

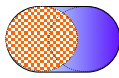
Mission Brief: Peer-to-Peer (P2P) How to be Combat it!!



Questnet 2005



Operational Background





www.allot.com

P2P – Definition*

- A **Peer-to-Peer (P2P)** computer network is a network that relies on computing power at the edges (ends) of a connection rather than in the network itself. P2P networks are used for sharing content like audio, video, data or anything in digital format.
- All peers can access other peers' available resources for free sharing of anything from Linux distributions to music and video.
- Collaboration tools - including messaging and more recently, Internet telephony (VoIP).
- Basic P2P technology has been around for a long time – Usenet, Fidonet, etc..

* From Wikipedia, the free encyclopedia.

3



www.allot.com

The Birth of Modern P2P - Napster

- Shawn "Napster" Fanning created Napster in 1999 to provide an easy way to download music.
- First widely-used P2P music sharing service
- Its technology allowed music fans to easily share MP3 format song files with each other.
- There were over 20 million users worldwide by end of 2000.
- Several lawsuits later, the Napster network was shutdown in July 2001.



4

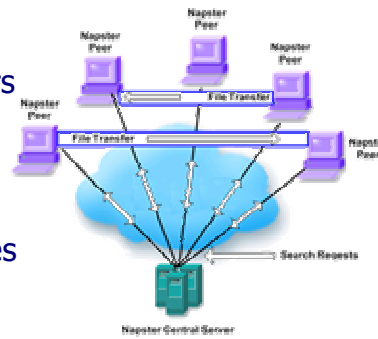




www.allot.com

1st Generation – Napster Model

- Comprises a centralized network
- Requires individual computers (peers) to log into a central indexing server, which maintains information on all connected peers and the files they share
- Peers query this server, which provides the contact details of all peers owning that file
- The requesting peer then accesses these peers to initiate a transfer directly.
- Used a fixed TCP port number



5

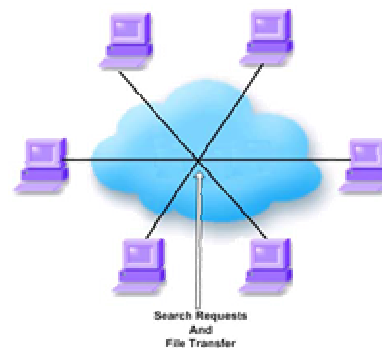
Allot
Communications
The Traffic Management Company™



www.allot.com

2nd Generation – Decentralized P2P

- No central server exists
- All peers "respond" and share files directly with other peers
- To make the searches more efficient, the flooding method is used: peers send search queries to other peers, which forward the query to other peers until the file requested is found
- Searches often scour thousands of peers before a result is found, however, reducing distributed P2P
- networks' hit ratio and search speed significantly.



6

Allot
Communications
The Traffic Management Company™



www.allot.com

"Evasion Techniques"

- **Port-hopping** - No fixed port number; instead, each peer uses a random or manually defined port number.
- **Well-known ports.** Some P2P applications use port 80, the official HTTP port, to evade firewall restrictions, gaining access to the Internet.
- **HTTP Tunneling.** On many enterprise networks, Internet access is only available when using an HTTP Proxy. Applications that are not HTTP-based and not accessible via an HTTP proxy cannot reach the Internet. To bypass such restrictions, many P2P applications have adopted HTTP as their base protocol, evading the network administrator once again.

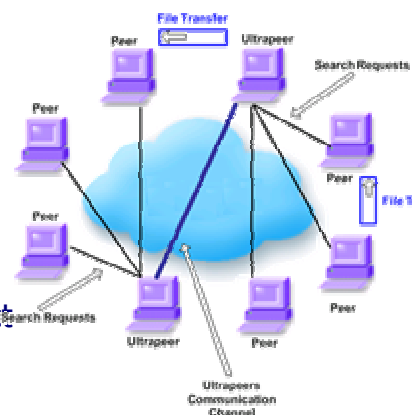
7



www.allot.com

3rd Generation – Hybrid P2P

- Hybrid network is a compromise between the centralized and distributed structures.
- These networks use ultrapeers (or super-nodes) acting as central servers to keep the network distributed while maintaining good search and hit ratios, speed and network scalability
- Peers are randomly chosen to act as ultrapeers, providing indexing services for a small number of peers while communicating with other ultrapeers



8





www.allot.com

Future P2P

CURRENT (WINNY/FREENET)

- Files are entered into the network then stored transparently by the Nodes.
- Files cannot be intentionally deleted once added to the network.
- Files are stored transparently on each Node they pass through, multiplying the potential sources for a file.
- If files are not accessed for a period of time, they time out and are deleted automatically from the Nodes.
- The network itself is a vast storage device that nodes access.
- Traffic is encrypted – HTTPS, Tunneling, etc..

