Pricing and Security of Residential Broadband Access

I. Hamadeh, Y. Jin, S. Walia and George Kesidis
Department of Computer Science and Engineering
and Department of Electrical Engineering
Pennsylvania State University
kesidis@engr.psu.edu

Carlos Kirjner
McKinsey and Company, New York
Carlos_Kirjner@Mckinsey.com

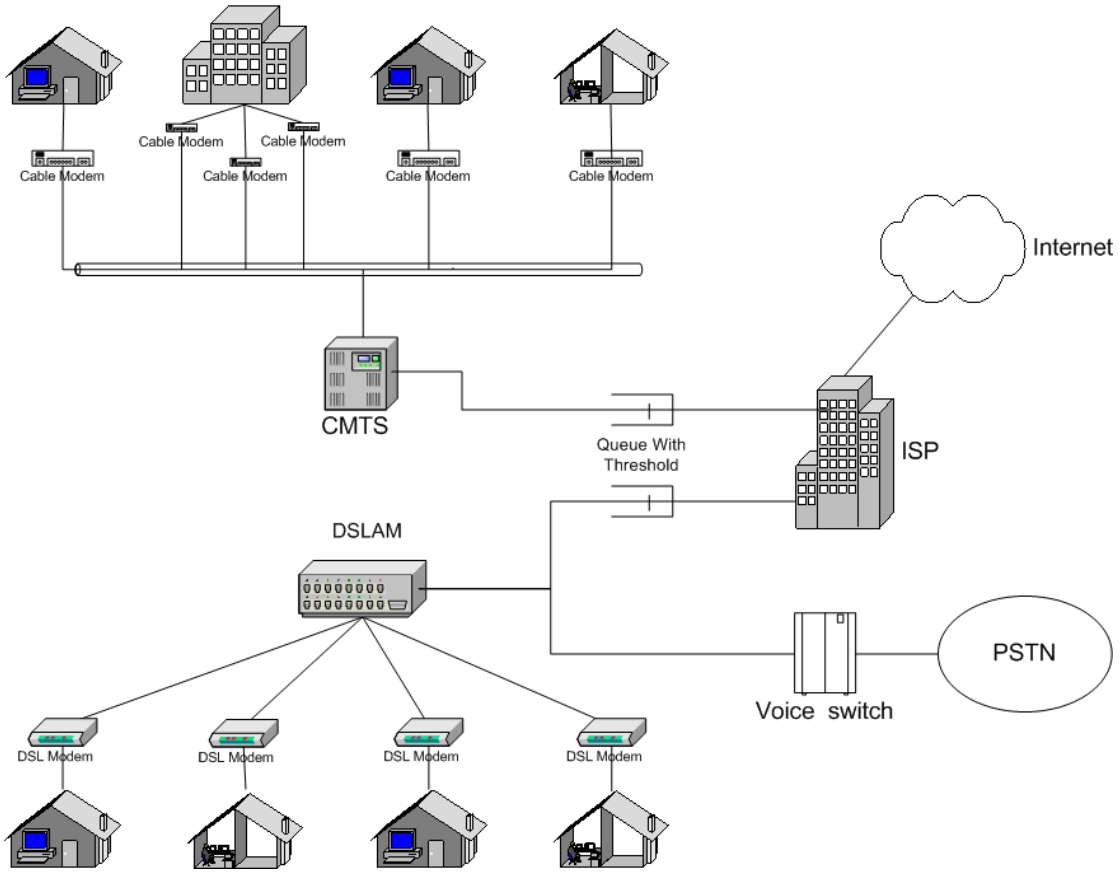
Outline

- Growth in residential broadband access
- Challenges faced by broadband access providers
  - Cost recovery from value-added services
  - Implications of broadband growth for cyber security
- First-hop authentication and packet marking
- A feasible pricing mechanism
- Authentication and authorization Issues

Growth in residential broadband access

- Wired residential broadband access encompasses DSL (telephone companies) and cable.
- All of Comcast's growth is due to broadband internet access.
- What is fueling residential broadband demand?
  - Tolerable incremental cost over a separate phone line (for dial-up access) with dramatic performance improvement in general.
  - Facilitation of "value-added" services such as VoIP, gaming, interactive and high-quality on-demand video.
- Visions of >100Mbps access via cable in near term.
- Goal of penetration from 22% of homes today to > 70%.

Wired residential broadband access



Cost recovery issues

- Expansion of residential broadband access infrastructure is very expensive.
- Probably individual subscription rates will not increase.
- DSL is bandwidth limited: phone companies need new technologies to reach >100 Mbps/user.
  - This, necessitates cost recovery from 3rd party vendors of valued-added services.
- Cost recovery: IP telephony (VoIP)
  - Consider a call between a cable modem IP phone and a plain-old telephone.
    - The VoIP user subscribes to (pays) a 3rd party provider, e.g., Vonage.
  - VoIP provider:
    - Pays telephone companies for circuits to telephone end-systems but
    - Does not currently pay cable/DSL providers for access to IP phones.
  - OK in short term: allows cable companies to “compete” with telephone companies for telephony market (even if they are not getting any revenue).

