

28C3 NOC Review

Topics

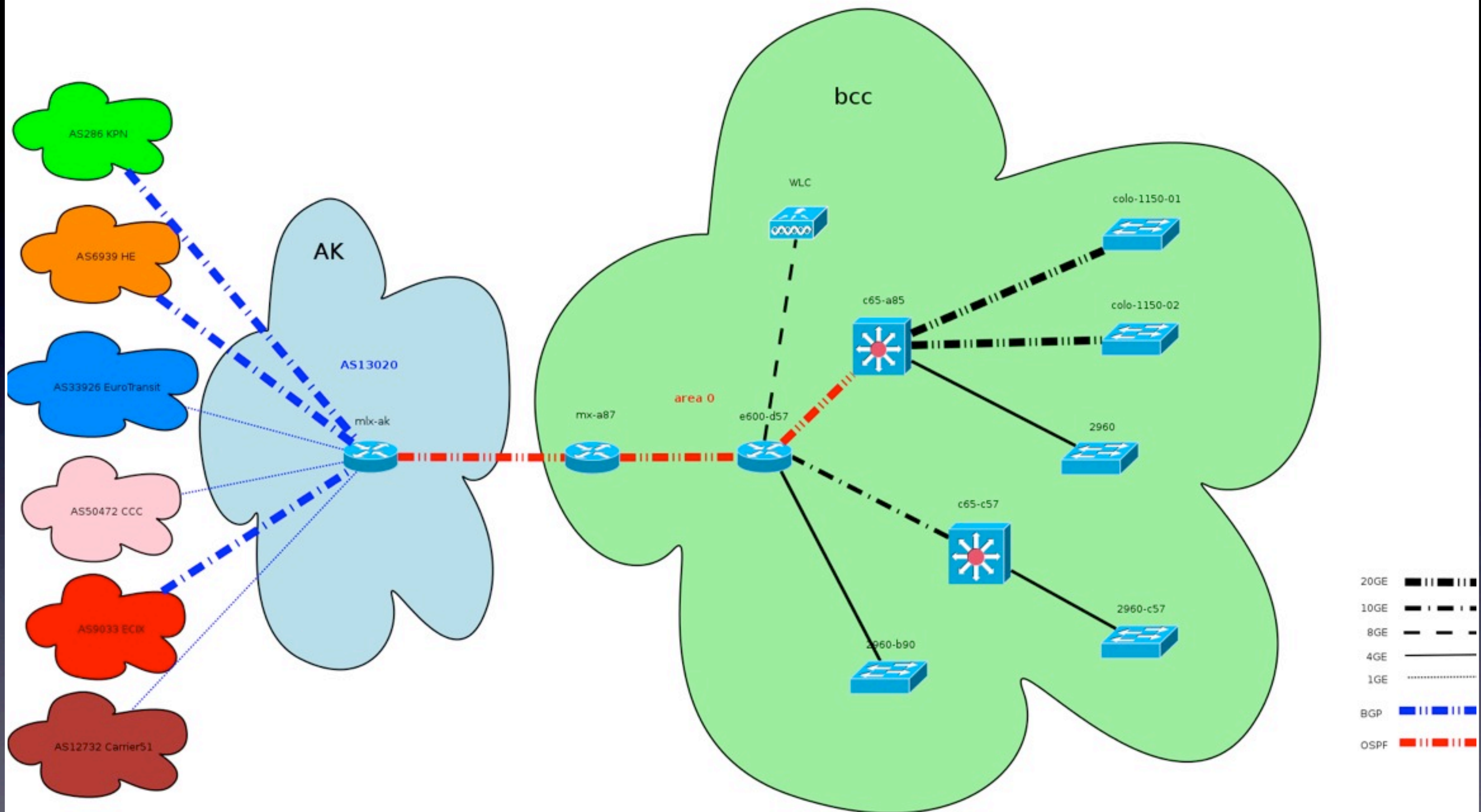
- Uplink
- Core / Distribution
- Access
- Wireless
- Colo
- Monitoring
- Abuse
- VPN
- Rules

