August Technical Presentation

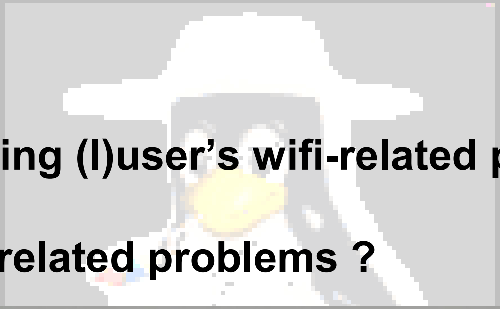
Wireless Security stress-free

Linux User Group of Mauritius -- http://www.lugm.org/

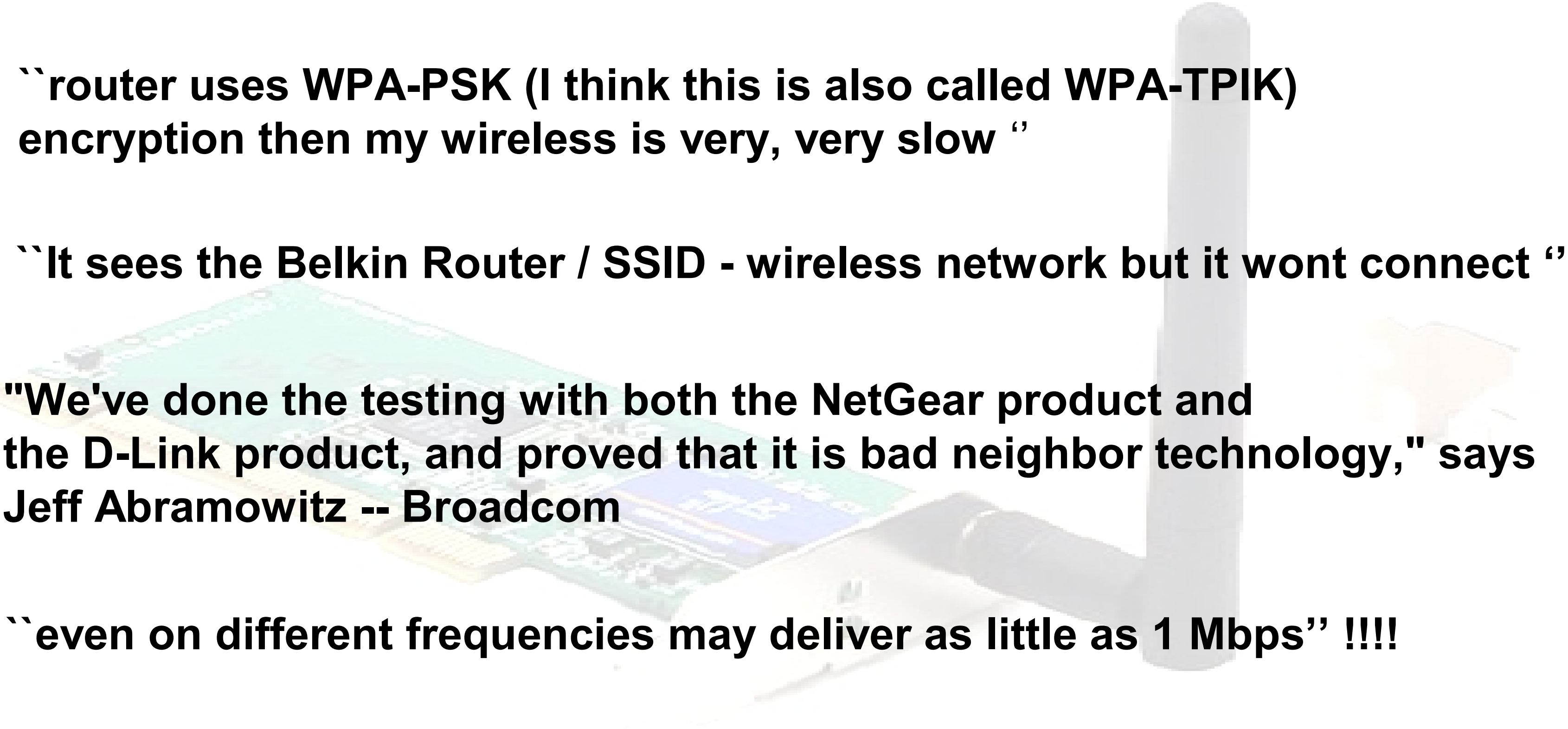
Frank - www.SysAdminDay.com

A few questions

- Who has ever managed Wireless Networks ?
- In a production environment ?
- WPA/WEP issues ?
- How much time you lost solving (l)user’s wifi-related problems ?
- What is your solution to wifi-related problems ?