Implications of broadband growth for cyber security

- Nation's end-systems are vulnerable to attack by viruses, worms, etc.
- Increasing access rates to >100 Mbps may exacerbate large-scale worm or DDoS attacks.
  - Imagine a DDoS attack involving bots with dial-up access vs 100 Mbps access.
- US Government cyber security policy today
  - Recent DMCA and anti-SPAM legislation indicate a shift in US govt towards greater regulation of the Internet.
  - Comments on "*National Strategy to Secure Cyberspace*" policy:

    "Policy makers should consider legislative responses to the failure of existing incentives to cause the market to respond adequately to the security challenge" [NAS-panel, 2003].
  - Government policy may mandate simultaneous "securing" of broadband access together with its expansion.

User versus packet priorities

- Two possible responses to cost-recovery and cyber security challenges are to assign:
  - User priorities: one is either a priority or non-priority user.
  - Packet priorities: each user will potentially have both a priority and non-priority flow.

- Prioritization is introduced to have premium services which will provide better:
  - Availability/reliability.
  - Service quality in terms of packet latency and loss.

Packet priorities: Why?

- User priorities:
  - Allow for simple flat-rate billing (two tier), but
  - need end-user authentication and
  - packets not requiring premium quality-of-service will be given priority treatment.
- Packet priorities:
  - Give "right" incentives for priority marking.
  - Do not completely block a user when there is congestion in access network queues.
- Basic assumption: During high demand contention will largely be at packet level (3rd layer) rather than at data-link level (2nd).

Packet marking: How?

- Unused 2-bit TOS field in IPv4 packet header.
- IETF RFC 3168 suggests using those as notification for congestion at end-nodes.
- Propose end-users employ a TOS bit to indicate packet priority.
- A priority mark could:
  - Indicate participation in a value-add (premium) service or
  - Denote a packet that is part of a more reliable service.
- Marks would have no meaning beyond the 1st PoP of the access provider, i.e., only first-hop packet marking.

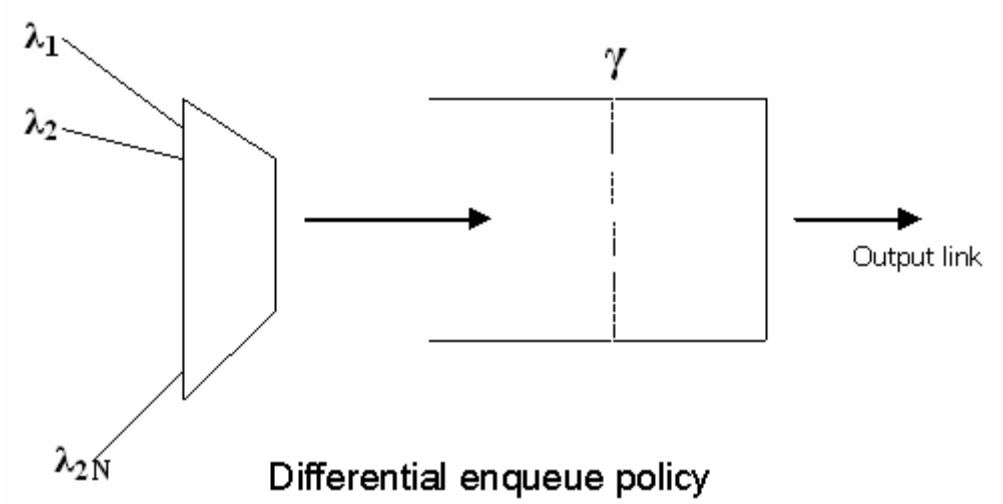
Packet marking: Billing

- Non-priority flow is billed at a flat rate.
- Usage-based pricing on priority flow.
- Need to inform each user of the current “priority spot prices.”
- Need to authenticate the priority flow of each user.
- Access provider can then do cost recovery from user and/or possibly from third-party vendor of value-added services.

Pricing of priority packets

- 1st PoP router handles two priorities of packets (two flows).
- Consider packet memories feeding output links.
- Suppose they use differential enqueue policy based on a threshold (T) rule: when averaged queue backlog exceeds T, drop all non-priority packets.
- Dynamics of such a queue for a fixed usage-price for priority service was previously studied by us.
- Basic assumption on relative significance of L3 congestion (at this queue) versus L2 congestion (between this queue and end-users).
- End-users perceive congestion and elevate certain packets to priority status which is analogous to bidding in a Vickrey auction.
- Can add dynamic “tatonnement” pricing mechanism based on averaged queue backlog (demand).
- Billing accomplished by 1st PoP router and current “spot” prices communicated back to end-users.

