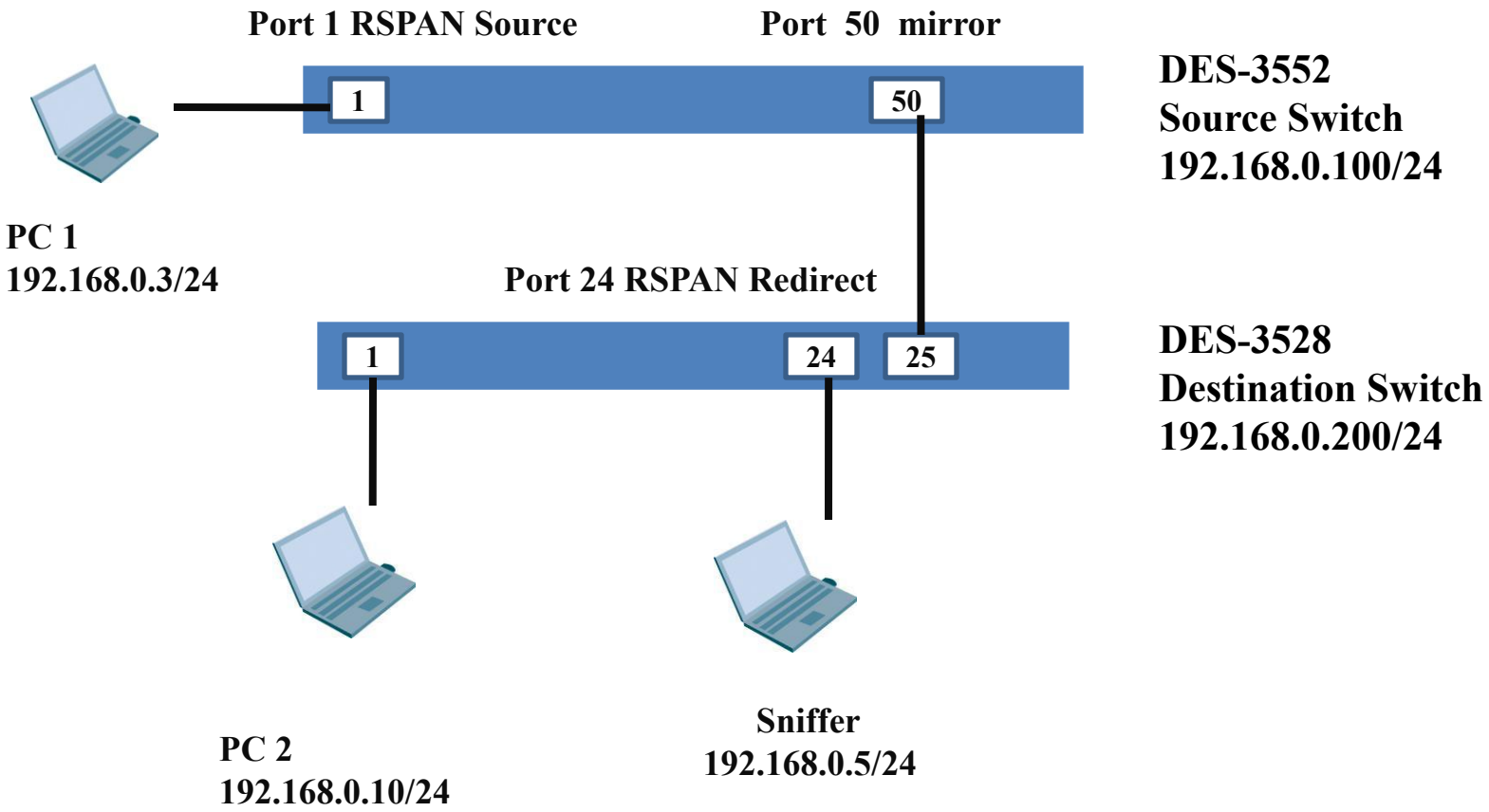
RSPAN

Jason Chang
2009.07.01

Topology


Port 1 RSPAN Source
Port 50 mirror
1
50
DES-3552
Source Switch
192.168.0.100/24
PC 1
192.168.0.3/24
Port 24 RSPAN Redirect
1
24
25
DES-3528
Destination Switch
192.168.0.200/24
PC 2
192.168.0.10/24
Sniffer
192.168.0.5/24

