Esempio di switch Catalyst serie 3850 con configurazione Wireshark incorporata

Sommario

Introduzione

In questo documento viene descritto come usare la funzione Wireshark integrata negli switch Cisco Catalyst serie 3850 con versione 3.3.0 o successive per acquisire i pacchetti in entrata o in uscita dallo switch.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di Wireshark.

Componenti usati

Per la stesura del documento, è stato usato uno switch Cisco Catalyst serie 3850 con versione 3.3.0 o successive.

Restrizioni

- Licenza: Richiede IPBASE o IPSERVICES.
- I filtri di acquisizione non sono supportati.
- EtherChannel di livello 2 e 3 non supportati.
- L'elenco di controllo di accesso (ACL) MAC è usato solo per i pacchetti non IP, ad esempio ARP. Non è supportato su una porta di layer 3 o su un'interfaccia virtuale dello switch (SVI).
- Durante l'acquisizione di un pacchetto Wireshark, l'inoltro hardware viene eseguito contemporaneamente.
- I pacchetti generati dalla CPU dello switch possono essere acquisiti e devono utilizzare il control-plane come interfaccia di origine.
- Non è possibile acquisire informazioni di riscrittura. Le acquisizioni in uscita non mostrano il pacchetto e le modifiche al pacchetto eseguite dallo switch Cisco Catalyst serie 3850.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Utilizzare questa tabella per la configurazione.

Definizione	Configurazione
Definire l'origine	monitor capture [nome] interface [nome interfaccia] [direzione]
Impostare le istruzioni di abbinamento	monitor capture [name] match ipv4 [source ip/xx] [dest ip/xx] monitor capture [name] match ipv4 any any
Impostare la destinazione	monitor capture [nome] percorso file [percorso]

Esempio di configurazione

Di seguito è riportato un esempio di configurazione. Gigabit Ethernet4/0/1 viene inserito con la richiesta Address Resolution Protocol (ARP) per 10.10.10.1, che si trova sullo switch Cisco Catalyst serie 3850. L'host è configurato come 10.10.10.10. Questa configurazione acquisisce sia l'entrata che l'uscita su Gigabit Ethernet4/0/1, corrisponde su qualsiasi pacchetto IPv4 e lo memorizza nella memoria flash come mycap.pcap. Quando le dimensioni del file hanno raggiunto 10 MB o 100 pacchetti, a seconda di quale condizione si verifica per prima, l'acquisizione viene interrotta automaticamente. Il file può anche essere archiviato in un'unità flash USB, se si seleziona **usbflash0:** e collegare una porta USB sul pannello anteriore dello switch Cisco Catalyst serie 3850.

```
monitor capture mycap interface GigabitEthernet4/0/1 both
monitor capture mycap match ipv4 any any
monitor capture mycap file location flash:mycap.pcap buffer-size 10
monitor capture mycap limit packets 100
```

Una volta configurata questa opzione, è necessario avviare l'acquisizione. Se sul flash esiste già un file con questo nome, viene richiesto se si desidera sovrascriverlo.

```
Switch#monitor capture mycap start
A file by the same capture file name already exists, overwrite?[confirm]
```

Confermare che lo stato è Attivo

```
Switch#show monitor capture mycap

Status Information for Capture mycap
Target Type:
Interface: GigabitEthernet4/0/1, Direction: both
Status : Active
Filter Details:
IPv4
Source IP: any
Destination IP: any
Protocol: any
Buffer Details:
Buffer Type: LINEAR (default)
File Details:
Associated file name: flash:mycap.pcap
Size of buffer(in MB): 10
Limit Details:
Number of Packets to capture: 100
Packet Capture duration: 0 (no limit)
Packet Size to capture: 0 (no limit)
Packets per second: 0 (no limit)
Packet sampling rate: 0 (no sampling)
```

Visualizza l'acquisizione

Èpossibile visualizzare l'acquisizione in diversi modi.

- Èpossibile visualizzare l'acquisizione direttamente sullo switch (brief):

```
Switch#show monitor capture file flash:mycap.pcap
1 0.000000 10.10.10.10 -> 10.10.10.1 IP Unknown (0xff)
2 0.000992 10.10.10.10 -> 10.10.10.1 IP Unknown (0xff)
3 0.000992 10.10.10.10 -> 10.10.10.1 IP Unknown (0xff)
4 0.000992 10.10.10.10 -> 10.10.10.1 IP Unknown (0xff)
5 0.000992 10.10.10.10 -> 10.10.10.1 IP Unknown (0xff)
```

- Èpossibile visualizzare l'acquisizione direttamente sullo switch (dettagli):