Current state of IEEE 802.11 b/g products



``router uses WPA-PSK (I think this is also called WPA-TPIK) encryption then my wireless is very, very slow ‘’

``It sees the Belkin Router / SSID - wireless network but it wont connect “

"We've done the testing with both the NetGear product and the D-Link product, and proved that it is bad neighbor technology," says Jeff Abramowitz -- Broadcom

``even on different frequencies may deliver as little as 1 Mbps’’ !!!!

Why is wifi plagued ?

- WPA/WPA2 is a complicated protocol (mess)

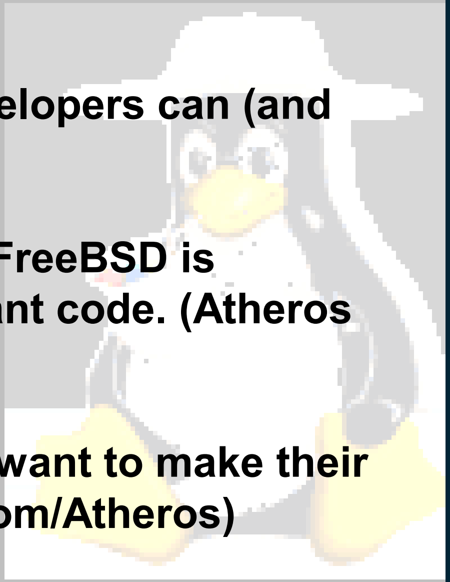
- Vendors introduce proprietary extensions to IEEE802.11b/g such as ``Super G’’

- Open Source /Free Software Developers can (and do) make mistakes

- wifi driver dev in Linux/NetBSD/FreeBSD is fragmented and contains redundant code. (Atheros Code/Licensing fiasco)

- Hardware makers still (!) do not want to make their documentation available (Broadcom/Atheros)

- Wifi-router code from vendor is ``Shoot and Forget’’ – Linksys WRT54G/GL



Another approach

- Use basic IEEE 802 b/g (relatively well tested stack)

- Push Authentication/Encryption outside of Kernel code

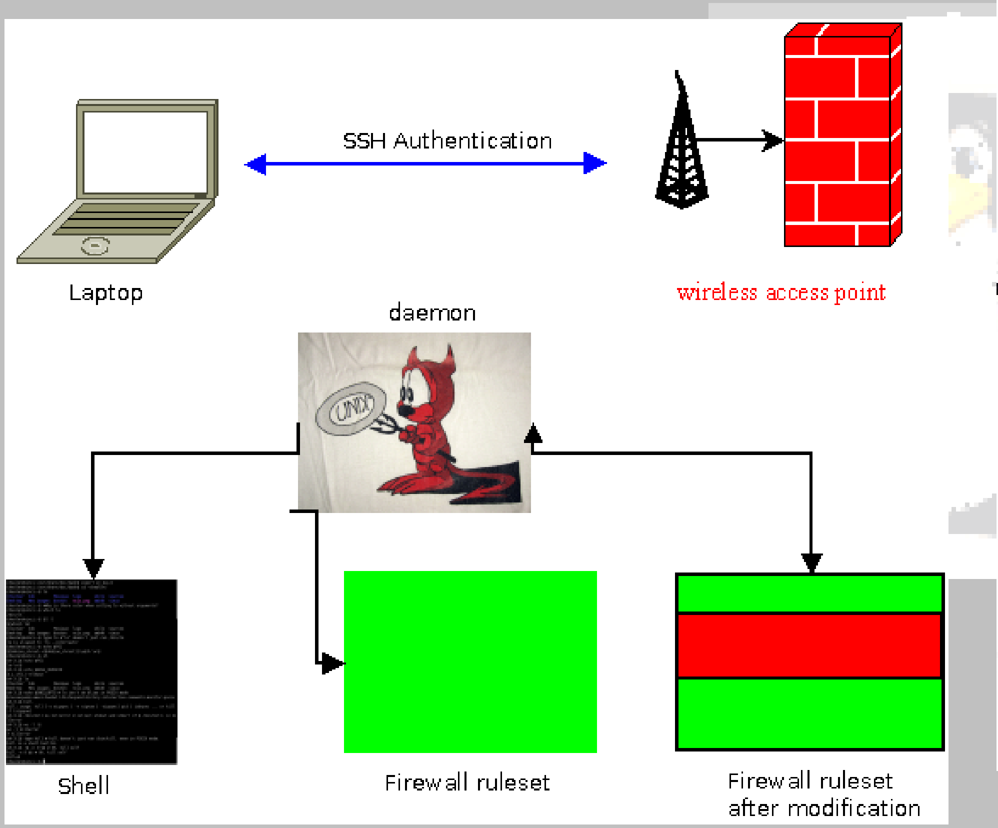
- Off-the-Shelf components (Old PCs do fine !)

