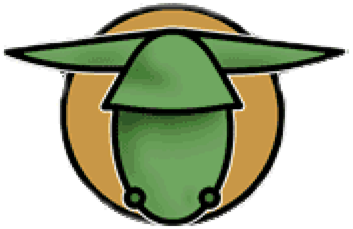
P2P Optimized Traffic Control

Riad Hartani & Joe Neil

Caspian Networks

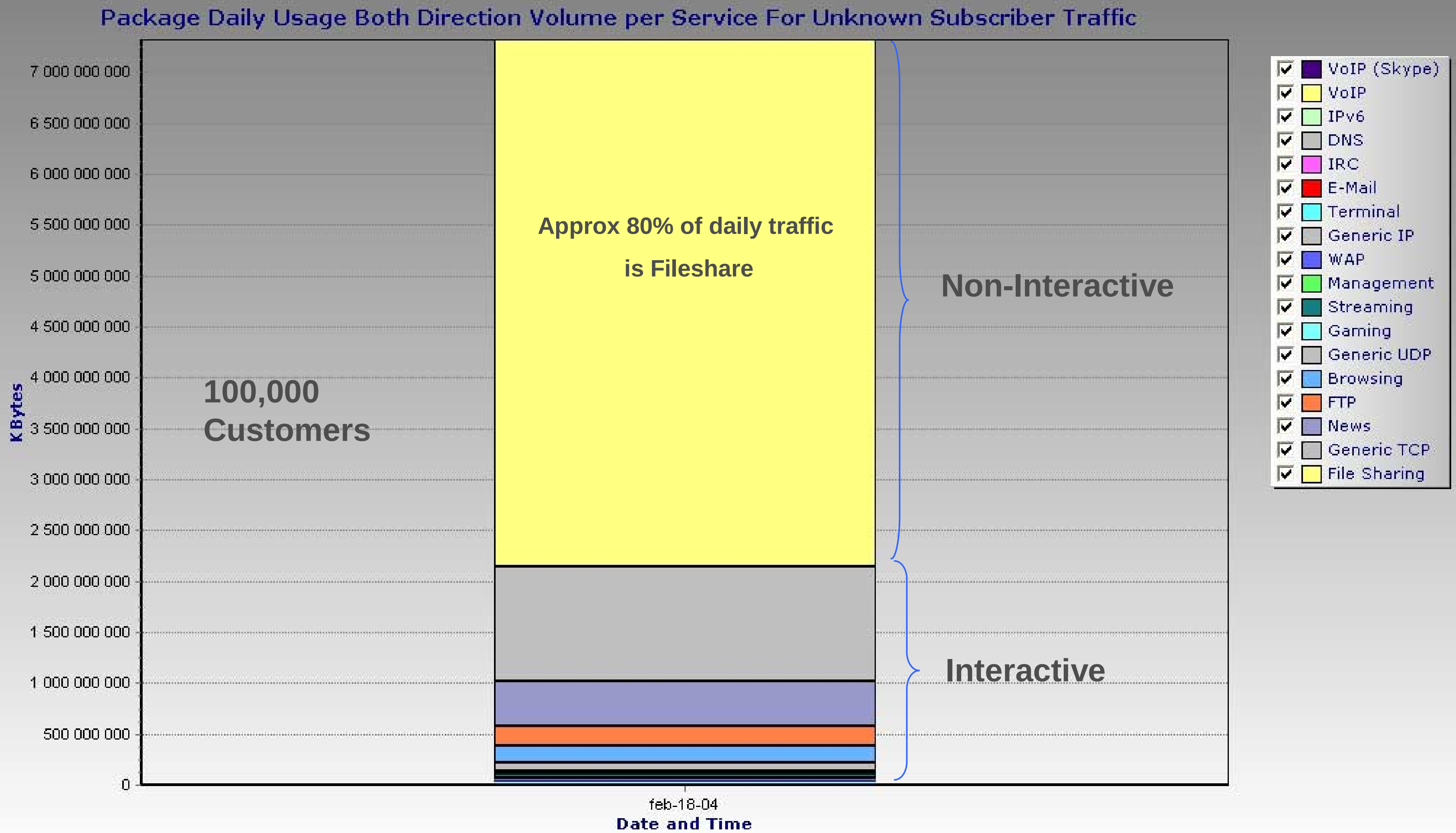
P2P Applications



WINNY

Rapid evolution of P2P applications, significant impact on network architectures and economics

