MIDCOM Working Group
Internet Draft
Category: Informational

C.Aoun
Nortel Networks

June 2001

Expires on December 2001

Network topology considerations in the MIDCOM Architectural framework <draft-aoun-midcom-network-00.txt>

Status of this Memo

Abstract

In the present Internet architecture, packet transparency is lost due to the introduction of Middle Boxes that either modifies the contents of the IP packet, or drops it (Ref [RFC2775]).
This draft presents in the context of the MIDCOM workgroup framework several Middle Boxes network deployment scenarios that needs to be considered.

This draft assumes that the reader has sufficient knowledge on NAT (Ref [RFC2663]) and it's consequences (Ref [NAT-COMP]).

This draft provides a list of topologies that needs to be considered (and their related implications) when deploying multimedia services over the Internet.

It MUST not be seen as a protocol description document or an overall framework architecture document.

Table of Contents

1 Introduction

The Middle Box (MB)terminology is aligned with the MIDCOM workgroup definition, i.e. a device that has router functionality and alters the content of either the IP header or it's content; or drops or forwards the packet depending on the filtering rule that is applied based on IP header/protocol type/transport port and this on packets coming from a certain group of users or interfaces.
The MB terminology will probably evolve in time, the draft will be updated to take into account the new taxonomy.
In order for the middle boxes to scale and have high performance, it is essential that the Middle boxes have no application awareness, which would require MBs to have at least a subset of the application's state machines.
This approach requires that all traversed MBs have the required application awareness; this represents a major stopper to development of applications.
Having the MB have application awareness is what is called having an Application Layer Gateway on the MB (Ref [RFC2663]).

Application awareness is provided by devices already implicated in the application (case of In path agents), this device communicates with the MB to provide it the necessary information to allow the application to work.
The MIDCOM protocol is the protocol used between the previous entities.

The instance communicating with the Middle Box is the MIDCOM Agent (MA), the peer on that interface is the MIDCOM Interface on the Middle Box.

The main reason for issuing this draft is to complement the current topologies taken into account within the MIDCOM framework (ref [MDCMFRWK].

Here is the main issue that this draft tries to get the MIDCOM WG to be concerned of:

-How does the MIDCOM Agent know that the application's packets (either control stream or bearer stream) traverses MBs?
Although this was decided to be out of scope of the MIDCOM WG, it is still a big piece of the puzzle. Manual provisioning of the encountered MBs and their applied functions on the MA will require a lot of effort (and probably won't scale).
This issue should be tackled in the MIDCOM WG or elsewhere.

This could prevent certain network topologies from being deployed.

In the following, the 'Customer' network is a network containing a group of network elements (hosts, routers, servers, etc _)that is not in the Internet Service Provider network neither in the Content Service Provider network.

2 Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119.

3 Network deployment scenarios

This section handles several main network types:
-The Content Service Provider (CSP)is the customer's Internet Service Provider (ISP).
-The CSP is a separate provider from the customer's ISP.
-The customer is in a remote site and is connected to it's enterprise VPN via a defined ISP.

In all cases the customer network could be connected via an Access Network Provider which is separate from the ISP, this could happen for cable access and xDSL access.
In the context of this document this is irrelevant considering that we are looking at the MB interaction problem.

The traversed ISPs could have border MBs at their edges, or it could be assumed that no MBs will be encountered.

The previous models are reflexive (i.e. the called parties have one of the previous network models), for clarity reasons the application pair (peers or Controlled) parties (i.e. calling and called parties,

IP phone/Media Gateway _) are not shown.

The CSP also has MBs that protect all the Content Service (voice per example) application devices (device controllers (i.e.MGCs), SIP Proxies, Element Management Systems (i.e. SNMP manager implementations), Media Gateways etc_) from the CSP internal network, the ISP network, the customers and the Internet.

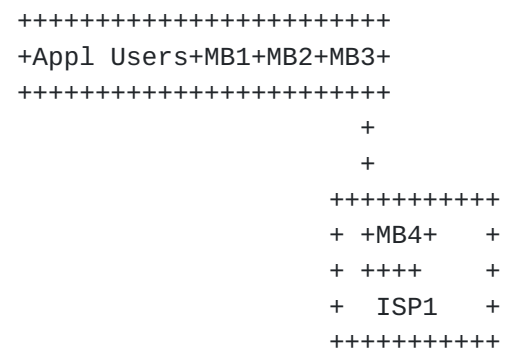
The following subsection provides a view on network topologies where several consecutive MBs are deployed to provide all the required MB services in the customer premise.

3.1 Particular customer network configurations

The current market status shows that it is quite often to find several MBs in the customer network in the path of flows.

These MBs could apply complementary MB functions to the packet flows that might traverse them.
The figure below shows an example of a network topology where within a customer network 3 MBs are used :
-MB1 provide secured access from the Internet and certain categories of users in the customer network; a packet filtering function is applied to the flow
-MB2 applies packet filtering and NAT to the flow
-MB3 applies QoS gating on per application's session basis
-In the customer's ISP side MB4 applies QoS gating and packet diversion (in case law enforcement authorities require it) on per session basis.
The QoS gating function allows reserving appropriate bandwidth for the application session. The reservation could also be accompanied with pre-emption on other existing flows of the same application (i.e. priority not defined on layer 2 or layer 3 priorities, but within the application).

