Boulevard of Broken Networks
Agenda

• Introduction
• Networks
• Findings
• What you can do
Introduction

Who am I?
Introduction

Why this presentation?

- NOT SURE IF NETWORK UNDER MAINTENANCE
- OR PS3 BROKEN
Introductions

What will we talk about?
How do we see all this?

We call in for backup

KEEP CALM
I'M JUST KIDDING
How do we see all this?

We are in the middle of the action

Attention to detail
How do we see all this?

Simple tools

snoopdog
tcpdump
perl
arpwatch
snmp[trap]
Peer connections

Types of network layouts

- Ring
- Mesh
- Star
- Fully Connected
- Line
- Tree
- Bus
Network diagram 1

- peer 1
- peer 2
- peer 3
- peer 4
Network diagram 2
Network diagram 3

Transit 1

Transit 2

Torix

Peer Switch

vlan 20

vlan 30

Peer Router

Transit 3

Layer 3 here

phy cable

.1q

PTP
Network diagram 4

Layer 3 here

Torix

Peer Switch

Transit 1

Transit 2

Peer Router

Customer

vlan 10

phy cable
.

1q
Network diagram 5

Torix

Transit 1

Customer

Peer Switch

Layer 3 here (secondary addresses)

Transit 2

Peer Router

Customer

LAN-X (basic) (no .1q support)

vlan 10
Network diagram 6
Network diagram 7
Network diagram 8
Physical

Where Internet problems start
Physical: survey

Facebook survey:

“If you were to crimp 100 RJ45/Ethernet copper cables, how many would you get wrong for any reasons, either wrong pin-out, bad crimp, upside down ends, etc.?”

Polls: 83
**Physical: survey**

....survey says

<table>
<thead>
<tr>
<th>Range</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-5</td>
<td>62%</td>
</tr>
<tr>
<td>6-10</td>
<td>22%</td>
</tr>
<tr>
<td>11-15</td>
<td>5%</td>
</tr>
<tr>
<td>16-20</td>
<td>11%</td>
</tr>
</tbody>
</table>
Physical: survey

....survey had great suggestions

“I’d just put my monoprice express order in”

“I am with Paul, zero as my summer student would know his/her job depends on it.”
Physical: optical

Splice or buy fiber?

Majority buy

Might clean
Physical: error tree

1. Receive Frame
2. Receive enable?
   - yes
     1. Frame too long?
        - yes
          1. Extra bits?
             - yes
               - Frame too long
             - no
               - Return to previous step
        - no
          1. Valid frame check sequence?
             - yes
               - Valid length/type field?
                  - yes
                    - Disassemble frame
                  - no
                    - Receive OK
             - no
               - Length Error

   - no
     1. Valid length/type field?
        - yes
          - Disassemble frame
        - no
          - Length Error
### Physical: errors

<table>
<thead>
<tr>
<th>Port</th>
<th>Align-Err</th>
<th>FCS-Err</th>
<th>Xmit-Err</th>
<th>Rcv-Err</th>
<th>UnderSize</th>
<th>OutDiscards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/27</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Eth1/30</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>35</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Eth2/21</td>
<td>4</td>
<td>415</td>
<td>0</td>
<td>449</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Eth2/23</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Eth2/24</td>
<td>0</td>
<td>87</td>
<td>0</td>
<td>97</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Eth2/25</td>
<td>2</td>
<td>3756162</td>
<td>0</td>
<td>3795765</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Eth2/30</td>
<td>0</td>
<td>216</td>
<td>0</td>
<td>247</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Eth3/4</td>
<td>0</td>
<td>6102</td>
<td>0</td>
<td>6102</td>
<td>257831</td>
<td>0</td>
</tr>
<tr>
<td>Eth3/15</td>
<td>2</td>
<td>36241</td>
<td>0</td>
<td>36243</td>
<td>1479957</td>
<td>0</td>
</tr>
<tr>
<td>Eth3/18</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>121</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Eth3/20</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Eth3/26</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>16734</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Eth3/30</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>253212352</td>
</tr>
<tr>
<td>Eth4/20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>939</td>
<td>0</td>
</tr>
<tr>
<td>Eth7/6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>975735</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Giants SQETest-Err Deferred-Tx IntMacTx-Er IntMacRx-Er Symbol-Err</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth3/15</td>
<td>0     -- 0 0 0 2521768</td>
</tr>
<tr>
<td>Eth3/26</td>
<td>1350  -- 0 0 0 0</td>
</tr>
</tbody>
</table>
### Ethertypes and MACs

