

Jarkko Niittylahti:

P2P

AND BANDWIDTH MANAGEMENT



Outline

- Peer-to-peer networking
- Network security issues
- Network overloading
- Compare: Distributed Denial of Service attack
- Congestion
- Solving problems due to P2P
- Fair bandwidth sharing
- Why you should not open the IP-packets
- Identifying P2P-servers
- Limiting network loads
- Example network
- Summary



Peer-to-peer networking

- P2P (peer-to-peer) causes 70% of traffic
- Distributed, fast file sharing
- 3,5 MB MP3 audio, 2,0 GB DivX video
- 75% of europeans use P2P monthly¹
- Developed in 1999, constant growth
- Numerous applications and software
- Causes equal traffic to both directions
- Kazaa, Gnutella, Morpheus, Skype, Groove, ...
- P2P -> subscribe broadband -> use P2P -> ...

¹ Jupiter Research



**Network
security
issues**

Peer-to-peer virus hits Gnutella users

From...
NetworkWorld
Fusion
AN IDG.net
S I T E

by Ashlee Vance

(IDG) -- File swapping on the Internet hit a sour note Tuesday with the appearance of a virus that attacks users of the Gnutella file-sharing service and that several security software vendors say is the first virus to affect peer-to-peer (P2P) communications.



FTC Puts Out P2P Virus, Spyware Alert

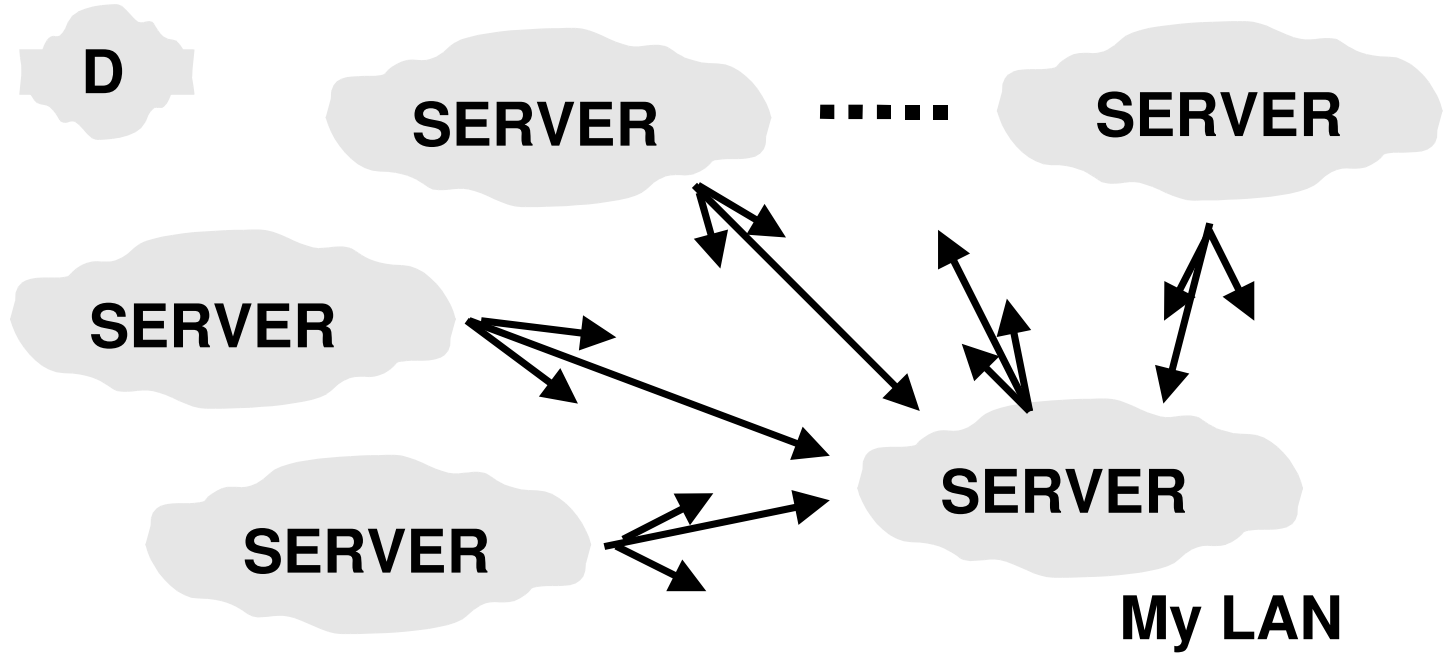
>> Charles Farrar

**SPY-WARE
GETS SNEAKY**

WASHINGTON - A formal warning to consumers about virus and spyware risks plus copyright problems and unwitting porn downloads, among other online file-swapping hazards, was released August 1 by the Federal Trade Commission.

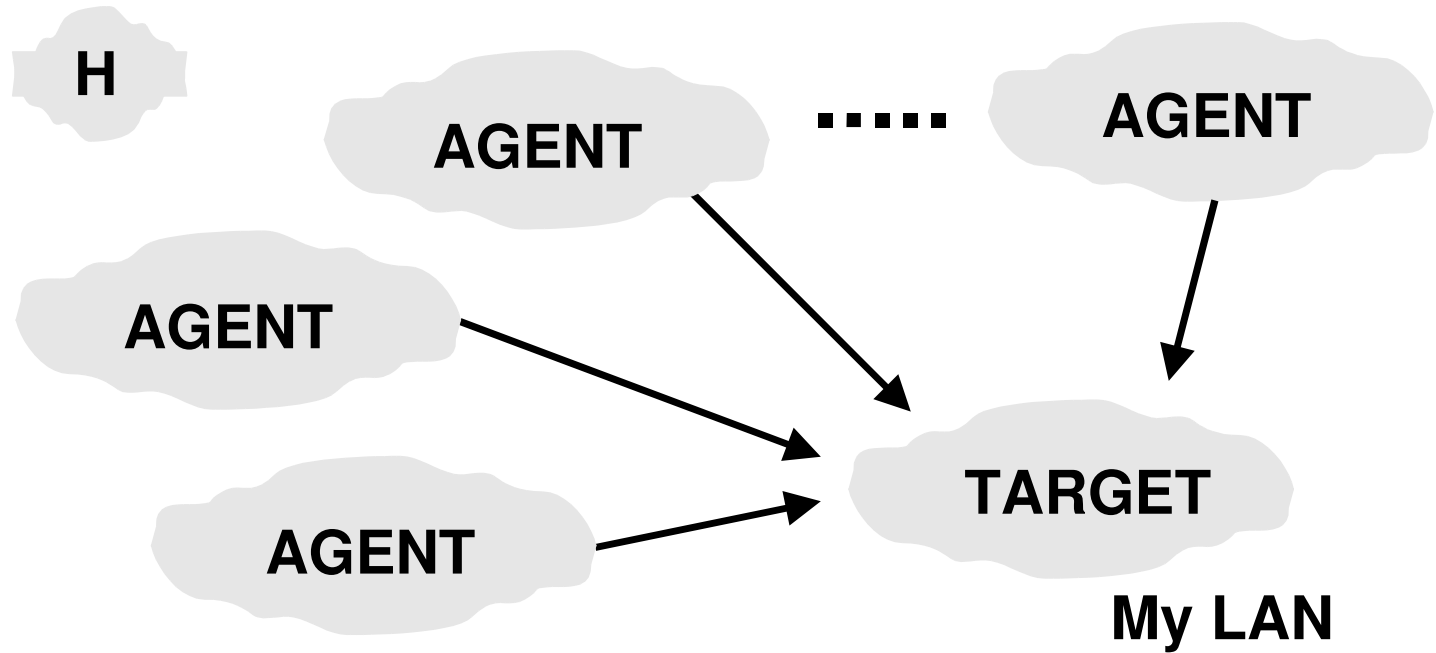
"(W)hen consumers are connected to file-sharing programs," the

