

State of the Art in Peer-to-Peer Performance Testing



European Advanced Networking Test Center

About EANTC

The European Advanced Networking Test Center (EANTC) offers vendor independent network quality assurance since 1991



EANTC Berlin, Germany

Business Areas

- Test and certification of network components for manufacturers
- Network design consultancy and proof of concept testing for service providers
- Request for Proposal (RfP) support, acceptance testing and network audits for large enterprises and government organizations



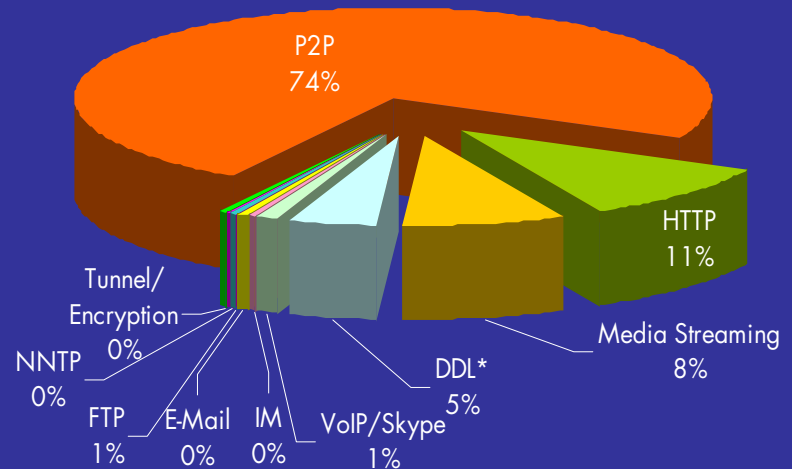
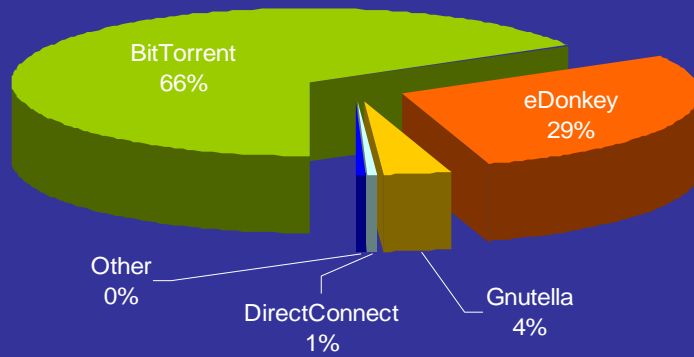
Agenda

1. How much P2P traffic is out there today?
2. What categories of DPI detection solutions exist?
3. How is EANTC testing P2P filters? What are the key performance indicators?
4. What were the results of the InternetEvolution test?

P2P Internet Statistics

Traffic Statistics Germany

P2P Protocols in Germany



* DDL: Direct download links of one-click file hoster like RapidShare.com or MegaUpload.com

Source: ipoque Internet study 2007

P2P Detection – Signature Based

- Each P2P protocol has its own mechanism to manage the P2P network and coordinate the traffic distribution
- P2P filter devices search for protocol specific pattern (signature) in each IP packet to identify P2P traffic
- Deep Packet Inspection (DPI) - once the signature is identified the detection reliability is high
- Encrypted P2P traffic is hard to identify with this method

