

VLAN Configuration and Network Traffic Monitoring using Port Mirroring

Part 1: Switch VLANs

SWITCH CONFIG

My system having the prompt based switch configuration because I'm using USB (enx00e04cc57dbf) as second Ethernet interface.

PROMPT BASED:

After entering into the prompt just type the enable to enter into enable mode.

To bring up the configuration mode just type "configure terminal"

To add the ip addresses and netmask I use ip address 10.133.36.10 netmask 255.255.255.0

```
BPS2000> enable
BPS2000# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BPS2000(config)#vlan mgmt 36
BPS2000(config)#ip address 10.133.36.10 netmask 255.255.255.0
```

To know the addresses are add or not just type the show ip addr you will get the address which are assign by us.

```
BPS2000(config)#show ip addr
```

	Configured	In Use	Last BootP
Stack IP Address:	0.0.0.0		0.0.0.0
Switch IP Address:	10.133.36.10	10.133.36.10	0.0.0.0
Subnet Mask:	255.255.255.0	255.255.255.0	0.0.0.0

After add the default gateway using ip addr default-gateway 10.133.36.254

```
BPS2000(config)#show vlan
```

Id	Name	Type	Protocol	User	PID	Active	IVL/SVL	Mgmt
1	VLAN #1	Port	None	0x0000	Yes	IVL	No	
	Port Members: 1-24							
36	VLAN #36	Port	None	0x0000	Yes	IVL	Yes	
	Port Members: 1							
136	VLAN #136	Port	None	0x0000	Yes	IVL	No	
	Port Members: 1-12							
236	VLAN #236	Port	None	0x0000	Yes	IVL	No	
	Port Members: 1,13-24							

```
BPS2000(config)#vlan ports 1 tagging enable
BPS2000(config)#
```

```
BPS2000>en
```

```
BPS2000#show vlan
```

Id	Name	Type	Protocol	User	PID	Active	IVL/SVL	Mgmt
1	VLAN #1	Port	None	0x0000		Yes	IVL	Yes
	Port Members: 1-24							
36	VLAN #36	Port	None	0x0000		Yes	IVL	No
	Port Members: 1							
136	VLAN #136	Port	None	0x0000		Yes	IVL	No
	Port Members: 1-12							
236	VLAN #236	Port	None	0x0000		Yes	IVL	No
	Port Members: 1,13-24							

```
BPS2000#show vlan interface info
```

Port	Filter Tagged Frames	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1	No	No	No	1	0	TagAll	Port 1
2	No	No	No	136	0	UntagAll	Port 2
3	No	No	No	136	0	UntagAll	Port 3
4	No	No	No	136	0	UntagAll	Port 4
5	No	No	No	136	0	UntagAll	Port 5
6	No	No	No	136	0	UntagAll	Port 6
7	No	No	No	136	0	UntagAll	Port 7
8	No	No	No	136	0	UntagAll	Port 8
9	No	No	No	136	0	UntagAll	Port 9
10	No	No	No	136	0	UntagAll	Port 10
11	No	No	No	136	0	UntagAll	Port 11
12	No	No	No	136	0	UntagAll	Port 12
13	No	No	No	236	0	UntagAll	Port 13
14	No	No	No	236	0	UntagAll	Port 14
15	No	No	No	236	0	UntagAll	Port 15
16	No	No	No	236	0	UntagAll	Port 16
17	No	No	No	236	0	UntagAll	Port 17
18	No	No	No	236	0	UntagAll	Port 18
19	No	No	No	236	0	UntagAll	Port 19
20	No	No	No	236	0	UntagAll	Port 20
21	No	No	No	236	0	UntagAll	Port 21
22	No	No	No	236	0	UntagAll	Port 22
23	No	No	No	236	0	UntagAll	Port 23
24	No	No	No	236	0	UntagAll	Port 24

```
BPS2000#
```

```
BPS2000#
```

