Network Working Group
INTERNET-DRAFT
Category: Informational

Eliot Lear
Cisco Systems

<draft-lear-middlebox-discovery-requirements-00.txt>
April 4, 2001

Requirements for Discovering Middleboxes

1 Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

2. Copyright Notice

2 Abstract

The end to end nature of the Internet has been broken. Boxes within the middle of the network may change contents of packets at the Internet layer or above without the knowledge of the end devices. As these middleboxes such as NATs and firewalls have proliferated within the Internet, protocols are being developed to communicate with them. This document addresses requirements for discovery of those boxes.

3 Introduction

The IPv4 Internet consists of a network of interconnected networks that may use public or private address space. The use of private address space [BCP5] has broken the classic connection model that

applications use to speak to other devices. Similarly, many networks are separated by firewalls.

In some cases, a firewall or a NAT may silently inhibit a communication between end hosts, either by design or incidental to the middlebox's function. Such failures may leave application developers, end users, or their administrators baffled as to the cause.

Herein we will review the nature of those sorts of communications, and we will develop requirements for mechanisms that would notify the end user of the possibility or eventuality of such failures.

The reader should be familiar with RFCs 1918, 2663, and 2775. We do not intend to fix all problems related to NATs or firewalls with this architecture. For instance, one will not find below a way to save a TCP connection in the face of a NAT failure. Instead, one may find a way to determine that in fact a failure has occurred, requiring the end hosts to attempt to re-establish communiations.

3.1 Terminology

All the terminology in this internet draft is subject to change, and will, in the end, conform to the consensus of appropriate working groups. It is assumed by the author that work on terminology will proceed elsewhere. Therefore, for brevity's sake the following terms are defined for purposes of this document.

Private Realm (PR) - an administratively defined group of computers, routers, and links that a middlebox may affect. ADs may encompass one another.

Internal Host (IH) - a device within an PR.

External Host (EH) - a device outside an PR.

Middlebox - a device that sits on the edge of an PR within the packet flow between an internal host and an external host, whose function is to inhibit, modify, or divert packets. For purposes of this document, a packet is modified if data other the IP TOS or TTL fields has been altered.

Application Controller (AC) - a device that actively manages application level communications between two devices.

Application Proxy - a device that represents an internal host to an external host, such that layer 3 knowledge of the internal host is completely kept from the external host.

Connection direction - the direction in which a transport connection is initiated.

4 The Simple Picture

Figure 1 contains a basic example of a deployment. There are XXX

communications that must be considered in the context of middlebox discovery.

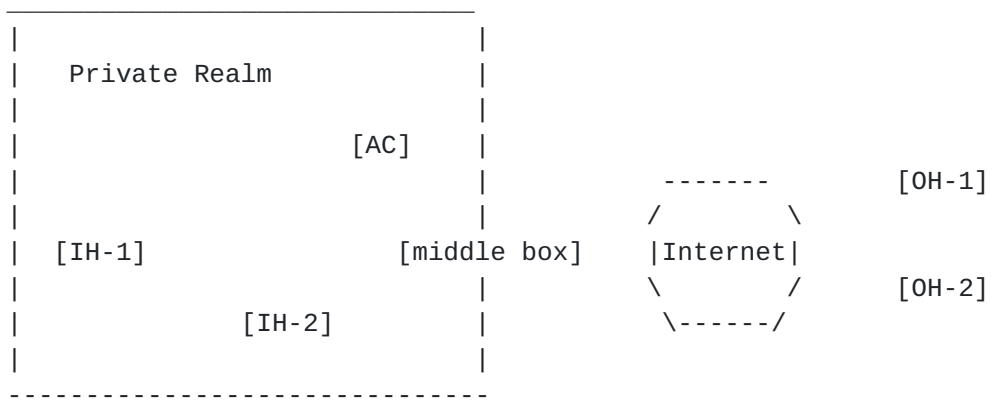

Figure 1.

4.1 Base Case: Non-use of Middleboxes

The first case is the case where either IH-1 and IH-2 communicate, or when OH-1 and OH-2 communicate. In this case, there is no middlebox to discovery. Any discovery mechanism MUST NOT burden or break this communication as it is the communication that is assumed by all existing applications. The devices IH-1 and IH-2 MUST not be required to have any additional topological knowledge, over and above what they would have today, in order to communicate. We will call this case "Duh".

