



Zentrales P2P- und VoIP-Bandbreitenmanagement für individuelle Nutzer und Subnetze

44. DFN-Betriebstagung
8. Februar 2006

Hendrik Schulze
Geschäftsführer, ipoque GmbH

- 1 Jahr PRX-Traffic Manager
 - Erfahrungen (P2P-Verkehr)
- PRX-Traffic-Manager
- Nutzer- /Subnetz-basiertes Traffic-Management
- Ausblick

- **Sehr populär**
 - eDonkey (emule), BitTorrent, Kazaa
- **50%-90% des Netzwerkverkehrs**
 - Beeinträchtigt anderen Verkehr
 - Teure Netzwerkerweiterungen
- **Größtenteils illegaler/fragwürdiger Inhalt**
- **Sicherheitsrisiko (Spyware/Trojaner/Viren)**
- **Mit bisherigen Mitteln schwer zu erkennen bzw. zu verhindern**



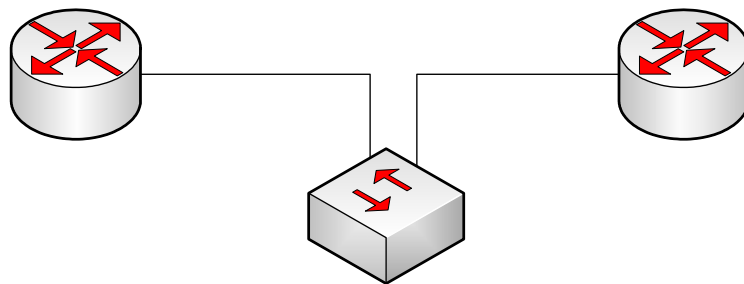
- Integration als transparente Bridge
- **Signatur**-basierte Erkennung von P2P Verkehr
 - Messen / Drosseln / Blockieren

Meist:

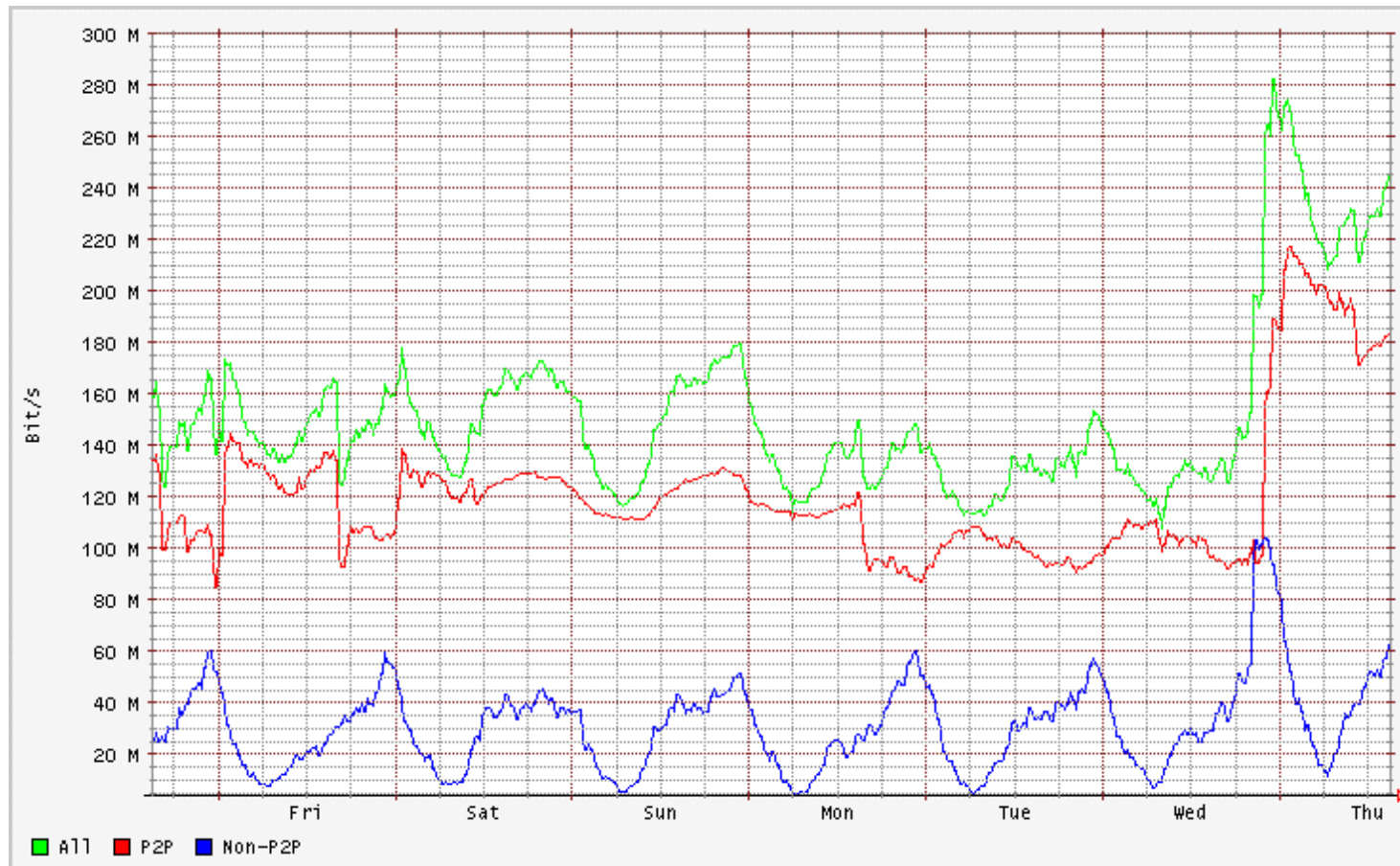
- direkt nach DFN-Router
- vor Studenten-WLAN
- vor Wohnheimen

