   Inbound packets
  out  Outbound packets
```

- LOGFLASH

LogFlash è un tipo di storage persistente disponibile sulle piattaforme Nexus come un compact flash esterno, un dispositivo USB o un disco incorporato nel supervisor. Se viene rimosso dallo switch, il sistema notifica periodicamente all'utente che LogFlash è mancante. Logflash è installato sul supervisor e contiene dati cronologici come registri di accounting, messaggi syslog, debug e output di Embedded Event Manager (EEM). L'EEM verrà discusso più avanti in questo articolo. È possibile controllare il contenuto di LogFlash con questo comando:

```
Nexus93180(config)# dir logflash:
          0    Nov 14 04:13:21 2019  .gmr6_plus
      20480    Feb 18 13:35:07 2020  ISSU_debug_logs/
         24    Feb 20 20:43:24 2019  arp.pcap
         24    Feb 20 20:36:52 2019  capture_SYB010L2289.pcap
       4096    Feb 18 17:24:53 2020  command/
       4096    Sep 11 01:39:04 2018  controller/
       4096    Aug 15 03:28:05 2019  core/
       4096    Feb 02 05:21:47 2018  debug/
    1323008    Feb 18 19:20:46 2020  debug_logs/
       4096    Feb 17 06:35:36 2020  evt_log_snapshot/
```

```
       4096    Feb 02 05:21:47 2018  generic/
       1024    Oct 30 17:27:49 2019  icamsql_1_1.db
      32768    Jan 17 11:53:23 2020  icamsql_1_1.db-shm
     129984    Jan 17 11:53:23 2020  icamsql_1_1.db-wal
       4096    Feb 14 13:44:00 2020  log/
      16384    Feb 02 05:21:44 2018  lost+found/
       4096    Aug 09 20:38:22 2019  old_upgrade/
       4096    Feb 18 13:40:36 2020  vdc_1/

Usage for logflash://sup-local
 1103396864 bytes used
 7217504256 bytes free
 8320901120 bytes total
```

Nel caso in cui un utente ricarichi il dispositivo o lo ricarichi da solo a causa di un evento, tutte le informazioni del registro andranno perse. In tali scenari, LogFlash può fornire dati cronologici che possono essere esaminati per identificare una probabile causa del problema. Naturalmente, è necessaria un'ulteriore dovuta diligenza per identificare la causa principale che fornisce suggerimenti su cosa cercare nel caso in cui questo evento si verifichi nuovamente.

Per informazioni su come installare logflash sul dispositivo, fare riferimento al collegamento Nexus 7000 Logging Capabilities - Cisco.

- **OBFL**

OBFL è l'acronimo di OnBoard Failure Logging. È un tipo di storage persistente disponibile sia per Nexus Top of Rack che per gli switch modulari. Analogamente a LogFlash, le informazioni vengono conservate una volta ricaricato il dispositivo. OBFL memorizza informazioni quali guasti e dati ambientali. Le informazioni variano a seconda della piattaforma e del modulo. Di seguito è riportato un esempio di output del modulo 1 della piattaforma Nexus 93108 (uno chassis fisso con un solo modulo):

```
Nexus93180(config)# show logging onboard module 1 ?
*** No matching command found in current mode, matching in (exec) mode ***
  <CR>
  >                     Redirect it to a file
  >>                    Redirect it to a file in append mode
  boot-uptime           Boot-uptime
  card-boot-history     Show card boot history
  card-first-power-on   Show card first power on information
  counter-stats         Show OBFL counter statistics
  device-version        Device-version
  endtime               Show OBFL logs till end time mm/dd/yy-HH:MM:SS
  environmental-history Environmental-history
  error-stats           Show OBFL error statistics
  exception-log         Exception-log
  internal              Show Logging Onboard Internal
  interrupt-stats       Interrupt-stats
  obfl-history          Obfl-history
  stack-trace           Stack-trace
  starttime             Show OBFL logs from start time mm/dd/yy-HH:MM:SS
  status                Status
  |                     Pipe command output to filter


Nexus93180(config)# show logging onboard module 1 status
---------------------------
OBFL Status
---------------------------
    Switch OBFL Log:                                Enabled
```