Uplink

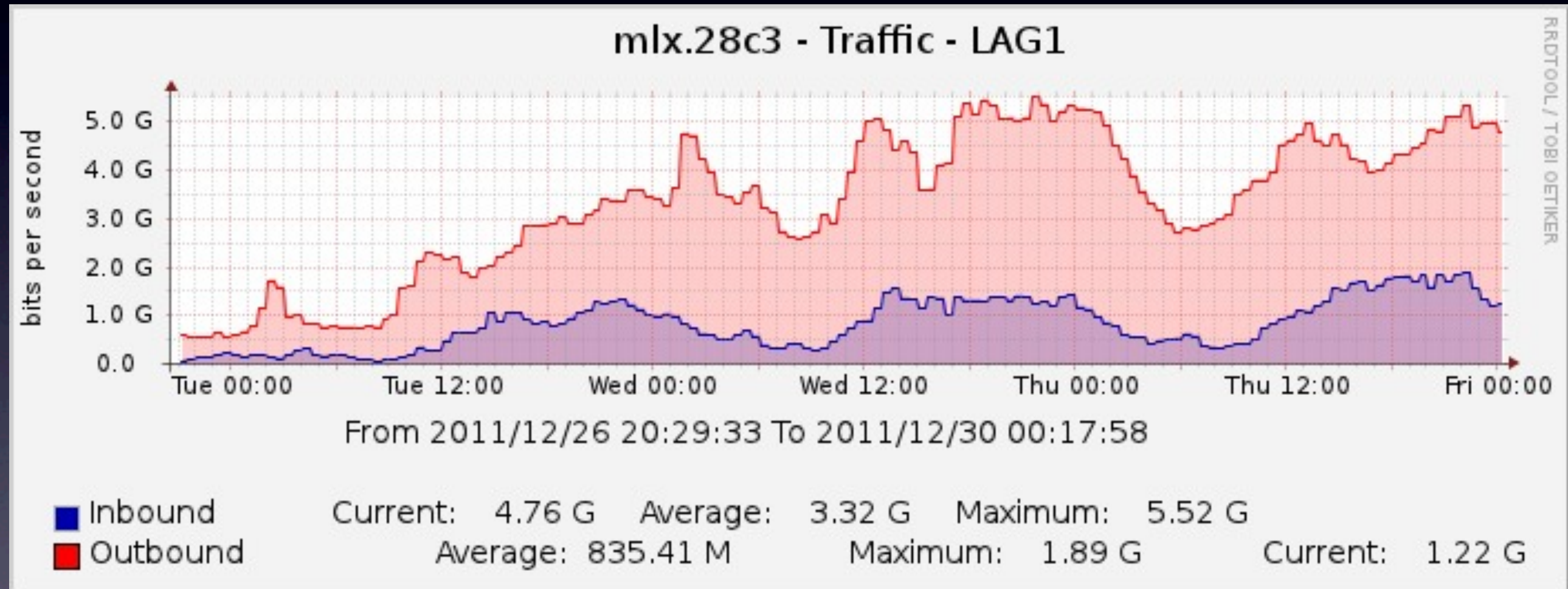
- 2*10GE (1470nm, 1490nm) building uplink over CWDM
- 2 10GE Transit (KPN, HE.net)
- 3 1GE Transit (EuroTransit, Carrier51, CCC)
- several Peerings at ECIX Berlin
- Brocade MLX-4 - BGP border router

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)



Stats



Top 10 Outbound ASN

ASN	Descr	Traffic avg Mbit/s
3320	DTAG	~600m
24940	Hetzner	~300m
31334	KDG	~250m
680	DFN	~230m
20825	UnityMedia	~220m