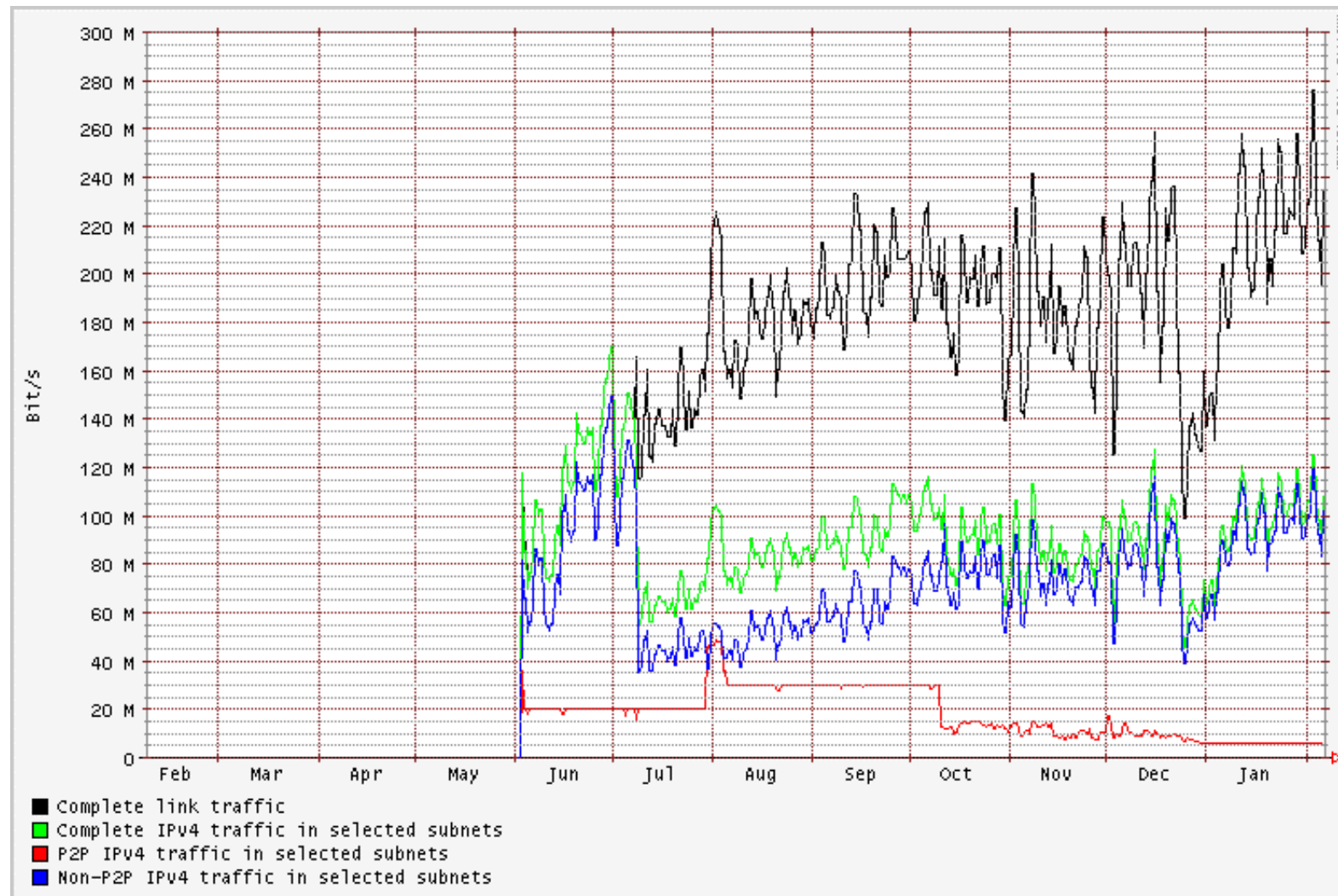
Referenzen

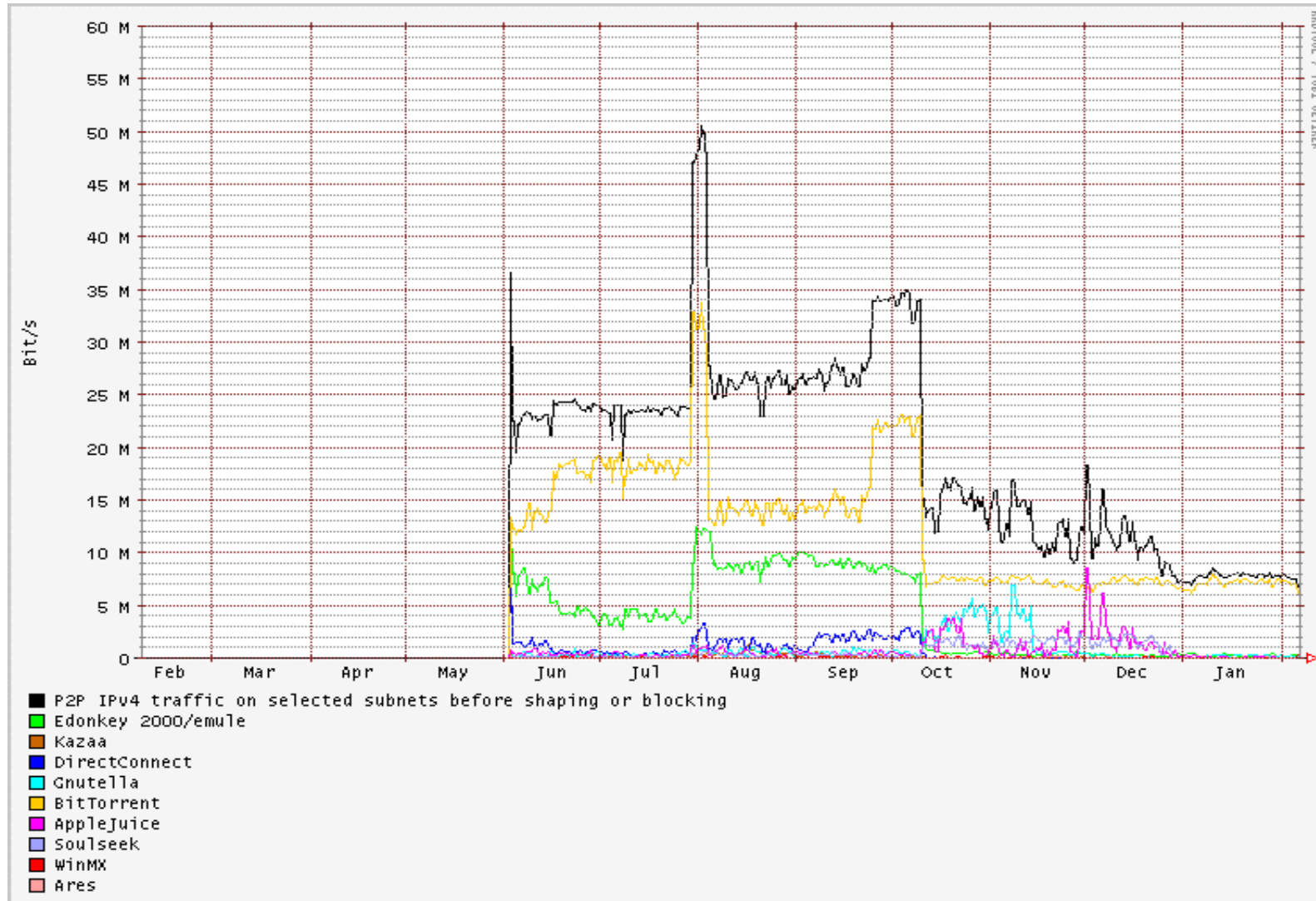
- Uni Marburg
- HS Anhalt
- FH Lippe und Höxter
- HS Zwickau
- HTWK Leipzig
- FH Bremerhaven
- FH Aachen