Pricing of priority packets



End-user dynamics

- N users each potentially with a low and high priority flow (2N flows and, effectively, 2N users).
- At i^{th} iteration, n^{th} user sets λ_n to:

  $$\lambda_{n,j+1} = G(y_n, \theta_n(\underline{\lambda}_j), \lambda_{n,j})$$

  where y_n is demand and θ_n is QoS.
- Under MIMD, assuming θ_n increases with λ_n:

  $$G(y, \theta, \lambda) = \lambda\theta/y.$$
- When equilibrium queue backlog q<T, continuous-time version of these dynamics were shown to have Lyapunov function:

  $$L(\underline{\lambda}) = \Sigma_n (y_n \lambda_n - I_n \lambda_n^2).$$
- Other differential enqueue/dequeue mechanisms possible that can, e.g., guarantee best-effort traffic is not starved of bandwidth.

Authentication and Authorization Issues

- Security benefits of priority-flow authentication:
  - Cyber attacks are often anonymously launched (at least initially).
  - Such malicious activity will hopefully be restricted to the non-priority flow category.
  - Thus, access of premium flows to the Internet may not be compromised during a cyber attack (assuming that premium flows are preferentially treated at the PoP and, perhaps, elsewhere).
  - So, authentication may improve the reliability of access of premium packets.

Securing priority flows from unauthorized access

- In a dedicated line network access systems (DSL, ISDN):
  - Services are tightly coupled with customer phone number.
  - Impersonation is impossible without physical wire- tapping and traffic injection.
- In a cable modem system:
  - The Data-Over-Cable Service Interface Specifications (DOCSIS) – a dominant US standard – includes Baseline Privacy Plus Interface Specification (BPI+)*.
  - BPI+ provides users with data privacy across the cable network and service protection for Multiple System Operators (MSOs).

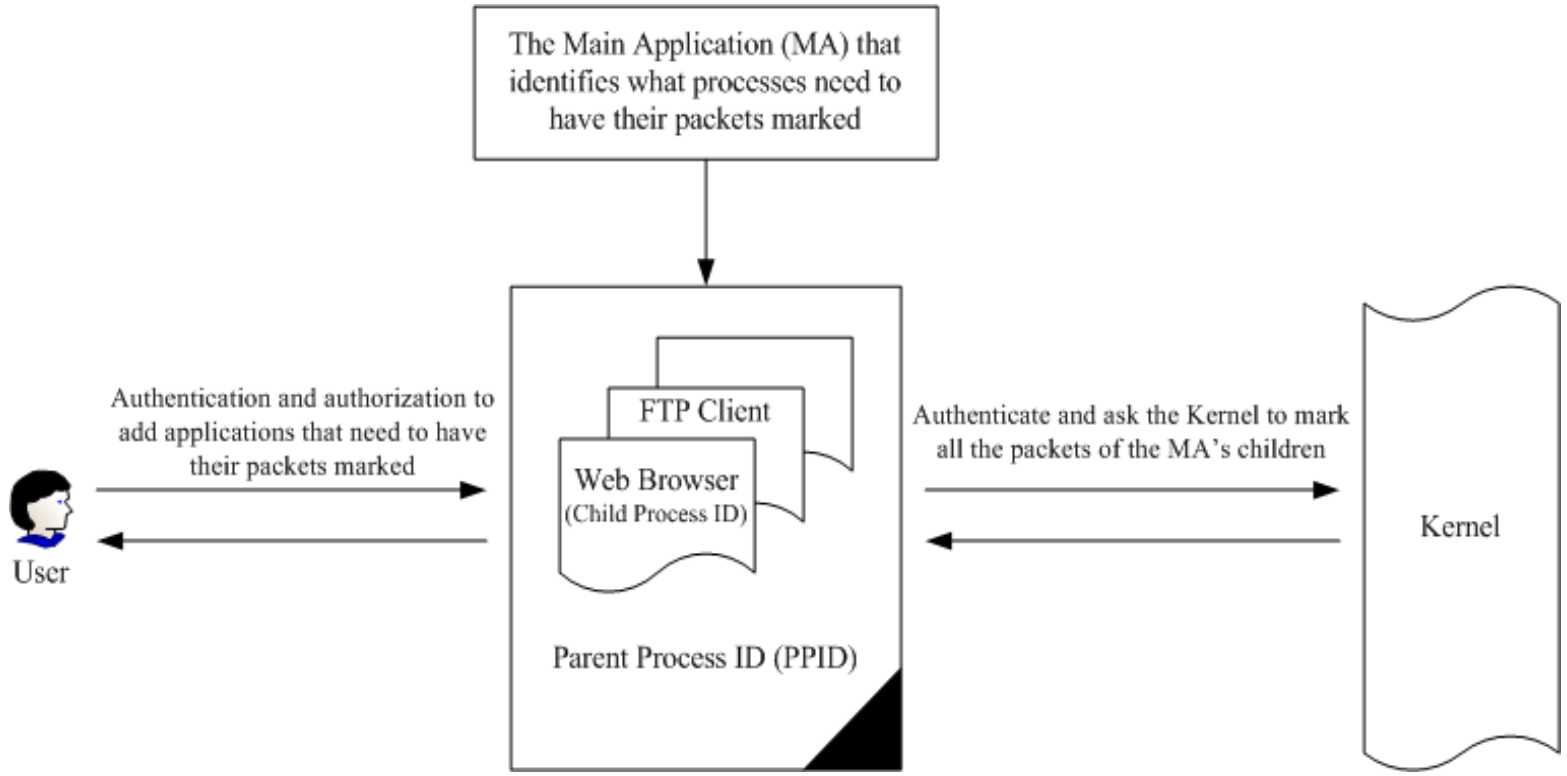
*BPI+ specification describes the MAC-layer security services between cable modems and their CMTS.

