Computer Networking Laboratory

Lab Report

Network Monitoring and Management

Arun Kumar Rajendra Kumar, Aswathi Saminathan

4.1

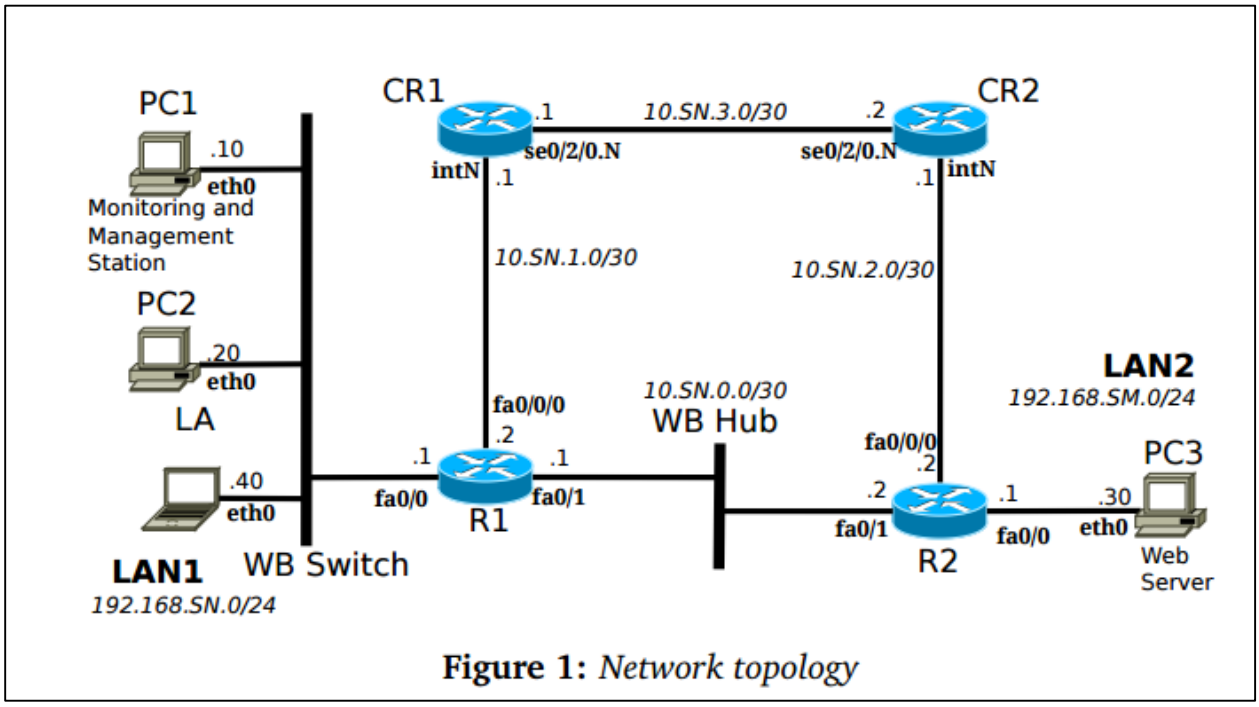


Figure 1: *Network topology*

Computers and routers were connected as shown in the figure above and IP addresses were assigned. Loopback0 interface was added to the workbench routers with IP address 10.99.1.1/32 and 10.99.1.2/32 respectively. Loopback0 interface was added to the core routers with IP address 99.99.99.1/32 and 99.99.99.2/32 respectively. OSPF was enabled on all the routers using area0. Also the OSPF was enabled on the loopback interfaces of all the routers. Verified that PC1 can ping all other PC's and also was able to ping the loopback interface of each router.