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

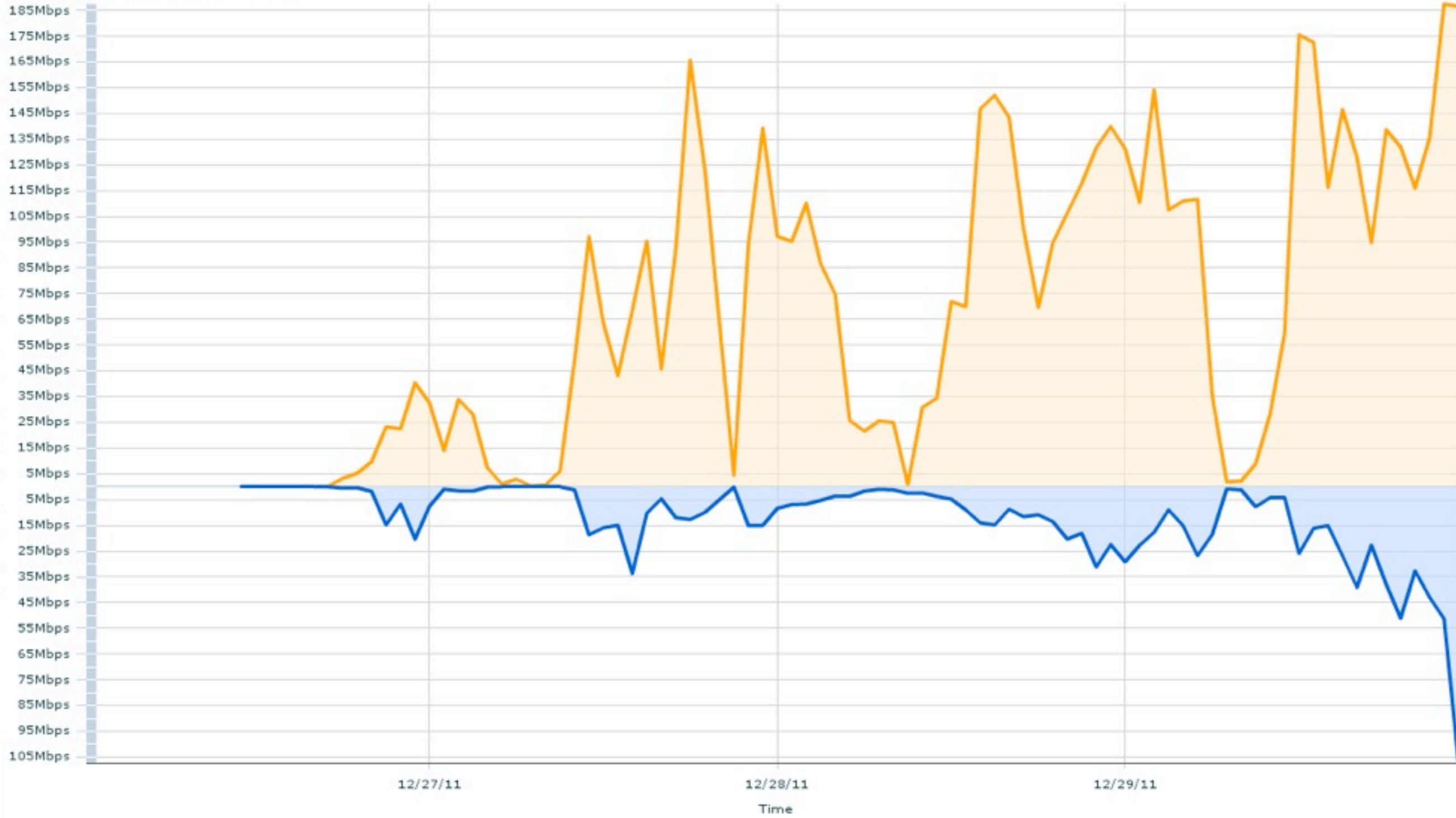
Stats WLAN

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

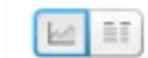
Client Traffic

6h | 1d | 1w | 2w | 4w | 3m | 6m | 1y | Custom

Bandwidth



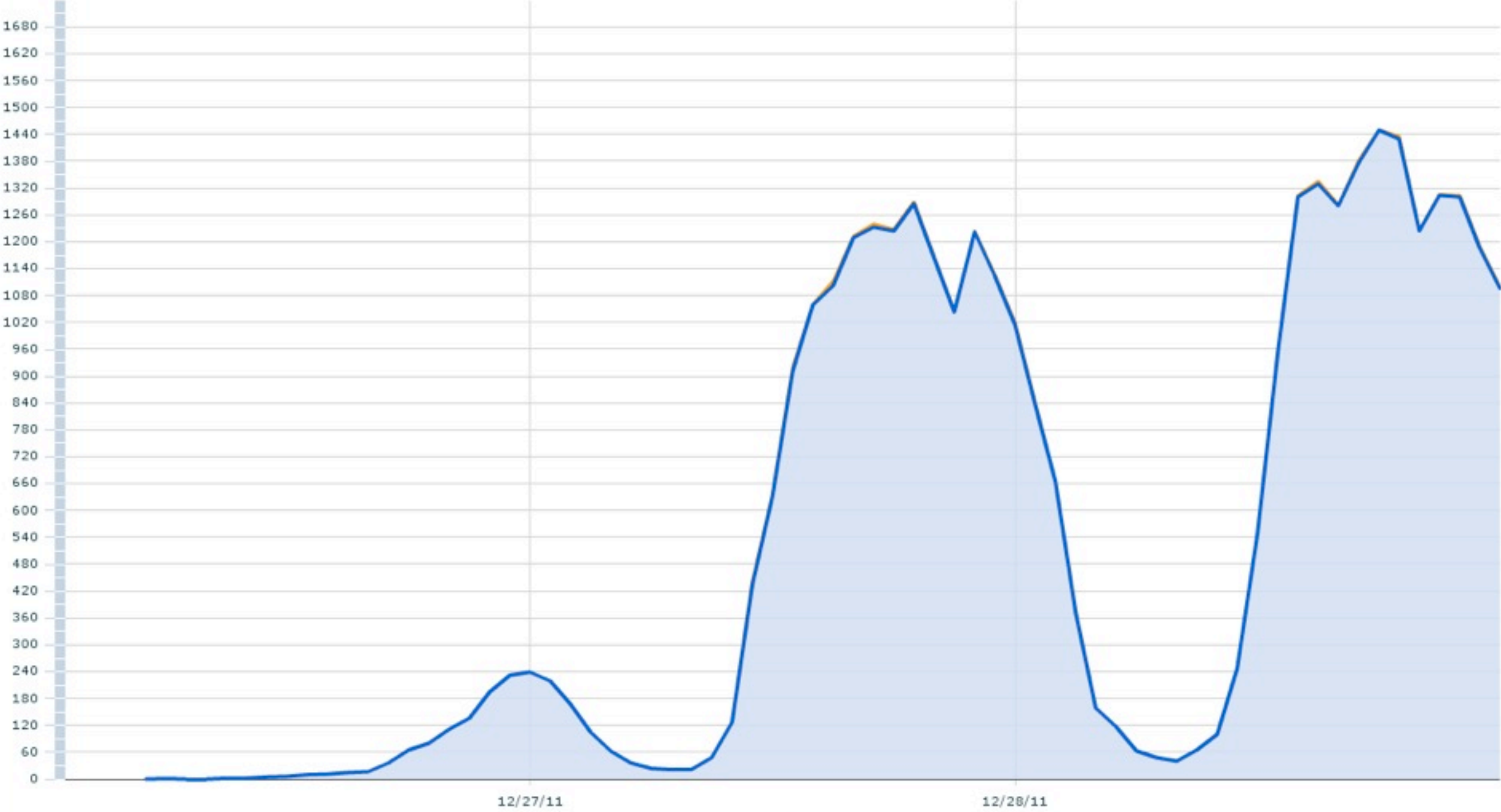
Downstream Upstream



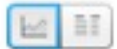
Client Count

6h | 1d | 1w | 2w | 4w | 3m | 6m | 1y | Custom