4.1.2 Modified Duh

Similarly, a discovery mechanism MUST NOT require application controllers to participate, so long as only only internal hosts are involved. Thus, an H.323 gatekeeper serving IH-1 and IH-2 MUST be able to process signaling between those two devices, just as they do today.

4.2 Internal to External, No Application Controller

In an IH to EH communication, the IH will have at its disposal the IP address and protocol information necessary to connect to the EH. Any such information MAY be used by the IH in a discovery protocol to determine which middleboxes may affect the communication. Examples of IH to EH communication would include a web connection, or a direct SIP connection.

When an internal host initiates a connection to an external host, the architecture MUST NOT require that either end host participate in the routing system more so than they do already. Put another way, it is unreasonable for end hosts to have topological knowledge of the network for purposes of middlebox discovery, and even more unreasonable for them to have to indicate changes of that topology to the routing system. Aside from security concerns existing

recommended Internet routing protocols are not well suited to the task of having every edge device participate.

4.3 External to Internal, No Application Controller

If we simply look at the flow between an internal and external host, the difference between this case and the previous is that the intended transport flow is reversed. Policy permitting, discovery of middleboxes should be no different than the previous case. However, the situation is a bit more complex.

Prior to connecting, an external host must acquire an IP address for the internal host. That internal host may not have an address in the external host's realm, and the internal host's address in its own realm may be temporary. Thus, some interaction with a name service will be required. In order for this to occur, the internal host must have established a binding between its address in its realm and its address in the external host's realm. If the internal host's realm is adjacent to more than one realm, the internal host may need more than one external address, and it will need to discover all the middleboxes adjacent to all the realms to which it wishes to make itself known.

4.4 Application Controller

In this case, the application controller is contacted by either the internal or external host prior to them contacting each other. The application controller may or may not be in the data flow, but the AC is contacted explicitly. The AC may then return communication parameters so that a transport connection would be established. The AC, however, is required to discover the middlebox. Because the AC may not be in the data flow this could pose complications for discovery.

5 Usage Examples

Below are a number of network topologies in which discovery could occur. An AC can be found in each figure. However, the case should also be considered without the AC. Similarly, since an AC may itself be a middlebox, consider the cases where it and the router are combined.

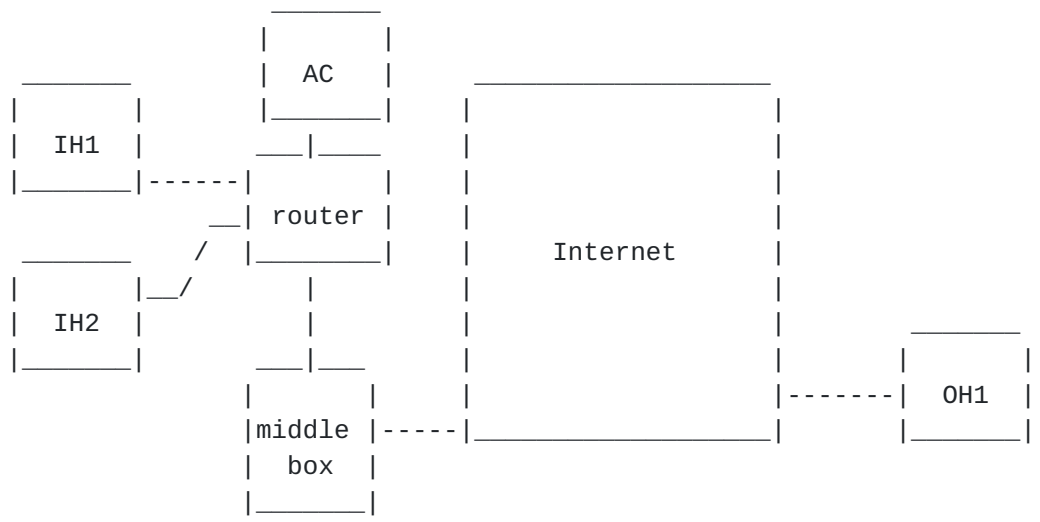

Figure 2: Simple Network Topology

The best example of the use of an AC is that of an incoming SIP call. See [HUITEMA] for a flow diagram. The key point to note in this diagram is that the AC will want to determine whether or not the middlebox will affect communication between IH1 and IH2 or between IH1 and OH1. Moreover, the AC must also keep track of which middlebox is used.

