

Bericht aus dem NOC

52. DFN-Betriebstagung Oktober
2009

Thomas Schmid
schmid@dfn.de

- Neuer Standort München
 - Fraunhofer-Zentrale
 - xr-fhm1 (Cisco 7600)
- Backup des Geant-Anschlusses in Erlangen
 - Geant3
 - Cross-border fiber nach Paris
 - somit volle Redundanz (node, link)
 - Kapazität 5 Gbps
- Upgrade T-Online Peerings auf 2 x 10Gbps steht vor der Tür (!)

- Derzeit ca. 100 private AS-Nummern vergeben
- Szenario 1 und 2 kommen zum Einsatz
- volle Routingtabelle bisher nur bei echtem Multihoming mit eigenem AS
- Fragestunde gestern

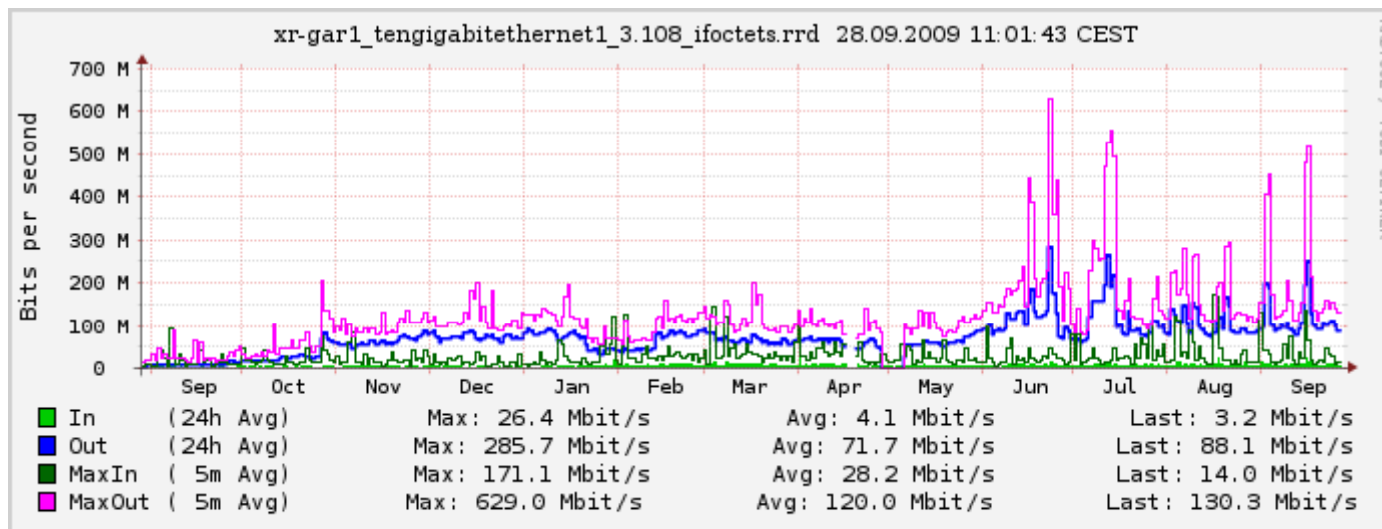
- dringender Update auf 12.2(33)SRB6
 - BGP Bug in Zusammenhang mit doppelter Anbindung
 - betrifft konditionale BGP-Announcements
 - soll: Router verschickt nur dann eine Default-Route, wenn er selbst eine Verbindung ins Internet hat
 - Bug: Default wird verschickt, sofort darauf wieder zurückgezogen (withdrawal)
 - Bug wurde in 12.2(33)SRB4 eingeführt (CSCsw73486)
 - Upgrade auf allen Routern durchgeführt

- Symptome: BGP Session zu Global Crossing fing an zu flappen
 - BGP Update-Storms (ca. 300.000 Routen) im Netz
 - CPU-Last auf 7600ern 100%
 - keine Antwort der Router auf ping, SNMP, ...
 - aber Forwarding davon nicht betroffen!
- Session heruntergefahren, GC kontaktiert.
- GC installierte BGP Filter, verweist auf Cisco TAC
- TAC: CSCtb42995
 - zu dem Zeitpunkt noch nicht öffentlich
- invalide BGP Updates führen zu Reset der BGP Session auf CRS-1. Kein Workaround auf dem Router.
- GC installierte BGP Filter, die die Updates blocken
- inzwischen Patch auf CRS-1 eingespielt.

- Teredo ‚heads up‘
 - Standardmässig aktiviert unter Windows Vista und 7
 - ermöglicht IPv6 Verbindung ohne eigenen nativen IPv6 Anschluss
 - globales Netz von Relays und Servern
 - topologisch nächstes Relay am LRZ München
 - Tunnelt durch NAT und Firewalls
 - benutzt IPv6 über IPv4 UDP Port 3544
 - somit werden alle anderen Firewallregeln ausgehebelt
 - RFC4380

http://www.symantec.com/avcenter/reference/Vista_Network_Attack_Surface_RTM.pdf

- kein Wachstum bei Anschlüssen
 - Erinnerung: wer nicht auf dual stack wechselt, wird mit Routing über NAT-Bottlenecks bestraft ☺
 - im Ernst: früher oder später Performance-Probleme ...
 - Ausnahme: IPv6-Verkehr LRZ



(s.o.)

- neuer Service Layer3 VPN
 - derzeit Pilotbetrieb
 - Erfahrungen bisher sehr gut
 - ermöglicht virtuelles Netz mit eigener Adressierung über das X-WiN
 - eigene Signalisierungsebene
 - Forwarding über MPLS
 - somit auch kein Zugriff von außerhalb des VPNs möglich

- Problem tritt auf bei fractional Ethernet (s. BT 49)
- Kurz: Router verschicken trotz Policing Bursts, die von den Leitungsendgeräten der Carrier nicht gepuffert werden können
- Empfehlung: Ethernet flow-control aktivieren
 - Leitungsendgeräte signalisieren via PAUSE Frames dem Router, dass Überlast besteht. Der Router stellt das Versenden von Daten für kurze Zeit ein und puffert lokal
 - wird allerdings nicht auf allen Plattformen unterstützt