Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2000 Proceedings

Americas Conference on Information Systems (AMCIS)

2000

Challenges to the End-to-End Internet Model

William Yurick
Illinois State University, wjyurci@ilstu.edu

David Doss
Illinois State University, dldoss@ilstu.edu

Hans Kruse
Ohio University, hkruse1@ohiou.edu

Challenges to the End-to-End Internet Model*

William Yurcik[1], Department of Applied Computer Science, J. Warren McClure School, Illinois State University, wjyurci@ilstu.edu
David Doss[2], Department of Applied Computer Science, J. Warren McClure School, Illinois State University, dldoss@ilstu.edu
Hans Kruse[3], Ohio University, hkruse1@ohiou.edu

***Abstract**: In 1981 Saltzer, Reed, and Clark identified "end-to-end" principles related to the design of modern layered protocols. The Internet today is not as transparent as envisioned by [SALTZER81]. While most of the intelligence remains concentrated in end-systems, users are now deploying more sophisticated processing within the network for a variety of reasons including security, network management, E-commerce, and survivability. Applications and application-layer protocols have been found to interact in unexpected ways with this new intelligent software within the network such as proxies, address translators, packet filters, intrusion detection, and differentiated service functions. In this paper we survey examples of the problems caused by the introduction of this new processing within the network which is counter to the end-to-end Internet model proposed by [SALTZER81].*

The conflict between the end-to-end Internet model and the introduction of new processing within the network is being addressed on a case-by-case basis in each development effort. There are no indications that new devices installed within the network (which break the end-to-end model) will disappear and in fact there has been dramatic growth in their implementation due to recent denial-of-service attacks. Transition to IPv6 only solves a subset of these issues, and its deployment is proceeding slowly. Future work is obviously needed to create a consistent environment for protocol development that preserves the transparency provided by the end-to-end Internet model.

Keywords: NAT, VPN, firewall, intrusion detection

1.0 Introduction

There are two classic models for intelligence within networks.[LEAR00] The first is end-systems that have no intelligence and the network devices to which they connect provide all the services. The telephone system is an example of just such a network. The absence of intelligence in end-devices makes them inexpensive to manufacture and manage but the network devices (central office switches) become expensive and complex to maintain.

The second model is the end-to-end Internet model[4] proposed by Saltzer, Reed, and Clark in 1981. [SALTER84] This model is a set of architectural principles that guide the placement of functions within a distributed system. According to this principle, lower layers of a distributed system should avoid attempting to provide functions that can be implemented in end-systems especially if the function cannot be completely implemented in lower layers and some applications might not benefit from such functions at all.

The end-to-end model shifts intelligence to the end-systems, thus also shifting cost and management complexity from routers/switches to end-systems. Another benefit of the end-to-end model is congestion control can be managed between end-systems, not requiring state information be kept within routers such that network devices can be optimized for performance.[5] In end-to-end design, the network simply acts as a transparent transport mechanism for individual packets with each packet being labeled by a globally unique source/destination addresses. The notion of "transparency" demands that network devices between two end-systems not modify information within the packet above layer 2 (data link layer), except

* supported in part by a grant from the John Deere & Company
[1] author for correspondence; additional contact information: telephone/fax: 309-438-8016/5113;
hardcopy mail: Campus Box 5150, 202 Old Union, Normal IL 61790 USA
[2] Associate Professor and Associate Department Chair, Ret. Lt. Cmdr. US Navy (SSN)
[3] Director of Telecommunications Program, J. Warren McClure School of Communication Systems

[4] we use the term "end-to-end model" while acknowledging that the original authors prefer to use the terminology "end-to-end arguments"
[5] noted Internet researcher Van Jacobson is quoted as stating, "Very simple. A router has only three choices when presented with a packet. It can transmit the packet. It can delay (queue) the packet. Or it can throw the packet away." [CHEN98]

under well-defined circumstances (i.e., decrement the TTL or record route). Changing IP addresses is not viewed as acceptable, nor is any change to layer 4 or above.