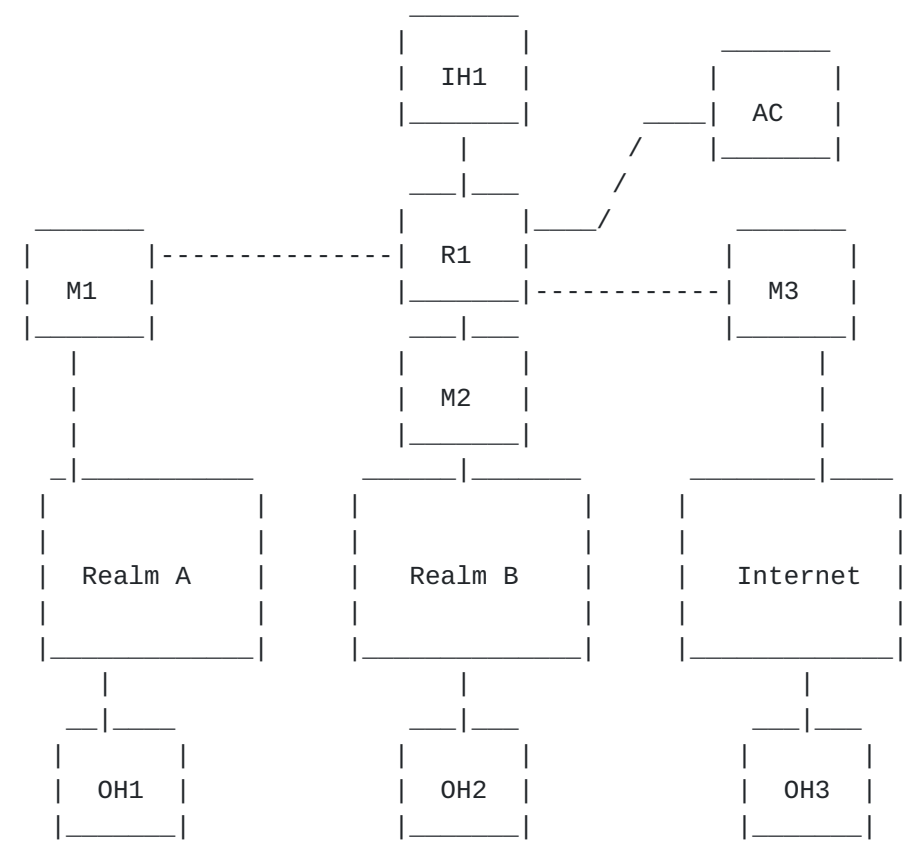

Figure 3: Corporate Network with Private Connections

Figure 3 depicts a case in which the application controller must not only determine that IH1 will use a middlebox to communicate with OH1, which is located in Realm A, but that it will use Middlebox M1, as opposed to M2 or M3. And of course, for IH1 to communicate with OH3, M3 will be used instead. Indeed M1, M2, and M3 may implement very different policies. For instance, Realm A may be within the same enterprise, whereas Realm B might be a private link to a partner, such as a supplier. Assuming each of these middleboxes are NATs, the addresses given will be specific to the realms of OH and OH2, and global for the case of OH3. This becomes important in our next case.