It is obvious that the order in which the Middle Box functions are applied is critical (especially for Nat and packet filtering)in this network type.



Currently it is not a lot frequent to find the likes of MB3 and MB4 in the network; but since the access interfaces (Customer <-> ISP

network) will still be bandwidth limited for a while, QoS gates will be required on this interface to meet the applications' QoS requirements.

This topology could be found in a lot of customer networks.

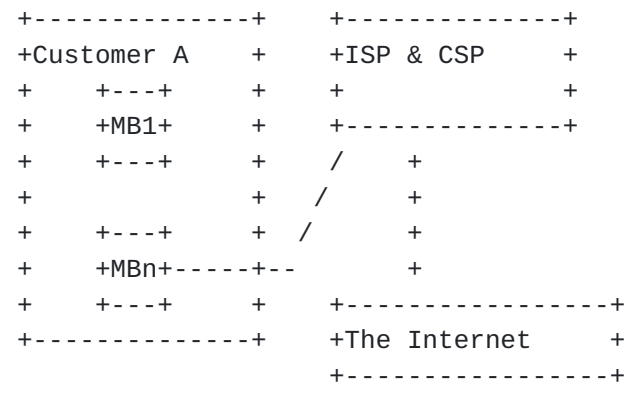
The end to end network types follows in the next sections.

3.2 The customer's ISP is the Content Service Provider

This type of network deployment is quite often in the context of delivering bundled data and voice services.
There are 2 variants to this scenario:

(1) The Middle Boxes (1 or many MBs) are managed by the customer network.
(2) The MBs are managed by the service provider.
In this model the MBs could be considered as trusted devices and are provided policy rules by a common policy server. This is what could be considered as complete carrier managed services.
Type 1:This scenario could be subdivided into 2, case where the customer has 1 MB, whereas in the other case the customer have more than one MB.

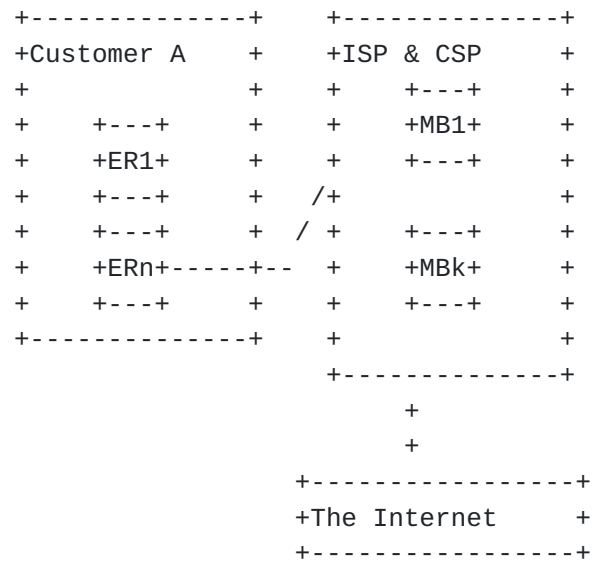
Typically several MBs are deployed in a customer's network when the customer has a VPN with widely spread sites, and the ISP provides several POIs to interconnect to the Internet.
The case where several MBs could be traversed is quite interesting since it is almost impossible to know in advance which MB will be traversed (the traversal is based on the routing infrastructure and the destination application endpoint).



Type 2: Again this network model could be subdivided into several Models:

- -The customer has one Edge Router (ER) and only one MB is used in the ISP/CSP
- -The customer has n Edge Routers, and the ISP/CSP has only one interface on MB used for customer A
- -The customer has n ERs and the ISP/CSP has k MBs or k interfaces on the MBs dedicated for customer A

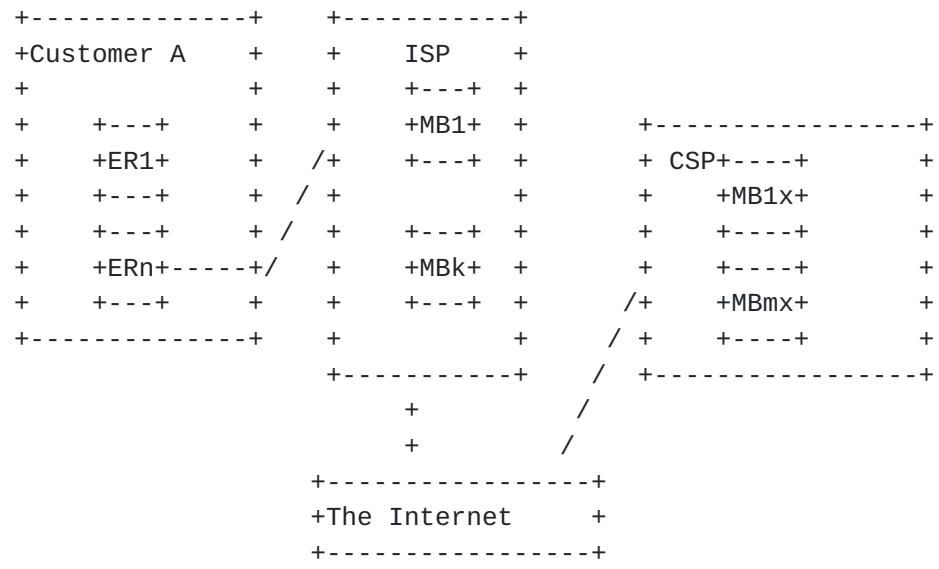
Again there are issues on determining in advance which MBs will be traversed when several MBs are deployed.