Daily Traffic Volumes By Traffic Type



Approx 80% of daily traffic is Fileshare

Non-Interactive

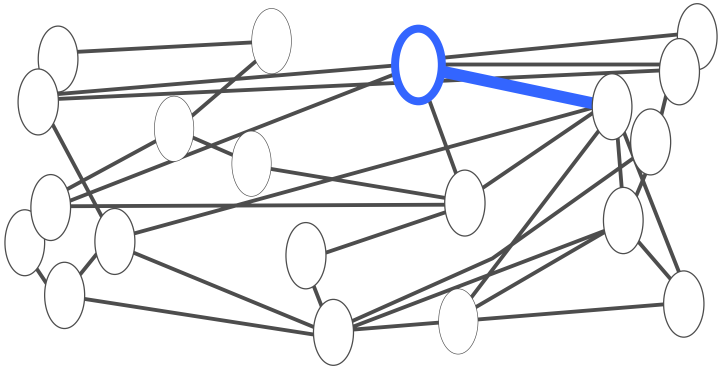
Interactive

100,000 Customers

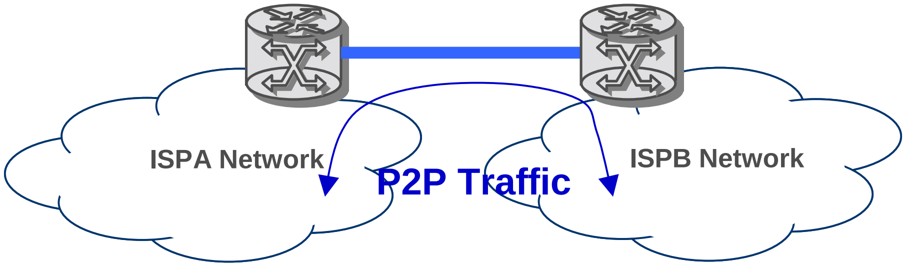
Measured on a peering link with primarily residential traffic

P2P Problem: where it surfaces

1. **Congested Link in Core or Access Network – Hot Spot**



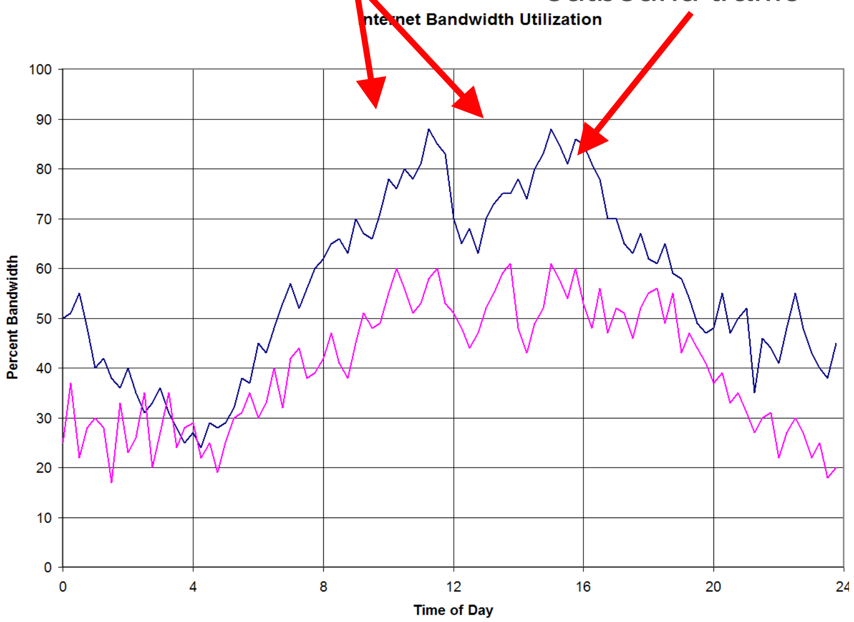
2. **Congestion at Peering Interface**
   - **>90% P2P traffic goes off-net**