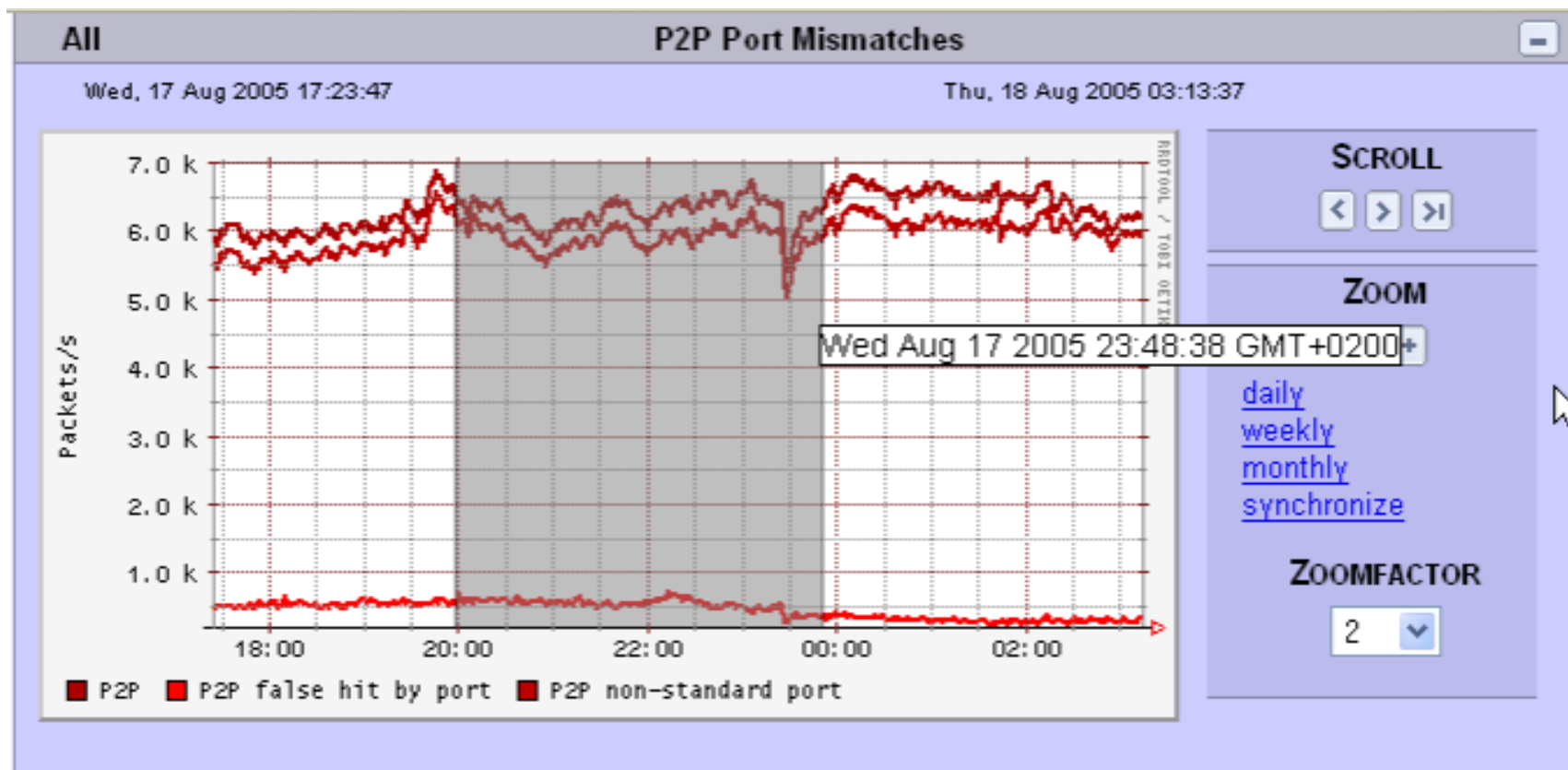
Gesamtverkehr (90% P2P-Traffic)