<table>
<thead>
<tr>
<th>Ethertype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0800</td>
<td>IPv4</td>
</tr>
<tr>
<td>0x0806</td>
<td>ARP</td>
</tr>
<tr>
<td>0x6002</td>
<td>MOP/RC</td>
</tr>
<tr>
<td>0x86DD</td>
<td>IPv6*</td>
</tr>
<tr>
<td>0x8809</td>
<td>LACP*</td>
</tr>
<tr>
<td>0x88CC</td>
<td>LLDP</td>
</tr>
<tr>
<td>01:80:C2:00:00:00</td>
<td>IEEE 802.1D</td>
</tr>
<tr>
<td>FF:FF:FF:FF:FF:FF:FF</td>
<td>Broadcast</td>
</tr>
</tbody>
</table>
STP: BPDUs

• Using single location for collection
• We always suggest peers turn off stp, why do you even need it facing us? Or other people in some cases.
• 117 Peers, 14 sending us BPDUs.
• Weird: two peers sending BPDUs from L3 interfaces. [vendor specific]
• Note: BPDUs are CPU processed, not line card processed.
FF: bcast

- Always interesting to see what ends up here.
- Normally at the IX we should only see ARP who-has.
ARP: 0x0806/FF

<table>
<thead>
<tr>
<th>Filtering</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of arp requests (who-has) in a 24 (HR)</td>
<td>3.3 - 3.4 million</td>
</tr>
<tr>
<td>Total number of arp requests to disconnected peers</td>
<td>629k – 786k</td>
</tr>
<tr>
<td>Valid requests</td>
<td>2.6 – 2.7 million</td>
</tr>
<tr>
<td>Invalid requests (percentage)</td>
<td>19-22%</td>
</tr>
<tr>
<td>Arp requests that are not part of 206.108.34.x/23?</td>
<td>3</td>
</tr>
</tbody>
</table>
MOP: 0x6002

- Maintenance Operation Protocol
  - Remote loading of software
  - Loopback testing
- MOP RC: layer 2 frame
- Enabled by default on many routers/ethernet interfaces
- Removing `transport input mop` from the VTY lines will **not** disable the MOP RC functionality
- Bonus: Linux tools latd/moprc
FF: bcast DNS

dns

root@snoopdog:/data/captures/snoop_ispsummit# tcpdump -nr listenAll_20131101.pcap 'ether dst ff:ff:ff:ff:ff:ff and not arp'

IP 206.108.34.YYY.53520 > 255.255.255.255.53: 308+ A? www.google.com
IP 206.108.34.YYY.57661 > 255.255.255.255.53: 309+ PTR? 33.158.104.38.in-addr.arpa.
IP 206.108.34.YYY.49531 > 255.255.255.255.53: 310+ PTR? 137.40.54.154.in-addr.arpa.
IP 206.108.34.YYY.51244 > 255.255.255.255.53: 311+ PTR? 165.40.54.154.in-addr.arpa.
IP 206.108.34.YYY.56892 > 255.255.255.255.53: 312+ PTR? 181.27.54.154.in-addr.arpa.
IP 206.108.34.YYY.51672 > 255.255.255.255.53: 313+ PTR? 5.42.54.154.in-addr.arpa.
IP 206.108.34.YYY.55308 > 255.255.255.255.53: 314+ PTR? 22.29.54.154.in-addr.arpa.
IP 206.108.34.YYY.58881 > 255.255.255.255.53: 315+ PTR? 10.5.54.154.in-addr.arpa.
IP 206.108.34.YYY.54027 > 255.255.255.255.53: 316+ PTR? 130.103.104.38.in-addr.arpa.
IP 206.108.34.YYY.59046 > 255.255.255.255.53: 317+ PTR? 254.103.104.38.in-addr.arpa.
IP 206.108.34.YYY.52373 > 255.255.255.255.53: 318+ PTR? 120.254.85.209.in-addr.arpa.
IP 206.108.34.YYY.56727 > 255.255.255.255.53: 319+ PTR? 150.240.85.209.in-addr.arpa.
RWHO: ~0x0800/FF

PC routers

Some (harmless) fun with this peer
1. Download source code.
2. Recompile with changes.
3. Send ‘suggestions’ to a peer.

root@snoopdog:/tmp/netkit-rwho-0.17/rwhod# rwho -a

nistor    torix-says-turn-off-rwho:pts/1  Oct  26 23:35  1:36
nistor    torix-says-turn-off-rwho:pts/2  Oct  27  00:14
p?u?      tr!!l:pts/2    Oct  19  00:26  99:59
p?u?      tr!!l:pts/7    Oct  19  00:29  99:59

root@snoopdog:/tmp/netkit-rwho-0.17/rwhod#
NTP: It’s what time?

TorIX: “We saw some issues around 20:09 EDT, could you quickly check your side, any errors you notice in the logs? Can you confirm the time?”

Peer: “I can’t tell” or “yes we have errors, not sure on time”

33w6d: %LINEPROTO-SP-5-UPDOWN: Line protocol on Interface FastEthernet1/36, changed state to down
33w6d: %LINK-3-UPDOWN: Interface FastEthernet1/36, changed state to up
33w6d: %LINK-SP-3-UPDOWN: Interface FastEthernet1/36, changed state to up
33w6d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/36, changed state to up
NTP: It’s what time?