BitTorrent Signature Example

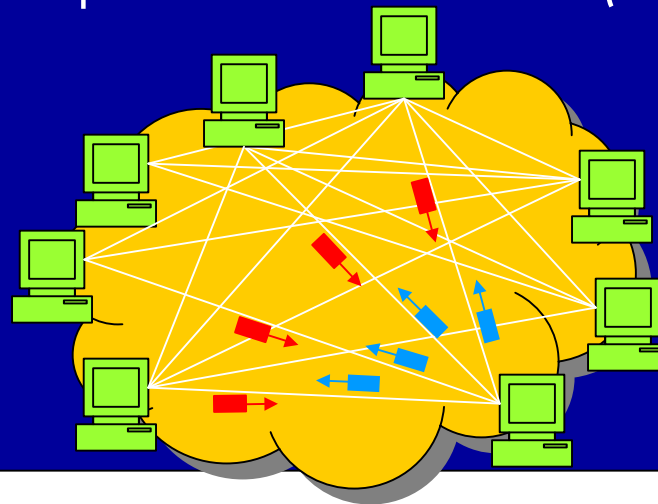
```
⊕ Frame 129 (122 bytes on wire, 122 bytes captured)
⊕ Ethernet II, Src: Fujitsus_c3:4d:cd (00:30:05:c3:4d:cd), Dst: Fujitsus_c3:4d:15 (00:30:05:c3:4d:15)
⊕ Internet Protocol, Src: 130.149.225.53 (130.149.225.53), Dst: 130.149.225.124 (130.149.225.124)
⊕ Transmission Control Protocol, Src Port: 44525 (44525), Dst Port: 3589 (3589), Seq: 0, Ack: 0, Len: 68
⊖ BitTorrent
  Protocol Name Length: 19
  Protocol Name: BitTorrent protocol
  Reserved Extension Bytes: 8000000000000000
  SHA1 Hash of info dictionary: B122FAE8F6A10077EAD34DC981AD57A739322A6E
  Peer ID: 2D415A323530342D347546475851504466693847

0000 00 30 05 c3 4d 15 00 30 05 c3 4d cd 08 00 45 00  .0..M..0 ..M...E.
0010 00 6c c3 3c 40 00 80 06 6f 72 82 95 e1 35 82 95  .l.<@... or...5..
0020 e1 7c ad ed 0e 05 7b 6f a4 2c 91 29 72 6f 50 18  .l [a] or
0030 ff bb e1 5e 00 00 13 42 69 74 54 6f 72 72 65 6e  ...A...B itTorren
0040 74 20 70 72 6f 74 6f 63 6f 6c 80 00 00 00 00 00  t protoc ol.....
0050 00 00 b1 22 fa e8 f6 a1 00 77 ea d3 4d c9 81 ad  ".....
0060 57 a7 39 32 2a 6e 2d 41 5a 32 35 30 34 2d 34 75  W_92*n-A Z2504-4U
0070 46 47 58 51 50 44 66 69 38 47  xQpdf1 8G
```

BitTorrent Signature

P2P Detection – Behavior Based

- P2P software implements mechanism to avoid detection – obfuscation (e.g. encrypted transfer)
- P2P traffic has specific behavior:
 - Each client opens connections to many other clients
 - file/tracker requests and file search (mostly not encrypted)



- ← File Search/Request (not encrypted)
- ← File Transfer (encrypted)