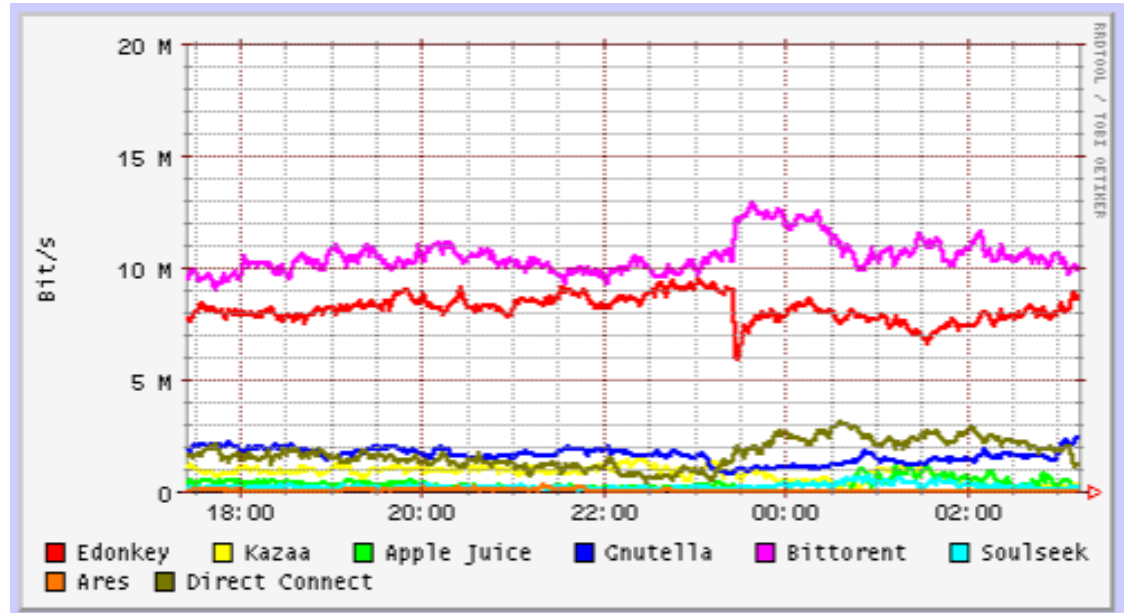


Signatur-basierte Erkennung verhindert Fehlklassifikationen



- Geänderte Protokolle

- Fasttrack
- WinMX
- BitComet (BitTorrent)
- Skype
- eDonkey
- Ares



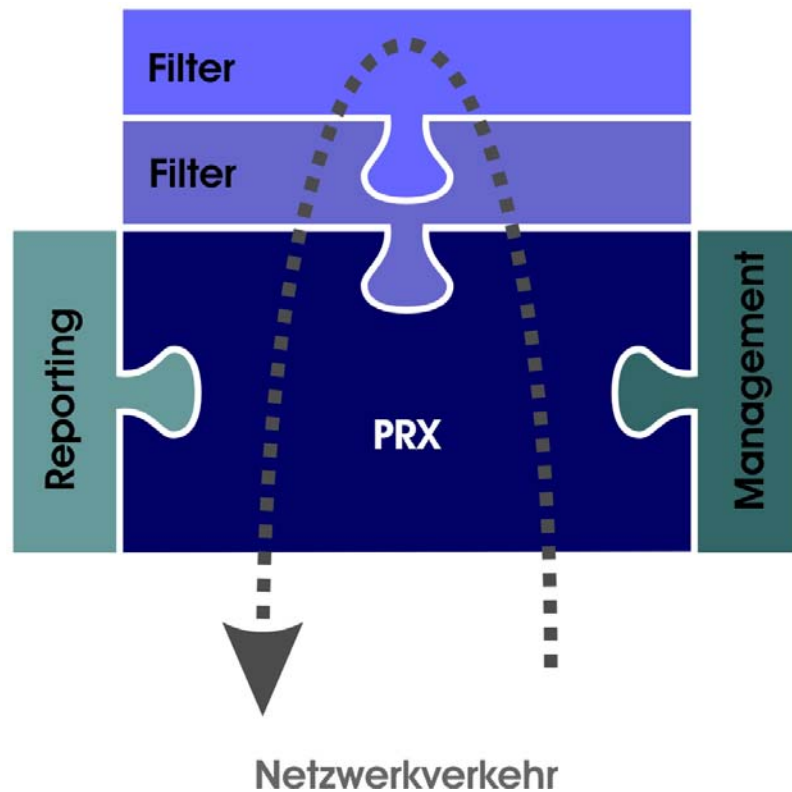
- Neue Protokolle

- XDCC
- Freenet
- Mute

- 1 Jahr PRX-Traffic Manager
 - Erfahrungen (P2P-Verkehr)
- PRX-Traffic-Manager
- Nutzer- /Subnetz-basiertes Traffic-Management
- Ausblick