- Unintentional file sharing of confidential material
- Virus in the files
- Network overloading
- Copyright violations possible
(P2P servers as such found legal in Canada)



Network overloading

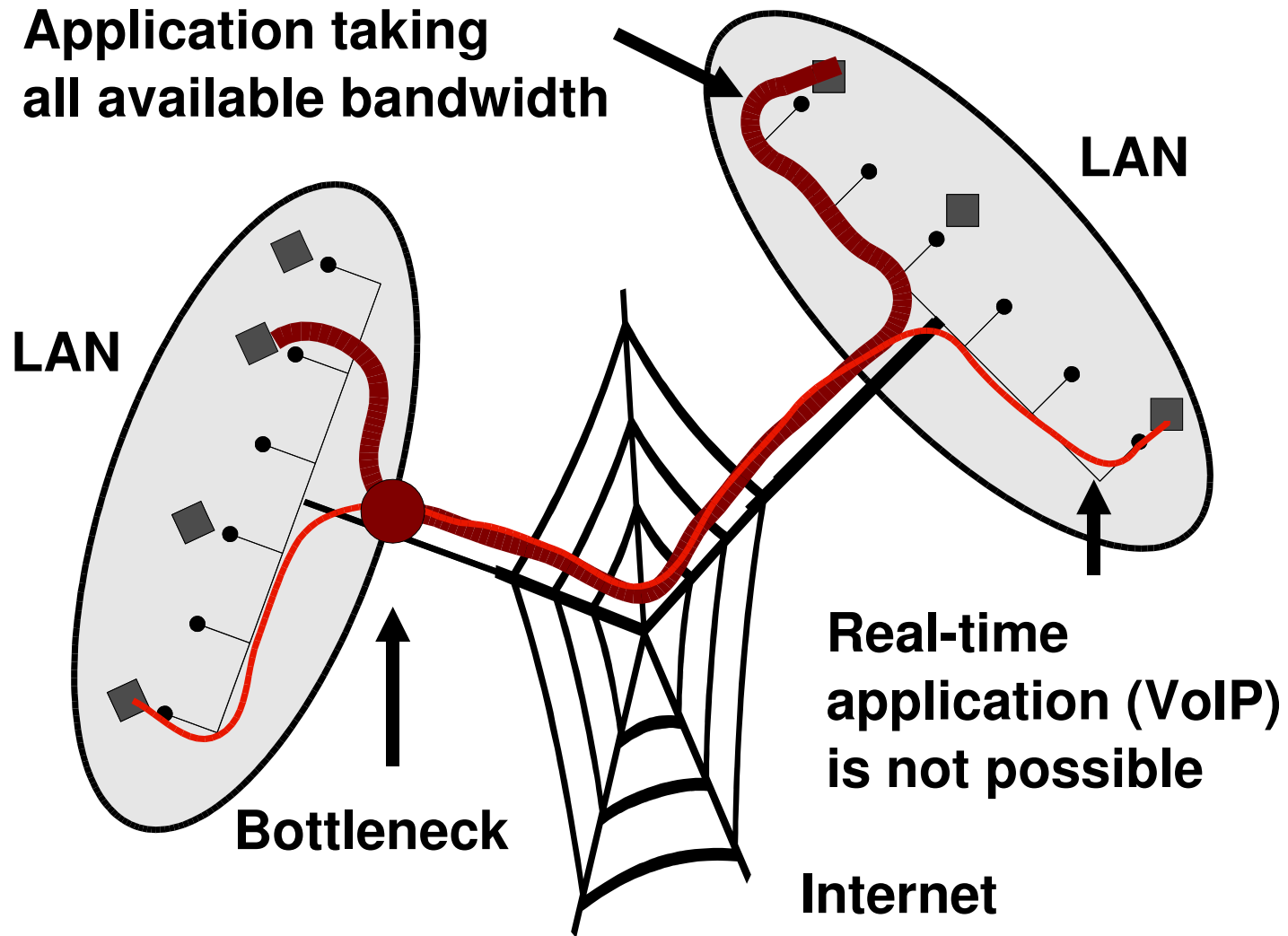
- P2P opens large number of parallel connections
- Any bandwidth and network can be filled
- Each user provides a server for others
- Directory (D) listing of material on the servers
- Each server may have large number of clients
- Large amount of traffic to both directions
- Large number of connections may overload server memory
- A single user may steal the bandwidth, everybody else suffers