Client Count

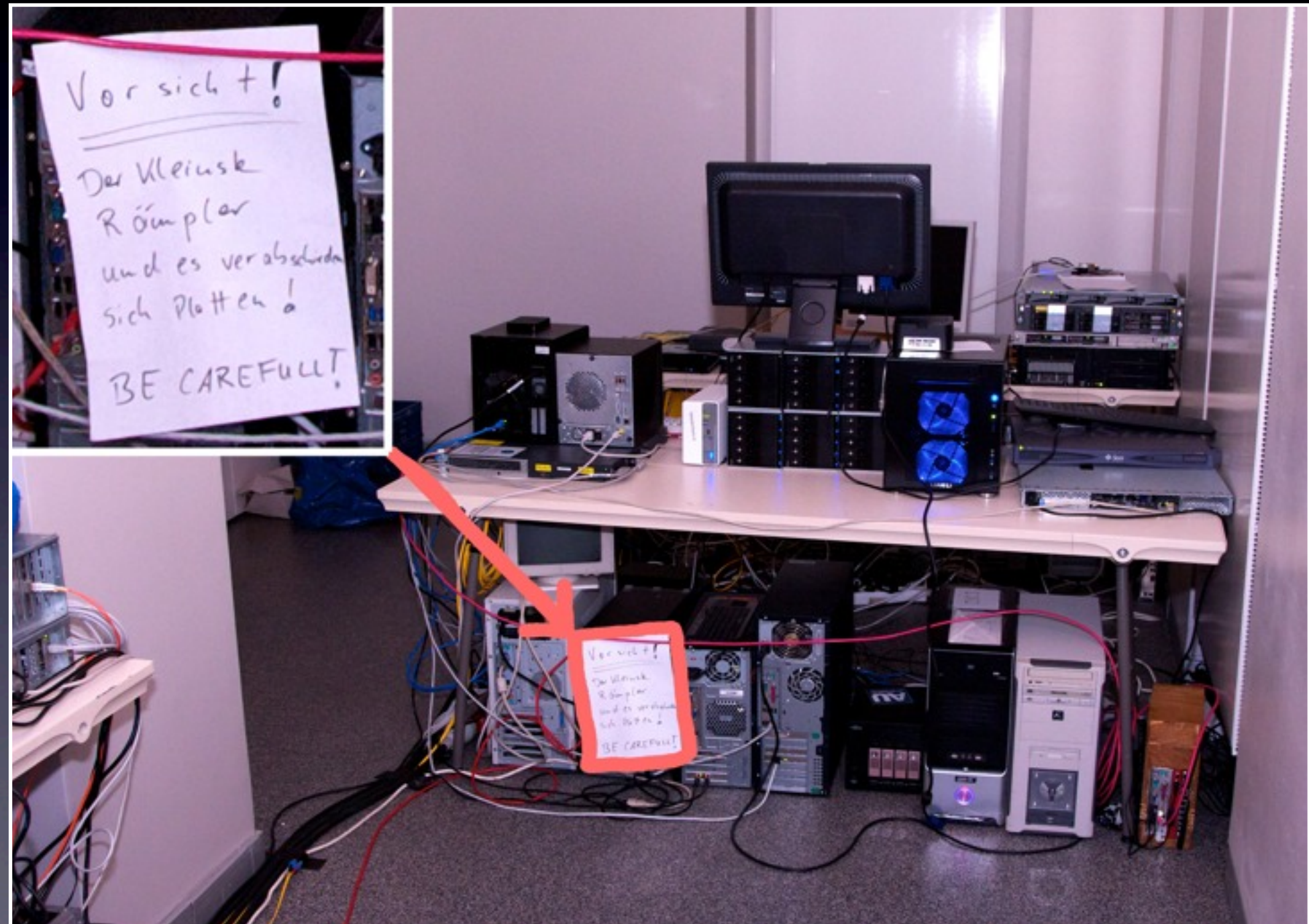


Associated Client Count Authenticated Client Count



Colo

- 2 Switches
- 2*10GE Uplink
- 48*GE Downlink
- smaller than last year
- plz bring better cases



MONITOR



memegenerator.net

dashboard.congress.ccc.de



c3netmon

Realtime 28c3 data served by nodejs + websockets
Thanks to the NOC, POC and FEM-Team for providing the data.
