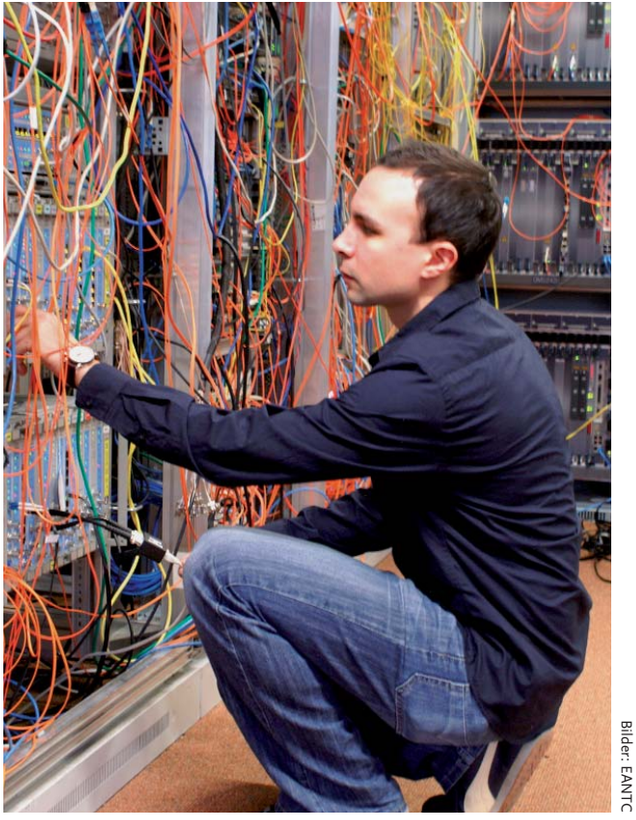


Bilder: EANTC

Peer-to-Peer-Filter im Test

Von Thomas Sladek

P2P-Filter, so versprechen ihre Hersteller, geben Providern die Möglichkeit, ihr Netz vor dem Kollabieren durch die immer stärker wachsende Flut an P2P-Verkehr zu bewahren. Ein Test.

Mehr als zwei Dutzend Hersteller rühmen sich, für die Kontrolle vom P2P-Verkehr (Peer to Peer) die passenden Geräte anzubieten: Filter zum erkennen und drosseln von P2P-Verkehr, der in Spitzenzeiten mittlerweile bis zu neunzig Prozent des Gesamtverkehrsaufkommens ausmachen kann. Aber halten die Systeme was die Hersteller versprechen?

Um dies herauszufinden, führte das EANTC (European Advanced Networking Test Center) Performance- und Funktionalitätstests von P2P-Filtern im Auftrag von SNEP (Syndicat National de l'Édition Phonographique – eine Organisation, die die Rechte der französischen Musikindustrie repräsentiert) und Internet Evolution durch. Die Tests haben dann zwischen April und Oktober 2007 im Labor des EANTC in Berlin stattgefunden.

28 namhafte Hersteller von P2P-Filterlösungen wurden zur Teilnahme an den Tests eingeladen, unter anderem Allot Communications, Cisco Systems, Arbor/Ellacoya Networks, F5 Networks, Huawei Technologies, Ipoque, Juniper Networks, Narus, Packeteer, Sandvine und weitere Hersteller. Nur fünf Hersteller nahmen die Herausforderung an, an diesem Test teilzunehmen. Drei der Hersteller widersprachen jedoch dann der Veröffentlichung ihrer Testergebnisse. Nur Arbor/Ellacocy Networks (USA) und Ipoque (Deutschland) stellen sich mit ihren Testergebnissen der Öffentlichkeit.

- Arbor/ Ellacoya Networks – E-30-Plattform
- Ipoque – PRX-5G Traffic Manager

Thomas Sladek ist Senior Testingenieur beim EANTC in Berlin.

Mit zwei Lastgeneratoren von Shenick Network Systems und Ixia emulierte das EANTC ein typisches Serviceprovider-Szenario mit maximal sieben Millionen parallelen TCP-Verbindungen in einem realistischen Mix aus Internet-Applikationen und zehn verschiedenen P2P-Protokollen über ein Netzwerk aus sieben realen MPLS-Core-Routern. Somit wurde die notwendige Performance erreicht, die von großen Serviceprovidern für diese Art von Filtergeräten gefordert wird.

Maximaler Durchsatz

Für die Ermittlung des Durchsatzes versetzte EANTC die Filtergeräte in einen so genannten Monitoring-Modus, in dem die P2P-Verbindungen nur erkannt und statistisch ausgewertet, aber nicht gefiltert werden. Beide Geräte erzielten sehr gute Durchsatzergebnisse, sehr nah an der maximal möglichen Linkbandbreite (Arbor/Ellacoya 973 MBit/s, Ipoque 922 MBit/s). Die Latenz lag im unteren Mikrosekundenbereich (Arbor/Ellacoya: 8 µs, Ipoque: 24 µs).