**Compare:
Distributed
Denial of
Service
attack**

- DDoS (Distributed Denial of Service)
- Intended to paralyze the target network
- Large amount of traffic is sent to the target
- Large number of agents sending in parallel
- Intentional network overload
- Intentional server memory overload
- Hostile attacker (H) uses malformed IP-packages, forged IP (spoofing), viruses etc.
- Result is the same as in case of DDoS

Application taking all available bandwidth



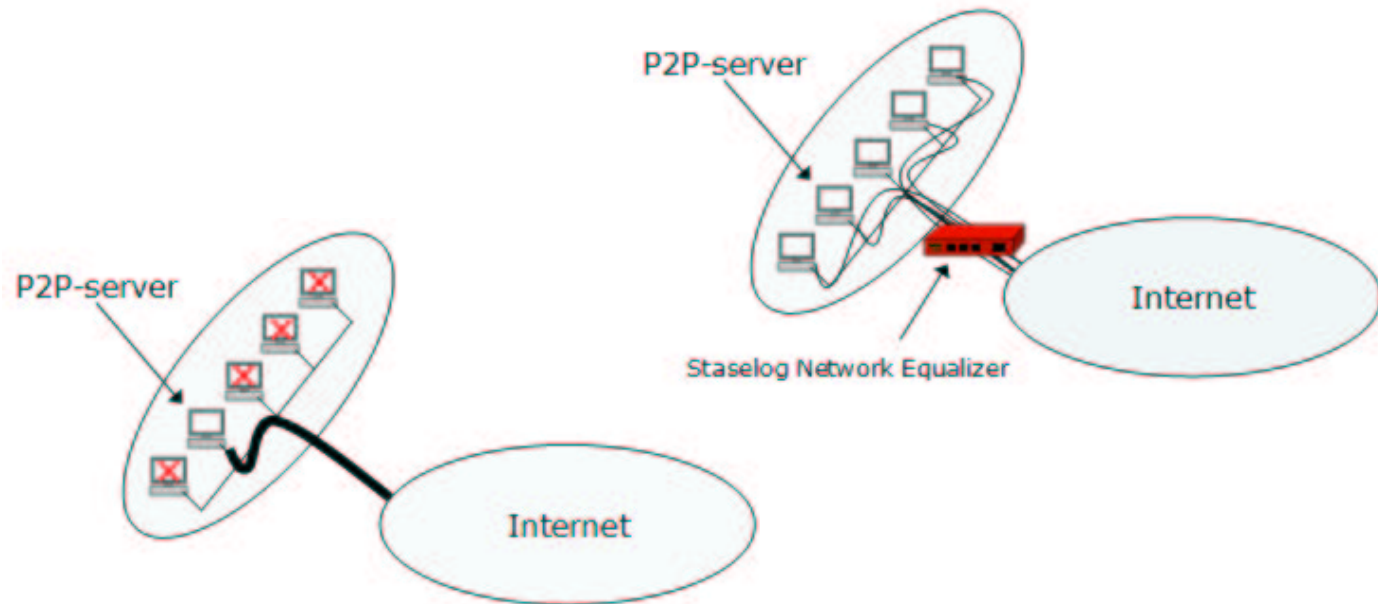
Congestion

- Certain type of traffic takes *all* the bandwidth
- > larger bandwidth is not a solution
- Slow response, poor performance
- Real time applications are not possible
- End-to-end solution is too complicated