9

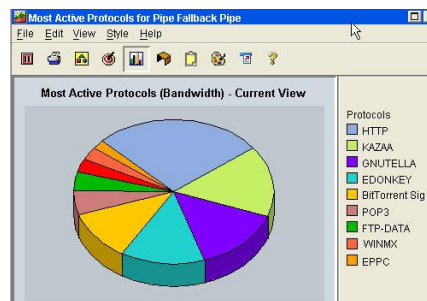


www.allot.com

P2P Downloads & Usage

P2P Application

P2P Application	Total Downloads*
Kazaa	240,759,939
Morpheus	113,014,928
Imesh	52,262,345
AudioGalaxy	31,408,240
BearShare	19,070,465
LimeWire	15,420,551
Grokster	8,445,256
WinMX	6,191,639
Blubster	3,361,874
Xolox	2,290,756
FileNavigator	1,250,260
Find MP3	1,217,585
EDonkey	920,180



Major Australian ISP with over 600Mb bandwidth (12/04)

* 2003 figures Source Download.com (CNet)

10





www.allot.com

Threat Assessment



11

satellite carrier SLA info enterprise service providers



www.allot.com

P2P: New and increased risks faced

- **Legal Risks:** Increased risk of corporate liability for actions of end-users. Increased risk of corporate liability due to P2P activity of other companies/subscribers that use your ISP.
- **Security Risks:** Increase in number and complexity of P2P-specific viruses.
- **Infrastructure Risks:** Increase in sharing of large files (i.e. 500+ Mb, movies and software) creates an unexpected bandwidth cost for the corporation.

12

satellite carrier SLA info enterprise service providers





www.allot.com

External Influencers

- BSA Business Software Association
- RIAA Recording Industry Association of America & Australia
- MPAA Motion Picture Association of America
- NMPA National Music Publishers Association
- IFPI International Federation of the Phonographic Industry

13



www.allot.com

Recording Industry Tactics

- PC Lockup: Placing code within files that would lock-up the PC on a P2P network
- Spoofing: Flooding the P2P network with low-quality or damaged versions of music files.
- Baiting: Placing a desirable file on the P2P network then determining the identity of the persons who choose to download it.
- Legal Action – Australian University and ISP Raids
 - Latest US court action against Grokster and Streamcast

14





www.allot.com

Security Risks

- **Distributed Denial of Service (DDOS)** - These viruses contains code that force the infected PC to participate in a DDOS, where the infected PC repeatedly connects and disconnects to specific websites.
- **Disable Anti-Virus and/or Firewall** - These viruses attempt to delete and/or disable the anti-virus and/or personal firewall applications installed on the infected PC.
- **Trojan/ Hack/ Keylogger** - These viruses generate malicious activity that represents a potentially severe threat to corporate security. Trojans open a port (channel) on the infected PC that can be used by an attacker/hacker to connect to the PC. Trojans can enable almost everything for an attacker to do harmful things like viewing/modifying/deleting data, accessing the network, etc.

15



www.allot.com

Security Risks Cont..

- **File Deletion/Infection** - These viruses will destroy specific file types, such as DOC (Word), MPG (movies) and MP3 (music). They may also infect data files (DOC, XLS) with the virus itself (i.e. 'push-mode').
- **Infect MS-Messenger** - These viruses will use MS-Messenger to distribute the virus – disguised as another file – to any and/or all of the online users listed on the users MS-Messenger 'buddy list'.
- **P2P-Applications and 3rd Party Malware** '*Malware*' collectively describes browser-based applications that are deemed as 'adware' (pop-ups, banners), 'trackware' ('context sensitive toolbars') or spyware (silent applications that track and transmit your web browsing habits).

