1. 장비별 TCPDUMP 조회 방법

ubiQuoss

STEP 1.

- **TCPDUMP 조회 방법**

명령어	모 드	설 명
tcpdump interface vlan<number>	privileged	특정 vlan에서 in/out되는 packet dump
tcpdump interface vlan<number> <arp/icmp/udp/tcp>	privileged	패킷유형별 in/out되는 packet dump
tcpdump interface vlan<number> not port 23	privileged	telnet port 23번을 제외한 packet dump
tcpdump interface vlan<number> ether src <mac-address>	privileged	특정 source mac으로 in/out되는 packet dump
tcpdump interface vlan<number> <protocol> and host <ip-address>	privileged	AND 조건으로 packet dump
tcpdump interface vlan<number> host <ip-address>	privileged	특정 source ip로 in/out되는 packet dump

```
Switch# tcpdump interface vlan4000
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vlan4000, link-type EN10MB (Ethernet), capture size 65535 bytes
11:46:28.988727 00:e0:91:56:1f:a6 > 70:30:5d:96:37:be, ethertype IPv4 (0x0800), length 64: 10.4.11.238.4265 > 10.4.11.44.23: Flags [.], ack 984033258, win 511, length 0

Switch# tcpdump interface vlan4000 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vlan4000, link-type EN10MB (Ethernet), capture size 65535 bytes
11:49:08.139681 00:e0:91:56:1f:a6 > 70:30:5d:96:37:be, ethertype IPv4 (0x0800), length 78: 10.4.11.238 > 10.4.11.44: ICMP echo request, id 1, seq 5126, length 40
11:49:08.140614 70:30:5d:96:37:be > 00:e0:91:56:1f:a6, ethertype IPv4 (0x0800), length 74: 10.4.11.44 > 10.4.11.238: ICMP echo reply, id 1, seq 5126, length 40

Switch# tcpdump interface vlan4000 not port 23
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vlan4000, link-type EN10MB (Ethernet), capture size 65535 bytes
12:01:21.650254 90:da:6a:03:c7:ed > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 598: 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 90:da:6a:03:c7:ed, length 548

Switch# tcpdump interface vlan4000 ether src  00:e0:91:56:1f:a6
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vlan4000, link-type EN10MB (Ethernet), capture size 65535 bytes
12:27:17.927448 00:e0:91:56:1f:a6 > 70:30:5d:96:37:be, ethertype IPv4 (0x0800), length 64: 10.4.11.238.4265 > 10.4.11.44.23: Flags [.], ack 984086148, win 511, length 0

Switch# tcpdump interface vlan4000 icmp and host 10.4.11.238
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vlan4000, link-type EN10MB (Ethernet), capture size 65535 bytes
12:28:26.638541 00:e0:91:56:1f:a6 > 70:30:5d:96:37:be, ethertype IPv4 (0x0800), length 78: 10.4.11.238 > 10.4.11.44: ICMP echo request, id 1, seq 5129, length 40
12:28:26.639662 70:30:5d:96:37:be > 00:e0:91:56:1f:a6, ethertype IPv4 (0x0800), length 74: 10.4.11.44 > 10.4.11.238: ICMP echo reply, id 1, seq 5129, length 40

Switch# tcpdump interface vlan4000 host 10.4.11.254
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vlan4000, link-type EN10MB (Ethernet), capture size 65535 bytes
12:29:16.531917 00:07:70:e6:51:ba > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 64: Request who-has 10.4.11.254 tell 10.4.11.254, length 50
```