2.0 The Problem: Unexpected Protocol Interactions

The Internet Engineering Task Force (IETF) has been instrumental in supporting the end-to-end Internet model with "rough consensus and working code."[6] In fact, one of the authors of the original end-to-end model paper, David Clark, chaired the Internet Activities Board (IAB) overseeing the IETF from 1981 to 1989. In reflecting on the state of the Internet in late 1999, a current member of the IAB and present/past chair of numerous IETF working groups, Steve Deering[7], summarized his thoughts on intelligence within networks with a slide - "Internet is Losing?"[8] Examples he used include:

- unique IP addresses are no longer necessary
- the Internet is not always on (many users log-on via American On-Line etc.)
- end-to-end transparency is often blocked behind network address translators and firewalls

While most of the intelligence remains concentrated in end-systems, users are increasingly deploying more sophisticated processing within the network for a variety of reasons including security, network management, E-commerce, and survivability. The following are some specific examples:

- The use of network address translators to solve IP address depletion problems.
- The use of performance enhancing proxies to tune protocols on links with unusual characteristics.
- The use of tunneling and other virtual private network techniques to provide secure connectivity over the Internet to an organization's intranet/extranet.
- The use of firewalls and intrusion detection to prevent and respond to malicious attacks.
- The deployment of quality-of-service mechanisms to provide delay, delay jitter, and packet loss guarantees to applications and network services.

Each of these examples address important problems that need to be solved. Rather than debate the benefit of each such device and or their legitimacy with the network, we accept the notion that such devices are here to stay for the short-term and that the transparency of the end-to-end model as we know it can not be re-established through requirements of their non-existence. The end-to-end Internet model is broken and needs to be repaired. The problem is acerbated in that it is impossible to detect intelligent network devices and there now actually exists guidance within the IETF itself on how to build such devices.

While IP next generation, IPv6, has been designed to solve many of these problems, migration will take time. Not only do protocol stacks and routers have to be upgraded but applications with hard-coded IPv4 addresses have to be changed (an effort similar to Y2K without a hard deadline). The good news is that IPv6 has been designed so that IPv4 and IPv6 can coexist with IPv6 deployed gradually. In the meantime, applications and application-layer protocols have been found to interact in unexpected ways with intelligent network devices within the current end-to-end IPv4 Internet model. This is to be expected since intelligent network devices reduce transparency and the key element of transparency is some ability to predict how the network will behave.[CHEN98] To quote from a 1998 paper from the original authors of the end-to-end model:

"Since lower-level network resources are shared among many different users with different applications, the complexity of potential interactions among independent users rises with the complexity of the behaviors that the users or applications can request. For example, when the lower layer offers a simple store-and-forward packet transport service, interactions take the form of end-to-end delay that can be modeled by relatively straightforward queueing models. ***Adding priority mechanisms (to limit the impact of congestion) that are fixed at design time adds modest complexity to models that predict the behavior of the system. But relatively simple programming capabilities, such as allowing packets to change priority dynamically within the network, may create behaviors that are intractable to model****…."[CHEN98]*

Thus, maintaining the largest degree of network transparency simultaneously constrains interactions among different users of a shared lower level such that network behavior can be predicted. We have also found the opposite is true: diminishing transparency increases unexpected interactions between protocols. We have identified three distinct types of protocol interactions that have been introduced by the diminishing of transparency due to the deployment of intelligent network devices:

- Some network devices either attempt to read/modify portions of transmitted packets which the sending system assumes fixed. [i.e., performance enhancing proxies, network address translators]

[6] motto of the IETF

[7] Steve Deering is also the inventor of IP multicast and lead designer of the next generation Internet Protocol (IPv6).

[8] Closing Talk of *Networked Group Communications Conference* (NGC'99), Pisa Italy, Nov. 19, 1999.

- The use of IP tunnels creates the design issue of how to construct the second "outer" IP header upon tunnel ingress[9], and the more complicated issue of whether the original "inner" IP header needs to be modified upon tunnel egress[10] based on changes that intermediate nodes made to the outer header.[i.e., tunneling and virtual private networks]
- Some devices on purpose, or due to limits in their design, prevent some packets from traversing that device. [i.e., firewalls, intrusion detection]

In this paper we examine these protocol interactions in an effort to understand recent protocol design decisions and their effect on the transparency provided by the end-to-end Internet model. We are particularly interested in examining the protocol structures involved to determine why the traditional protection against protocol interactions inherent in the layered protocols could not prevent the observed problems. The remainder of this paper is organized as follows: Section 3 describes the use and interaction of network address translators and performance enhancing proxies. Section 4 examines the use of tunneling to create virtual private networks. Section 5 discusses the use and interaction of packet filtering/correlation with firewalls and intrusion detection devices and the implications of IPsec. Section 6 discusses the use and interactions of proposed quality-of-service mechanisms. In Section 7 we close with a summary and directions for future work.