16





www.allot.com

Infrastructure Risks

- **Increased Usage & Over-usage:** A few P2P users can disproportionately consume most/all of the bandwidth intended for a much larger user base.
- **Usage patterns disrupted:** Previously, one could anticipate peak usage at certain times of the day and lower usage at other times. With P2P applications, the PCs can automatically transfer data throughout the day (and overnight).
- **Upstream/Downstream traffic ratios reversed:** upstream traffic is much larger then the downstream traffic. This results in network congestion on the link that was never planned for with initial deployments.

17

satellite enterprise carrier SLA online service provided



www.allot.com

Combat Strategy



18

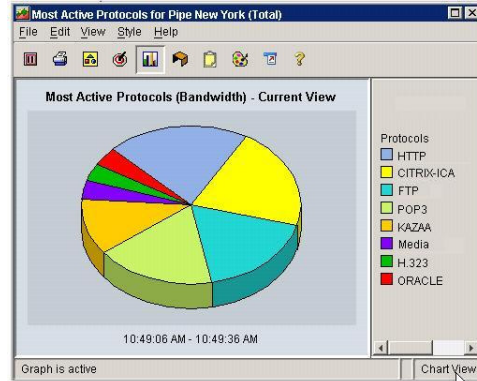
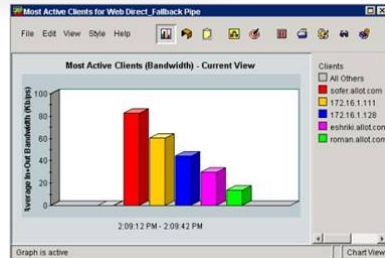
satellite enterprise carrier SLA online service provided





www.allot.com

Recon - Monitoring the Situation

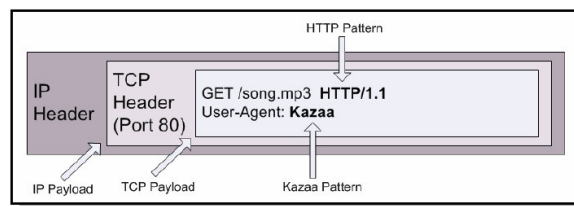


Allot
Communications
The Traffic Management Company™



www.allot.com

Intelligence - The Signature



Deep Packet Inspection – Layer 7 and beyond

- New P2P Applications are arriving all the time.
- Allot releases new signature updates once every 1-2 weeks.
- Allot's advantage in the Service Provider market – they will identify a new P2P application within hours of release.

Allot
Communications
The Traffic Management Company™



www.allot.com

Know the Enemy

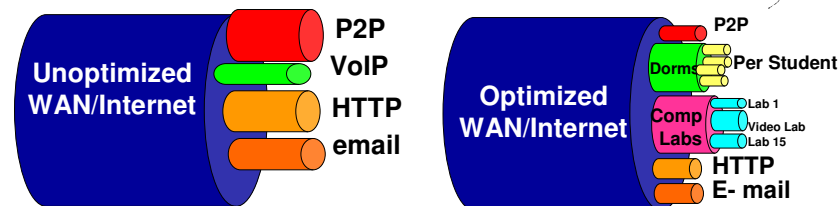
- Ares Lite
- Ares Galaxy
- BitTorrent
- Azureus BitTorrent
- BitComet
- G3 Torrent
- Direct Connect
- DC++
- BCDC++
- Opera's DC (oDC)
- RevConnect
- Earthstation V
- eDonkey
- eMule
- xMule
- ExoSee
- FastTrack
- Diet Kazaa
- Download Accelerator Pro
- Grokster
- Kazaa (v1 & v2)
- PeerEnabler
- Poisoned
- Jabber
- FileTopia
- Freenet
- Frost
- Furthur
- giFT
- Gnutella
- Acquisition
- Ares
- Bearshare
- FreeWire
- Gluz
- Gnucleus
- Gtk-Gnutella
- KCeasy
- LimeWire
- LordofSearch
- NEONapster
- Nova
- Phex
- Shareaza
- XoloX
- Hopster
- HotLine
- Madster-Aimster
- MP2P
- Motilino
- Blubster
- Piolet
- RockitNet
- Multi-Network
- Epicea
- iMesh
- Morpheus
- Morpheus w/NEOnet
- Mute
- Napster2
- Overnet
- Poco
- Share
- Soribada
- SoulSeek
- WareZ
- Waste
- WinMX
- Winny (1 & 2)
- Zultrax