Linux CONFIGURATION

- See the Netplan Examples (<https://netplan.readthedocs.io/en/stable/examples/#how-to-create-vlans>)
- Make enp2s0 the parent interface. This will ensure it will append/remove tags
- Create a virtual interface on the 10.133.1XX.0/24 network with the address 10.133.1XX.254/24 with enp2s0 as its link and 1XX as the id
- Create a 2nd virtual interface on the 10.133.2XX.0/24 network with the address 10.133.2XX.254/24 with enp2s0 as its link and 2XX as the id
- Create a 3rd virtual interface on the 10.133.XX.0/24 network with the address 10.133.XX.254/24

```
ethernets:
  eno1:
    addresses:
      - 146.163.133.36/24
    nameservers:
      addresses:
        - 127.0.0.1
        - 146.163.252.126
        - 146.163.252.127
    search:
      - siue.edu
      - ece.siue.edu
      - exp.ece.siue.edu
    routes:
      - to: default
        via: 146.163.133.254
  enx00e04cc57dbf:
    addresses:
      - 192.168.36.254/24
vlans:
  vlan136:
    id: 136
    link: enx00e04cc57dbf
    addresses:
      - 10.133.136.254/24
    nameservers:
      addresses:
        - 127.0.0.1
  vlan236:
    id: 236
    link: enx00e04cc57dbf
    addresses:
      - 10.133.236.254/24
    nameservers:
      addresses:
        - 127.0.0.1
  vlan36:
    id: 36
    link: enx00e04cc57dbf
    addresses:
      - 10.133.36.254/24
    nameservers:
      addresses:
        - 127.0.0.1
```

- Do a `#netplan apply` (or `$sudo netplan apply`) to update the configuration
- Reconfigure your DHCP and DNS servers to work on your two new VLAN networks. NAT should still work too.

```

GNU nano 6.2 /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    //=====
    dnssec-validation auto;

    listen-on port 53 { 146.163.133.36; 127.0.0.1; 10.133.136.254; 10.133.236.254; 10.133.36.254; };
};

```

```

# This is a very basic subnet declaration.
#subnet 192.168.36.0 netmask 255.255.255.0 {
#    # range 192.168.36.100 192.168.36.120;
#    #option routers 192.168.36.254;
#}
subnet 10.133.136.0 netmask 255.255.255.0 {
    range 10.133.136.100 10.133.136.120;
    option domain-name-servers 10.133.136.254;
    option routers 10.133.136.254;
}
subnet 10.133.236.0 netmask 255.255.255.0 {
    range 10.133.236.100 10.133.236.120;
    option domain-name-servers 10.133.236.254;
    option routers 10.133.236.254;
}
subnet 10.133.36.0 netmask 255.255.255.0 {
    range 10.133.36.100 10.133.36.120;
    option domain-name-servers 10.133.236.254;
    option routers 10.133.236.254;
}

```

```

"/etc/dhcp/dhcpd.conf" 131L, 4243B

```



```
# nat Table rules
*nat
:POSTROUTING ACCEPT [0:0]

# Forward traffic from eth1 through eth0.
#-A POSTROUTING -s 192.168.36.0/24 -o eno1 -j MASQUERADE
-A POSTROUTING -s 10.133.136.1/24 -o eno1 -j MASQUERADE
-A POSTROUTING -s 10.133.236.1/24 -o eno1 -j MASQUERADE
#-A POSTROUTING -s 10.133.36.0/24 -o eno1 -j MASQUERADE
```

Now, on the host side, open up a terminal and type:

1. user@host\$ telnet 10.133.XX.10

```
cpidugu@pyrophobia:~$ telnet 10.133.36.10
```

2. and you should get the same menu as the serial port. If you reset the switch, you shouldn't have anything to reconfigure until the next lab, but it is nice to be able to poke around if necessary.