Authentication issues (cont)

- Cable Modem: An Issue
  - Problem: Spoofing IP address of the service provider's TFTP server to reconfigure cable modem to illegally increase end-user's bandwidth.
  - Solution: Prohibit a cable modem from registering if there is no matching TFTP traffic through the CMTS preceding the registration attempt.

- Securing priority flow services from malware (worm, trojan, etc.)
  - Include a kernel patch to disable raw sockets.
  - Include a patch to authorize special applications exclusive access to certain fields in IP header.

Authentication Issues (cont)



A security mechanism to protect per-packet pricing services from malware

Summary

- Proposed a mechanism for dual-priority access to residential broadband internet access networks.
- Usage-based and flat-rate pricing for priority service was explored.
- Primary focus was: usage-based pricing as it has
  - Advantages in terms of user incentives.
  - But significantly greater security challenges.

References

1. [RAnderson] R.Anderson. Why information security is hard - an economic perspective. available at http://www.cl.cam.ac.uk/~rja14/econsec.html
2. [Edell99] R.Edell and P.Varaiya. Providing Internet access: What we learn from INDEX. *IEEE Network*, Vol. 13, No. 5:18--25, Sept-Oct, 1999.
3. [RFC2267] P.Ferguson and D.Senie. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. IETF RFC 2267, Jan. 1998, available from URL www.ietf.org
4. [Fernandez02] P.M. Fernandez, N. McKeown and H. Zhang. *Is IP going to take over the world (of communications).* in Proc. HotNets 2002.
5. [Kesidis02] G. Kesidis and Y. Jin. Feasible pricing of differentiated services for the emerging Internet *Proc. 40th Allerton Conference on Communications*, Oct. 2002.
6. [NAS-panel] NAS Panel Report, "Cyber Security Today and Tomorrow: Pay Now or Pay Later," 2003; quote cited by S.Lohr, "Fixing flaws, Microsoft invites attack", *New York Times*, 9/29/03.
7. [Odlyzko01] A.Odlyzko. Paris Metro Pricing for the Internet *ACM Conference on Electronic Commerce9EC '99*, pp.140-147, 1999.
8. [McKeown02] D.Shah, S.Iyer, B.Prabhakar, and N.McKeown. Maintaining statistics counters in router line cards. *IEEE Micro*, Vol. 22, No. 1:76--81, Jan-Feb, 2002.
9. [Webb03] C.L. Webb. *Cybersecurity Talk Is Cheap.* washingtonpost.com, Dec.,2003.
10. [Haley] C.C. Haley. *Comcast sees "spectacular" broadband growth.* internetnews.com, Oct. 30, 2003.
11. Cisco Security Advisory. *Cable Modem Termination System Authentication Bypass.* Cisco Systems, Sept, 2003. http://www.cisco.com/warp/public/707/cmts-MD5-bypass-pub.shtml
12. K. Poulsen. *Cable Modem Hackers Conquer the Co-ax.* Securityfocus, Feb, 2004. http://www.securityfocus.com/news/7977
13. Data-Over-Cable Service Interface Specifications DOCSIS 1.1. *Baseline Privacy Plus Interface Specification.* CableLabs, July, 2003. http://www.cablemodem.org/
14. C. Franklin. *How Cable Modems Work.* http://computer.howstuffworks.com/cable-modem.htm
15. The National Strategy to Secure Cyberspace *National Policy and Guiding Principles.* A White House report, Feb. 2003. http://www.whitehouse.gov/pcipb/policy_and_principles.pdf