Embedded Wireshark로 Catalyst 3850 Series 스위치 구성

목차

[소개](#)

[사전 요구 사항](#)

- [요구 사항](#)
- [사용되는 구성 요소](#)
- [제한 사항](#)

[구성](#)

- [컨피그레이션 예시](#)
  - [Status(상태)가 Active(활성)인지 확인합니다](#)
  - [캡처 보기](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[컨트롤 플레인 트래픽 캡처](#)

- [설정](#)
- [결과](#)

소개

이 문서에서는 패킷을 캡처하기 위해 Cisco Catalyst 3850 Series Switch에 포함된 Wireshark 기능에 대해 설명합니다.

사전 요구 사항

요구 사항

Wireshark에 대한 지식이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 버전 3.3.0 이상을 실행하는 Cisco Catalyst 3850 Series 스위치를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

제한 사항

- 라이센스: IPBASE 또는 IPSERVICES가 필요합니다.
- 캡처 필터는 지원되지 않습니다.
- 레이어 2 및 레이어 3 EtherChannel은 지원되지 않습니다.
- MAC ACL(Access Control List)은 ARP와 같은 비 IP 패킷에만 사용됩니다. 레이어 3 포트 또는 SVI(Switch Virtual Interface)에서는 지원되지 않습니다.
- Wireshark 패킷 캡처 중에 하드웨어 포워딩이 동시에 발생합니다.
- 스위치 CPU에서 생성된 패킷을 캡처할 수 있으며 소스 인터페이스로 컨트롤 플레인을 사용해야 합니다.
- 재작성 정보를 캡처할 수 없습니다. 이그레스 캡처는 Cisco Catalyst 3850 Series Switch에서 수행한 패킷을 표시하지 않으며 해당 패킷에 대한 변경 사항을 표시합니다.

구성

이 표는 구성에 사용합니다.

정의	설정
출처 정의	monitor capture [name] interface [interface name] [direction]
일치 문 설정	monitor capture [name] match ipv4 [source ip/xx] [dest ip/xx] 모니터링 캡처 [name] match ipv4 any any
대상 설정	모니터링 캡처 [name] 파일 위치 [location]

컨피그레이션 예시

다음은 샘플 컨피그레이션입니다.

GigabitEthernet4/0/1에는 Cisco Catalyst 3850 Series 스위치에 있는 10.10.10.1에 대한 ARP(Address Resolution Protocol) 요청이 주입됩니다.

호스트는 10.10.10.10으로 구성됩니다. 이 컨피그레이션은 GigabitEthernet4/0/1에서 인그레스 및 이그레스 모두를 캡처하고, 모든 IPv4 패킷에서 매칭하며, 이를 플래시에 mycap.pcap로 저장합니다.

파일 크기가 10MB 또는 100 패킷 중 먼저 오는 패킷에 도달하면 캡처가 자동으로 중지됩니다.

usbflash0:을 선택하고 Cisco Catalyst 3850 Series Switch의 전면에 USB를 꽂으면 USB 플래시 드라이브에도 파일을 저장할 수 있습니다.

```
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
```

구성이 완료되면 캡처를 시작해야 합니다. 이 이름의 파일이 플래시에 이미 있는 경우 이 파일을 덮어쓸지 묻는 메시지가 표시됩니다.

```
<#root>

Switch#

monitor capture mycap start


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

Status(상태)가 Active(활성)인지 확인합니다

```
<#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)
```

캡처 보기

여러 가지 방법으로 캡처를 볼 수 있습니다.

- 스위치에서 직접 캡처를 볼 수 있습니다(요약).

```
<#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)
```

- 스위치에서 직접 캡처를 볼 수 있습니다(자세히).

<#root>

F340.09.11-3800-1#

show monitor capture file flash:mycap.pcap detailed

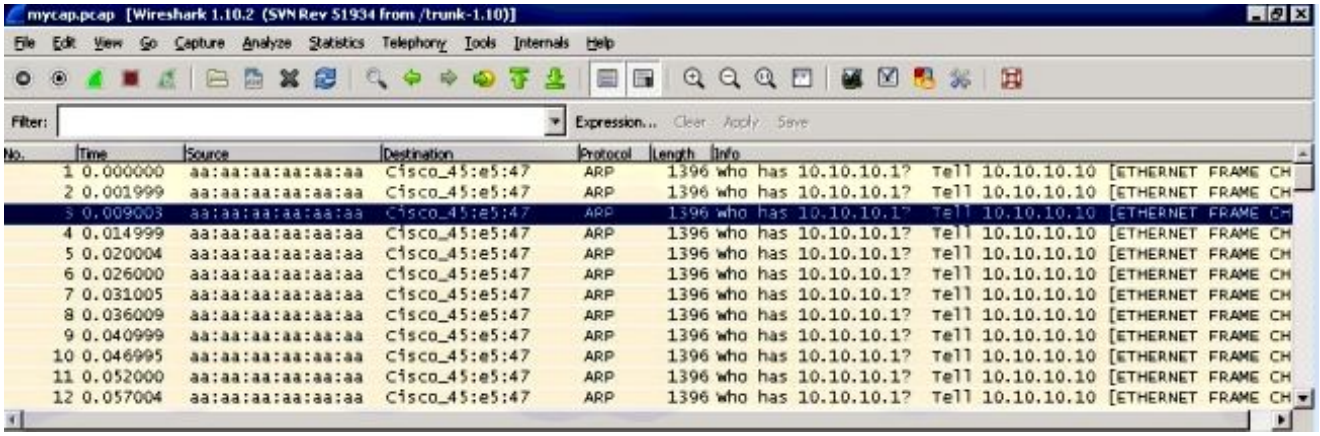
```
Frame 1: 1396 bytes on wire (11168 bits), 1396 bytes captured (11168 bits)
    Arrival Time: Oct  9, 2013 12:15:29.371974000 UTC
    Epoch Time: 1381320929.371974000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 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   @ABCDEFGHIJKLMNO
0550  50 51                                             PQ
    Data&colon; 000102030405060708090a0b0c0d0e0f1011121314151617...
    [Length: 1362]
```

- 스위치에서 pcap 파일을 TFTP/FTP로 제거하고 Wireshark에서 캡처 파일을 볼 수 있습니다.



다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

<#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
```

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

컨트롤 플레인 트래픽 캡처

다음은 Cisco Catalyst 3850 Series 스위치 자체에서 인그레스(ingress) 트래픽과 이그레스(egress) 트래픽을 모두 보여주는 샘플 컨피그레이션입니다.

이는 Cisco Catalyst 3850 Series Switch의 CPU에 어떤 트래픽이 도달하는지 확인할 수 있는 좋은 방법입니다.

이를 결합하여 CPU 사용량이 많은 상황을 진단할 수 있습니다

설정

<#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
```

결과

```
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
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.