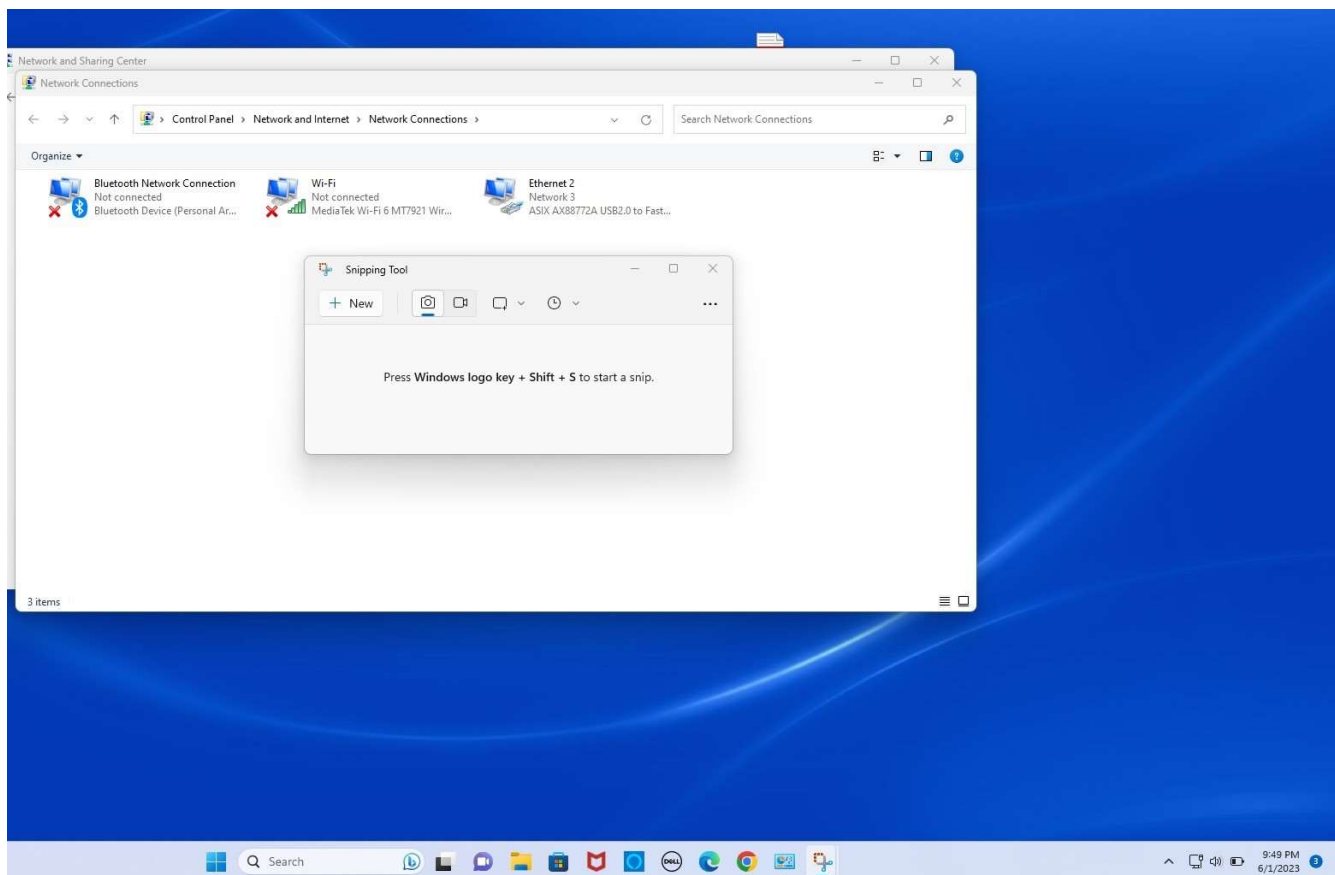
```
###      ### #####      #####      #####      #####      ###
#####   ### #####      #####      #####      #####      ###
#####   ### ###      ### ###      ###      ###      ###
#####   ### ###      ### ###      ###      ###      ###
### ###   ### ###      ### #####      ###      #####      ###
###   ### ###      ### #####      ###      #####      ###
###   #####   ###      ### ###      ###      ###      ###
###   #####   ###      ### ###      ###      ###      ###
###   #####   #####      ###      ###      ###      #####      #####
###   ###   #####      ###      ###      ###      #####      #####
###   ###   #####      ###      ###      ###      #####      #####
```

Enter Ctrl-Y to begin.

```
*****
*** Business Policy Switch 2000          ***
*** Nortel Networks                      ***
*** Copyright (c) 1996-2006, All Rights Reserved ***
*** BOSS 3.1 SSH                        ***
*** HW:11      FW:3.6.0.6   SW:v3.2.1.05 ISVN:3      ***
*****
```

```
BPS2000>EN
BPS2000#ping 10.133.36.254
Host is reachable. time=10 ms
BPS2000#
```

Your switch+Linux should now get you back out to the Internet. The left half should be on the 10.133.1XX.0/24 network and the right half should be on the 10.133.2XX.0/24 network! It should basically be just like we have on campus in our labs. This also makes your Linux machine a "one-armed router" between the two VLANs. If our switches weren't old, this would be built-in to them and they would be a L3 switch.