Eliminating problems due to P2P

- 1) Increase bandwidth?
 - > more P2P usage and more problems
- 2) Decrease bandwidth?
 - > poor Quality of Service, the customers will choose another service provider
- 3) Limit P2P only?
 - > must identify the P2P traffic, which is not easy
 - > P2P users will choose another service provider
- 4) Use appropriate bandwidth management
 - > few suitable solutions exist



Fair bandwidth sharing

- In case of congestion, fair bandwidth sharing
- Everybody gets a fair share of bandwidth
- Limit the bandwidth consuming applications, guarantee bandwidth for critical applications, and make a fair share of bandwidth among users
- Eliminates congestion, P2P can be used
- A single user can not fill the whole network



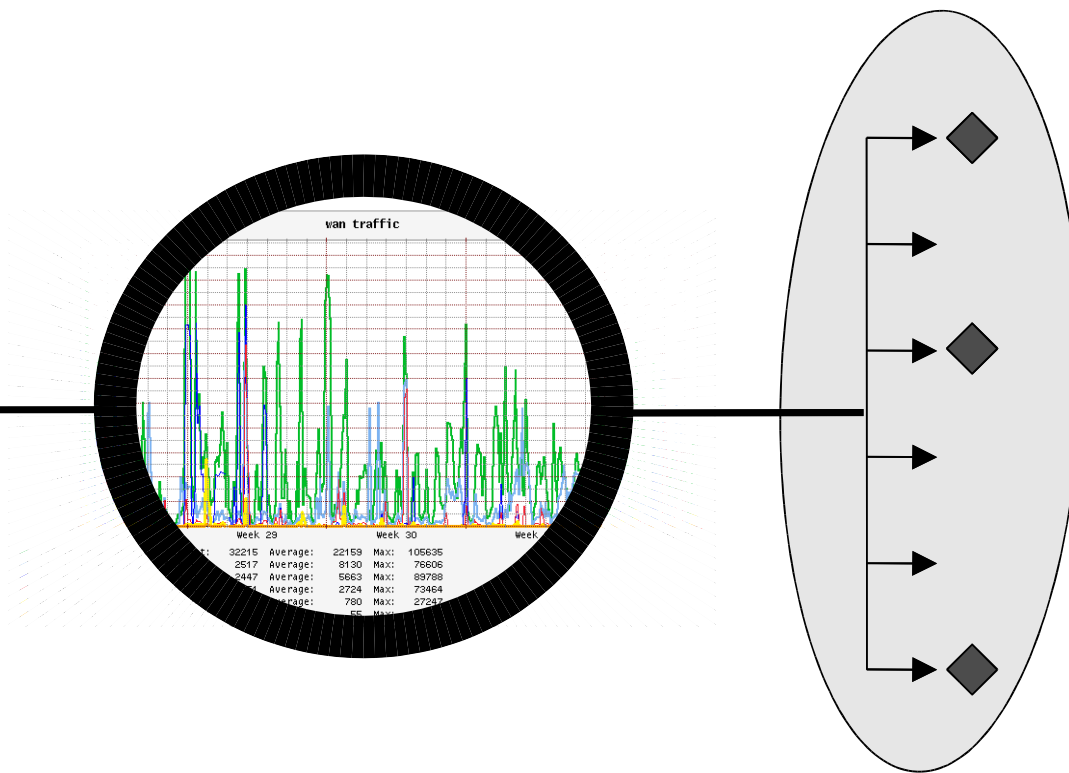
7 Application
6
5
4 Port
3 IP
2 Ethernet
1 Physical

Requires opening the packet
§?