4.2

Started httpd on PC3 and verified that we were able to open http://localhost/ locally on PC3. Logged in to PC3 via SSH from PC1 (monitoring station). Started capturing packets on interface eth0 but filtered out the SSH session. Accessed webserver running on PC3 by using firefox browser on PC2 and observed the following captures on PC1. Here, we see the communication between 192.168.31.20 (PC2) and 192.168.35.30 (PC3). PC2 is trying to access webserver running on PC3 and that is the reason we see HTTP in the logs suggesting that it is http traffic. The first three lines above are part of 3 way handshake and the one after that is the http GET request and the then the webserver replying to the request as shown in the capture above. Httpd was stopped on PC3. Webserver was again accessed from PC2. Following captures were obtained on PC1

```
14:49:01.460337 IP 192.168.31.20.34301 > 192.168.35.30.http: S
3570477742:3570477742(0) win 5840 <mss 1460,sackOK,timestamp
608650283 0,nop,wscale 7>
14:49:01.460361 IP 192.168.35.30.http > 192.168.31.20.34301: R
0:0(0) ack 3570477743 win 0
14:49:01.483188 IP 192.168.31.20.34302 > 192.168.35.30.http: S
3565528579:3565528579(0) win 5840 <mss 1460,sackOK,timestamp
608650306 0,nop,wscale 7>
14:49:01.483201 IP 192.168.35.30.http > 192.168.31.20.34302: R
0:0(0) ack 3565528580 win 0
```

In these captures PC2 is sending the request to PC3 but PC3 is replying with the Reset as the webserver is not running there. Ping session was started from laptop to PC3 and tcpdump was
restarted with the correct options to capture the ICMP traffic. Following captures were observed

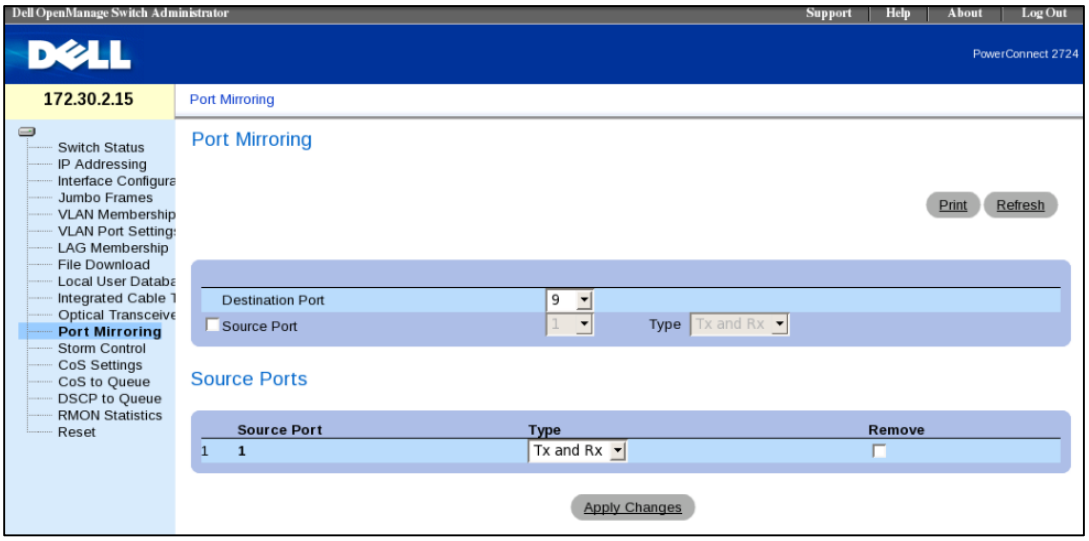
```
[team1@netlab-wb1pc3 ~]$ sudo tcpdump -n -i eth0 host
192.168.31.40 and icmp
tcpdump: verbose output suppressed, use -v or -vv for full
protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96
bytes
14:50:49.419953 IP 192.168.31.40 > 192.168.35.30: ICMP echo
request, id 21516, seq 23, length 64
14:50:49.419991 IP 192.168.35.30 > 192.168.31.40: ICMP echo reply,
id 21516, seq 23, length 64
14:50:50.419897 IP 192.168.31.40 > 192.168.35.30: ICMP echo
request, id 21516, seq 24, length 64
14:50:50.419908 IP 192.168.35.30 > 192.168.31.40: ICMP echo reply,
id 21516, seq 24, length 64
14:50:51.419808 IP 192.168.31.40 > 192.168.35.30: ICMP echo
request, id 21516, seq 25, length 64
14:50:51.419818 IP 192.168.35.30 > 192.168.31.40: ICMP echo reply,
id 21516, seq 25, length 64
14:50:52.419716 IP 192.168.31.40 > 192.168.35.30: ICMP echo
request, id 21516, seq 26, length 64
14:50:52.419726 IP 192.168.35.30 > 192.168.31.40: ICMP echo reply,
id 21516, seq 26, length 64
14:50:53.419647 IP 192.168.31.40 > 192.168.35.30: ICMP echo
request, id 21516, seq 27, length 64
14:50:53.419659 IP 192.168.35.30 > 192.168.31.40: ICMP echo reply,
id 21516, seq 27, length 64
14:50:54.419560 IP 192.168.31.40 > 192.168.35.30: ICMP echo
request, id 21516, seq 28, length 64
```