3. **Congestion at undersea links (expensive and cannot throw b/w at the problem)**

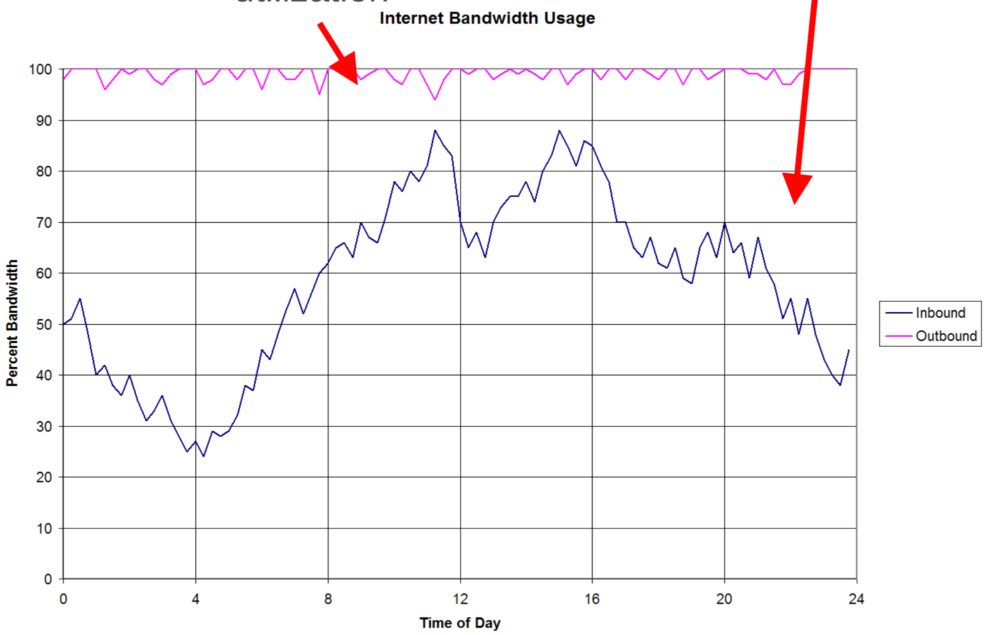
CASPIAN

P2P Changing Network Engineering Paradigm



Double-Humped Curve

More inbound than outbound traffic



Near 100% outbound utilization

More evening activity

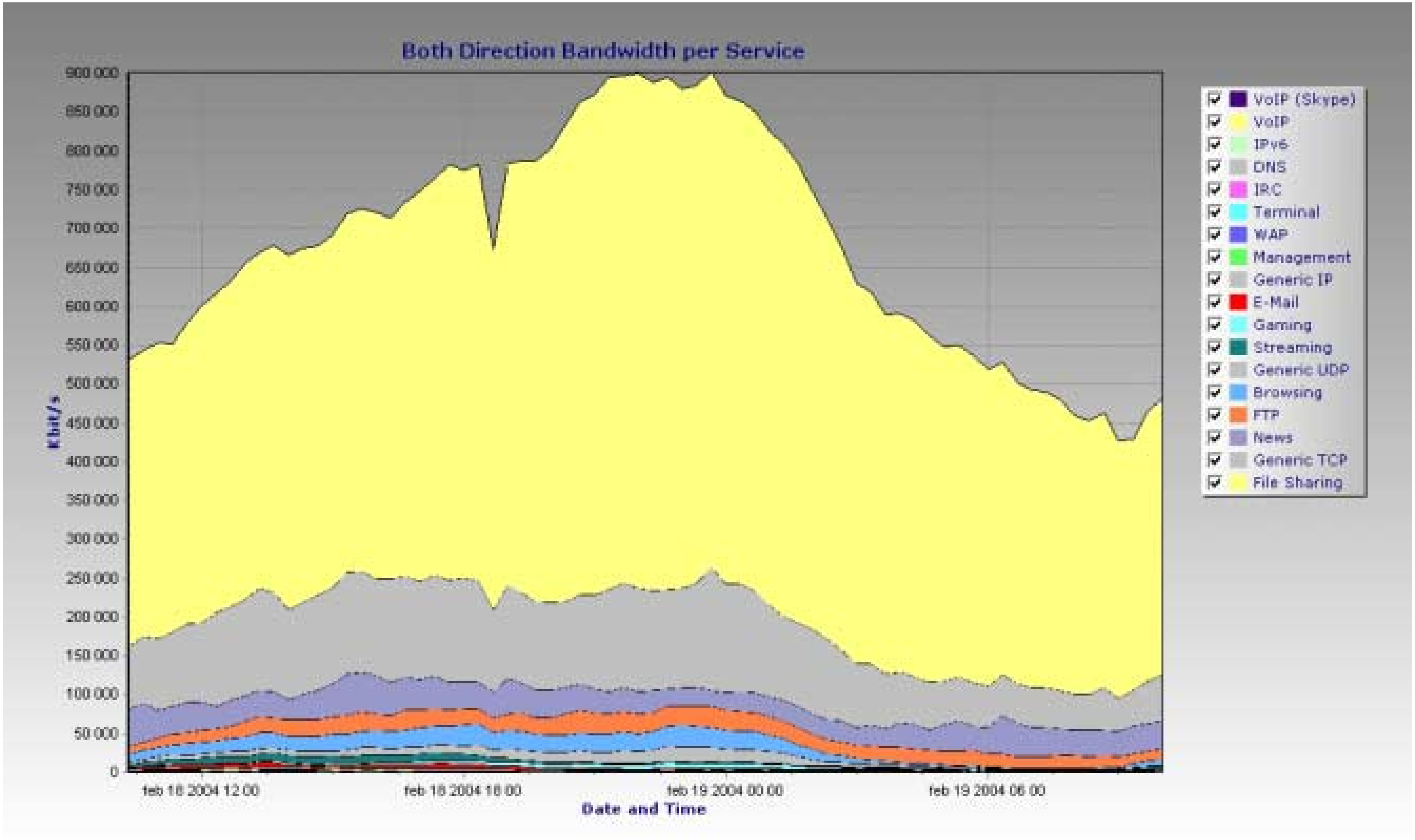
Before P2P

After P2P

P2P results in almost continuous, almost synchronous traffic loads …

Changes network design and provisioning assumptions

Impact of P2P Traffic