21



www.allot.com

Tactics: Contain and Control



Before

After



22





www.allot.com

The Control Room

Policy Editor

File Edit View Insert Catalogs Tools Settings Help

Name	In Use	Connection Source	Dir	Connection Destination	Service	Time	TOS	VLAN	Access	Quality of Service
Video	✓	Video	✓	Any	All IP	Anytime	Ignore	Any	Accept	2 mb min pip...
Trouble	✓	Trouble Host	✓	Any	All IP	Anytime	Ignore	Any	Accept	1 mb in 1 mb ...
Dorm	✓	dorm0	✓	Any	All IP	Anytime	Ignore	Any	Accept	Individual Dor...
DormD	✓	dorm4	✓	Any	All IP	Anytime	Ignore	Any	Accept	Individual Dor...
Dorm 108	✓	dorm	✓	Any	All IP	Anytime	Ignore	Any	Accept	Individual Dor...
Dorm I	✓	dorm1	✓	Any	All IP	Anytime	Ignore	Any	Accept	Individual Dor...
Dorm 14	✓	dorm14	✓	Any	All IP	Anytime	Ignore	Any	Accept	Individual Dor...
Dorm 15	✓	dorm15	✓	Any	All IP	Anytime	Ignore	Any	Accept	Individual Dor...
Dorm 19	✓	dorm19	✓	Any	All IP	Anytime	Ignore	Any	Accept	Individual Dor...
Dorms	✓	dorms	✓	Any	All IP	Anytime	Ignore	Any	Accept	Normal Prior...
ICMP	✓	Any	✓	Any	ICMP	Anytime	Ignore	Any	Accept	1 mb in 1 mb ...
HTTP Business Hours	✓	Any	✓	Any	HTTP	Business Hou...	Ignore	Any	Accept	10 mb in 10 ...
HTTP After Hours	✓	Any	✓	Any	HTTP	After hours	Ignore	Any	Accept	20 mb in 20 ...
P2P Business Hours	✓	Any	✓	Any	KaZaA-FastTr...	Business Hou...	Ignore	Any	Accept	20 mb in 5 m...
P2P After Hours	✓	Any	✓	Any	KaZaA-FastTr...	After hours	Ignore	Any	Accept	40 mb in 10 ...
Business Hours	✓	Any	✓	Any	All IP	Business Hou...	Ignore	Any	Accept	20 mb in 20 ...
After Hours	✓	Any	✓	Any	All IP	After hours	Ignore	Any	Accept	20 mb in 20 ...
Fallback	✓	Any	✓	Any	All Service	Anytime	Ignore	Any	Accept	Normal Prior...