In the captures we can see that Laptop(192.168.31.40) is sending icmp request packet and receiving a reply from PC3(192.168.35.40). There are few differences between ICMP captures and the HTTP captures. ICMP captures include ID (id 21516) but http don't.

Also, http capture has a timestamp parameter in each line of capture which icmp capture lacks. Finally the SSH session was terminated.

4.3

Eth1 of PC1 was connected to Port9 on the switch (monitoring port). Also, fa0/0 of router R1 was located to be connected to Port1 on the switch.(monitored port). PC2 interface eth1 was used to connect to switch management web interface at http://172.30.2.15 Using Port Mirroring item on the left menu, monitored and monitoring port is set to Port1 and Port9. The changes were applied.



Traffic was generated between LAN1 and the external network. Traffic was captured using tcpdump on PC1 eth1 (monitoring port).

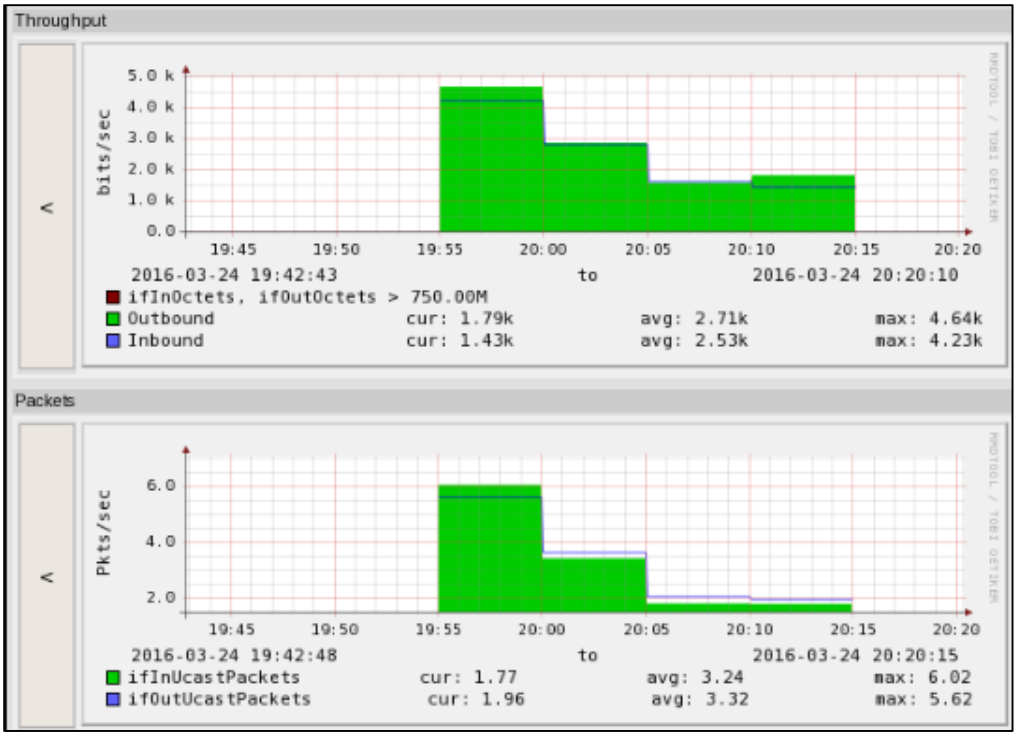
```
[team31@netlab-wb1pc1 ~]$ sudo tcpdump -i eth1
tcpdump: verbose output suppressed, use -v or -vv for full
protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 96
bytes
19:31:54.150330 IP 192.168.31.20 > 192.168.35.30: ICMP echo
request, id 34392, seq 189, length 64
19:31:54.150707 IP 192.168.35.30 > 192.168.31.20: ICMP echo reply,
id 34392, seq 189, length 64
19:31:54.151704 arp who-has 172.30.2.1 tell 172.30.2.11
19:31:55.150333 IP 192.168.31.20 > 192.168.35.30: ICMP echo