Measured on a peering link with primarily residential traffic
78% Known File Sharing Traffic

P2P: Current Solutions

» Approach

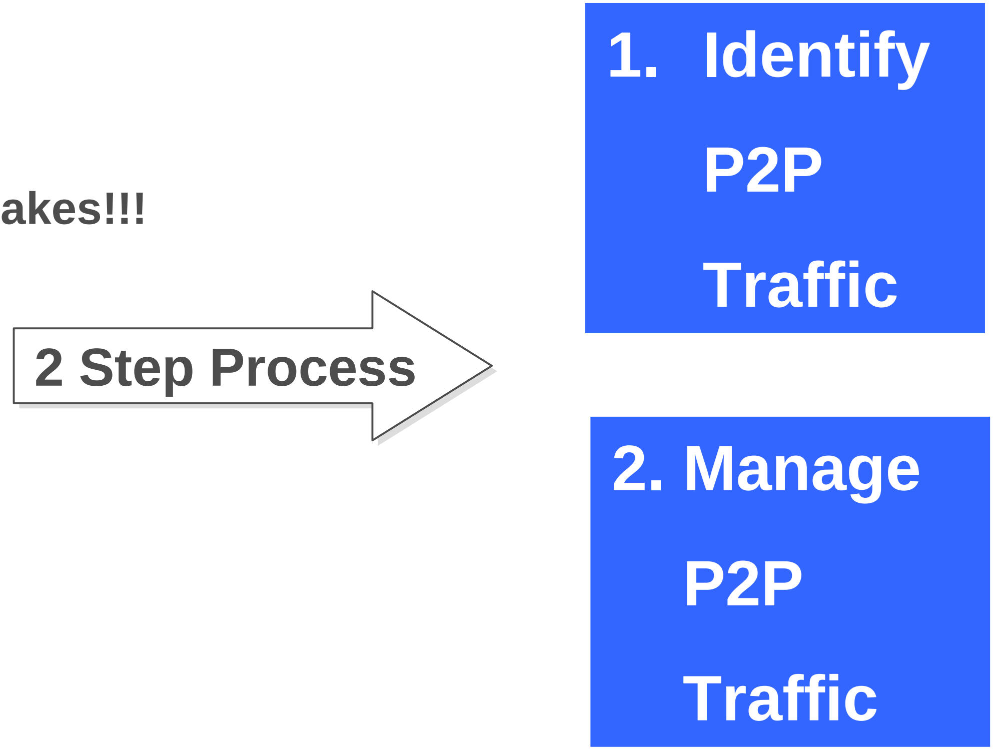
- Protect against P2P applications masquerading as http traffic (port 80)
- Deal with higher layer (application) inspection and classification
- Typically targeted for network edges / onramps partly because these functions are available on lower speed interfaces only due to performance requirements of these solutions