Detailed graphs can be found [here](#).

DATA SENT

91246 GB

DATA RECEIVED

23338 GB

Upstream usage (18%):

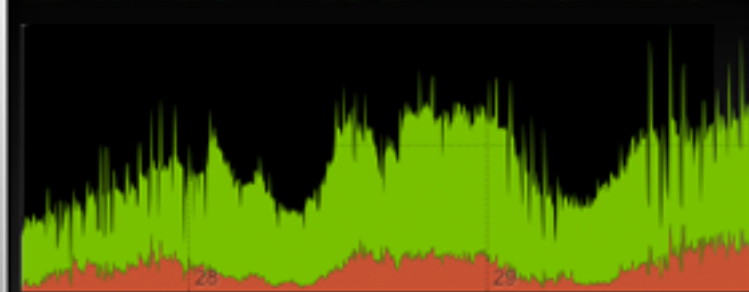


Downstream usage (5%):



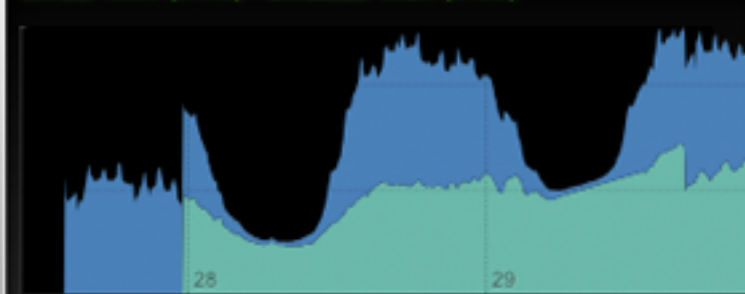
BANDWIDTH

Out: 4557mbit/s (6868mbit/s) · In: 1760mbit/s (2348mbit/s)



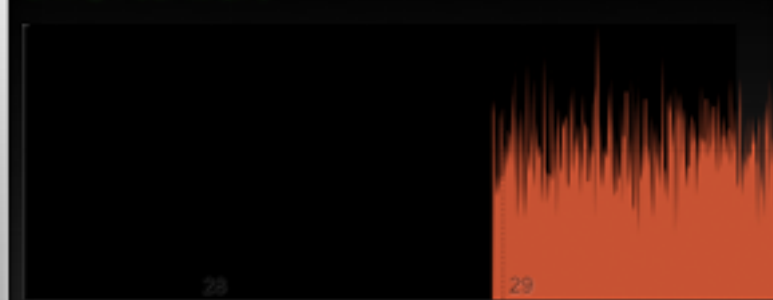
CLIENTS

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



RADIATION LEVEL

CPM @ POC: 32 (37)