request, id 34392, seq 190, length 64
19:31:55.150690 IP 192.168.35.30 > 192.168.31.20: ICMP echo reply,
id 34392, seq 190, length 64
19:31:55.151703 arp who-has 172.30.2.1 tell 172.30.2.11
19:31:56.150352 IP 192.168.31.20 > 192.168.35.30: ICMP echo
request, id 34392, seq 191, length 64
19:31:56.150704 IP 192.168.35.30 > 192.168.31.20: ICMP echo reply,
id 34392, seq 191, length 64
19:31:56.150800 IP 192.168.31.10.33059 > 192.168.1.1.domain: 36443
+ PTR? 30.35.168.192.in-addr.arpa. (44)
19:31:56.151481 IP 192.168.31.1 > 192.168.31.10: ICMP host
192.168.1.1 unreachable, length 36
19:31:56.151701 arp who-has 172.30.2.1 tell 172.30.2.11
19:31:57.150341 IP 192.168.31.20 > 192.168.35.30: ICMP echo
request, id 34392, seq 192, length 64
19:31:57.150688 IP 192.168.35.30 > 192.168.31.20: ICMP echo reply,
id 34392, seq 192, length 64
19:31:57.215659 IP 192.168.34.1 > 224.0.0.5: OSPFv2, Hello,
length: 56
```

ICMP traffic was generated between PC2 (192.168.31.20) and PC3(192.168.35.30). This traffic pass through the fa0/0 interface of R1 which is the monitored port. Since, PC1 interface eth1 is connected to the monitoring Port9 of the switch, therefore the traffic is being seen when we capture the traffic on the PC1 using the tcpdump. A copy of the traffic is forwarded to PC1 eth1. Apart from the ICMP traffic that we generated we also saw the ARP and OSPF traffic. This traffic was also passing through R1 interface fa0/0.

