

Re: TV Card setup (repost) – basketcaise, help please! :-)

Source: <http://linux.derkeiler.com/Newsgroups/alt.os.linux.suse/2004-10/0411.html>

From: Hactar (*ebenONE_at_tampabay.ARE-ARE.com.unmung*)

Date: 10/04/04

Date: Mon, 04 Oct 2004 02:46:18 GMT

In article <415e8d8e@duster.adelaide.on.net>, JPB <jpb@email.pt> wrote:

> *basketcaise* wrote:

> > *JPB adjusted his/her tin foil beanie and asbestos underwear to write:*

> >

> > > "Oct 2 10:23:35 amd kernel: SFW2-INext-ACC-TCP IN=eth1 OUT=

> > > MAC=00:40:f4:29:04:c4:00:90:1a:40:bd:ac:08:00 SRC=193.217.226.190

> > > DST=203.122.244.179 LEN=48 TOS=0x00 PREC=0x20 TTL=103 ID=2755 DF

> > > PROTO=TCP SPT=13673 DPT=6600 WINDOW=65535 RES=0x00 SYN URGP=0 OPT

> > > (0204058C01010402)"

> >

> >

> > *These are messages from your firewall and can get a bit out of hand the*

> > *source is 193.217.226.190 destination 203.122.244.179, is the first*

> > *number your DNS server by any chance?*

>

> *No idea, really...I confess I am a bit green when it comes to these*

> *things...*

I'm going to try to make it readable, but my knowlege of this is spotty:

MAC=00:40:f4:29:04:c4:00:90:1a:40:bd:ac:08:00

MAC ID "Media access card identification" Usually only 6 bytes long (six pair of hex digits separated by colons, every MAC ID is unique, it's printed on the card) but this is 12 pairs. I don't know what's up.

SRC=193.217.226.190

"Source". Where the packet's from.

DST=203.122.244.179

"Destination". Where the packet's to.

LEN=48

alt.os.linux.suse: Re: TV Card setup (repost) – basketcaise, help please! :-)

"Length" of IP packet. Min=40 bytes.

TOS=0x00

"Type of service". Unused?

PREC=0x20

?

TTL=103

"Time to live". Decrement by 1 by each router it passes.

ID=2755

?

DF

"Don't fragment" this IP packet if it's too big, drop it and send an ICMP error.

PROTO=TCP

"Protocol" is TCP, not UDP or some other.

SPT=13673

"Source port". Ports <1024 require root privs on a *nix box.

DPT=6600

"Destination port". grep 6600 /etc/services ... heck if I know. 6000 is X, so it might be related to that.

WINDOW=65535

Window size?

RES=0x00

?

SYN

As in, part of the 3-way handshake?

URGP=0

Urgent?

Re: TV Card setup (repost) – basketcaise, help please! :-)

alt.os.linux.suse: Re: TV Card setup (repost) – basketcaise, help please! :-)

OPT

?

> *The second number belongs to my ISP, but the first one, when looked up
> on reverse DNS lookup site, resolves as "revertdist-adsl.dax.net" –*

JPB's machine

> *which is something I've never heard of, and when attempting to contact
> that site, it gives out "connection refused". I can ping it, but that's
> all.*

He's not running any services that you know about.

> *My firewall settings in Yast are set up to log critical lost packets,
> but I have no idea what the message above may relate to...*

Timing may yield a clue.

--

```
-eben      ebQenWl@EtaRmpTabYayU.rIr.OcoPm      home.tampabay.rr.com/hactar
CAPRICORN: The stars say you're an exciting and wonderful person...
but you know they're lying.  If I were you, I'd lock my doors and
windows and never never never never leave my house again.  -- Weird Al
```