Erkennung von P2P Verkehr

Um ein möglichst breites Spektrum an P2P-Protokollen zu untersuchen, emulierte das EANTC die zehn geläufigsten P2P-Protokolle. Parallel dazu wurden andere Internetanwendungen wie HTTP, FTP, SMTP, POP3 und RTP emuliert. Die Herausforderung war, die P2P-Ströme zu erkennen, aber den restlichen Verkehr nicht zu beeinträchtigen. Die Arbor/Ellacoya-E-30-Plattform erkannte neun von zehn P2P-Protokollen. Die bekanntesten P2P-Protokolle Bit-Torrent und E-Donkey wurden sehr gut erkannt. Der Ipoque PRX-5G Filter lieferte ein hervorragendes Ergebnis, alle zehn P2P-Protokolle wurden erkannt. Die Erkennungsgenauigkeit der vier wichtigsten Protokolle war überwältigend: Bit-Torrent 97, E-Donkey 88, Fasttrack 97 und Gnutella 96 Prozent.

Drosselung von P2P-Verkehr

Nachdem sichergestellt und P2P-Verkehr erkannt wurde, wollte das EANTC nun wissen, wie gut und wie genau die Geräte P2P-Verkehr drosseln können. Dazu wurden drei verschiedene Tests mit unterschiedlich starker Drosselung durchgeführt, von 25 über 50 bis hin zu 75 Prozent Drosselung. Arbor/Ellacoya erzielte bei diesem Test für die Protokolle Bit-Torrent und MP2P ein sehr gutes Ergebnis (Genauigkeit über 80 Prozent), andere Protokolle konnten weniger genau gedrosselt werden; I-Mesh, Win-MX sowie Soul-Seek wurden gar nicht gedrosselt.

Das Gerät von Ipoque erzielte ein etwas besseres Ergebnis: Bit-Torrent, Gnutella, Fasttrack und MP2P konnten mit einer hohen Genauigkeit (über 80 Prozent) gedrosselt werden. Nur Win-MX konnte aufgrund der schlechten Erkennungsrate kaum gedrosselt werden.

Erkennung und Drosselung von verschlüsseltem P2P-Verkehr

Einige P2P-Implementationen, vor allem die am verbreitetsten Protokolle Bit-Torrent und E-Donkey, bieten mittlerweile einige Möglichkeiten den P2P-Verkehr zu verschlüsseln – mit dem einzigen Ziel, einer Erkennung durch den Provider und der Musikindustrie zu entgehen. Es sollte ge-

klärt werden, ob dieser Verkehr tatsächlich nicht durch heutige Filtertechnik erkannt werden kann, oder ob es den Herstellern auch hier gelungen ist, Möglichkeiten der Erkennung zu implementieren. Die folgenden Verschlüsselungsmethoden wurden genutzt:

- E-Donkey-Plain-Header-Verschlüsselung (nur Header-Verschlüsselung)
- Bit-Torrent-Plain-Header-Verschlüsselung (nur Header-Verschlüsselung)
- Bit-Torrent-Full-Stream-Verschlüsselung (RC4-Header- und Daten-Verschlüsselung)
- Filetopia-Full-Stream-Verschlüsselung (AES-Header- und Daten-Verschlüsselung)
- Freenet-Full-Stream-Verschlüsselung (AES-Header- und Daten-Verschlüsselung)

Der verschlüsselte Freenet- und E-Donkey-Verkehr konnte von keinem der getesteten Geräte erkannt werden. Bit-Torrents-RC4-Verschlüsselung wurde jedoch von den Filtergeräten erkannt. Arbor/Ellacoya erkannte P2P-Verkehr bei dem ausschließlich der Header verschlüsselt war, Ipoque erkannte selbst Bit-Torrent-Verkehr mit Header- und Datenverschlüsselung. Für Serviceprovider und die Musikindustrie ist das ein positives Signal, da BitTorrent nahezu 50 Prozent des gesamten P2P-Verkehrs ausmacht.

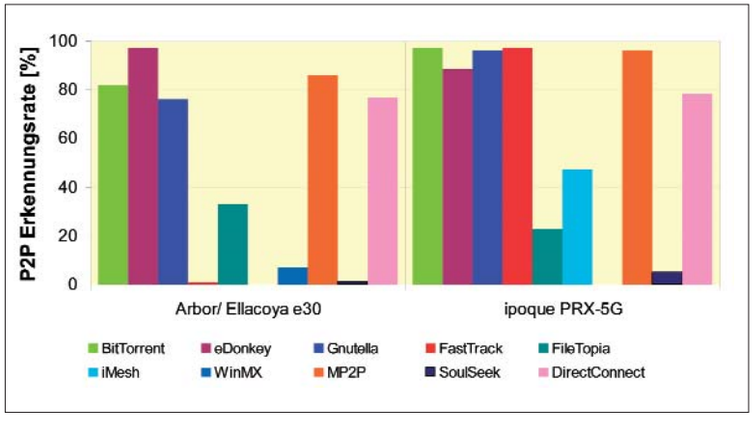
Weitere Tests

In weiteren Tests zeigte sich, dass die Geräte auch P2P-Verkehr erkennen, wenn die IP-Pakete über MPLS-VPN-Tunnel übertragen (nur Arbor/Ellacoya) oder während der Übertragung fragmentiert werden. Ein Dauerbelastungstest mit hoher Auslastung (rund 900 MBit/s bidirektional) ergab eine gleich bleibende Zuverlässigkeit der Erkennung von P2P-Verkehr. Auch die Durchsatzperformance konnte über einen längeren Zeitraum gehalten werden.