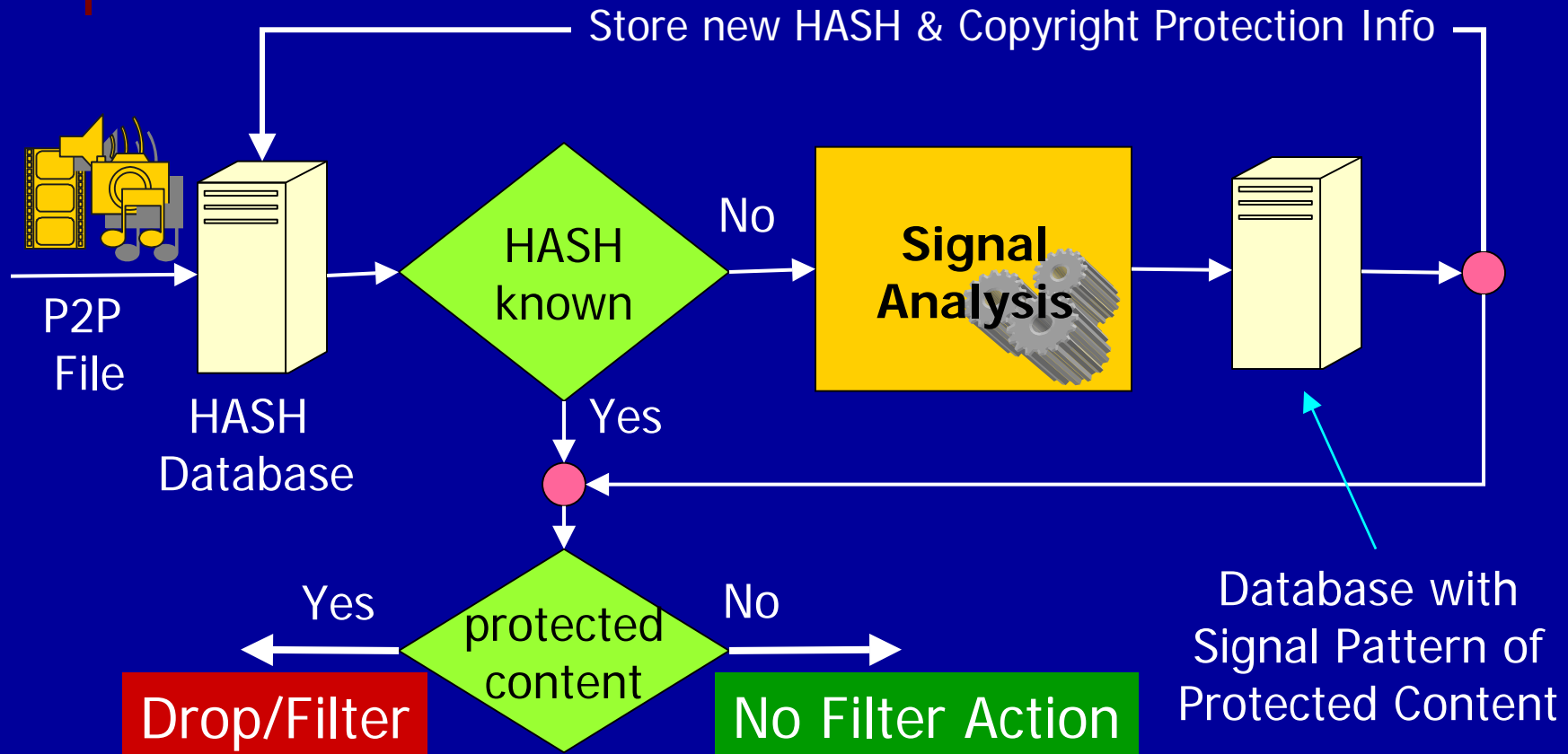
P2P Detection – Behavior Based

- Some P2P filtering devices detect P2P based on the behavior
- Encrypted P2P protocols can be detected by behavior based filter, as you can see on our test results (published on Internet Evolution)
- Compared to the signature based filtering false positive rate could be higher (other application with similar behavior)

Detecting the Content, not the Protocol

- Not all P2P traffic contains copyright protected content
- P2P is also used to distribute open source material (software, documents) like Linux
- Not all music and video files are copyright protected
- Need for distinguish between copyright protected material and free material
- New filter solutions provide the capability to identify copyright protected material in file payload

Content Recognition – How It Works



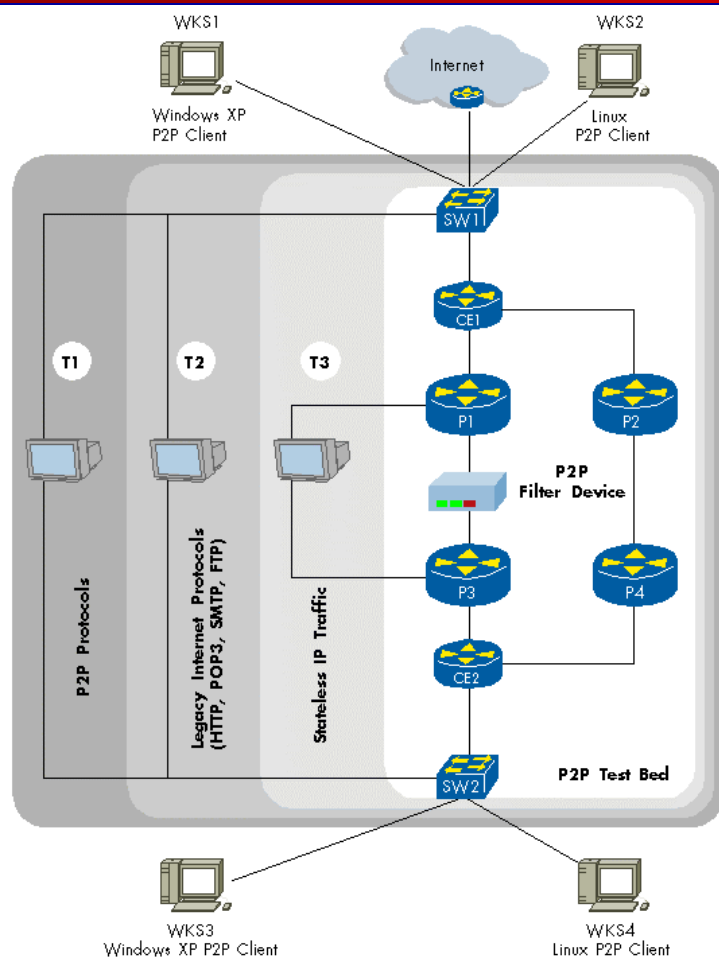
EANTC Test in **internet evolution**

- In March 2008, Internet Evolution published first results of EANTC's independent performance and functionality test of P2P filter solutions
- 28 vendors invited, only 5 agreed to take part
-> only under the condition that if they didn't like their results they could withdraw from publishing the results
- Three vendors exercised their veto right
- Only two vendors agreed with publication:
 - Arbor/Ellacoya, based in the U.S.
 - ipoque GmbH, a German vendor