PRX	Durchsatz (MBit/s)	Netzwerk-interfaces	Bypass	Passiv gekühlt	Rackmount
100e	2*25	100-BaseT		X	
100	195	100-BaseT		X	
250	250	1000-BaseT		X	
1000e	2*175	1000-BaseT	X		X
1000	1600	1000-BaseT	X		X



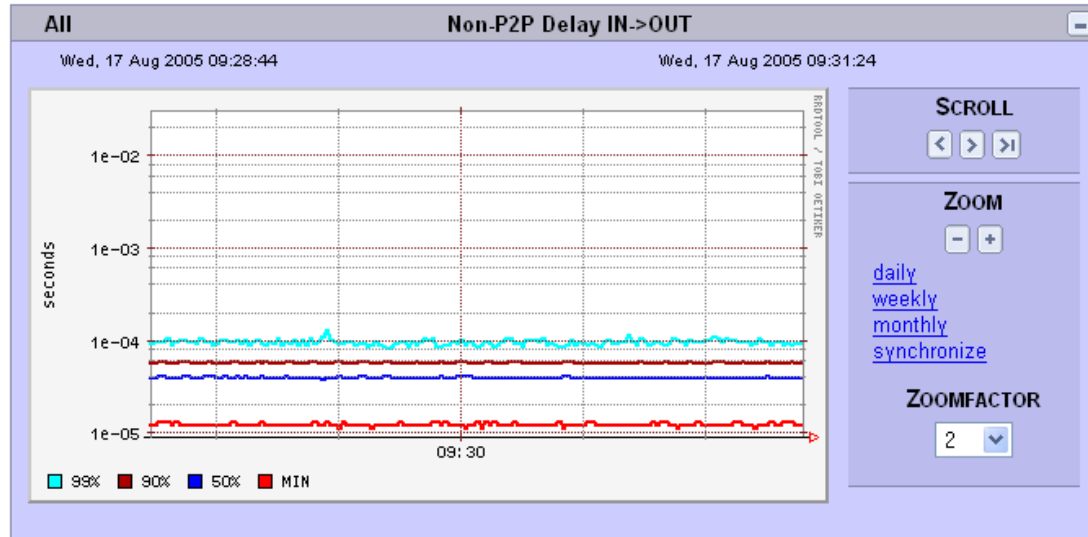
- **Modulare Architektur**
 - Hohe Performanz
 - Geringe Latenz
 - Geringe Kosten
- **Filtermodule**
 - P2P
 - VoIP
 - IM
 - URL
 - IP-Control
- **Managementmodule**
 - SNMP (1000e/1000)
 - Advanced Reporting
 - Statistik

- **Neuer Trend → hohe Wachstumsraten**
 - Bandbreite/Kosten schwer kalkulierbar für Netzbetreiber
 - Administrative Restriktionen
- **Sicherheitsrisiko**
- **In einigen Netzwerken unerwünscht**
 - Torpediert Fair-Use-Policy
 - Nutzt fremde Netzwerkinfrastruktur

- **Sicherheitsrisiko (Spyware, Trojaner, Backdoors in Clientsoftware)**
- **Senkung von Produktivität in Firmen**
- **Steuermechanismus zum Verbreiten von Spam, Viren, Würmern und illegalem Content**
- **Mechanismus zum Steuern von Distributed Denial of Service Attacks**

- **einfaches Blockieren bestimmter Websites**
 - auch Zugriff über externe Proxies wird verhindert
- **Erfüllung bestimmter gesetzlicher Auflagen**
 - z.B. in NRW

- **Transparente Bridge**
 - keine Änderungen an der Konfiguration
- **Konfiguration über Webinterface**
 - einfache Administration
- **Ausfallsicherheit**
 - Hardware-Bypass (PRX-1000e/1000)
 - Passive Kühlung (PRX-100e/100/250)