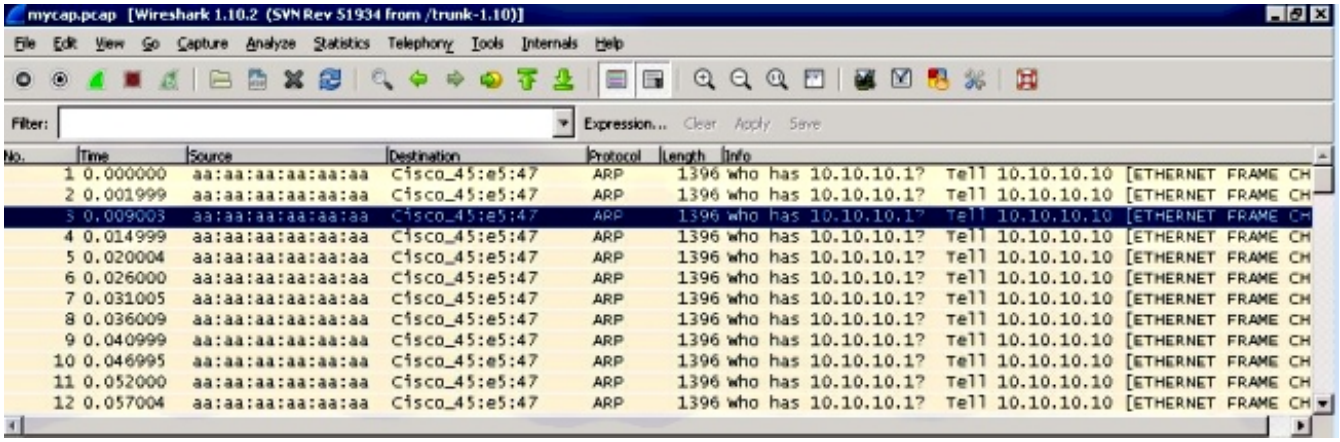
```
F340.09.11-3800-1#show monitor capture file flash:mycap.pcap detailed
Frame 1: 1396 bytes on wire (11168 bits), 1396 bytes captured (11168 bits)
Arrival Time: Oct 9, 2013 12:15:29.371974000 UTC
Epoch Time: 1381320929.371974000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 1396 bytes (11168 bits)
Capture Length: 1396 bytes (11168 bits)
```

```
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ip:data]
Ethernet II, Src: aa:aa:aa:aa:aa:aa (aa:aa:aa:aa:aa:aa), Dst: 0c:68:03:45:e5:47
(0c:68:03:45:e5:47)
Destination: 0c:68:03:45:e5:47 (0c:68:03:45:e5:47)
Address: 0c:68:03:45:e5:47 (0c:68:03:45:e5:47)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
.... ..0. .... .... .... .... = LG bit: Globally unique address
(factory default)
Source: aa:aa:aa:aa:aa:aa (aa:aa:aa:aa:aa:aa)
Address: aa:aa:aa:aa:aa:aa (aa:aa:aa:aa:aa:aa)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
.... ..1. .... .... .... .... = LG bit: Locally administered address
(this is NOT the factory default)
Type: IP (0x0800)
Internet Protocol, Src: 10.10.10.10 (10.10.10.10), Dst: 10.10.10.1 (10.10.10.1)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 1382
Identification: 0x0000 (0)
Flags: 0x00
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: Unknown (255)
Header checksum: 0x4c7b [correct]
[Good: True]
[Bad: False]
Source: 10.10.10.10 (10.10.10.10)
Destination: 10.10.10.1 (10.10.10.1)
Data (1362 bytes)

0000 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f ................
0010 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f ................
0020 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f !"#$%&'()*+,-./
0030 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 0123456789:;<=>?
0040 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f @ABCDEFGHIJKLMNO
0050 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f PQRSTUVWXYZ[\]^_
0060 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f `abcdefghijklmno
0070 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f pqrstuvwxyz{|}~.
0080 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f ................
0090 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f ................
00a0 a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af ................
00b0 b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd be bf ................
00c0 c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf ................
00d0 d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df ................
00e0 e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef ................
00f0 f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff ................
0100 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f ................
0110 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f ................
0120 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f !"#$%&'()*+,-./
0130 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 0123456789:;<=>?
0140 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f @ABCDEFGHIJKLMNO
0150 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f PQRSTUVWXYZ[\]^_
0160 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f `abcdefghijklmno
0170 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f pqrstuvwxyz{|}~.
0180 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f ................
```

```
0190 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f ................
01a0 a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af ................
01b0 b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd be bf ................
01c0 c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf ................
01d0 d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df ................
01e0 e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef ................
01f0 f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff ................
0200 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f ................
0210 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f ................
0220 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f !"#$%&'()*+,-./
0230 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 0123456789:;<=>?
0240 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f @ABCDEFGHIJKLMNO
0250 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f PQRSTUVWXYZ[\]^_
0260 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f `abcdefghijklmno
0270 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f pqrstuvwxyz{|}~.
0280 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f ................
0290 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f ................
02a0 a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af ................
02b0 b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd be bf ................
02c0 c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf ................
02d0 d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df ................
02e0 e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef ................
02f0 f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff ................
0300 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f ................
0310 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f ................
0320 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f !"#$%&'()*+,-./
0330 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 0123456789:;<=>?
0340 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f @ABCDEFGHIJKLMNO
0350 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f PQRSTUVWXYZ[\]^_
0360 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f `abcdefghijklmno
0370 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f pqrstuvwxyz{|}~.
0380 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f ................
0390 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f ................
03a0 a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af ................
03b0 b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd be bf ................
03c0 c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf ................
03d0 d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df ................
03e0 e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef ................
03f0 f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff ................
0400 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f ................
0410 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f ................
0420 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f !"#$%&'()*+,-./
0430 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 0123456789:;<=>?
0440 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f @ABCDEFGHIJKLMNO
0450 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f PQRSTUVWXYZ[\]^_
0460 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f `abcdefghijklmno
0470 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f pqrstuvwxyz{|}~.
0480 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f ................
0490 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f ................
04a0 a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af ................
04b0 b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd be bf ................
04c0 c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf ................
04d0 d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df ................
04e0 e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef ................
04f0 f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff ................
0500 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f ................
0510 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f ................
0520 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f !"#$%&'()*+,-./
0530 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 0123456789:;<=>?
0540 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f @ABCDEFGHIJKLMNO
0550 50 51 PQ
Data&colon; 000102030405060708090a0b0c0d0e0f1011121314151617...
[Length: 1362]
```