http://www.internetevolution.com/document.asp?doc_id=148803

http://www.eantc.com/test_reports_presentations/test_reports.html

EANTC Test Setup



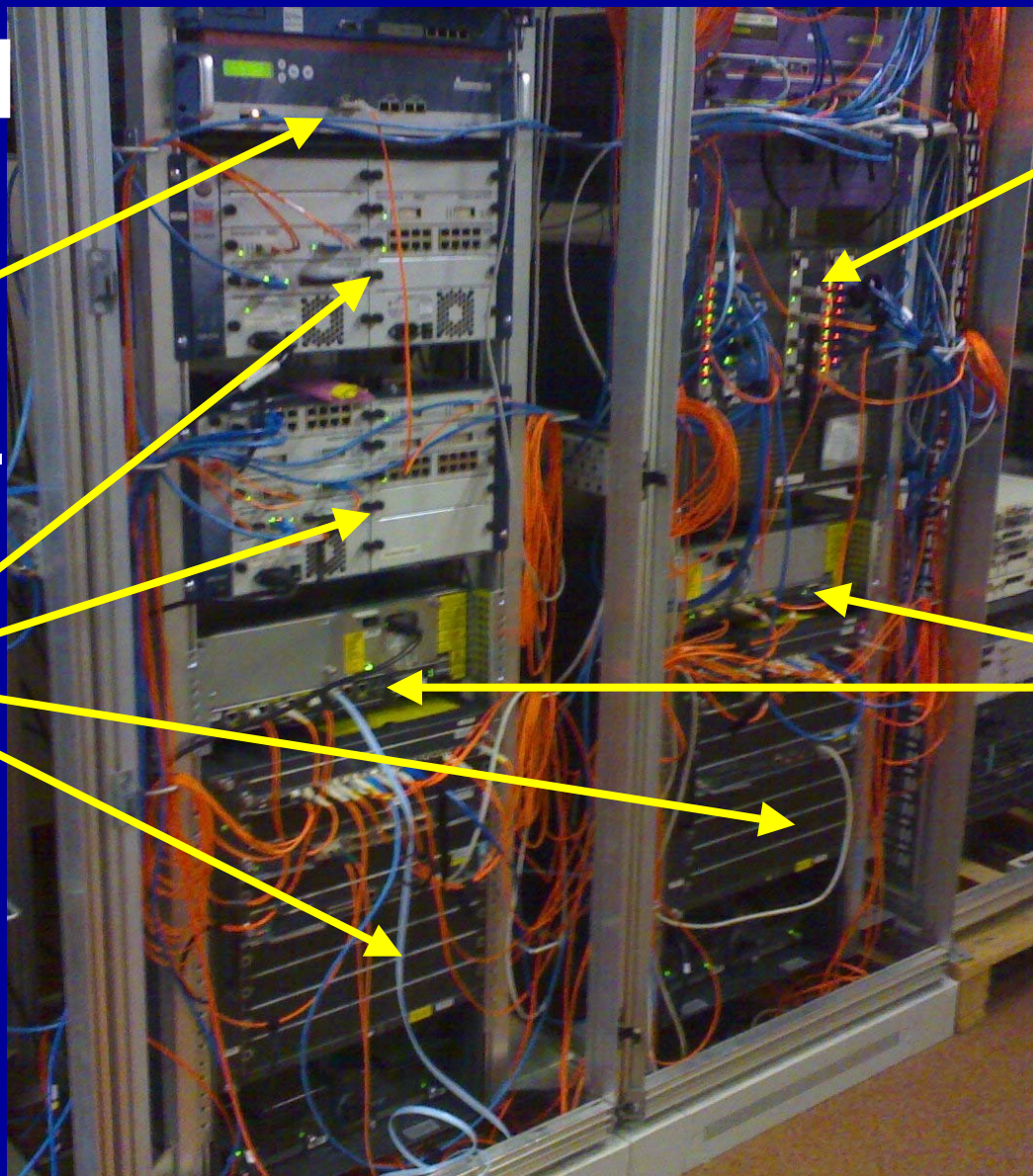
- Up to 10 Gbit/s
- Up to 1 million TCP sessions
- Emulated 13 different P2P applications
- Emulated HTTP, FTP, SMTP, POP3, RTP