WIRELESS BAND USAGE

802.11 · a: 95 · g: 96 · n (2,4GHz): 551 · n (5GHz): 328



✓ 802.11n 5GHz Clients
✓ 802.11n 2.4GHz Clients
✓ 802.11g Clients
✓ 802.11a Clients

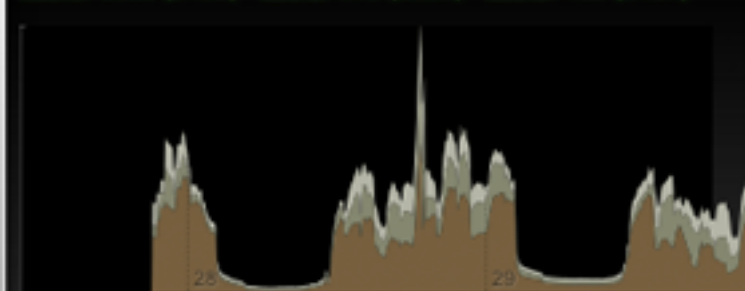
POC

Connected: 1004 (1004)



STREAMING

Saal1: 1160 (3456) · Saal2: 372 (1529) · Saal3: 490 (1417)



OPENBEACON (R0KET)

r0kets visible via OpenBeacon: 164 (169)