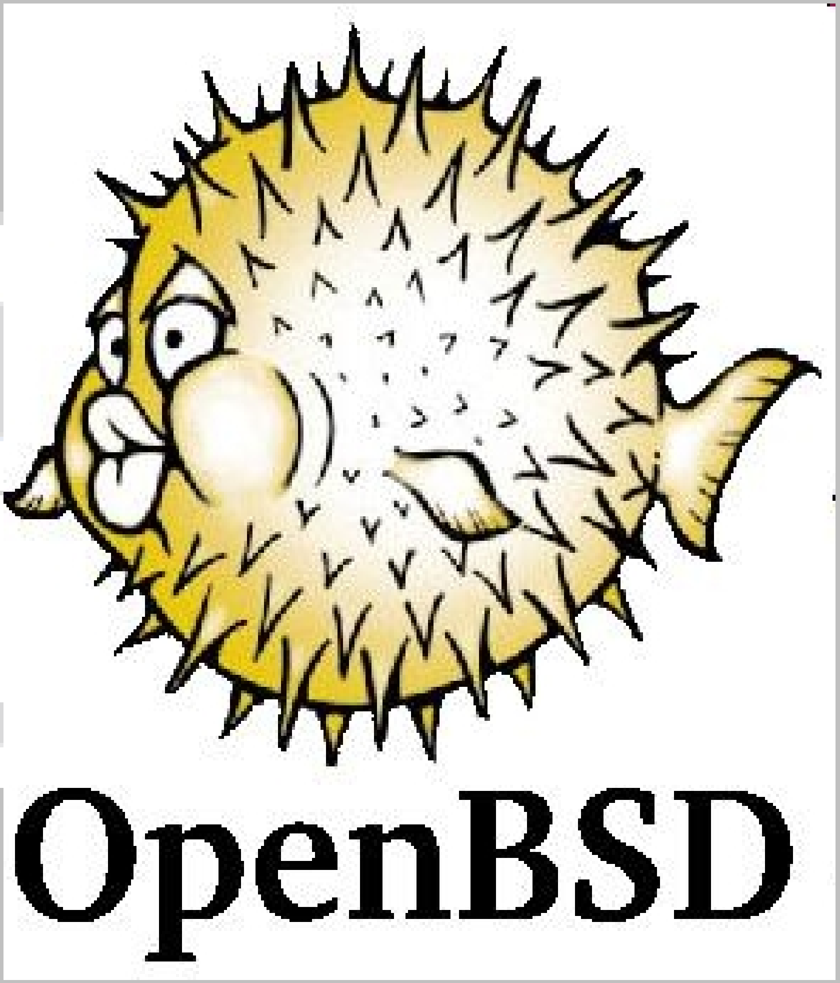
- OpenBSD (PF + Other cool stuff)

Authentication gateway

- Authpf – handles authentication & routing.

