28C3 NOC Review
Topics

• Uplink
• Core / Distribution
• Access
• Wireless
• Colo

• Monitoring
• Abuse
• VPN
• Rules
Uplink

- 2*10GE (1470nm, 1490nm) building uplink over CWDM
- 2 10GE Transit (KPN, HE.net)
- 3 1GE Transit (EuroTransit, Carrier51, CCC)
- several Peerings at ECIX Berlin
- Brocade MLX-4 - BGP border router
Core / Distribution

- Router:
  - Juniper MX80 (A87)
  - Force10 E600 (D57)
  - Cisco 6509 - SUP720-3BXL (A85)

- Switches
  - Cisco 6509 - SUP720-3BXL (C57)
  - 4 Cisco 2960S as Stack (B90.01)
# Top 10 Outbound ASN

<table>
<thead>
<tr>
<th>ASN</th>
<th>Descr</th>
<th>Traffic avg Mbit/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>3320</td>
<td>DTAG</td>
<td>~600m</td>
</tr>
<tr>
<td>24940</td>
<td>Hetzner</td>
<td>~300m</td>
</tr>
<tr>
<td>31334</td>
<td>KDG</td>
<td>~250m</td>
</tr>
<tr>
<td>680</td>
<td>DFN</td>
<td>~230m</td>
</tr>
<tr>
<td>20825</td>
<td>UnityMedia</td>
<td>~220m</td>
</tr>
</tbody>
</table>
Wireless LAN

- 1* Cisco WLC 5508
- 30* Cisco 3502i (a/g/n)
- 6* 1242 (a/g)
- Bug: enabling a v4 acl that passes all traffic will disable v6 bridging
- works great: leeching with 30Mbit/s, videochatting
Stats WLAN

- maximum simultaneous users: \(~1350\)
- average users per AP: 87.3
- unique users detected: 3300
- client distribution: .11a: 11\% -- .11g: 30\% -- .11n (2.4ghz): 36\% -- .11n(5ghz): 23\%
- traffic distribution: .11a: 10\% -- .11g: 16\% -- .11n (2.4ghz): 21\% -- .11n(5ghz): 53\%
Colo

- 2 Switches
- 2*10GE Uplink
- 48*GE Downlink
- smaller than last year
- plz bring better cases
c3netmon
Realtime 2013 data served by nodes + websockets
Thanks to the HOC POC and ERT Team for providing the data.
Detailed graphs can be found here.

DATA SENT  DATA RECEIVED
91246 GB  23338 GB

BANDWIDTH
Out: 4557mbit/s (6496mbit/s)  In: 1760mbit/s (2346mbit/s)

CLIENTS
Wired: 1230 (1446)  Wireless: 1228 (1436)

RADIATION LEVEL
CPM @ POC: 32 (37)

WIRELESS BAND USAGE
802.11: 85  80: 95  2.4GHz: 551  5GHz: 323

OPENBEACON (ROKET)
Photo visible via OpenBeacon: 104 (149)

IP PROTOCOL DISTRIBUTION
IPv4: 94%  IPv6: 5%

Note: Values in parentheses are peaks.
Historical data in JSON format is available here. Current values for your own projects can be found here.
c3netmon code will be released on github.com/FremarkGmbh/c3netmon-public shortly after the congress.
If you have any questions contact morphaus@morphushome.net.

Freitag, 30. Dezember 2011
Icinga

- ~200 Hosts
- ~1100 Services
- All Equipment
  - Servers, Routers, Switches, APs...
- Environment
- Congestion
- Attacks
- IRC Bot for Alarms
More tools!

- as-stats (AS-based sFlow analysis)
- MRTG
- ring.nlnog.net
Abuse

- PHP 0day
  - against an online shop via a tor exit node in the colo (register stuff in the wiki)
  - against a news portal
- udp flood from amazon ec2 against our DNS/DHCP Server
- YOU DoSed events.ccc.de ;) (just kidding, too weak setup, fixed now)
VPN

- 20 Beacons with Congress Network
- 150mbit Traffic peak
- dn42 & ChaosVPN Peering
Rules

- don’t unplug switches
- talk to us if:
  - the switch is too loud
  - you want to replace it with your own
  - wallsockets are usable - most at 1G
Questions??

We love the NOC team 😊