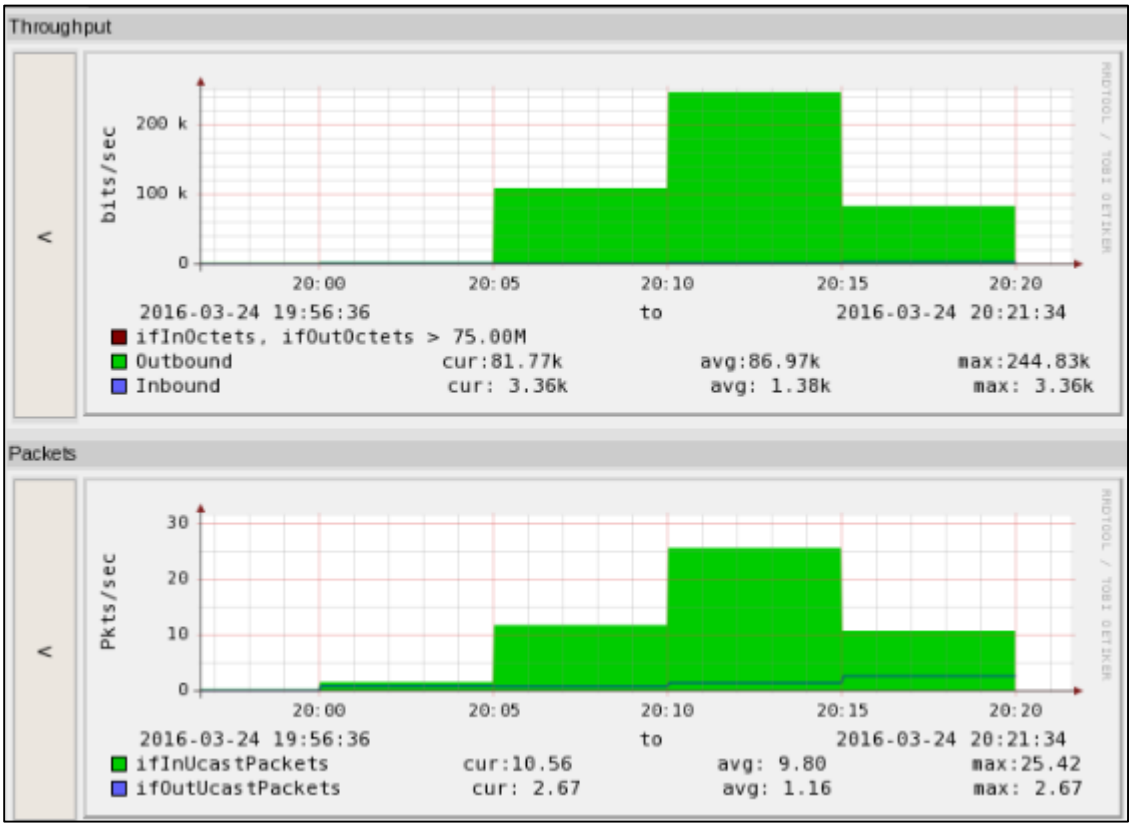
4.4

SNMP agent was enabled on all the routers. SNMP agent was started/enabled on all the PC's. Zenoss was started on PC1 using the below command and accessed using web interface http://192.168.31.10:8080 Logged in and the existing devices are removed from the device list to start with an empty configuration.PC's and routers were added using add device item from the left menu. Each device added was configured with IP address, Class Path, SNMP Community. After the devices were added, the statistics of an interface of a couple of devices were observed. Screenshots are given below.

PC1 eth0:


Throughput
bits/sec
5.0 k
4.0 k
3.0 k
2.0 k
1.0 k
0.0
19:45
19:50
19:55
20:00
20:05
20:10
20:15
20:20
2016-03-24 19:42:43
to
2016-03-24 20:20:10
ifInOctets, ifOutOctets > 750.00M
Outbound
cur: 1.79k
avg: 2.71k
max: 4.64k
Inbound
cur: 1.43k
avg: 2.53k
max: 4.23k
Packets
Pkts/sec
6.0
4.0
2.0
19:45
19:50
19:55
20:00
20:05
20:10
20:15
20:20
2016-03-24 19:42:48
to
2016-03-24 20:20:15
ifInUcastPackets
cur: 1.77
avg: 3.24
max: 6.02
ifOutUcastPackets
cur: 1.96
avg: 3.32
max: 5.62

PC3 etho:


Throughput
bits/sec
200 k
100 k
0
20:00
20:05
20:10
20:15
20:20
2016-03-24 19:56:36
to
2016-03-24 20:21:34
ifInOctets, ifOutOctets > 75.00M
Outbound
cur:81.77k
avg:86.97k
max:244.83k
Inbound
cur: 3.36k
avg: 1.38k
max: 3.36k
Packets
Pkts/sec
30
20
10
0
20:00
20:05
20:10
20:15
20:20
2016-03-24 19:56:36
to
2016-03-24 20:21:34
ifInUcastPackets
cur:10.56
avg: 9.80
max:25.42
ifOutUcastPackets
cur: 2.67
avg: 1.16
max: 2.67