```
    Module:  1 OBFL Log:                                    Enabled
    card-boot-history                                       Enabled
    card-first-power-on                                     Enabled
    cpu-hog                                                 Enabled
    environmental-history                                   Enabled
    error-stats                                             Enabled
    exception-log                                           Enabled
    interrupt-stats                                         Enabled
    mem-leak                                                Enabled
    miscellaneous-error                                     Enabled
    obfl-log (boot-uptime/device-version/obfl-history)  Enabled
    register-log                                            Enabled
    system-health                                           Enabled
    temp Error                                              Enabled
    stack-trace                                             Enabled
```

Anche in questo caso, queste informazioni sono utili nel caso di un dispositivo che viene ricaricato intenzionalmente dall'utente o a causa di un evento che ha attivato un ricaricamento. In questo caso, le informazioni OBFL possono aiutare a identificare il problema dal punto di vista di una scheda di linea. Il comando **show logging onboard** è un buon punto di partenza. È necessario acquisire i dati dall'interno del contesto del modulo per ottenere tutto il necessario. Assicurarsi di utilizzare il comando **show logging onboard module x** o **attach mod x ; mostra accesso a bordo.**

- ## Cronologie degli eventi

Le cronologie degli eventi sono uno dei potenti strumenti in grado di fornire informazioni sui vari eventi che si verificano per un processo eseguito su Nexus. In altre parole, ogni processo che viene eseguito su una piattaforma Nexus ha cronologie di eventi che vengono eseguite in background e memorizzano informazioni sui vari eventi di quel processo (pensate come debug che vengono eseguiti costantemente). Queste cronologie di eventi non sono persistenti e tutte le informazioni memorizzate vengono perse al momento del ricaricamento del dispositivo. Si tratta di funzionalità molto utili quando si identifica un problema con un determinato processo e si desidera risolverlo. Ad esempio, se il protocollo di routing OSPF non funziona correttamente, è possibile utilizzare le cronologie degli eventi associate a OSPF per identificare il punto in cui si è verificato un errore del processo OSPF. È possibile trovare le cronologie degli eventi associate a quasi tutti i processi sulla piattaforma Nexus, ad esempio CDP/STP, UDLD, LACP/OSPF, EIGRP/BGP e così via.

In questo modo viene in genere verificata la cronologia degli eventi per un processo con esempi di riferimento. Ogni processo ha più opzioni quindi utilizzare **?** per controllare le varie opzioni disponibili in un processo.

```
Nexus93180(config)# show
```

```
Nexus93180# show ip ospf event-history ?
  adjacency       Adjacency formation logs
  cli             Cli logs
  event           Internal event logs
  flooding        LSA flooding logs
  ha              HA and GR logs
  hello           Hello related logs
  ldp             LDP related logs
  lsa             LSA generation and databse logs
  msgs            IPC logs
  objstore        DME OBJSTORE related logs
```

```
  redistribution  Redistribution logs
  rib             RIB related logs
  segrt           Segment Routing logs
  spf             SPF calculation logs
  spf-trigger     SPF TRIGGER related logs
  statistics      Show the state and size of the buffers
  te              MPLS TE related logs

Nexus93180# show spanning-tree internal event-history ?
  all      Show all event historys
  deleted  Show event history of deleted trees and ports
  errors   Show error logs of STP
  msgs     Show various message logs of STP
  tree     Show spanning tree instance info
  vpc      Show virtual Port-channel event logs
```

- Debug

I debug sono strumenti potenti di NX-OS che consentono di eseguire in tempo reale gli eventi di risoluzione dei problemi e di registrarli in un file o visualizzarli nella CLI. Si consiglia di registrare gli output di debug su un file in quanto influiscono sulle prestazioni della CPU. procedere con cautela prima di eseguire il debug direttamente dalla CLI.

I debug vengono in genere eseguiti solo quando il problema è stato identificato come un singolo processo e si desidera verificare il comportamento del processo in tempo reale con il traffico reale sulla rete. È necessario abilitare una funzionalità di debug basata sui privilegi dell'account utente definiti.

Analogamente alle cronologie degli eventi, è possibile eseguire il debug per ogni processo su un dispositivo Nexus come CDP/STP, UDLD, LACP/OSPF, EIGRP/BGP e così via.

In questo modo viene in genere eseguito un debug per un processo. Ogni processo ha più opzioni quindi utilizzare **?** per controllare le varie opzioni disponibili in un processo.