- Èpossibile eseguire il protocollo TFTP/FTP sul file pcap dallo switch e visualizzare il file di acquisizione in Wireshark:



Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

```
Switch#show monitor capture mycap parameter
monitor capture mycap interface GigabitEthernet4/0/1 in
monitor capture mycap match ipv4 any any
monitor capture mycap buffer size 10
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Acquisisci traffico Control Plane

Di seguito è riportata una configurazione di esempio che mostra sia il traffico in entrata che in uscita diretto allo switch Cisco Catalyst serie 3850. Questo è un ottimo modo per verificare quale traffico colpisce la CPU degli switch Cisco Catalyst serie 3850. Può essere combinata per diagnosticare situazioni di elevato utilizzo della CPU

Configurazione

```
Switch#show monitor capture mycap parameter
monitor capture mycap control-plane both
monitor capture mycap match any
monitor capture mycap file location flash:mycap.pcap buffer-size 10
monitor capture mycap limit packets 100
```

Risultati

```
1   0.143990 aa:aa:aa:aa:aa:aa -> 0c:68:03:45:e5:47 ARP Who has 10.10.10.1?
Tell 10.10.10.10
2 0.148003 aa:aa:aa:aa:aa:aa -> 0c:68:03:45:e5:47 ARP Who has 10.10.10.1?
Tell 10.10.10.10
3 0.153999 aa:aa:aa:aa:aa:aa -> 0c:68:03:45:e5:47 ARP Who has 10.10.10.1?
Tell 10.10.10.10
4 0.159004 aa:aa:aa:aa:aa:aa -> 0c:68:03:45:e5:47 ARP Who has 10.10.10.1?
Tell 10.10.10.10
5 0.163993 aa:aa:aa:aa:aa:aa -> 0c:68:03:45:e5:47 ARP Who has 10.10.10.1?
Tell 10.10.10.10
6 0.168998 aa:aa:aa:aa:aa:aa -> 0c:68:03:45:e5:47 ARP Who has 10.10.10.1?
Tell 10.10.10.10
7 0.174003 aa:aa:aa:aa:aa:aa -> 0c:68:03:45:e5:47 ARP Who has 10.10.10.1?
Tell 10.10.10.10
8 0.178992 0c:68:03:45:e5:47 -> aa:aa:aa:aa:aa:aa ARP 10.10.10.1 is at
0c:68:03:45:e5:47
9 0.184988 0c:68:03:45:e5:47 -> aa:aa:aa:aa:aa:aa ARP 10.10.10.1 is at
0c:68:03:45:e5:47
10 0.189993 0c:68:03:45:e5:47 -> aa:aa:aa:aa:aa:aa ARP 10.10.10.1 is at
0c:68:03:45:e5:47
11 0.194998 0c:68:03:45:e5:47 -> aa:aa:aa:aa:aa:aa ARP 10.10.10.1 is at
0c:68:03:45:e5:47
12 0.200994 0c:68:03:45:e5:47 -> aa:aa:aa:aa:aa:aa ARP 10.10.10.1 is at
0c:68:03:45:e5:47
13 0.205999 0c:68:03:45:e5:47 -> aa:aa:aa:aa:aa:aa ARP 10.10.10.1 is at
0c:68:03:45:e5:47
14 0.210988 0c:68:03:45:e5:47 -> aa:aa:aa:aa:aa:aa ARP 10.10.10.1 is at
0c:68:03:45:e5:47
15 0.215993 0c:68:03:45:e5:47 -> aa:aa:aa:aa:aa:aa ARP 10.10.10.1 is at
0c:68:03:45:e5:47
16 0.221989 0c:68:03:45:e5:47 -> aa:aa:aa:aa:aa:aa ARP 10.10.10.1 is at
0c:68:03:45:e5:47
```