dhcp							
No.	Time	Source	Destination	Protocol	Length	Info	
40	25.209431090	0.0.0.0	255.255.255.255	DHCP	346	DHCP Inform	- Transaction ID 0x79af8597
56	27.080148661	0.0.0.0	255.255.255.255	DHCP	346	DHCP Inform	- Transaction ID 0x79af8597
70	30.077577442	0.0.0.0	255.255.255.255	DHCP	346	DHCP Inform	- Transaction ID 0x79af8597
130	33.593618355	0.0.0.0	255.255.255.255	DHCP	348	DHCP Discover	- Transaction ID 0x15c43e6f
135	34.594466095	10.133.236.254	10.133.236.100	DHCP	346	DHCP Offer	- Transaction ID 0x15c43e6f
136	34.596756769	0.0.0.0	255.255.255.255	DHCP	374	DHCP Request	- Transaction ID 0x15c43e6f
137	34.599975956	10.133.236.254	10.133.236.100	DHCP	346	DHCP ACK	- Transaction ID 0x15c43e6f

> Frame 130: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits) on interface enx00e04cc57dbf, id 0

> Ethernet II, Src: AsixElec_f0:24:34 (00:0e:c6:f0:24:34), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 236

- 000..... = Priority: Best Effort (default) (0)
- ...0..... = DEI: Ineligible
-0000 1110 1100 = ID: 236
- Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

> User Datagram Protocol, Src Port: 68, Dst Port: 67

> Dynamic Host Configuration Protocol (Discover)

For port-mirroring purposes we need to tag the 24 port and change the pvid to 1

```

BPS2000(config)#vlan ports 24 tagging enable
BPS2000(config)#show vlan interface info

```

Port	Filter Tagged Frames	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1	No	No	No	1	0	TagAll	Port 1
2	No	No	No	136	0	UntagAll	Port 2
3	No	No	No	136	0	UntagAll	Port 3
4	No	No	No	136	0	UntagAll	Port 4
5	No	No	No	136	0	UntagAll	Port 5
6	No	No	No	136	0	UntagAll	Port 6
7	No	No	No	136	0	UntagAll	Port 7
8	No	No	No	136	0	UntagAll	Port 8
9	No	No	No	136	0	UntagAll	Port 9
10	No	No	No	136	0	UntagAll	Port 10
11	No	No	No	136	0	UntagAll	Port 11
12	No	No	No	136	0	UntagAll	Port 12
13	No	No	No	236	0	UntagAll	Port 13
14	No	No	No	236	0	UntagAll	Port 14
15	No	No	No	236	0	UntagAll	Port 15
16	No	No	No	236	0	UntagAll	Port 16
17	No	No	No	236	0	UntagAll	Port 17
18	No	No	No	236	0	UntagAll	Port 18
19	No	No	No	236	0	UntagAll	Port 19
20	No	No	No	236	0	UntagAll	Port 20
21	No	No	No	236	0	UntagAll	Port 21
22	No	No	No	236	0	UntagAll	Port 22
23	No	No	No	236	0	UntagAll	Port 23
24	No	No	No	1	0	TagAll	Port 24

Part 2: Port Mirroring

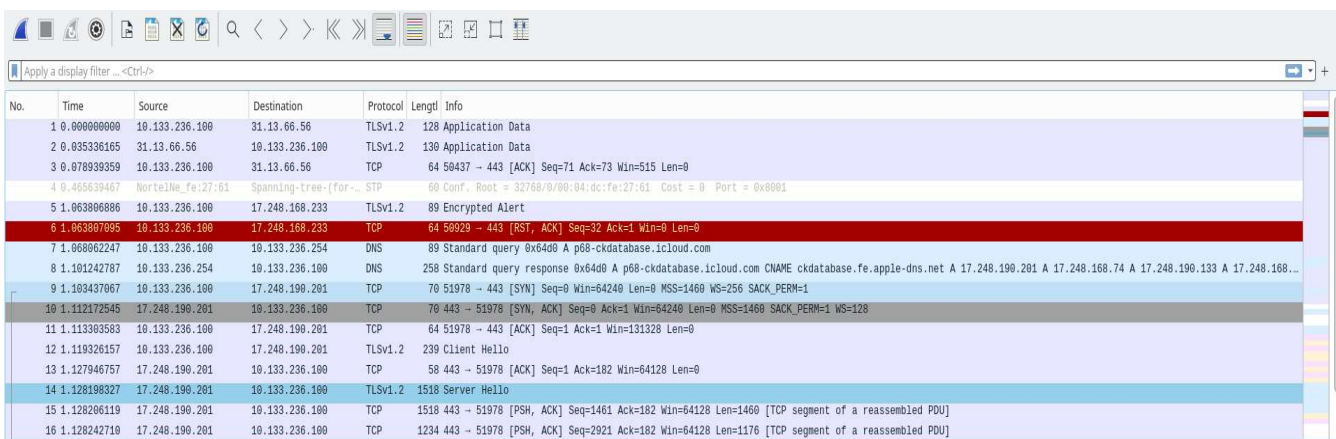
Introduction:

Port mirroring is a feature common to many switches. It allows the switch to copy inbound/outbound traffic on one or multiple ports to another port for monitoring. It is useful for diagnostics, as under normal operation, any other port on a switch can not monitor any other port. By mirroring target ports to a monitor port(s), this traffic can now be observed, and any potential problems, all the way down to Layer 2, might be more easily diagnosed. The big drawback is security, as all traffic for one station is now visible by another.

Exercise:

In this part of the lab, you are to use port mirroring on your switch to mirror all traffic (Inbound and Outbound) from Port 1 (the one connected to your Linux machine) to Port 24 (you can remove Port 24 from VLAN 2XX if necessary). Once enabled, plug your laptop or a neighbor's computer into Port 24 on your switch and use tcpdump/wireshark/etc. to view the traffic. If mirroring is done correctly, then you will essentially see any traffic from the switch to Linux and vice versa. You could grab another laptop, plug it in on any other port, and you should be able to monitor the DHCP configuration and any traffic from that laptop to the rest of the Internet using Wireshark. If you don't have another laptop, you could potentially configure the switch to have remote access through Telnet/SSH. Then you can remote into the switch from your Linux machine, and this traffic should also be seen on your monitoring laptop.

1. Normal traffic traces on wireshark in my laptop and lab machine.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.133.236.100	31.13.66.56	TLv1.2	128	Application Data
2	0.035336165	31.13.66.56	10.133.236.100	TLv1.2	130	Application Data
3	0.078939359	10.133.236.100	31.13.66.56	TCP	64	58437 → 443 [ACK] Seq=71 Ack=73 Win=515 Len=0
4	0.465639467	NortelNe_fe:27:61	Spanning-tree-for...	STP	60	Conf. Root = 32768/0/00:04:dc:fe:27:61 Cost = 0 Port = 0x0001
5	1.063806886	10.133.236.100	17.248.168.233	TLv1.2	89	Encrypted Alert
6	1.063807095	10.133.236.100	17.248.168.233	TCP	64	58929 → 443 [RST, ACK] Seq=32 Ack=1 Win=0 Len=0
7	1.068062247	10.133.236.100	10.133.236.254	DNS	89	Standard query 0x6400 A p68-ckdatabase.1cloud.com
8	1.101242787	10.133.236.254	10.133.236.100	DNS	258	Standard query response 0x6400 A p68-ckdatabase.1cloud.com CNAME ckdatabase.fe.apple-dns.net A 17.248.190.201 A 17.248.168.74 A 17.248.190.133 A 17.248.168...
9	1.103437067	10.133.236.100	17.248.190.201	TCP	70	51978 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
10	1.112172545	17.248.190.201	10.133.236.100	TCP	70	443 → 51978 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
11	1.113303583	10.133.236.100	17.248.190.201	TCP	64	51978 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
12	1.119326157	10.133.236.100	17.248.190.201	TLv1.2	239	Client Hello
13	1.127946757	17.248.190.201	10.133.236.100	TCP	58	443 → 51978 [ACK] Seq=1 Ack=182 Win=64128 Len=0
14	1.128198327	17.248.190.201	10.133.236.100	TLv1.2	1518	Server Hello
15	1.128206119	17.248.190.201	10.133.236.100	TCP	1518	443 → 51978 [PSH, ACK] Seq=1461 Ack=182 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
16	1.128242710	17.248.190.201	10.133.236.100	TCP	1234	443 → 51978 [PSH, ACK] Seq=2921 Ack=182 Win=64128 Len=1176 [TCP segment of a reassembled PDU]