Test Bed

**Device
under Test**

**Core
Routers**

Staged at
EANTC lab,
Berlin

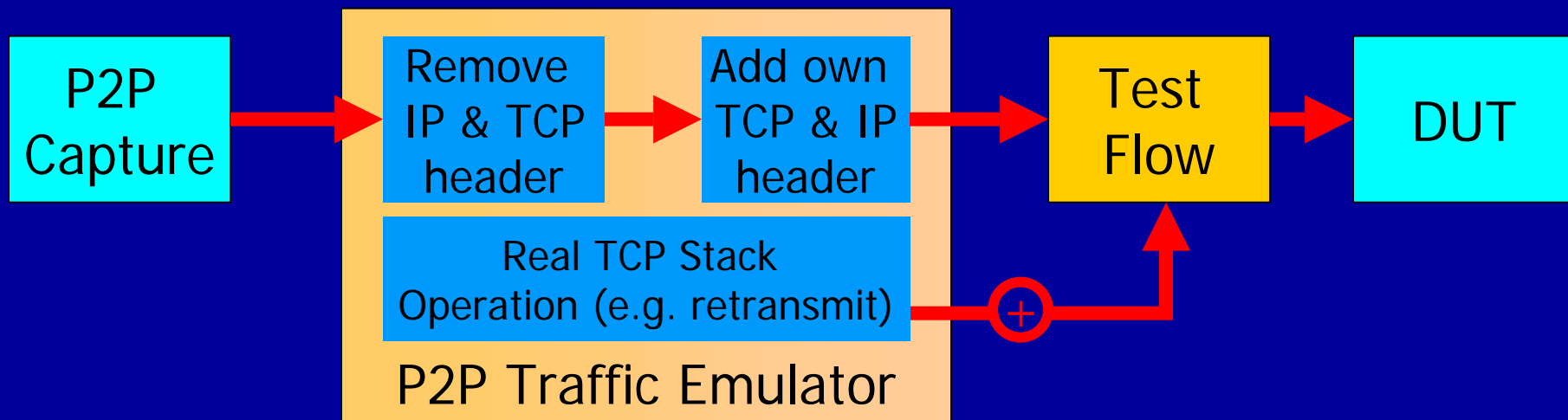


**Load
Generators
(Shenick, Ixia)**

**Edge
Routers**

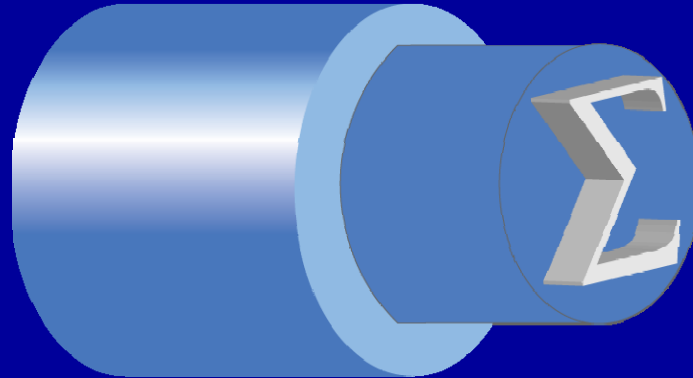
Emulated P2P Traffic – How it Works

- Real stateful TCP stack used by the traffic emulator
- P2P traffic pattern is captured during live operation of P2P clients and put into own TCP stack