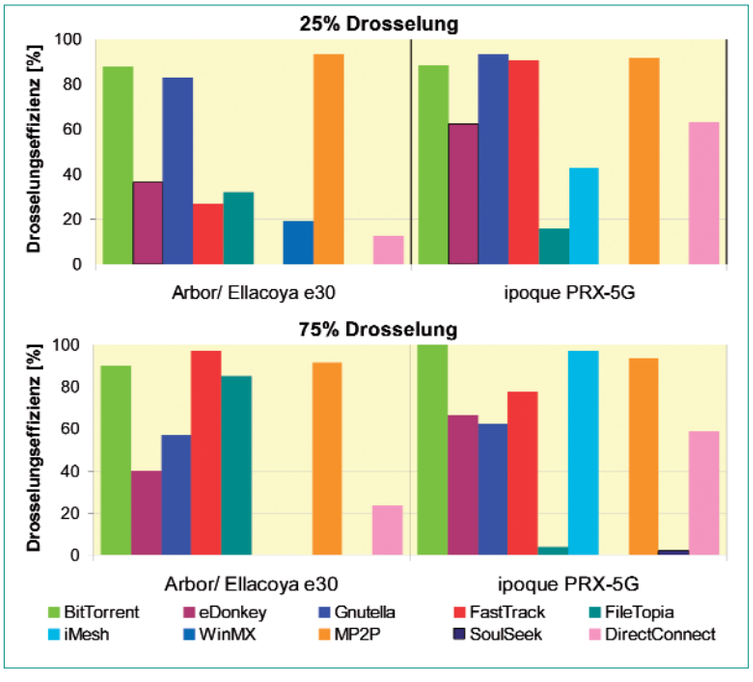
Redundanz und Hochverfügbarkeit

Die Arbor/Ellacoya-E-30-Plattform bietet redundante Stromversorgungen und die Möglichkeit eines so genannten „hitless“ Software Reload, welcher ein Neustart der Software (zum Beispiel für ein Update) mit nur minimalen Verkehrsbeeinträchtigung gewähren soll. Unsere Ergebnisse zeigen, dass der Ausfall eines Netzteils keine Beeinträchtigung für den fließenden Verkehr hat. Während eines Software-Reloads wurde eine Ausfallzeit von zehn Sekunden ermittelt.

Der Ipoque PRX-5G Traffic Manager bietet ein sehr nützliches Feature: im Falle eines Softwarefehlers oder Stromverlust geht das Gerät zu einem so genannten „Transparent-Mode“ über, bei dem die ein- und ausgehenden Netzwerkinterfaces physikalisch miteinander verbunden werden. Für den Fall des Stromausfalls ermittelte das Testlabor eine Ausfallzeit von 3,5 Sekunden.



Die Ergebnisse der P2P-Erkennung



Die Ergebnisse der P2P-Drosselung

Verschlüsselten Verkehr erkennen

P2P Protokoll	Verschlüsselung	Arbor/ Ellacoya e30	Ipoque PRX-5G
Bit-Torrent	Nur Header-Verschlüsselung	93	52
Bit-Torrent	RC4 (gesamter Verkehr)	0	54
eDonkey	Nur Header-Verschlüsselung	0	0
Filetopia	AES (gesamter Verkehr)	98	94
Freenet	AES (gesamter Verkehr)	0	0

(Angaben in Prozent)

Beide Geräte zeigten, dass die versprochenen Redundanzmechanismen prinzipiell funktionieren. Für TCP-Anwendungen würden die gemessenen Ausfallzeiten kaum Auswirkungen haben, da TCP versucht, verlorene Pakete erneut zu übertragen. Bei zeitkritischen Anwendungen wie zum Beispiel Voice over IP würden die gemessenen Ausfallzeiten jedoch deutlich spürbar werden, Sprachaussetzer oder sogar Verbindungsabbruch können die Folge sein.

Abschließende Bemerkungen zu den Testergebnissen

Beide Geräte zeigten eine exzellente Performance und sehr gute Implementationen zur Erkennung von P2P-Verkehr. Wenn sich die Tester beim EANTC die Ergebnisse der anderen Hersteller anschauen, die einer Veröffentlichung widersprochen haben, können diese nur dringend dazu raten, vor einer Integration solcher Geräte entsprechende Funktionalitäts-, Performance- und Redundanztests durchzuführen.

Einen ausführlicher Bericht zu den in diesem Artikel beschriebenen Tests hat das EANTC in den beiden amerikanischen Online-Magazinen Internet Evolution und Lightreading veröffentlicht. *(AW)*