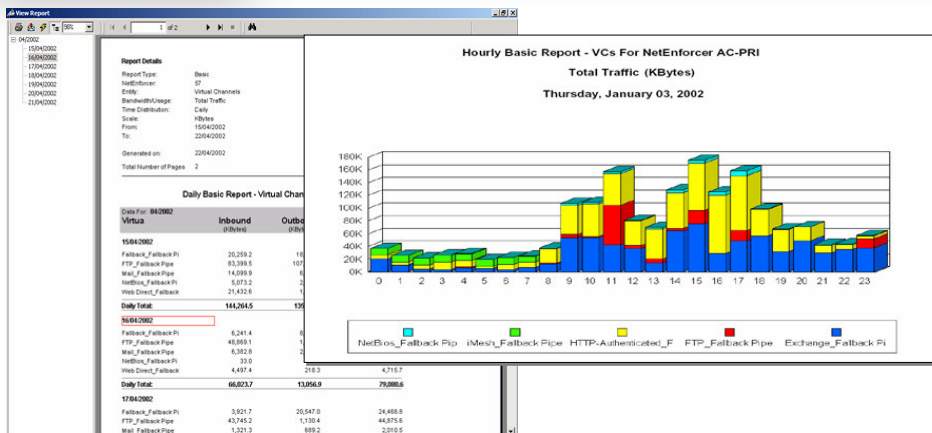
Ready

Customized View



www.allot.com

Mission Assessment





www.allot.com

Questions



25



www.allot.com

Allot – Successful Operations

- | | | |
|--|-------------------------------|--------------------------------|
| • Albert Einstein/ Yeshiva University | • Carnegie Mellon | • Concordia University |
| • Aarhus University | • Case Western University | • Connecticut College |
| • Atlanta Girls School | • Catholic University | • Cornell College |
| • Austin College | • Central College | • Cumberland University |
| • Baptist Bible College | • Central Methodist College | • Daemen College |
| • Bard College | • Champlain College | • Daemen College |
| • Belhaven College | • Chehalis School District | • Daniel Webster College |
| • Benedictine College | • Chesapeake College | • Delgado Community College |
| • Ben-Gurion University of the Negev | • Chichester College | • Dong Muang University |
| • BERRY COLLEGE | • Chosun University | • Doshisha University |
| • Birmingham-Southern College | • Chung Kang University | • Eastern Kentucky University |
| • BOCES Southern Westchester | • Cisco Junior College | • Eastern Mennonite University |
| • Boston College | • Clafin University | • EBD |
| • Brandeis University | • Cleveland State University | • Eckerd College |
| • Brevard College | • CNRS Observatoire | • Education Highway |
| • Bridgewater State College | • Colby Sawyer College | • ESD 113 |
| • Business College | • Colgate University | • ESIC (University) |
| • C.S. des Bois-Francis | • College of Abermarle | • Fachhochschule Oensingen |
| • Cal State University, San Bernardino | • College of Saint Rose | |
| • Carlow College | • College of Souther Maryland | |
| | • Columbia College | |
| | • Columbia College | |

26





www.allot.com

Allot – Successful Operations

- Fachhochschule Technikum Kaernten
- Fachhochschule Wolfenbuettel
- Fachhochschulen O?
- Fairleigh Dickinson University
- Five Towns College
- Fort Hays State University
- Geneva College
- Graceland University
- Great Basin College
- Groupe ESC-Chambery Savoie
- Gurton College
- Gwinnett Technical College
- Hamilton College
- HanYang University
- Harvey Mudd College
- Haute Ecole Galil?e
- HBK BRAUNSCHWEIG
- Hebrew University
- Helena School District
- Hong Kong University
- Hope College
- Howard College
- Husson College
- Huston-Tillotson College
- ICAM
- IEP
- Illinois Wesleyan University
- Info-Logic EBM INC
- International Islam University
- IPB – Instituto Polit?cnico de Beja
- ISC -Institut Supérieur du Commerce
- Itsos
- John Brown University
- Kagoshima National College
- Kangwon University
- Kansas State University
- Kansas Wesleyan University
- Kean University
- Khonkaen University
- Kolej University Kejuruteraan dan Teknik
- Konuren University
- Lake Forest College
- Landmark College
- Langston University
- Lawrenceville School
- Leader University
- LGCA
- Limestone College
- Lindenwood University
- Louisiana State University
- Maharakham University
- Malaspina University-College
- Marian College
- Maryville College
- Mehidol University (Computer Dpt)
- Messiah College

27



www.allot.com

Allot – Successful Operations

- Methodist College
- Michigan Tech University
- Middlebury College
- Mills College
- Millsaps College
- Minot state University
- Missouri Baptist University
- Missouri Southern State University
- Monroe Community College
- Montana State University
- Mt. Ida College
- Multimedia University
- Murray State College
- NACE
- Nassau Community College
- National Yunlin University of ScienceTec
- Nazarene Headquarters
- Netanya College
- New Hampshire College
- Nicholls State University
- North Central University
- North Country Community College
- Oberlin College
- North East Wales Institute
- Northeast Service Cooperative
- Northern Malaysia Engineering College
- Nottingham Trent University
- NTU University Singapore
- Odense Tekniske Skole
- Oklahoma Baptist University
- Oklahoma City University
- Oklahoma Wesleyan University
- Ottawa University
- Oxford University Press
- Paul Smith's College
- Pembroke College
- Peninsula Technikon
- Pepperdine University
- Philadelphia Community College
- Phillips Academy
- Politecnico
- Prince of Songkla University
- PSU -Prince Of Songkla University
- PWCS.EDU
- Queen's University
- Ramapo College
- Rand Afrikaans University
- Rice University
- Richard Stockton College of NJ
- Rider University
- Rivers Community College
- Robotiker
- Roger Williams University
- Rogers State University
- Rogers State University-1
- Saint Louis University
- Sandong University
- Sangmyoung University
- Santa Maria Joint Union High Sch. Dist.