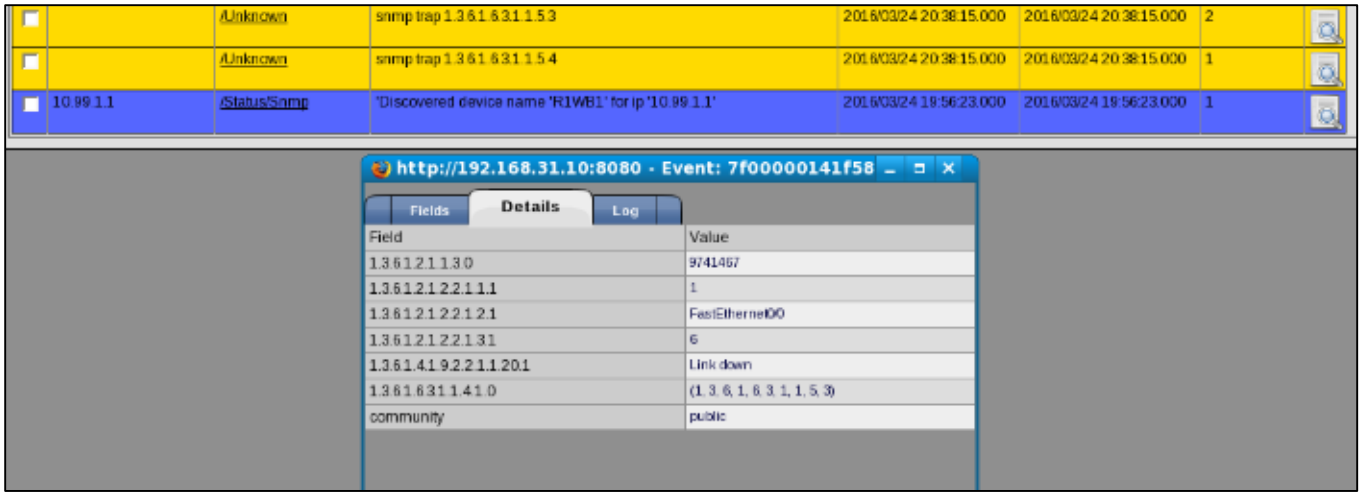
HTTP and SSH are added to the list of Services monitored under the hosting server PC. Under Host PC3, OS tab was chosen, Add IpService option was chosen from drop-down menu to the left of the IP services box. In Ip Service Class field, http and TCP protocol was selected. After the HTTP service page comes up, monitor option was set to true. Similarly SSH service was also added.

The status of both HTTP and SSH services is shown as active in the snapshot above. Now the HTTP server was stopped. Once this was done the status of HTTP was shown as inactive. Snapshot shown below.