3.0 Network Address Translators (NATs) / Performance Enhancing Proxies (PEPs)

NATs allow the use of private IP addresses in a private intranet while maintaining connectivity to the Internet through one or more global IP addresses. Since many applications assume that the end-system address is globally unique, NATs usually require application level gateways which modify application-specific sections of the packet where the end-system address has been embedded. These gateways cause changes in the packet that are unanticipated by the end-systems.[HAIN00, HOLDREGE00] A Network Address and Port Translator (NAPT) cannot forward a connection request from the Internet to a private network unless an administrative mapping has been provided for the port requested in the incoming packet. Other packets may be dropped or misrouted because the NAPT does not have the appropriate application-level gateway and thus fails to make corrections in the packet to allow the application's peer to respond.[11]

PEPs are used in networks with unusual link characteristics.[ALLMAN99] These proxies may attempt to read transport-level information in the packet or they may add and delete packets from the flow. Many of these proxies can be bypassed by flows that do not permit such interactions, at risk of suffering from poor performance. Both NAT and PEP devices vastly complicate the deployment of IP-level security between end-systems [KRUSE99], and they may cause other failures that can be difficult to diagnose [CARPENTER00]. For instance, both the NAT and PEP devices usually do not report the fact that they either failed to correctly handle a packet, were bypassed, or dropped a packet they could not process due to insufficient information. Encrypted packets will be examined by the security software at the receiving end where modifications made by the NAT or PEP device will be interpreted as illegal tampering and the packet will be discarded by the security software. While dropping packets is an auditable event, the sender of the packet is usually not notified.

The deployment of NAPT devices is usually driven by a shortage of IPv4 addresses, and the resulting ISP policies and rates that limit the number of permanent addresses a user can acquire. IPv6 deployment is the obvious, but long-term, solution to this issue. PEP devices are introduced for different reasons and will continue to exist in the IPv6 network.

4.0 Tunneling and Virtual Private Networks (VPNs)

IP tunnels are defined as a section of the network in which IP packets are encapsulated inside a second IP header (often called the "outer header"). The tunnel is designed to transport packets between two intermediate points in the network, without making reference to the actual IP packets during the tunnel section of the packet's path. Tunnels can serve a number of purposes including:

- Transport of multiple protocols over an IPv4 router infrastructure (i.e., IPv6, IPX, Appletalk) as well as service types not supported by intermediate nodes (i.e., multicast backbone or MBONE).
- Tunnels provide secure passage between two nodes at the edges of trusted domains. Inside the tunnel,

[9] **in**gress is a path going **in**to a network

[10] **e**gress is a path **e**xiting from a network

[11] It should also be noted that with the advent of dial-up Internet users whose IP address is allocated at dial-up time, the actual IP addresses of such users is purely transient. During their period of validity they can be relied upon end-to-end but these IP numbers have no permanent associations with the domain name of any host and are recycled for reuse at the end of every session. Similarly, LAN-based users typically use DHCP (Dynamic Host Control Protocol) to acquire a new address at system restart

original IP packets are encrypted and therefore completely inaccessible.

- Creation of VPNs. In this scheme, packets between two sites are carried over IP tunnels to provide isolation from the addressing and routing requirements of the Internet. A similar type of tunnel can be used to connect an off-site user to the corporate network.

The use of tunnels creates specific types of protocol interaction problems. Specifically how should the outer IP header be constructed at the tunnel ingress point? In general it seems reasonable to copy fields from the original IP header, however, this is not always the correct approach. In networks that provide quality of service control through resource reservation [TERZIS00] or differentiated service [BLAKE98], the tunnel may be used to traverse a portion of the network that cannot provide these services, and therefore requires that some of the original IP settings not be copied. In other cases [FLOYD00], the ability of the tunnel egress point to provide certain types of processing will determine how to construct the outer IP header.