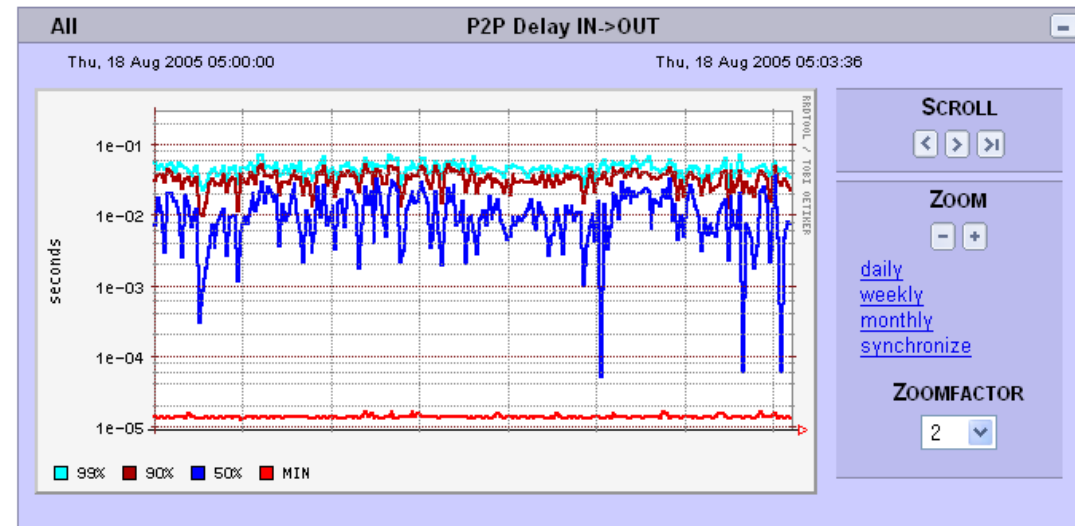


Nicht-P2P Verkehr

- Normallast ~ 0.1 ms
- Vollast < 1ms

P2P Verkehr

→ Warteschlangenabhängig



- 1 Jahr PRX-Traffic Manager
 - Erfahrungen (P2P-Verkehr)
- PRX-Traffic-Manager
- Nutzer- /Subnetz-basiertes Traffic-Management
- Ausblick

„Aber mit P2P-Filesharing kann man
doch viele nützliche Dinge machen..“

- **IP-Control & Advanced-Reporting**
 - 2 neue Module
 - verfügbar nach CeBit

- **Accounting**
 - pro IP oder pro Subnetz
 - für Gesamtverkehr
 - für einzelne Protokolle oder Protokollklassen
 - vorgegebenes Freivolumen möglich

- **Bei Überschreiten des Freivolumens:**
 - Benachrichtigen → Adv.Reporting
 - Drosseln oder Blockieren
 - Gesamtverkehr
 - Protokollklassen