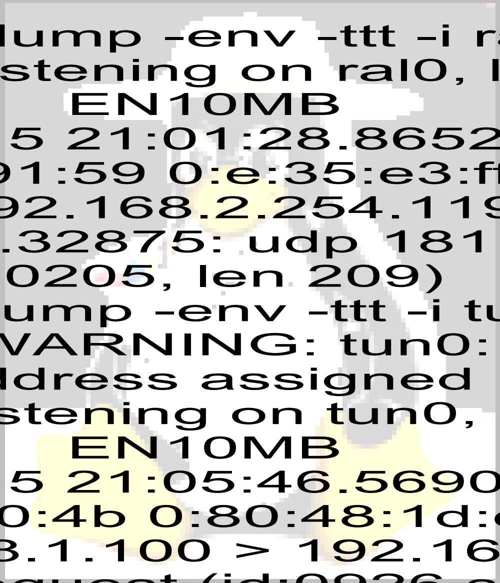
- User logs in through SSH, spawns a special Shell, which modifies the PF ruleset.





Authentication gateway (2) VPN

# allow authenticated hosts to connect to openvpn daemon
pass in quick on $wlan_if proto udp from $user_ip to ($wlan_if) port 1194 keep state



```
# tcpdump -env -ttt -i ral0
tcpdump: listening on ral0, link-type
EN10MB
Nov 15 21:01:28.865218
0:11:6b:34:91:59 0:e:35:e3:ff:51 0800
223: 192.168.2.254.1194 >
192.168.2.1.32875: udp 181 (ttl 64, id
20205, len 209)
# tcpdump -env -ttt -i tun0
tcpdump: WARNING: tun0: no IPv4
address assigned
tcpdump: listening on tun0, link-type
EN10MB
Nov 15 21:05:46.569068
be:88:12:eb:0:4b 0:80:48:1d:e:28 0800
98: 192.168.1.100 > 192.168.1.254:
icmp: echo request (id:0926 seq:1) (DF)
(ttl 64, id 0, len 84)
```

Tip: Use autossh/VBscript for Unix/Windows Clients to automatically login on disconnect

OpenSSH + PF bits

```
 Protocol 2
 ClientAliveInterval 15
 ClientAliveCountMax 3
```

```
pass in quick on $wifi_if proto tcp to ($wifi_if)
port ssh $tcp_flags (max-src-conn 30,
max-src-conn-rate 10/5,
overload <blacklist> flush global)
```

```
ps -ax | grep ssh    23664 p0  Is+     0:00.11
 -ssh: foo@192.168.2.4 (sshd)
```