» Challenges:

- Encryption – making it impossible to identify application type
- Performance – current offerings are “flow-based” but operate at lower speed interfaces
- Complexity (rules change daily with application changes). Operationally challenging.
- Not efficient under class congestion – random discard mechanisms only
- Extra box(s) in network

Managing P2P Use – different approaches

- » Ignore the problem
- » Management by written or other policy
- » Throw Bandwidth at it
  - ▪ More b/w you give, more it takes!!!
- » P2P Traffic Control
  - ▪ Port Blocking
  - ▪ Rate limiting
  - ▪ Bandwidth quotas
  - ▪ QoS



2 Step Process

1. Identify P2P Traffic

2. Manage P2P Traffic

The Issue

Unknown Traffic

- Browsing
- Streaming
- Voice/Video over IP
- Some P2P (skype, small transfers, etc.)
- Small web downloads
- Large FTP Transfers
- Some P2P (large transfers)

All Traffic Treated Equally Under Congestion

Poor QoE for Interactive Applications

Currently too costly to maintain adequate QoE

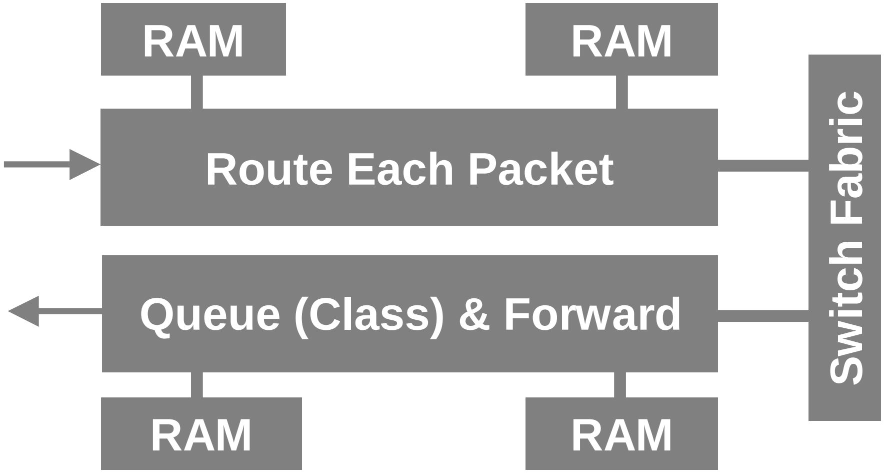
Conventional routers cannot identify / classify P2P traffic.