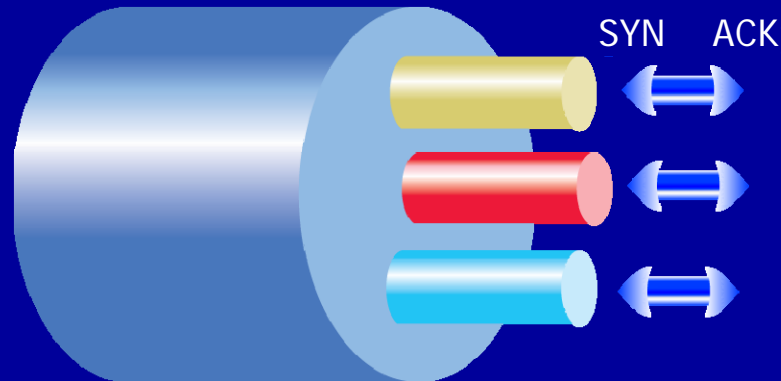


Shenick DiversifEye P2P Emulation

Traditional
Stateless L2/3
'Packet blast' model



Shenick diversifEye™
Stateful L2-7 traffic
Per Application Flow

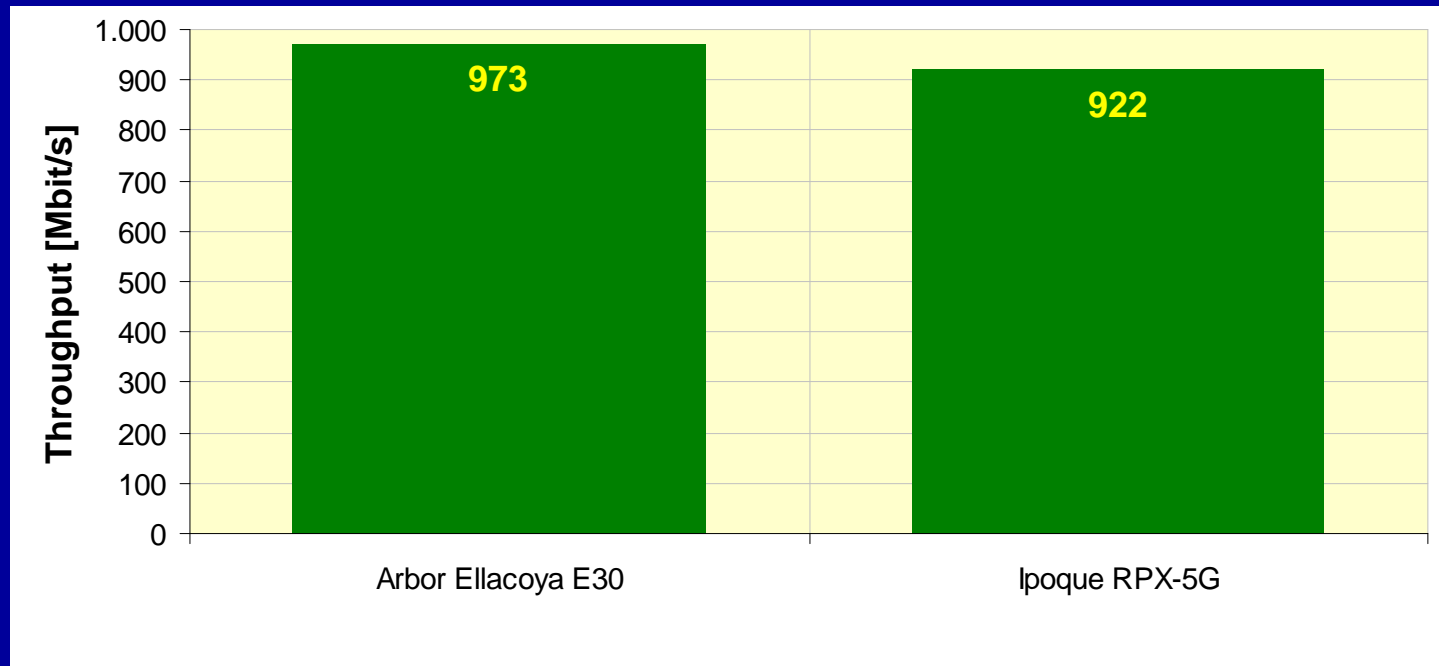


Testing P2P Filtering - Throughput

- Maximum throughput of the DPI device :
 - Large session numbers of different applications like P2P, WWW, email, and file transfers
- Does the DUT still have sufficient resources left?
 - To forward large numbers of sessions without packet loss
 - And without increased latency
- Application-layer traffic handling is an important metric
 - Challenge is to perform real-time P2P session analyses
 - Ability to handle a large number of unique flows is important