By far the more complicated issues arise upon tunnel egress. Some portions of the outer IP header may have been modified during tunnel traversal. Examples include updating of header fields that mark the packet as being in a particular differentiated service group, or updating of fields designed to provide explicit congestion notification to end-points. The tunnel egress node must merge the original IP header with the – possibly modified – outer IP header. The rules for doing this are ambiguous and different rules may emerge. For example, from a performance and application perspective, one may wish to propagate congestion notification information across security tunnels. From a security perspective, one may wish to discard the outer IP header, regardless of its content, to prevent attacks based on the ability of hostile systems to modify the unprotected outer IP header inside the tunnel.

5.0 Firewalls, Intrusion Detection, and IPsec

Several devices discard packets before they reach the end-system destination address. Most prominently, firewalls are designed to do just that for all packets that have not been entered in a permission list. Firewalls, by their very nature, fundamentally diminish transparency. Typically the source is not notified of the fact that the packet was dropped (although auditing of dropped packets can be performed at the firewall). In order to prevent attacks, many corporate firewalls will not permit network management packets (i.e., ICMP) to pass through. Note that these issues are unrelated to the availability of address space, and will continue into the IPv6 network.

Intrusion detection (ID) is a monitoring and auditing system for attempted and successful system breaches with the goal of detecting and ultimately preventing such activity. Because many attacks can be recognized by their signature (headers), the best place to process information is at the network layer. Since ID is based on algorithms which correlate network layer information with signatures, it requires large amounts of storage. The state-of-the-art is reactive off-line processing. ID systems are currently maturing and the next generation will rely on integration with routers to proactively monitor activity in real-time. One example of a transparency issue related to ID systems is fragmentation. While fragmentation is a useful method for supporting various media on internetworks, it may mean caching packets at the ID system to reassemble for inspection – a process that destroys transparency and could be a performance bottleneck.

At the other end of the spectrum from filtering and correlating packets is security. IPsec is actually an architecture - a collection of protocols, authentication, and encryption mechanisms – as described in [KENT98]. The loss of transparency is both a bug and a feature from the security standpoint. To the extent it prevents the end-to-end deployment of IPsec, it damages security and creates vulnerabilities. For example, if a NAT is in the path, the best that can be done is to decrypt and re-encrypt IP traffic in the NAT with the traffic momentarily in plaintext. Noting NATs are prime targets for attack already, this is unacceptable. Indeed, NATs break other security mechanisms as well, such as Kerberos and DNSSEC, since they rely upon address values. In a weaker sense, the loss of transparency at an Intranet/Internet boundary may be considered a security feature since it is a well-defined point to enforce security policy. However, such a security strategy is vulnerable to insider attack and boundary penetrations which expose the entire intranet to trivial attack. Lastly, where cryptographic algorithms are used, protocols should be designed to permit alternative algorithms to be used. There have been several efforts by corporations to embed their own patented cryptographic algorithms within a protocol to capture a market while at the same time severely limiting end-to-end transparency.

6.0 Quality-of-Service (QoS) Mechanisms

Classically, the end-to-end model views the network as a monolithic entity that provides a single QoS to all users, best-effort delivery. The Internet has expanded to incorporate applications with requirements for guarantees on network behavior beyond the best-effort delivery. In the case of mechanisms such as RSVP, the host signals to the network the level of service it requires, whereas with differentiated services the network prioritizes traffic without the host's knowledge or consent.[BRADEN97, BLAKE98] Both end-systems and network devices co-

operate to provide deterministic and statistical guarantees on QoS metrics such as delay, delay jitter variation, and packet loss rates.

7.0 Summary

In this paper we have presented the evolving challenges to the overall transparency of the end-to-end Internet model as proposed by Saltzer, Reed, and Clark. It can be argued that the transparency inherent to the end-to-end model is in many ways responsible for the engineering success of the Internet. However, with unprecedented growth of the Internet has come pressure to violate the end-to-end model. We have documented examples of where Internet protocols designed for end-to-end transparency will not work in a world where packets have to traverse intelligent network devices such as NATs and firewalls. The large investment in intelligent network devices has been for valid reasons and this installed infrastructure will not be easily changed.