Appliance approach using signatures has operational, accuracy and cost issues

Flow-based Routing: The Technology

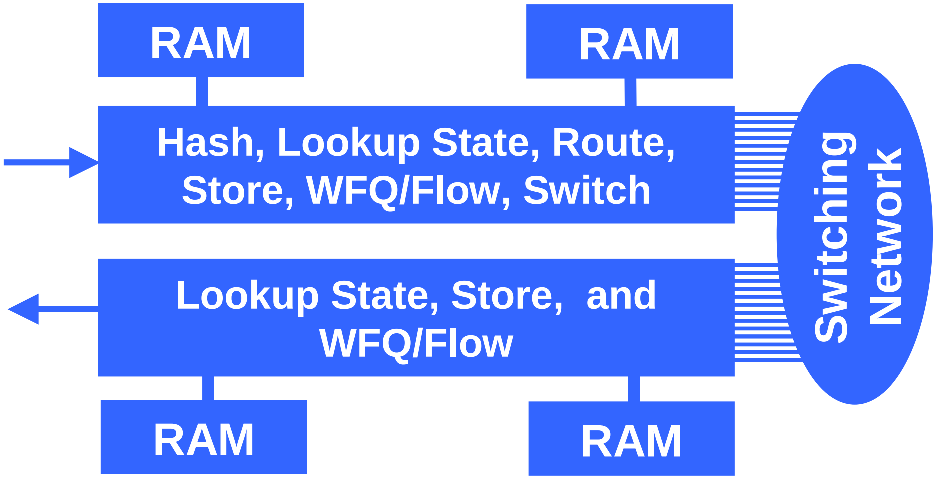
Conventional Router

1. Route each packet
2. Switch to output
3. Class-based QoS



Flow-based Router

1. Hash for flow identification
   - 2M flows/s and 6M flows per 10 Gig
   - Flexible definition of flows: IP flows, PWoMPLS flows, IPoMPLS flows
2. Create "soft" state or look up
   - Route, switch, filters, stats
3. Per-flow QoS behavior
   - Leverage flow state for advanced QoS
   - Shape, police, CAC, congestion control


RAM
RAM
Hash, Lookup State, Route, Store, WFQ/Flow, Switch
Lookup State, Store, and WFQ/Flow
RAM
RAM
Switching Network

Flow Routing: QoS and Network Benefits

- Customized congestion control schemes
- Flexible connection admission control (CAC)
- Advanced shaping/policing schemes
- Guaranteeing services → network scalability
- Next evolutionary steps towards routers with integrated traffic control capabilities

State → Intelligence → Improved nodal behavior → Enhanced network services at lower cost

Customized Congestion Control Schemes

- Providers can select & enforce explicit congestion control policies

  (responsive vs. unresponsive, high rate vs. low rate, short lived vs. long lived)

- Flow routers leverage state information to characterize traffic flows

    - Can enforce specified congestion control policies

- Providers can decide on different congestion based their requirements

<u>Examples</u>

- Guarantee (weighted) fairness between TCP flows
- Congestion control based on “flow abusiveness concept”
- Ensure quasi zero-loss for certain types of traffic (e.g. TDM, emulated circuit)