Testing P2P Filtering - Throughput

- Both Ellacoya and Ipoque showed excellent throughput

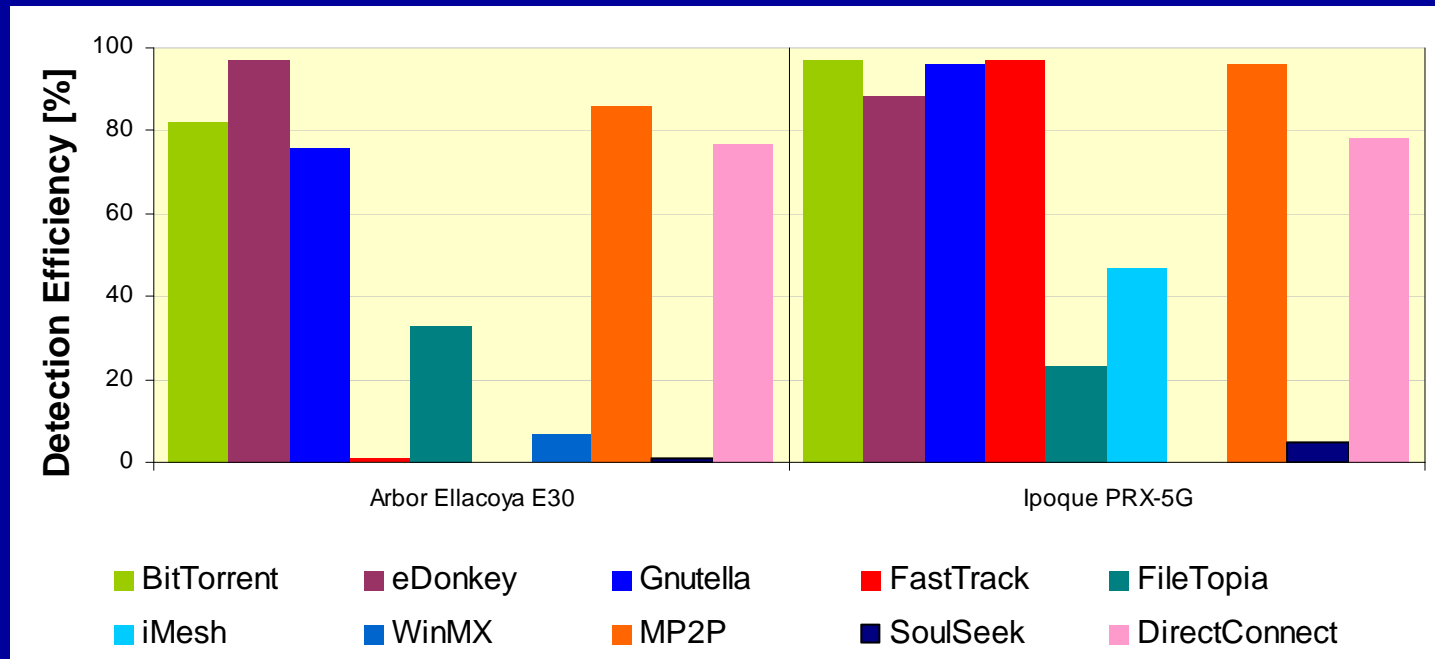


Testing Recognition Accuracy

- P2P protocol recognition
 - Accurate reports of application/bandwidth usage support service providers to take educated decisions regarding P2P traffic control
- Accurate P2P bandwidth regulation
 - DPI filter is used to regulate P2P traffic in many cases
 - Regulation means applying a bandwidth limit, not just blocking P2P traffic completely
 - Regulation requires good detection capabilities – only detected P2P sessions can be regulated