IP PROTOCOL DISTRIBUTION

IPv4: 94% · IPv6 5%

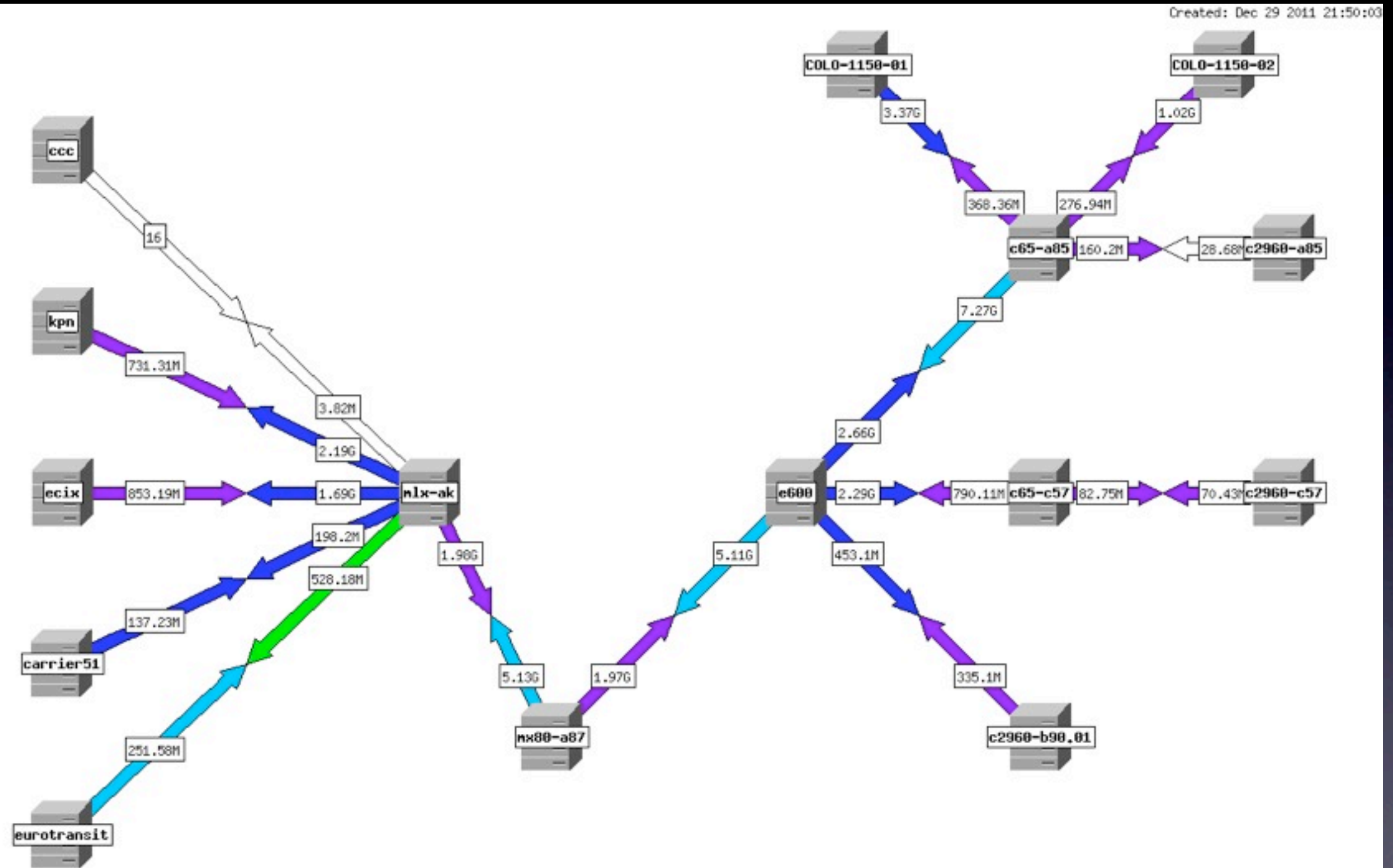


Info: Values in parentheses are peaks.

Historical data in json format is available [here](#). Current values for your own projects can be found [here](#)

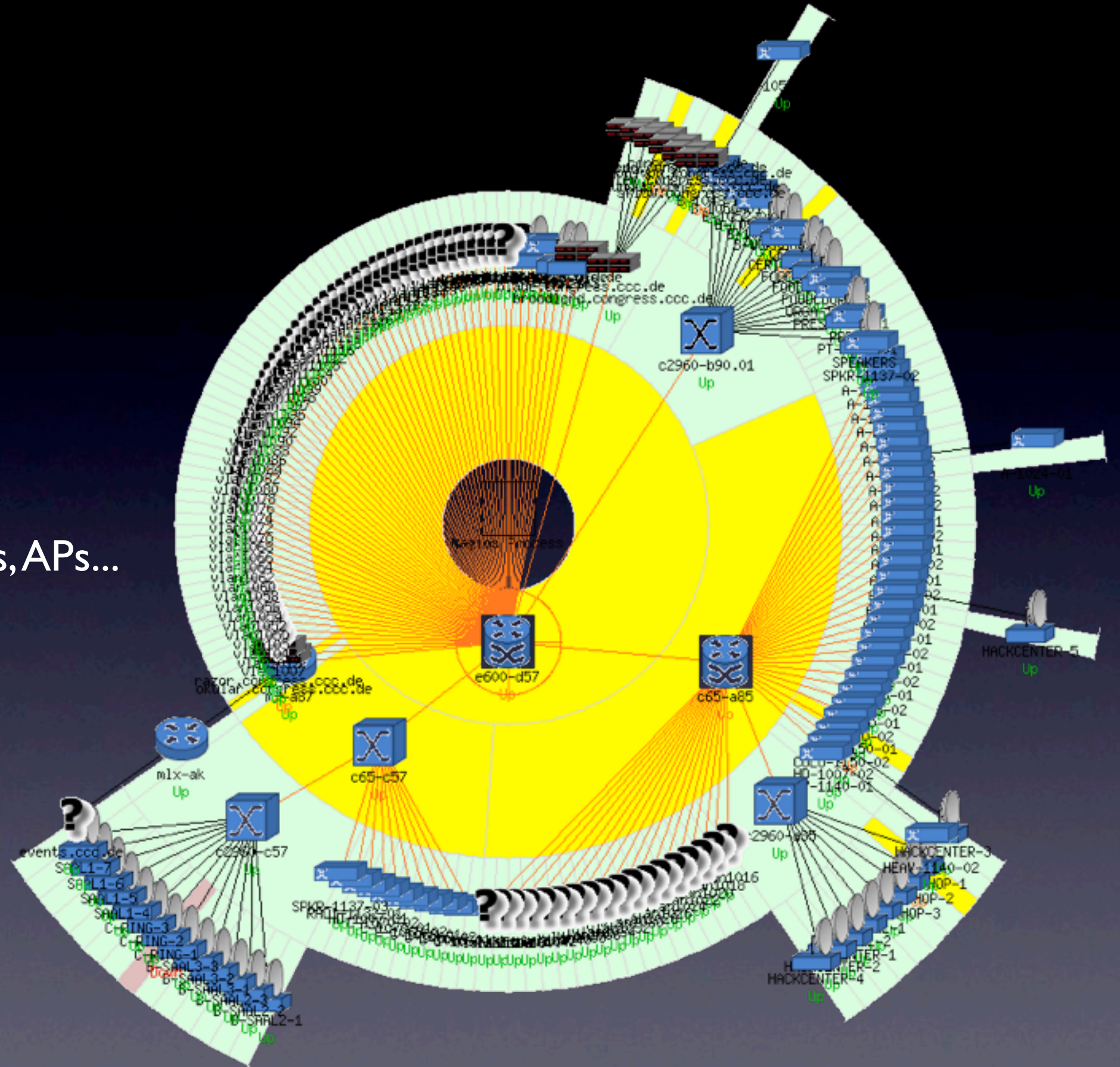
c3netmon code will be released on github.com/FremaksGmbH/c3netmon-public shortly after the congress.
If you have any questions contact morpheus@morphome.net.