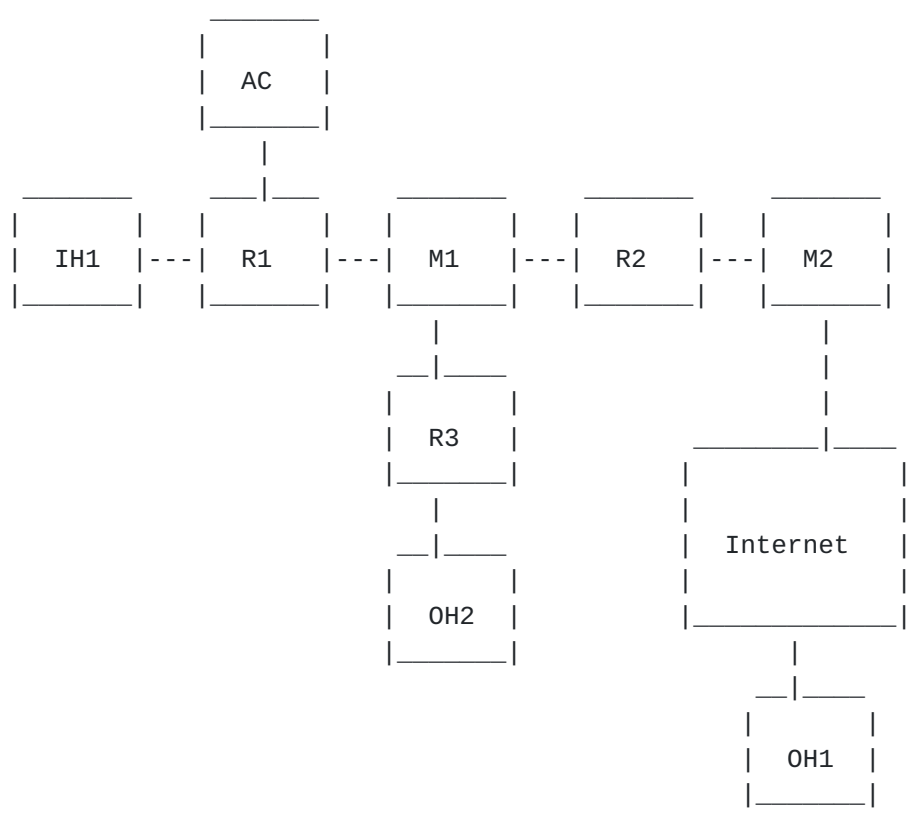

Figure 4: Mass Chaos

In this case, the application controller must discover either one or two middleboxes, depending on whether IH1 will communicate with OH1 or OH2. Note that it is possible that Middlebox M2 won't be in the same address realm as AC, making knowledge of the topology a difficult option under existing technology. Also note in this example that the information that OH1 wants is the global address to use for IH1. Thus, information provided by middlebox M1 to AC1 is at best of no use and certainly misleading.

It is possible to combine figures 3 and 4 to be truely horrifying.

6 Requirements

What can we conclude about requirements for discovery, based on the above cases? First, we must handle both the existance and non-existance of application controllers.

In addition, whereever there is a middlebox there will be policy associated with that middlebox. If policy does not permit it to do so, a middlebox MAY NOT respond to any form of discovery. Discovery mechganisms, therefore SHOULD be configurable within a middlebox (we say "SHOULD" in with the hopes that they will be present at all).

Discovery SHOULD be possible in the presence of multiple middleboxes, both in the case where they are serially between two end hosts, or where there is a choice between two middleboxes based on the destination. Discovery messages themselves may need to be modified by middleboxes.

In order for internal hosts to function as servers, discovery of a middlebox may need to occur prior PRIOR to a communication with any external host.

7 Security Considerations

There are numerous security considerations that middle boxes will encounter, and the ones we list below should be viewed as far from complete.

The diagnostics and discovery discussed in this draft are useful only within the boundaries of a single administrative domain. The middle boxes on the borders of that domain should prevent external devices from participating by not transmitting diagnostic messages outside, and by not listening for signaling requests on interfaces external to that domain.

8 IANA Considerations

None.

9 References

[1] Rekhter et. al., "Address Allocation for Private Internets", RFC 1918, February 1996.

[2] Carpenter, B., "Internet Transparency", RFC 2775, February 2000.

[3] Srisuresh, P., Holdrege, M., "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August, 1999.

[4] Huitema, C., "Middlebox Scenarios", Internet Draft, April 2001.

10 Author's Address

Eliot Lear
Cisco Systems, Inc.
170 W. Tasman Dr.
San Jose, CA 95134-1706
Email: lear@cisco.com
Phone: +1 (408) 527 4020

11 Intellectual Property Statement

12 Full Copyright Statement

THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES,

EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."

17 Expiration Date

This memo is filed as <draft-lear-middlebox-discovery-requirements-00.txt>, and expires October 5, 2001.