Command

- DES-3552 Source Switch (FW 2.11.B008)

enable rspan
create vlan vlanid 100
config mirror port 50 add source ports 1 both
enable miror
config vlan vlanid 100 name RSPAN_VLAN
create rspan vlan vlan_name RSPAN_VLAN
config rspan vlan vlan_name RSPAN_VLAN source add ports 1 both

Command (cont.)

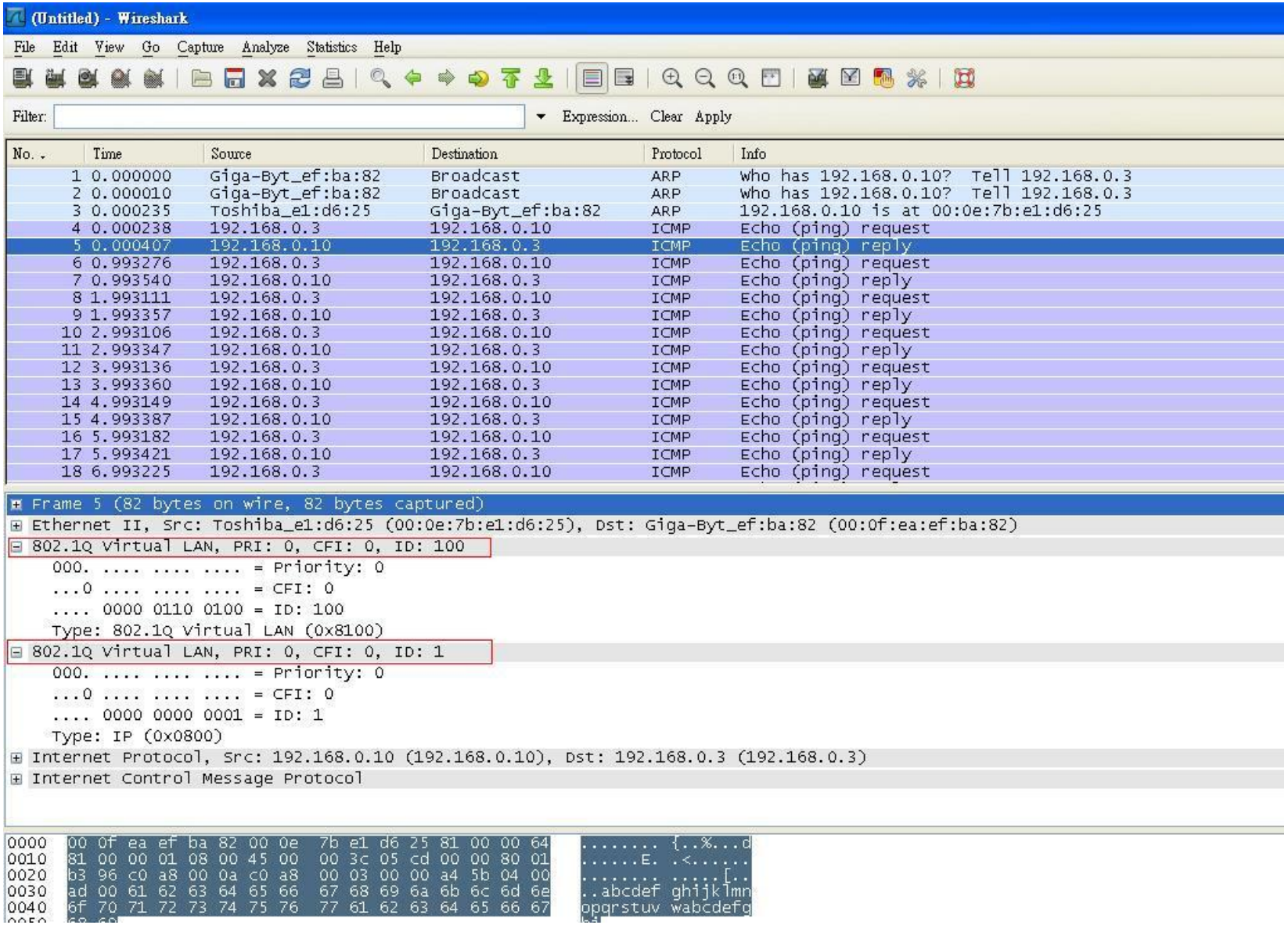
- DES-3528 Destination Switch (FW 2.00.B003)