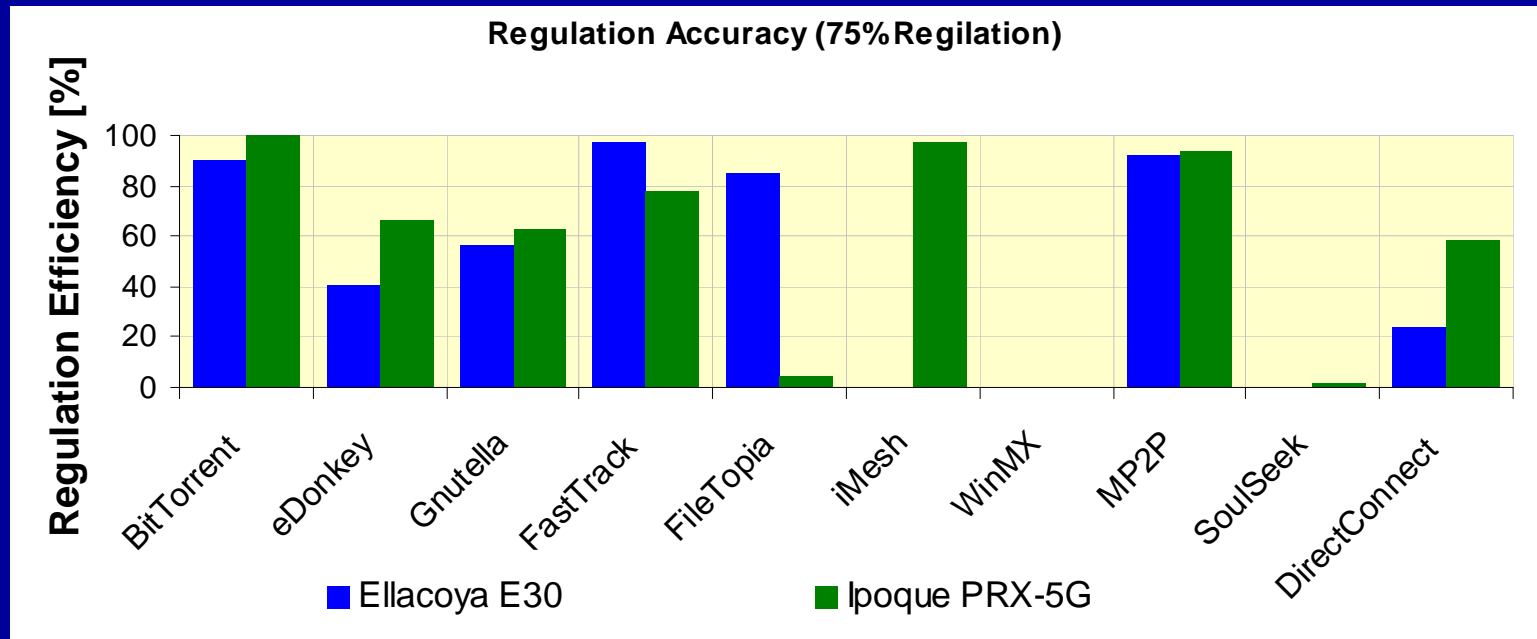
Testing Recognition Accuracy

- Good detection accuracy for the two major protocols BitTorrent and eDonkey (95% market share)



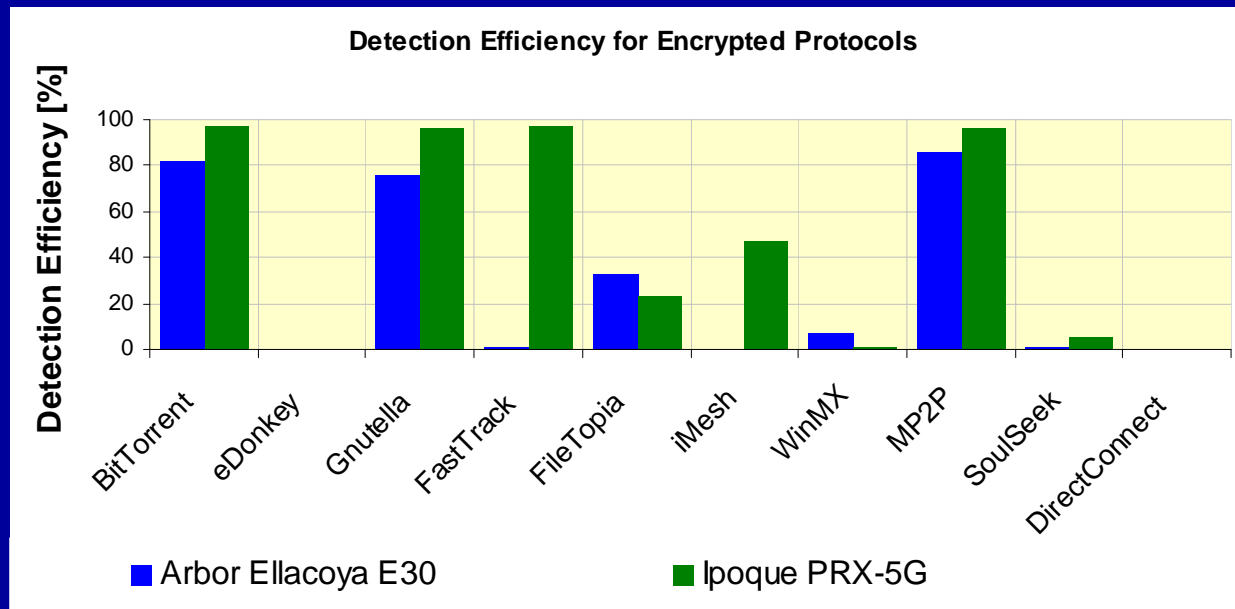
Testing Regulation Accuracy

- Similar results for both devices
- Accurate recognition is required to achieve good regulation results



Testing Detection of Encrypted Traffic

- *Single* intent of encryption/obfuscation is to prevent detection
- Some encrypted protocols were detected by both devices
- Encrypted Freenet & eDonkey never detected



Outlook

- Market for P2P filtering grows (specifically in countries not dealing with „NetNeutrality“)
- State of the art in DPI filtering advances fast
- Important to keep pace, improving test methodology in parallel
- EANTC continues to test DPI solutions for vendors and service providers

Thank You For Your Interest!

For further information, please contact us:

EANTC AG
Einsteinufer 17
D-10587 Berlin
Germany

Phone: +49.30.318 05 95-0
Fax: +49.30.318 05 95-10
E-mail: info@eantc.de
www.eantc.de