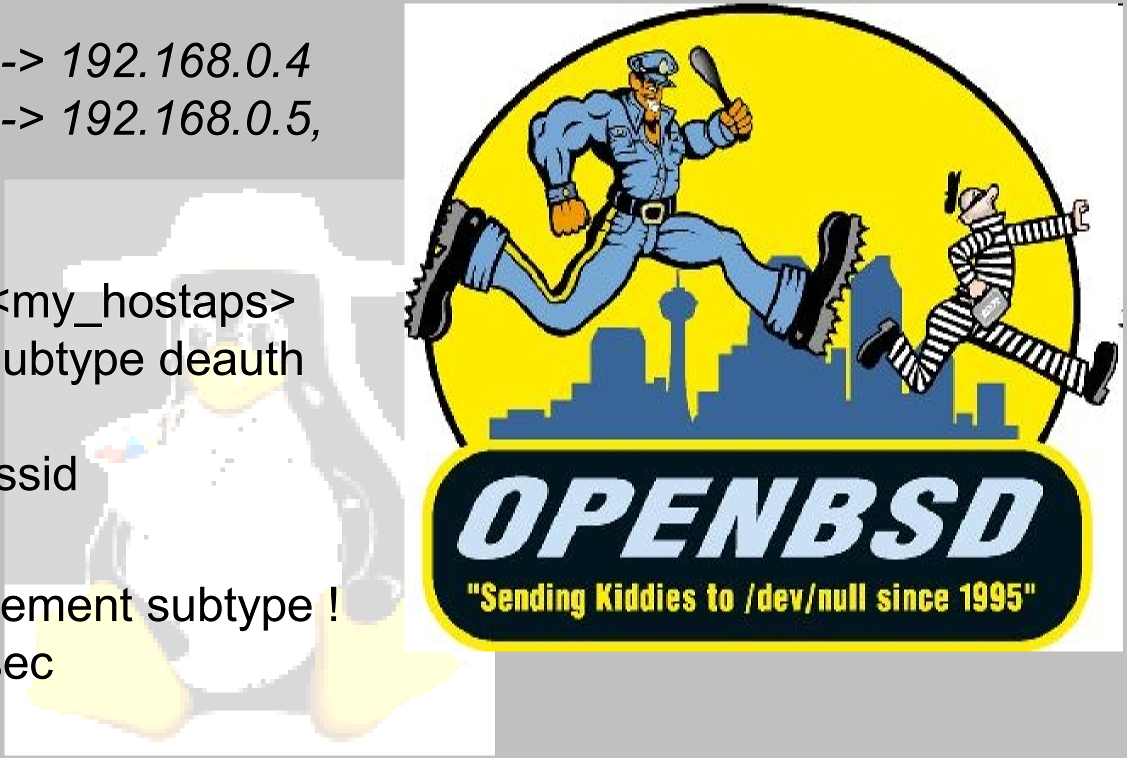
```
kill -TERM 23664
```

Going further with hostap !

```
table <myaccesspoints> const
{                 00:00:25:c1:38:18 -> 192.168.0.4
,                 00:00:30:d6:40:29 -> 192.168.0.5,
                        }
```

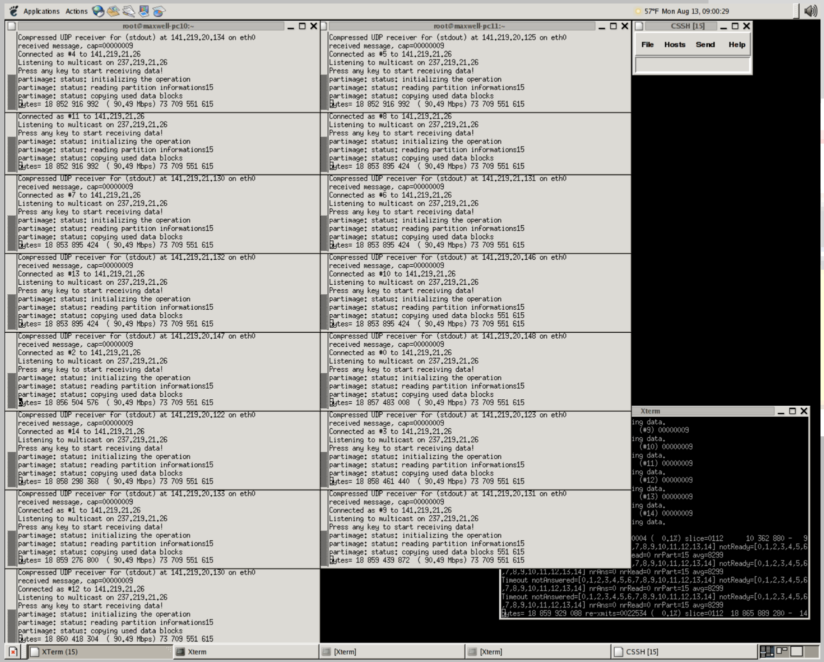
```
hostap handle type data bssid !<my_hostaps>
\ with frame type management subtype deauth
reason auth expire
\ from &bssid to &from bssid &bssid
```

```
 hostap handle skip type management subtype !
  beacon \ with log rate 100 / 5 sec
```