enable rspan
create vlan vlanid 100
config vlan vlanid 100 add tagged 24-25
config vlan vlanid 100 name RSPAN_VLAN
create rspan vlan vlan_name RSPAN_VLAN
config rspan vlan vlan_name RSPAN_VLAN redirect add port 24

Test Result

- PC1 (192.168.0.3) can ping PC2 (192.168.0.10) successfully!
- Sniffer PC can capture ICMP packets (both RX & TX) form the traffic between PC1 & PC2

Test Result


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 Giga-Byt_ef:ba:82 Broadcast ARP Who has 192.168.0.10? Tell 192.168.0.3
2 0.000010 Giga-Byt_ef:ba:82 Broadcast ARP Who has 192.168.0.10? Tell 192.168.0.3
3 0.000235 Toshiba_e1:d6:25 Giga-Byt_ef:ba:82 ARP 192.168.0.10 is at 00:0e:7b:e1:d6:25
4 0.000238 192.168.0.3 192.168.0.10 ICMP Echo (ping) request
5 0.000407 192.168.0.10 192.168.0.3 ICMP Echo (ping) reply
6 0.993276 192.168.0.3 192.168.0.10 ICMP Echo (ping) request
7 0.993540 192.168.0.10 192.168.0.3 ICMP Echo (ping) reply
8 1.993111 192.168.0.3 192.168.0.10 ICMP Echo (ping) request
9 1.993357 192.168.0.10 192.168.0.3 ICMP Echo (ping) reply
10 2.993106 192.168.0.3 192.168.0.10 ICMP Echo (ping) request
11 2.993347 192.168.0.10 192.168.0.3 ICMP Echo (ping) reply
12 3.993136 192.168.0.3 192.168.0.10 ICMP Echo (ping) request
13 3.993360 192.168.0.10 192.168.0.3 ICMP Echo (ping) reply
14 4.993149 192.168.0.3 192.168.0.10 ICMP Echo (ping) request
15 4.993387 192.168.0.10 192.168.0.3 ICMP Echo (ping) reply
16 5.993182 192.168.0.3 192.168.0.10 ICMP Echo (ping) request
17 5.993421 192.168.0.10 192.168.0.3 ICMP Echo (ping) reply
18 6.993225 192.168.0.3 192.168.0.10 ICMP Echo (ping) request
Frame 5 (82 bytes on wire, 82 bytes captured)
Ethernet II, Src: Toshiba_e1:d6:25 (00:0e:7b:e1:d6:25), Dst: Giga-Byt_ef:ba:82 (00:0f:ea:ef:ba:82)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 100
000. .... = Priority: 0
...0 .... = CFI: 0
.... 0000 0110 0100 = ID: 100
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 1
000. .... = Priority: 0
...0 .... = CFI: 0
.... 0000 0000 0001 = ID: 1
Type: IP (0x0800)
Internet Protocol, Src: 192.168.0.10 (192.168.0.10), Dst: 192.168.0.3 (192.168.0.3)
Internet Control Message Protocol
0000 00 0f ea ef ba 82 00 0e 7b e1 d6 25 81 00 00 64 .... {..%...d
0010 81 00 00 01 08 00 45 00 00 3c 05 cd 00 00 80 01 ......E. .<......
0020 b3 96 c0 a8 00 0a c0 a8 00 03 00 00 a4 5b 04 00 ....[..
0030 ad 00 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e ..abcdef ghijklmn
0040 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 opqrstuv wabcdefg