

freebsd-net: FW: Curiosity in IPFW/Freebsd bridge. [more] 802.1q VLAN at fault?

## FW: Curiosity in IPFW/Freebsd bridge. [more] 802.1q VLAN at fault?

*Source:* <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2004-12/0263.html>

---

*From:* Andrew Seguin ([asegu\\_at\\_borgtech.ca](mailto:asegu_at_borgtech.ca))

*Date:* 12/17/04

To: <[freebsd-net@freebsd.org](mailto:freebsd-net@freebsd.org)>

Date: Fri, 17 Dec 2004 10:47:46 +0100

My apologies: Sometimes I feel just so stupid... hitting reply replies to me instead of the list. Ooops!

-----Original Message-----

From: Andrew Seguin [<mailto:asegu@borgtech.ca>]

Sent: Friday, December 17, 2004 10:16 AM

To: 'Andrew Seguin'

Subject: RE: Curiosity in IPFW/Freebsd bridge. [more]

Ok, through all my bugging of you all, I just want to mention that I am still working at my own end to figure this out..

I've used tcpdump to capture a sample of all traffic for each nic (tcpdump -s 1500 -i fxp1 -c 1000 -w tcpdump.fxp1), which I am now looking at in ethereal.

So my initial observation: traffic flowing through the bridge doesn't filter, while on the console access nic, it does.

Looking through the ethereal dumps, I have spotted one difference.

Packets for the console look like this:

```
Frame 1 (106 bytes on wire, 106 bytes captured)
Ethernet II, Src: MAC1, Dst: MAC2
Internet Protocol, Src Addr: MyPC, Dst Addr: FIREWALL
SSH Protocol
```

Packets from the bridge look like this:

```
Frame 1 (64 bytes on wire, 64 bytes captured)
Ethernet II, Src: MAC1, Dst: MAC2
802.1q Virtual LAN
Internet Protocol, Src Addr: x, Dst Addr: y
Transmission Control Protocol, ...
```

So it would seem that the part "802.1q Virtual LAN" in the protocol is

freebsd-net: FW: Curiosity in IPFW/Freebsd bridge. [more] 802.1q VLAN at fault?

stopping IPFW from investigating the traffic? (At times like this I wish I would have not studied computer engineering but networking for 4 years!).

Question then:

What in IPFW is stopping it from reading into a VLAN tagged packet (if it is such that it can be called).

All help and pointers (especially to documentation) would be highly appreciated!

-----Original Message-----

From: Andrew Seguin [mailto:asegu@borgtech.ca]

Sent: Friday, December 17, 2004 8:27 AM

To: 'Andrew Seguin'

Subject: RE: Curiosity in IPFW/Freebsd bridge. [more]

I have done a bit of further research and I have to question myself what is going on.

I set the system back up with only two nics in use, and put an IP address up on one side only, nothing different.

Back to the three nic setup: Four rules:

1 allow ip from any to LOCALIP 22

10 allow tcp from any to any

11 allow udp from any to any

100 allow log ip from any to any

The counts climb very very slowly f