28





www.allot.com

Allot – Successful Operations

- ✦ Sapir College
- ✦ Shue Yan College
- ✦ Siena University
- ✦ Skidmore College
- ✦ sms Tech Solutions
- ✦ Southern Illinois University
- ✦ Southern Nazarene University
- ✦ Southwest Baptist University
- ✦ Southwestern University
- ✦ Spring Hill College
- ✦ St Mary's University
- ✦ St Mary's University
- ✦ St. Lawrence University
- ✦ St. Louis College Pharmacy
- ✦ St. Mary's College- Notre Dame
- ✦ St. Norbert College
- ✦ St.Olaf College
- ✦ Sterling College
- ✦ SunMoon University tender
- ✦ Swarthmore College
- ✦ Syracuse University
- ✦ Taegu University
- ✦ Technion - Israel Institute of Technolog
- ✦ Teikyo Loretto Heights University
- ✦ Teikyo Post University
- ✦ Tel-Aviv University
- ✦ Texas Christian University
- ✦ The Art Institute of Pittsburgh
- ✦ The Hong Kong Institute of Education
- ✦ The Kings University College
- ✦ The Nottingham Trent University
- ✦ The University of Nottingham
- ✦ Three Rivers Community College
- ✦ Trinity College
- ✦ Union College
- ✦ Universidad de Oviedo
- ✦ Universit? De Neuchatel
- ✦ Universit? di Torino
- ✦ University - Flinders
- ✦ University of Central England
- ✦ University Islamic International UII
- ✦ University of Alberta
- ✦ University of Botswana
- ✦ University of Bradford
- ✦ University of Burgos
- ✦ University of California, Santa Cruz
- ✦ University of East Anglia
- ✦ University of Fribourg
- ✦ University of Hawaii at Manoa
- ✦ University of Islam International Indone
- ✦ University of Laval
- ✦ University of Maine
- ✦ University of Miami
- ✦ University of Miguel Hernandez

29



www.allot.com

Allot – Successful Operations

- ✦ University of Missouri
- ✦ University of N. Texas
- ✦ University of Nebraska
- ✦ University of Northern Iowa
- ✦ University of Nottingham (UniM)
- ✦ University of Redlands
- ✦ University of Rochester
- ✦ University of Ryukyus
- ✦ University of San Francisco
- ✦ University of St. Mary
- ✦ University of Tampa
- ✦ University of Tennessee
- ✦ University of the South
- ✦ University of Vermont
- ✦ University of Warwick
- ✦ University of Wisconsin - Whitewater
- ✦ University of Wisconsin College
- ✦ University of Wisconsin Eau Claire
- ✦ University of Wisconsin, River Falls
- ✦ University of Wisconsin-Stout
- ✦ University Of Yogyakarta
- ✦ University Village of Fresno
- ✦ UPM-National University of Agricultural
- ✦ Upper Iowa University
- ✦ UTAD
- ✦ Utica College
- ✦ UUM
- ✦ Vassar College
- ✦ Vega Business Technologies
- ✦ Vermont Tech College
- ✦ Victoria College
- ✦ Villanova University
- ✦ Waseda University
- ✦ Washington Bible College
- ✦ Washington College
- ✦ Wayne State University
- ✦ Wells College
- ✦ West Texas A&M University
- ✦ Western Carolina University (WCU)
- ✦ Western Oklahoma State College
- ✦ Westwood Independant School District
- ✦ Wheaton College
- ✦ Widener University
- ✦ WIFI
- ✦ WIFI O?
- ✦ Williams College
- ✦ WTC
- ✦ Yeosu University
- ✦ Yeshiva University
- ✦ York College of PA

30