Router# `show clock detail`

*02:58:19.871 UTC Sun Mar 27 2011

Time source is hardware calendar

Hardware calendar, fabulous right?  Nope!
LLDP: 0x88CC

14:09:05.562344  AABBCDDEEFF > 01:80:c2:00:00:0e, ethertype LLDP (0x88cc), length 239
   Chassis ID TLV (1), length 7
   Port ID TLV (2), length 15
      Subtype Interface Name (5): Gi0/7/0/16.610
   Time to Live TLV (3), length 2: TTL 120s
   System Name TLV (5), length 27: TOROONXNPED01.PEER-NOT-NAMED.COM
   System Description TLV (6), length 87
      Cisco IOS XR Software, Version 4.1.1[Default]\0x0aCopyright (c) 2012 by Cisco Systems, Inc.
   Port Description TLV (4), length 27: GigabitEthernet0/7/0/16.610
   System Capabilities TLV (7), length 4
      System Capabilities [Router] (0x0010)
      Enabled Capabilities [Router] (0x0010)
   Management Address TLV (8), length 12
      Management Address length 5, AFI IPv4 (1): 142.xxx.yyy.2
      Interface Index Interface Numbering (2): 1540
   Management Address TLV (8), length 24
      Management Address length 17, AFI IPv6 (2): 2604:XXXX::YYYY:ZZZZ:1002
      Interface Index Interface Numbering (2): 1540
   End TLV (0), length 0
OSPF: 0x800

23:53:19.566225 aabbccddeeff > 01:00:5e:00:00:05, ethertype IPv4 (0x0800), length 90:
(tos 0xc0, ttl 1, id 6406, offset 0, flags [none], proto OSPF (89), length 76)
206.108.34.XXX > 224.0.0.5: OSPFv2, Hello, length 56 [len 44]
  Router-ID XXX.XXX.XXX.XXX, Backbone Area, Authentication Type: none (0)
  Options [External, LLS]
    Hello Timer 10s, Dead Timer 40s, Mask 255.255.254.0, Priority 1
    LLS: checksum: 0xfff6, length: 3
      Extended Options (1), length: 4
        Options: 0x00000001 [LSDB resync]
BGP: ~0x8000 / ~0x86DD

- wrong prefix filters
- wrong route-maps
- ignoring your peers
### BGP: wrong prefix list

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>30.0.0.0/22</td>
<td>206.108.34.xx</td>
<td>54321</td>
</tr>
<tr>
<td>31.0.0.0/19</td>
<td>206.108.34.xx</td>
<td>54321</td>
</tr>
<tr>
<td>66.0.0.0/24</td>
<td>206.108.34.xx</td>
<td>54321 3333</td>
</tr>
<tr>
<td>99.100.0.0/18</td>
<td>206.108.34.xx</td>
<td>54321 2222</td>
</tr>
<tr>
<td>101.255.0.0/20</td>
<td>206.108.34.xx</td>
<td>54321 100 200</td>
</tr>
<tr>
<td>150.0.0.0/23</td>
<td>206.108.34.xx</td>
<td>54321 4444</td>
</tr>
</tbody>
</table>
BGP: wrong route-map

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>206.108.34.xx</td>
<td>54321</td>
</tr>
<tr>
<td>10.0.21.1/32</td>
<td>206.108.34.xx</td>
<td>54321</td>
</tr>
<tr>
<td>10.0.21.2/32</td>
<td>206.108.34.xx</td>
<td>54321</td>
</tr>
<tr>
<td>10.0.21.3/32</td>
<td>206.108.34.xx</td>
<td>54321</td>
</tr>
<tr>
<td>30.0.0.0/22</td>
<td>206.108.34.xx</td>
<td>54321</td>
</tr>
<tr>
<td>31.0.0.0/19</td>
<td>206.108.34.xx</td>
<td>54321</td>
</tr>
<tr>
<td>66.0.0.0/24</td>
<td>206.108.34.xx</td>
<td>54321 3333</td>
</tr>
<tr>
<td>99.100.0.0/18</td>
<td>206.108.34.xx</td>
<td>54321 2222</td>
</tr>
</tbody>
</table>
SNMP: In your network?
SNMP: errors in your network?

IF-MIB::ifInErrors.369098853 = 1364386973
IF-MIB::ifInErrors.436326400 = 1364386338
IF-MIB::ifInErrors.436830208 = 3756164
IF-MIB::ifInDiscards.436240384 = 511
IF-MIB::ifOutDiscards.437297152 = 6138
EtherLike-MIB::dot3StatsAlignmentErrors.436326400 = 1535
EtherLike-MIB::dot3StatsFCSErrors.436830208 = 3756162
Homework

Things you or your staff should do

.. and no excuses!

icq 1429373
Homework

At a minimum

Check network for phy issues
Ensure all your devices are time sync’d
turn off services you don’t use
Are all of your neighbour sessions up?
Are you monitoring?