

# Configure Catalyst 3850 Series Switch with Embedded Wireshark

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Restrictions](#)

[Configure](#)

[Configuration Example](#)

[Confirm that the Status is Active](#)

[View the Capture](#)

[Verify](#)

[Troubleshoot](#)

[Capture Control-Plane Traffic](#)

[Configuration](#)

[Results](#)

## Introduction

This document describes the embedded Wireshark feature of the Cisco Catalyst 3850 Series Switch in order to capture packets.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of Wireshark.

### Components Used

The information in this document is based on the Cisco Catalyst 3850 Series Switch that runs Version 3.3.0 or later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

### Restrictions

- License: Requires IPBASE or IPSERVICES.
- Capture filters are not supported.
- Layer 2 and Layer 3 EtherChannels are not supported.
- MAC Access Control List (ACL) is only used for non-IP packets such as ARP. It is not supported on a Layer 3 port or Switch Virtual Interface (SVI).
- During a Wireshark packet capture, hardware forwarding happens concurrently.
- Switch CPU generated packets can be captured and must use the control-plane as the source interface.

- It is not possible to capture rewrite information. Egress captures do not show and changes to the packet performed by the Cisco Catalyst 3850 Series Switch.

## Configure

Use this table for your configuration.

Definition	Configuration
Define your source	monitor capture [name] interface [interface name] [direction]
Set your match statement(s)	monitor capture [name] match ipv4 [source ip/xx] [dest ip/xx] monitor capture [name] match ipv4 any any
Set your destination	monitor capture [name] file location [location]

## Configuration Example

Here is a sample configuration.

GigabitEthernet4/0/1 is injected with the Address Resolution Protocol (ARP) request for 10.10.10.1, which is located on the Cisco Catalyst 3850 Series Switch.

The host is configured as 10.10.10.10. This configuration captures both ingress and egress on GigabitEthernet4/0/1, matches on any IPv4 packets, and stores it to the flash as mycap.pcap.

Once the size of the file has reached 10MB or 100 packets, whichever comes first, the capture automatically stops.

The file can also be stored to a USB flash drive, if you select **usbflash0:** and plug a USB into the front of the Cisco Catalyst 3850 Series Switch.

```
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
```

Once this is configured, you must start the capture. If a file already exists on the flash with this name, it prompts you if wish to overwrite this.

```
<#root>
```

```
Switch#
```

```
monitor capture mycap start
```

```
A file by the same capture file name already exists, overwrite?[confirm]
```

## Confirm that the Status is Active

```
<#root>
```

```
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)
```

## View the Capture

There are multiple ways to view the capture.

- You can view the capture directly on the switch (brief):

```
<#root>
```

```
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)
```

- You can view the capture directly on the switch (detailed):

```
<#root>
```

```
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  .....

```

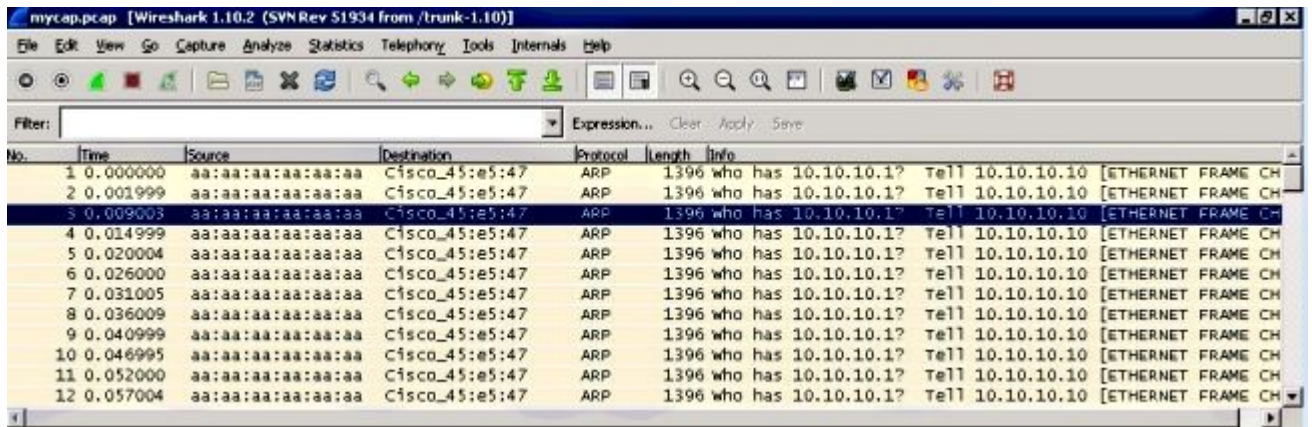
00d0	d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df	.....
00e0	e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef	.....
00f0	f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff	.....
0100	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f	.....
0110	10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f	.....
0120	20 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 @ABCDEFGHJKLMNO
0550 50 51 PQ
Data: 000102030405060708090a0b0c0d0e0f1011121314151617...
[Length: 1362]

```

- You can TFTP/FTP the pcap file off of the switch and view the capture file in Wireshark:



## Verify

Use this section in order to confirm that your configuration works properly.

```
<#root>
```

```
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

```

## Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

## Capture Control-Plane Traffic

Here is a sample configuration that shows both ingress and egress traffic sourced to and from the Cisco Catalyst 3850 Series Switch itself.

This is a great way to see what traffic hits the CPU of the Cisco Catalyst 3850 Series Switch.

This can be combined in order to diagnose high CPU usage situations

## Configuration

```
<#root>
```

```
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
```

## Results

```
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
```