The trend continues toward incorporating more processing within the network. Active network research ranges from packets programming routers to routers making pre-programmed decisions based on packet content.[12][TENNENHOUSE97] In response to recent denial-of-service attacks, the IETF is convening an *"itrace"* BOF[13] to process reverse path state information on packets within intermediate routers using ICMP traceback mechanisms. There is a tension building between providing end-systems knowledge of network conditions to provide enhanced services versus increased security vulnerabilities based on this knowledge.[14] The IETF has issued an Internet draft on "Fog Lamps" to improve **visibility** of network devices to end-systems, a view directly opposed to the **transparency** view of the end-to-end Internet model.[LEAR00]

Nothing less than the future of the Internet as we know it is at stake.[CARPENTER00] In one scenario a complete migration to IPv6 potentially allows the restoration of a global address space and end-to-end transparency albeit with firewalls and PEPs still remaining. At the other extreme, only a partial IPv6 deployment leads to fragmentation of the network layer, with global connectivity resembling islands of connectivity. The eventual solution to this debate will determine the utility of the Internet and its future as the next generation infrastructure.

[12] While some researchers have attacked "active networking" as not scalable and destabilizing, it is premature to make such determinations.

[13] ICMP Traceback (itrace) Birds-of-a-Feather (BOF) at the 47th IETF meeting, Chair: Steve Bellovin, 3/30/00 15:30-17:30

[14] Increased knowledge of conditions within the network may make additional diagnostic information available to interloping devices.

8.0 References

[ALLMAN99] Allman, M. et. al., *"Enhancing TCP Over Satellite Channels Using Standard Mechanisms"* RFC 2488, 1999.

[BLAKE98] Blake, S. et. al., *"An Architecture for Differentiated Service"*, RFC 2475, Dec. 1998.

[BRADEN97] Braden, R. et. al., *"Resource ReSerVation Protocol –- Version 1 Functional Specification"* RFC2205, Sept. 1997.

[CARPENTER00] Carpenter, Brian. *"Internet Transparency"* RFC 2775, 2000.

[CHEN98] Chen, Thomas M. and Alden Jackson et. al., *"Commentaries on Active Networking and End-to-End Arguments"* IEEE Network Magazine, May/June 1998.

[DEERING00] Deering, Steve, personal communications, Cisco Corp., March 2000.

[KENT98] Kent, S. and R. Atkinson. *"Security Architecture for the Internet Protocol"* RFC2401.

[KRUSE00] Kruse, Hans. *"The Pitfalls of Distributed Protocol Development: Unintentional Interactions between Network Operations and Applications Protocols."* 8th Intl. Conf. on Telecom. Systems (ICTS), Nashville TN. USA, March 2000, pp. 289-293.

[KRUSE99] Kruse, Hans. *"Protocol Interactions and Their Effects on Internet-Based E-Commerce"* 2nd Intl. Conf. Telecom. and E-Commerce (ICTEC), Nashville. TN USA, Oct. 1999.

[HAIN00] Hain, T. *"Architectural Implications of NAT"* (work in progress) http://www.ietf.org/internet-drafts/draft-iab-nat-implications-04.txt

[HOLDREGE00] Holdrege M and P. Srisuresh. *"Protocol Complications with the IP Network Address Translator (NAT)"* (work in progress, March 2000) http://www.ietf.org/internet-drafts/draft-ietf-nat-protocol-complications-02.txt

[FLOYD00] Floyd, S. et. al., *"IPsec Interactions with ECN"* (work in progress) http://www.ietf.org/internet-drafts/draft-ipsec-ecn-00.txt

[LEAR00] Lear, Eliot. "NAT and other Network 'Intelligence': Clearing Architectural Haze through the Use of Fog Lamps" (work in progress, December 1999) http://www.ietf.org/internet-drafts/draft-lear-foglamps-01.txt

[SALTZER84] Saltzer, Jerome H., Reed David P. and David D. Clark. "*End-to-End Arguments in System Design*" ACM Trans. on Comp. Systems, Vol. 2 No. 4, Nov. 1984, pp. 277-288. (an earlier version appeared in 2nd Intl. Conf. on Distr. Computer Systems, April 1981, pp. 509-512.)

[TENNENHOUSE97] Tennenhouse, D. et. al., "*A Survey of Active Research Network Research*" IEEE Communications Magazine, Vol. 35 No. 1, 1997.

[TERZIS00] Terzis A. "*RSVP Operation Over IP Tunnels*", RFC 2746, 2000.