```
Nexus93180# debug
```

```
Nexus93180# debug spanning-tree ?
  all      Configure all debug flags of stp
  bpdu_rx  Configure debugging of stp bpdu rx
  bpdu_tx  Configure debugging of stp bpdu tx
  error    Configure debugging of stp error
  event    Configure debugging of Events
  ha       Configure debugging of stp HA
  mcs      Configure debugging of stp MCS
  mstp     Configure debugging of MSTP
  pss      Configure debugging of PSS
  rstp     Configure debugging of RSTP
  sps      Configure debugging of Set Port state batching
  timer    Configure debugging of stp Timer events
  trace    Configure debugging of stp trace
  warning  Configure debugging of stp warning

Nexus93180# debug ip ospf ?
  adjacency               Adjacency events
  all                     All OSPF debugging
```

```
  database                OSPF LSDB changes
  database-timers         OSPF LSDB timers
  events                  OSPF related events
  flooding                LSA flooding
  graceful-restart        OSPF graceful restart related debugs
  ha                      OSPF HA related events
  hello                   Hello packets and DR elections
  lsa-generation          Local OSPF LSA generation
  lsa-throttling          Local OSPF LSA throttling
  mpls                    OSPF MPLS
  objectstore             Objectstore Events
  packets                 OSPF packets
  policy                  OSPF RPM policy debug information
  redist                  OSPF redistribution
  retransmission          OSPF retransmission events
  rib                     Sending routes to the URIB
  segrt                   Segment Routing Events
  snmp                    SNMP traps and request-response related events
  spf                     SPF calculations
  spf-trigger             Show SPF triggers
```

- ORO

GOLD è l'acronimo di Generic OnLine Diagnostics. Come suggerisce il nome, questi test sono generalmente utilizzati come controllo dello stato del sistema e sono utilizzati per controllare o verificare l'hardware in questione. Esistono vari test online eseguiti e basati sulla piattaforma in uso, alcuni dei quali sono dirompenti, mentre altri non comportano interruzioni. I test online possono essere classificati come segue:

- **Diagnostica Di Avvio:** Questi test sono i test eseguiti all'avvio del dispositivo. Verificano inoltre la connettività tra il supervisore e i moduli, inclusa la connettività tra i dati e il control plane per tutti gli ASIC. Test come ManagementPortLoopback e EOBCLoopback sono distruttivi, mentre i test per OBFL e USB non sono distruttivi.
- **Diagnostica monitoraggio stato o runtime:** Questi test forniscono informazioni sullo stato del dispositivo. Questi test non comportano interruzioni e vengono eseguiti in background per garantire la stabilità dell'hardware. È possibile attivare/disattivare questi test in base alle esigenze o per la risoluzione dei problemi.
- **Diagnostica su richiesta:** Tutti i test citati possono essere rieseguiti su richiesta per localizzare un problema.

Èpossibile verificare i vari tipi di test online disponibili per lo switch con questo comando:

```
Nexus93180(config)# show diagnostic content module all
Diagnostics test suite attributes:
B/C/* - Bypass bootup level test / Complete bootup level test / NA
P/*   - Per port test / NA
M/S/* - Only applicable to active / standby unit / NA
D/N/* - Disruptive test / Non-disruptive test / NA
H/O/* - Always enabled monitoring test / Conditionally enabled test / NA
F/*   - Fixed monitoring interval test / NA
X/*   - Not a health monitoring test / NA
E/*   - Sup to line card test / NA
L/*   - Exclusively run this test / NA
T/*   - Not an ondemand test / NA
A/I/* - Monitoring is active / Monitoring is inactive / NA

Module 1: 48x10/25G + 6x40/100G Ethernet Module (Active)

                                                        Testing Interval
ID     Name                                 Attributes      (hh:mm:ss)
```