System Integration

- ClusterSSH – SSH `multiplexor’
- Cacti – RRD Graphs
- Swatch – Log analyzer
- Mail server – Send Alerts



```
Compressed UDP receiver for (stdout) at 141.219.20.134 on eth0
received message, cap=00000009
Connected as #4 to 141.219.21.26
Listening to multicast on 237.219.21.26
Press any key to start receiving data!
partimage: status: initializing the operation
partimage: status: reading partition informations15
partimage: status: copying used data blocks
Bytes= 18 852 916 992  ( 90.49 Mbps) 73 709 551 615
```

```
Connected as #11 to 141.219.21.26
Listening to multicast on 237.219.21.26
Press any key to start receiving data!
partimage: status: initializing the operation
partimage: status: reading partition informations15
partimage: status: copying used data blocks
Bytes= 18 852 916 992  ( 90.49 Mbps) 73 709 551 615
```

```
Compressed UDP receiver for (stdout) at 141.219.21.130 on eth0
received message, cap=00000009
Connected as #7 to 141.219.21.26
Listening to multicast on 237.219.21.26
Press any key to start receiving data!
partimage: status: initializing the operation
partimage: status: reading partition informations15
partimage: status: copying used data blocks
Bytes= 18 853 895 424  ( 90.49 Mbps) 73 709 551 615
```

```
Compressed UDP receiver for (stdout) at 141.219.21.132 on eth0
received message, cap=00000009
Connected as #13 to 141.219.21.26
Listening to multicast on 237.219.21.26
Press any key to start receiving data!
partimage: status: initializing the operation
partimage: status: reading partition informations15
partimage: status: copying used data blocks
Bytes= 18 853 895 424  ( 90.49 Mbps) 73 709 551 615
```

```
Compressed UDP receiver for (stdout) at 141.219.20.147 on eth0
received message, cap=00000009
Connected as #2 to 141.219.21.26
Listening to multicast on 237.219.21.26
Press any key to start receiving data!
partimage: status: initializing the operation
partimage: status: reading partition informations15
partimage: status: copying used data blocks
Bytes= 18 856 504 576  ( 90.49 Mbps) 73 709 551 615
```

```
Compressed UDP receiver for (stdout) at 141.219.20.122 on eth0
received message, cap=00000009
Connected as #14 to 141.219.21.26
Listening to multicast on 237.219.21.26
Press any key to start receiving data!
partimage: status: initializing the operation
partimage: status: reading partition informations15
partimage: status: copying used data blocks
Bytes= 18 858 298 368  ( 90.49 Mbps) 73 709 551 615
```

```
Compressed UDP receiver for (stdout) at 141.219.20.133 on eth0
received message, cap=00000009
Connected as #1 to 141.219.21.26
Listening to multicast on 237.219.21.26
Press any key to start receiving data!
partimage: status: initializing the operation
partimage: status: reading partition informations15
partimage: status: copying used data blocks
Bytes= 18 859 276 800  ( 90.49 Mbps) 73 709 551 615
```

```
Compressed UDP receiver for (stdout) at 141.219.20.130 on eth0
received message, cap=00000009
Connected as #12 to 141.219.21.26
Listening to multicast on 237.219.21.26
Press any key to start receiving data!
partimage: status: initializing the operation
partimage: status: reading partition informations15
partimage: status: copying used data blocks
Bytes= 18 860 418 304  ( 90.49 Mbps) 73 709 551 615
```

```
Compressed UDP receiver for (stdout) at 141.219.20.125 on eth0
received message, cap=00000009
Connected as #5 to 141.219.21.26
Listening to multicast on 237.219.21.26
Press any key to start receiving data!
partimage: status: initializing the operation
partimage: status: reading partition informations15
partimage: status: copying used data blocks
Bytes= 18 852 916 992  ( 90.49 Mbps) 73 709 551 615
```

```
Connected as #8 to 141.219.21.26
Listening to multicast on 237.219.21.26
Press any key to start receiving data!
partimage: status: initializing the operation
partimage: status: reading partition informations15
partimage: status: copying used data blocks
Bytes= 18 853 895 424  ( 90.49 Mbps) 73 709 551 615
```

```
Compressed UDP receiver for (stdout) at 141.219.21.131 on eth0
received message, cap=00000009
Connected as #6 to 141.219.21.26
Listening to multicast on 237.219.21.26
Press any key to start receiving data!
partimage: status: initializing the operation
partimage: status: reading partition informations15
partimage: status: copying used data blocks
Bytes= 18 853 895 424  ( 90.49 Mbps) 73 709 551 615
```

```
Compressed UDP receiver for (stdout) at 141.219.20.146 on eth0
received message, cap=00000009
Connected as #10 to 141.219.21.26
Listening to multicast on 237.219.21.26
Press any key to start receiving data!
partimage: status: initializing the operation
partimage: status: reading partition informations15
partimage: status: copying used data blocks 551 615
Bytes= 18 853 895 424  ( 90.49 Mbps) 73 709 551 615
```