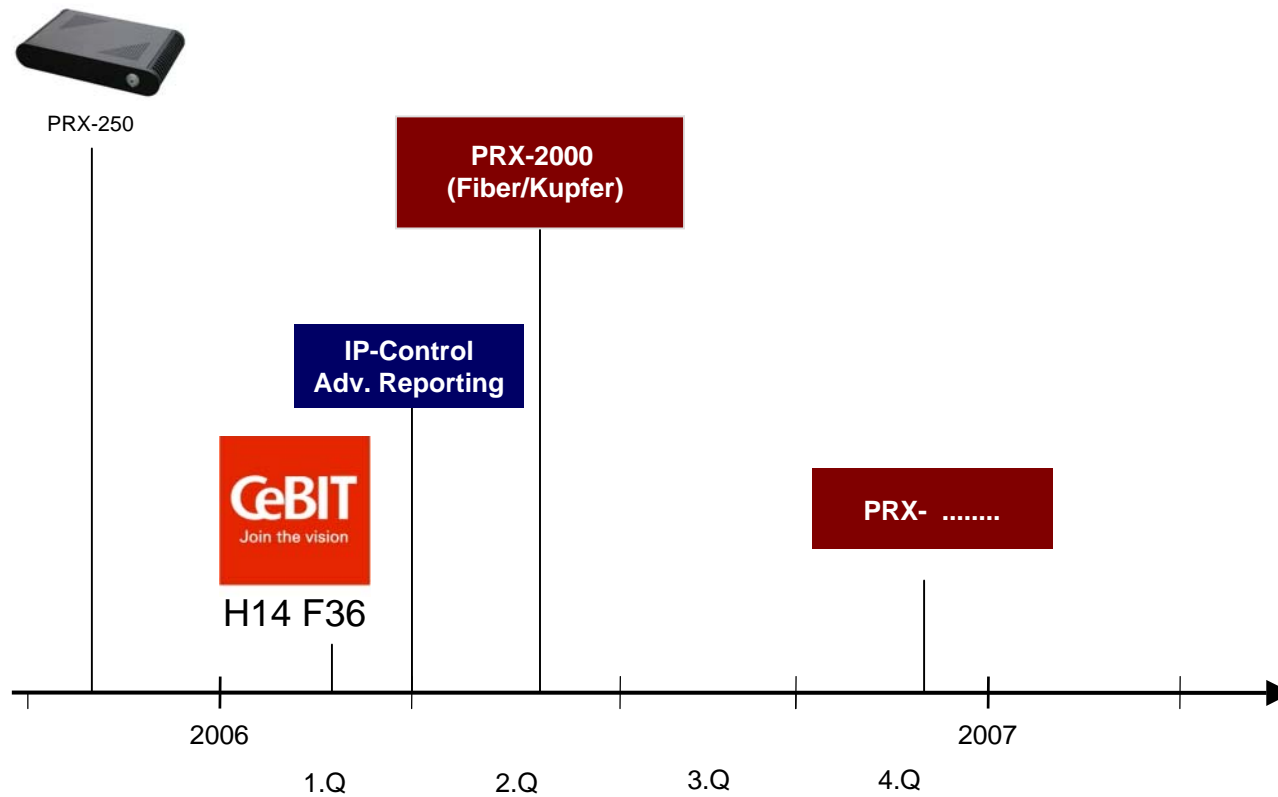
Mögliches Szenario:

- Außer BitTorrent sind alle P2P-Protokolle gesperrt.
- Jede IP-Adresse hat 1 GB Freivolumen pro Monat.
- Bei Überschreiten wird auch BitTorrent gesperrt.

Verbesserte Integration in bestehendes Netzwerkmanagement

- Nachrichten über Syslog
 - Überschreiten von Freivolumen
 - Verbindungsversuche für IM/VoIP
- IP/Subnetz-Statistik
 - Download als CSV

- 1 Jahr PRX-Traffic Manager
 - Erfahrungen (P2P-Verkehr)
- PRX-Traffic-Manager
- Nutzer- /Subnetz-basiertes Traffic-Management
- Ausblick



Wiki-Uni-DSL (http://aachen.uni-dsl.de/wiki/index.php?title=Mein_Filesharingprogramm_ist_langsam)

Mein Filesharingprogramm ist langsam

Das liegt wahrscheinlich daran, daß die RWTH [...] ein Gerät der Firma ipoque [...] installiert hat.

Eine Möglichkeit dieses Gerät zu umgehen ist nicht bekannt [...] Seit dem Einsatz des Gerätes ist das Abuse-Postfach deutlich entlastet und es reduzierten sich auch die Kontakte mit "gewissen Ermittlungsbehörden".

Das Gerät untersucht alle Pakete [...] und *bremst* die zugehörigen Verbindungen auf zusammen 10 Mbit/s [...] Also bringt euch weder das Ausweichen auf einen anderen Port weiter, noch die Benutzung irgendwelcher Proxys.

Gulli.Board (<http://board.gulli.com/thread/457430-ipoque-umgehen/>)

Hallo allerseits,

wollte mal fragen, ob jemand weiss, ob und wenn ja wie es möglich ist, das Programm Ipoque [...] zu umgehen, wenn man dies von seinem Netzadministrator vor die Nase gesetzt bekommen hat.

Hi, habe leider selbiges Problem. Da ipoque quasi den Inhalt deiner Kommunikation abhört und auswertet [...] ist es nicht möglich das zu umgehen. Ausser du benutzt P2P-Programme die ipoque noch nicht kennt. Allerdings werden die wiederum wohl nur von wenigen genutzt werden und somit unbrauchbar sein.

Klagen und/oder ISP wechseln.

Du willst deine Firma oder die Uni verklagen? Na dann viel spass. Einfacher ist es da doch Software zu nehmen die ihre Header verschlüsselt, Bitcomet kann das. Azureus arbeitet daran. Müssen halt nur alle dann updaten damit es funktioniert.

Vielen Dank!

- - -

Hendrik Schulze

Hendrik.Schulze@ipoque.com