Flow-based congestion control schemes allow

- Differentiation between service providers
- Definition of new services

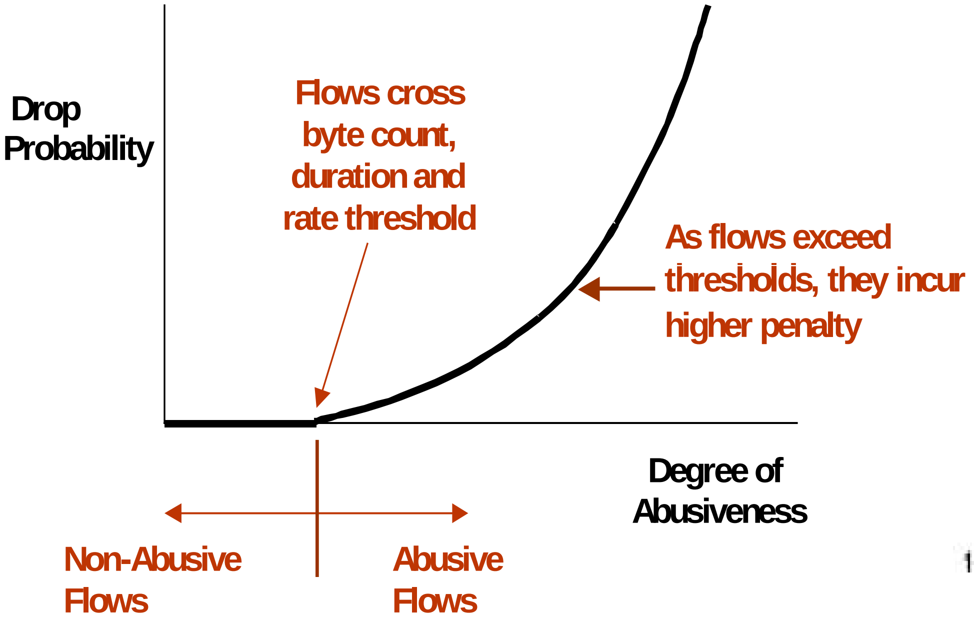
Identifying P2P flows

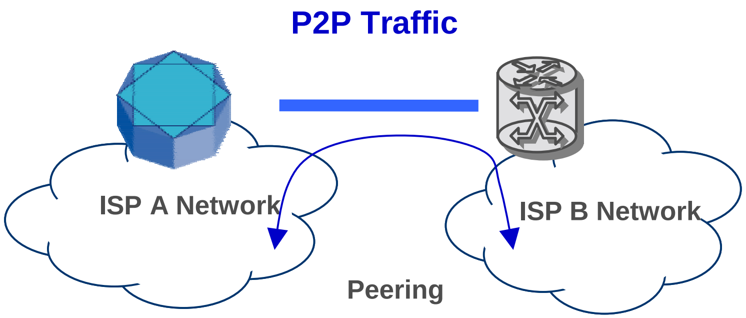
Service	*Duration*	*Average Rate*	*Bytecount*
HTTP	Short	High	Low to High
VPN	Long	Low	High
Games	Long	Low	High
Streaming	Long	Medium	High
Telnet	Long	Low	Medium
Fileshare / P2P	Long	Medium-High	High

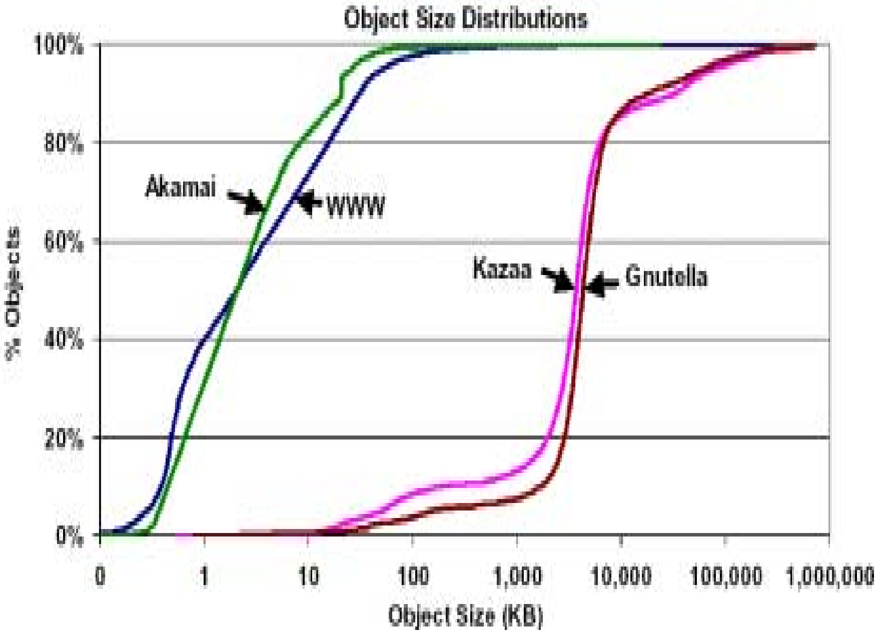
Anomaly based detection approach of P2P flows

Based on an exhaustive characterization of P2P traffic

Managing P2P Traffic







- Multiple dimensions used to identify P2P traffic
  - - Traffic rates, flow lengths, packet sizes
  - - Flows per user & traffic per flow
- Provides customized control behavior under congestion
- Leads to optimized ROI for costly peering links

Conclusions

- P2P traffic to grow, changing network and traffic engineering assumptions

- Flow-based routing enhances IP routers nodal behavior, based on a dynamic identification and policy based action schemes

- Flow based routing allows optimized resources management, significantly improve service providers economics

- P2P applications and impact on services and network architectures: threats and opportunities !