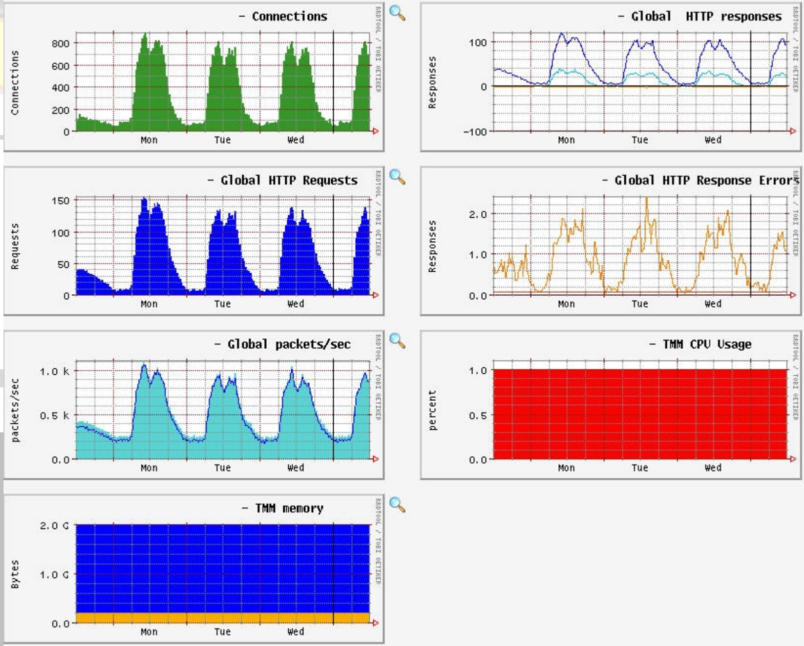
```
Compressed UDP receiver for (stdout) at 141.219.20.148 on eth0
received message, cap=00000009
Connected as #0 to 141.219.21.26
Listening to multicast on 237.219.21.26
Press any key to start receiving data!
partimage: status: initializing the operation
partimage: status: reading partition informations15
partimage: status: copying used data blocks
Bytes= 18 857 483 008  ( 90.49 Mbps) 73 709 551 615
```

```
Compressed UDP receiver for (stdout) at 141.219.20.123 on eth0
received message, cap=00000009
Connected as #3 to 141.219.21.26
Listening to multicast on 237.219.21.26
Press any key to start receiving data!
partimage: status: initializing the operation
partimage: status: reading partition informations15
partimage: status: copying used data blocks
Bytes= 18 858 461 440  ( 90.49 Mbps) 73 709 551 615
```

```
Compressed UDP receiver for (stdout) at 141.219.20.131 on eth0
received message, cap=00000009
Connected as #9 to 141.219.21.26
Listening to multicast on 237.219.21.26
Press any key to start receiving data!
partimage: status: initializing the operation
partimage: status: reading partition informations15
partimage: status: copying used data blocks 551 615
Bytes= 18 859 439 872  ( 90.49 Mbps) 73 709 551 615
```

```
ing data.
  (#9) 00000009
ing data.
  (#10) 00000009
ing data.
  (#11) 00000009
ing data.
  (#12) 00000009
ing data.
  (#13) 00000009
ing data.
  (#14) 00000009
ing data.

0004 (  0.1%) slice=0112      10 362 880 -   9
,7,8,9,10,11,12,13,14] notReady=[0,1,2,3,4,5,6
ead=0 nrPart=15 avg=8299
,7,8,9,10,11,12,13,14] notReady=[0,1,2,3,4,5,6
,7,8,9,10,11,12,13,14] nrAns=0 nrRead=0 nrPart=15 avg=8299
Timeout notAnswered=[0,1,2,3,4,5,6,7,8,9,10,11,12,13,14] notReady=[0,1,2,3,4,5,6
,7,8,9,10,11,12,13,14] nrAns=0 nrRead=0 nrPart=15 avg=8299
Timeout notAnswered=[0,1,2,3,4,5,6,7,8,9,10,11,12,13,14] notReady=[0,1,2,3,4,5,6
,7,8,9,10,11,12,13,14] nrAns=0 nrRead=0 nrPart=15 avg=8299
Bytes= 18 859 929 088 re-xmits=0022534 (  0.1%) slice=0112  18 865 889 280 -  14
```



Zen sysadmin