```
____   ___________________________________ ___________   _________________
 1)    USB--------------------------->     C**N**X**T*     -NA-
 2)    NVRAM------------------------->     ***N******A     00:05:00
 3)    RealTimeClock----------------->     ***N******A     00:05:00
 4)    PrimaryBootROM---------------->     ***N******A     00:30:00
 5)    SecondaryBootROM-------------->     ***N******A     00:30:00
 6)    BootFlash--------------------->     ***N******A     00:30:00
 7)    SystemMgmtBus----------------->     **MN******A     00:00:30
 8)    OBFL-------------------------->     C**N**X**T*     -NA-
 9)    ACT2-------------------------->     ***N******A     00:30:00
10)    Console----------------------->     ***N******A     00:00:30
11)    FpgaRegTest------------------->     ***N******A     00:00:30
12)    Mce--------------------------->     ***N******A     01:00:00
13)    AsicMemory-------------------->     C**D**X**T*     -NA-
14)    Pcie-------------------------->     C**N**X**T*     -NA-
15)    PortLoopback------------------>     *P*N**XE***     -NA-
16)    L2ACLRedirect----------------->     *P*N***E**A     00:01:00
17)    BootupPortLoopback------------>     CP*N**XE*T*     -NA-
```

Per visualizzare lo scopo di ognuno dei 17 test citati, è possibile utilizzare questo comando:

```
Nexus93180(config)#show diagnostic description module 1 test all
USB :
        A bootup test that checks the USB controller initialization
        on the module.

NVRAM :
        A health monitoring test, enabled by default that checks the
        sanity of the NVRAM device on the module.

RealTimeClock :
        A health monitoring test, enabled by default that verifies
        the real time clock on the module.

PrimaryBootROM :
        A health monitoring  test that verifies the primary BootROM
        on the module.

SecondaryBootROM :
        A health monitoring  test that verifies the secondary BootROM
        on the module.

BootFlash :
        A Health monitoring test, enabled by default, that verifies
        access to the internal compactflash devices.

SystemMgmtBus :
        A Health monitoring test, enabled by default, that verifies
        the standby System Bus.

OBFL :
        A bootup test that checks the onboard flash used for failure
        logging (OBFL) device initialization on the module.

ACT2 :
        A Health monitoring test, enabled by default, that verifies
        access to the ACT2 device.

Console :
        A health monitoring test,enabled by default that checks health
        of console device.
```

```
FpgaRegTest :
        A health monitoring test,enabled by default that checks read/write
        access to FPGA scratch registers on the module.

Mce :
        A Health monitoring test, enabled by default, that check for
        machine errors on sup.

AsicMemory :
        A bootup test that checks the asic memory.

Pcie :
        A bootup test that tests pcie bus of the module

PortLoopback :
        A health monitoring test that tests the packet path from
        the Supervisor card to the physical port in ADMIN DOWN state
        on Linecards.

L2ACLRedirect :
        A health monitoring test, enabled by default, that does a
        non disruptive loopback for TAHOE asics to check the ACL Sup
        redirect with the CPU port.

BootupPortLoopback :
        A Bootup test that tests the packet path from the Supervisor
        card to all of the physical ports at boot time.
```

- ## EEM

EEM è l'acronimo di Embedded Event Manager. Si tratta di uno strumento potente che consente di programmare il dispositivo per eseguire attività specifiche nel caso in cui si verifichi un determinato evento. Esegue il monitoraggio di vari eventi sul dispositivo e quindi intraprende le azioni necessarie per risolvere il problema ed eventualmente eseguire il ripristino. L'EEM è costituito da tre componenti principali, ciascuno dei quali è brevemente descritto di seguito:

- **Istruzione evento:** Si tratta degli eventi che si desidera monitorare e di cui si desidera che Nexus esegua una determinata azione, ad esempio una soluzione o semplicemente la notifica a un server SNMP o la visualizzazione di un log CLI e così via.
- **Azioni:** Queste sarebbero le azioni che EEM intraprenderebbe una volta attivato un evento. Queste azioni potrebbero consistere semplicemente nel disabilitare un'interfaccia o nell'eseguire alcuni comandi show e copiare gli output in un file sul server FTP, inviare un messaggio di posta elettronica e così via.
- **Criteri:** Si tratta fondamentalmente di un evento in combinazione con una o più istruzioni di azione che è possibile configurare sul supervisor tramite CLI o uno script bash. È inoltre possibile richiamare EEM con uno script Python. Una volta che la policy è stata definita sul supervisore, la applica al relativo modulo.

Per ulteriori informazioni su EEM, fare riferimento al collegamento Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, release 9.2(x) - Configuring the Embedded Event Manager [Cisco Nexus serie 9000 Switch] - Cisco.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).