Application by port number
User by IP address

**Why
you should
not open the
packets**

- The application is at the topmost level
- Checking layer 7 requires opening the packets
- In practise, a stateful device for tracking the connections at layer 7 is required
- New applications appear frequently, only 60% can be positively identified
- Expensive hardware needed
- Frequent software updates required



Identifying P2P servers

- In case of congestion, fair bandwidth sharing
- Everybody gets a fair share of bandwidth
- Create traffic counters for all users
- Look for large update traffic to find servers
- Use port number to identify application
- Note: a large network requires a device with high throughput and fine granularity

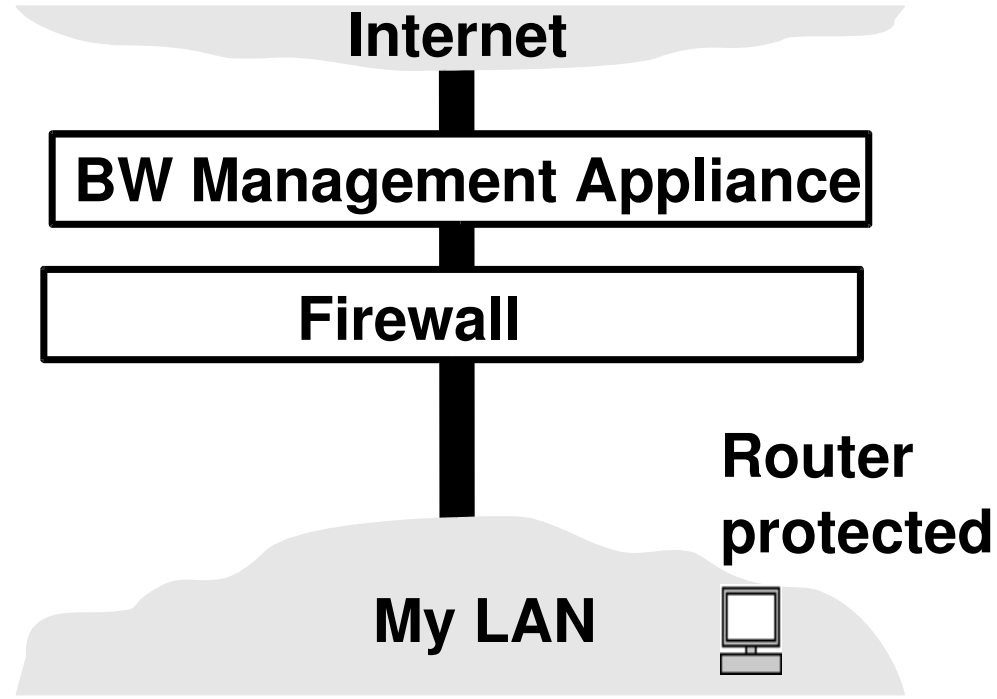


Overload protection

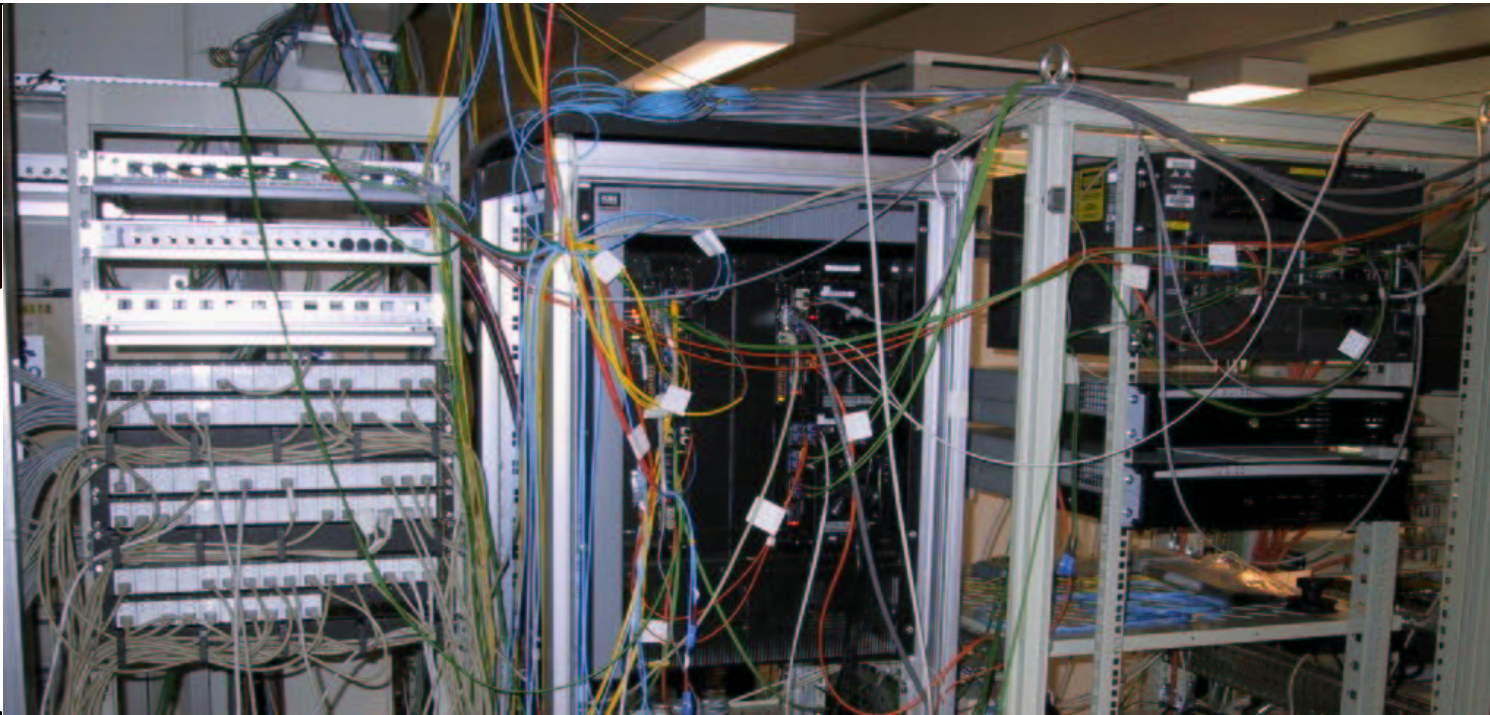
Intentional bottleneck

Firewall protected

Network protected



- In practise, it is possible to identify P2P servers without opening packets of all users
- Use stateless, bridging device
- Suitable protection device can not be overloaded
 - > Avoid network overload
 - > Avoid firewall (router, server etc.) overload
- Protection against DDoS attacks
- Smaller and cheaper hardware will be OK
- Peak loading is eliminated
- Faster network, smaller latency



Example network

- TOASNet campus network at Tampere (TUT)
- 5,000 fixed broadband users around the city with 1 Mbit/s or more bandwidth
- Internet access 100 Mbit/s (full duplex)
- 35 000 packets/second, up to 100% load
- NE200 "Big Brother" is the firewall and eliminates congestion and other P2P problems
- Traffic statistics for each user (100,000 rules)
- "The Network Solution of the Year 2003" (Elisa)

Bandwidth management appliance requirements:

High Availability

Immunity

Stand-alone

High Performance

Compatibility



Fine-grained

Bridging

Stateless

Service

- P2P overloads servers and upstream bandwidth
- A single P2P user can "steal" the whole network
- P2P can fill any bandwidth and server

Summary

- Paying customers want to use P2P
- > Banning P2P is not a solution
- Limiting P2P only (at layer 7) is not a solution
- Intelligent bandwidth management *is* a solution
- Security issues must be covered