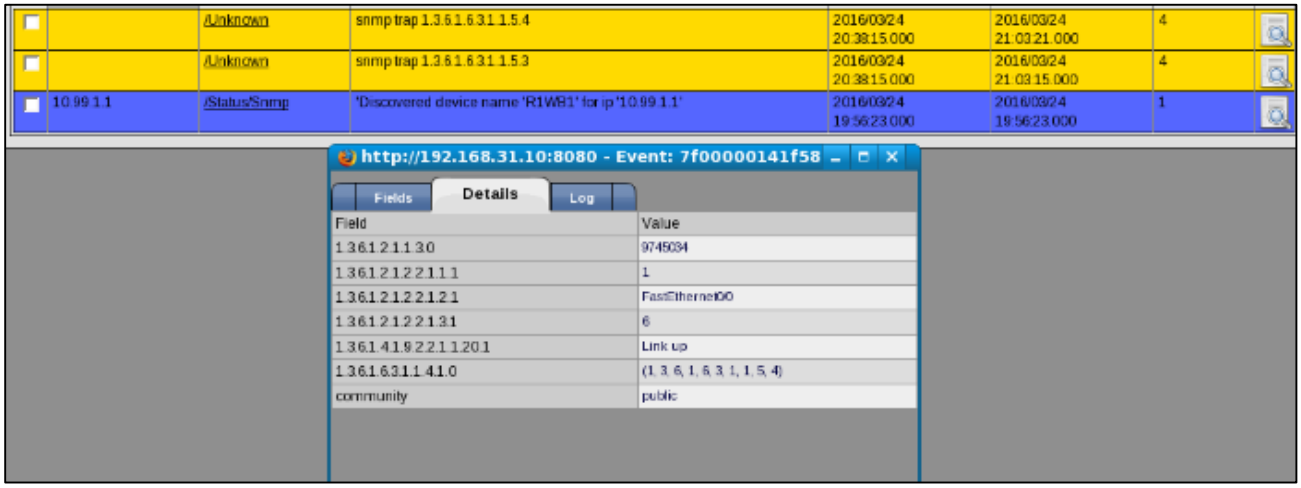
An event was also seen in the event list in red (critical) that HTTP service is down.

HTTP was restarted and we saw the critical event had disappeared from the event list and the status of HTTP was shown as active. HTTP event history logs are shown below.

Now to have the router R1 send traps to the monitoring station the following commands were applied on router R1. The cable between the 2 workbench routers was disconnected. After a while a yellow event showed up in the event list indicating that the link went down.



The cable was reconnected. Another trap appeared indicating that the link is up.



4.5:

Applied the following commands on each WB router in **global configuration mode**:

Checked the retrieved data with the defined MIB view on Linux machine using following command snmpwalk –c public –v 2c 10.31.0.1 The below output is from PC1.

```
[team31@netlab-wb1pc1 ~]$ snmpwalk -c public -v 2c 10.99.1.1
IF-MIB::ifNumber.0 = INTEGER: 6
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifIndex.4 = INTEGER: 4
IF-MIB::ifIndex.5 = INTEGER: 5
IF-MIB::ifIndex.6 = INTEGER: 6
IF-MIB::ifDescr.1 = STRING: FastEthernet0/0
IF-MIB::ifDescr.2 = STRING: FastEthernet0/1
IF-MIB::ifDescr.3 = STRING: FastEthernet0/0/0
```

IF-MIB::ifDescr.4 = STRING: VoIP-Null0
IF-MIB::ifDescr.5 = STRING: Null0
IF-MIB::ifDescr.6 = STRING: Loopback0

Interface fa0/1 of R1 is Shutdown using following command**.**

snmpset –c public –v 2c 10.31.0.1 ifAdminStatus.2 = 2

```
[team31@netlab-wb1pc1 ~]$ snmpset -c public -v 2c 10.99.1.1 ifAdminStatus.2 = 2
IF-MIB::ifAdminStatus.2 = INTEGER: down(2)
```

Verified the status of the interface using **show ip interface brief** command.

```
R1WB1(config)#
*Mar 25 02:37:40.209: %SYS-5-CONFIG_I: Configured from 192.168.31.10 by snmp
*Mar 25 02:37:40.209: %OSPF-5-ADJCHG: Process 100, Nbr 10.99.1.2 on FastEthernet0/1 f
rom FULL to DOWN, Neighbor Down: Interface down or detached
R1WB1(config)#
*Mar 25 02:37:42.209: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to ad
ministratively down
*Mar 25 02:37:43.209: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1
, changed state to down
R1WB1(config)#
R1WB1#
*Mar 25 02:38:11.829: %SYS-5-CONFIG_I: Configured from console by console
R1WB1#sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.31.1    YES manual up                    up
FastEthernet0/1            10.31.0.1       YES manual administratively down down
FastEthernet0/0/0          10.31.1.2       YES manual up                    up
Loopback0                  10.99.1.1       YES manual up                    up
R1WB1#
```