Weathermap



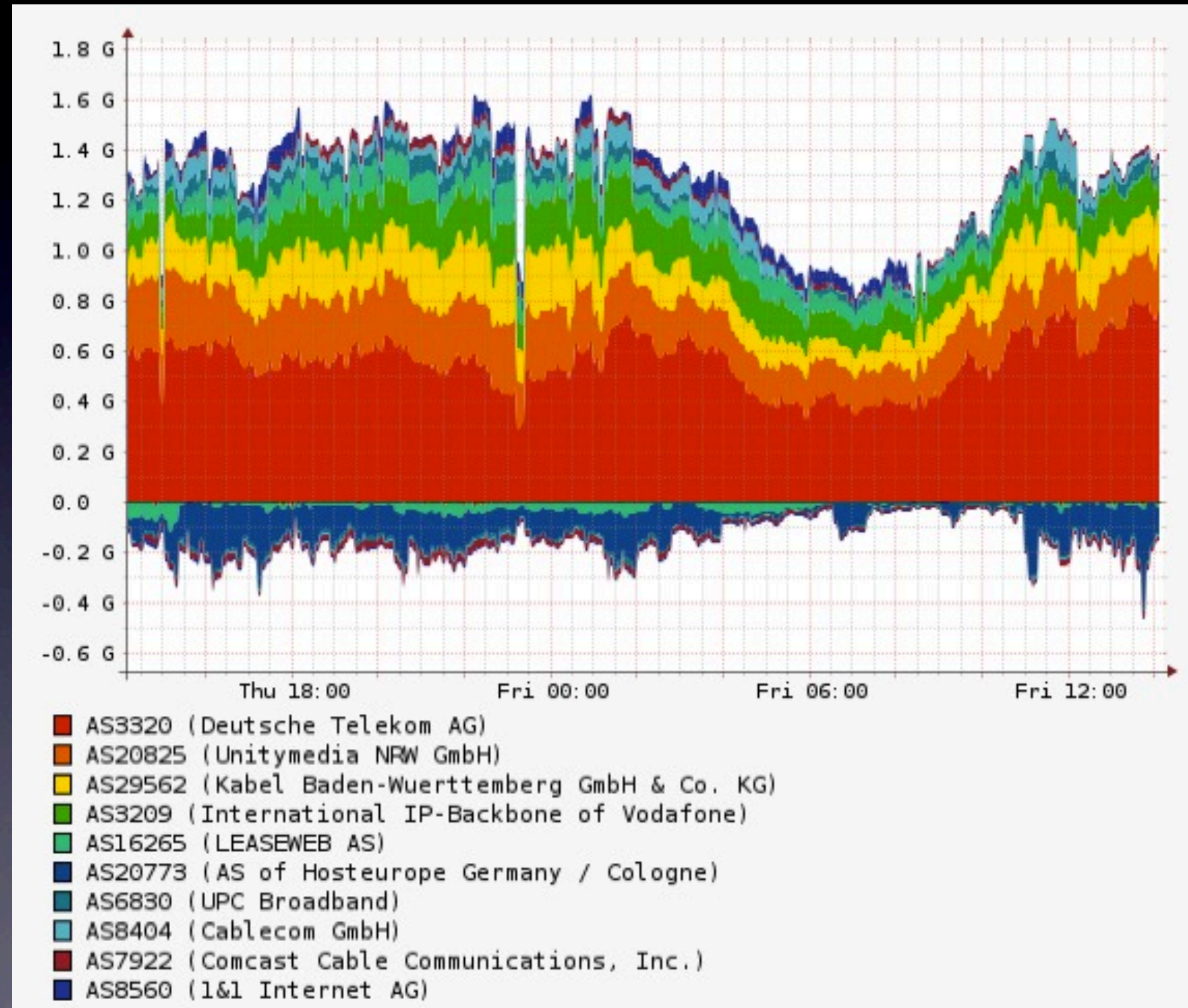
Icinga

- ~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 I G

Questions??