3.3 The customer's ISP and the CSP are different legal entities

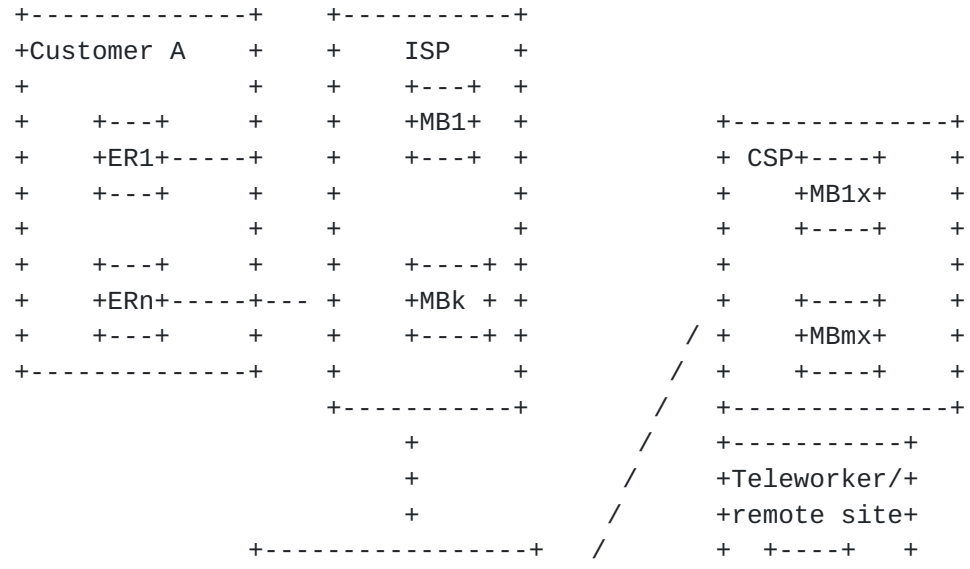
In these network types, the customer purchases the application services from a service provider different from its ISP.

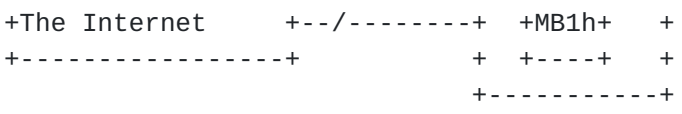
We shall assume that the customer's ISP is not directly connected to the application service provider, in case it is the model still applies.



In this network model, the MBs could also be in the Customers premise, i.e. both type 1 and type 2 network types apply to these networks.

3.4 The Teleworker or small remote customer sites case




+The Internet
+MB1h+

This network model has several variants that could be inherited from 2.1 and 2.2.
This model is not completely different from the previous ones, from a VoIP perspective since the application (VoIP) is provided through the customer's VPN. Hence the Teleworker/remote site, establishes a tunnel (IPSEC ESP per example, other IP tunneling protocols could be used as well)for all the traffic related to the customer A VPN.
All the tunneled information will not be altered, therefore there is no different constraints/interaction with the MBs (from a VoIP perspective) from 2.1 and 2.2.

4 Summary

The network topologies in the previous sections show new deployment considerations, where the MA will need to negotiate network parameters with :

- Various Middle Boxes with different MB functions
- Different Middle Boxes for the application signaling protocol than for the media packets

[MDCMFRWK] does not take into account topologies where the bearer path is traversing either a different interface then the application protocol messages or even a different MB.

The ideal is to define a model that meets carrier managed network type (i.e. Type 2 networks, with the service provider providing the Middle Box services) as well as type 1 networks (where the Middle Boxes are managed by the customer, and most likely this customer has few, probably 1 MB).

Initiatives need to be actively started within the IETF either in the MIDCOM WG or in another WG, to start looking at MBs discovery.

There are two approaches to this, either build a mechanism around MB discovery specifically or around "special" network elements discovery to take into account various "special type" network nodes. Obviously the later approach should never be handled in the MIDCOM WG.

5 References

[RFC2663] P.Srisuresh, M. Holdrege, "IP Network Address Translator(NAT)Terminology and Considerations", RFC 2663 August 1999.

[NAT-COMP]P.Srisuresh, M. Holdrege, " Protocol Complications with the IP Network Address Translator", RFC 3027 Jan 2001

[MDCMFRWK]P.Srisuresh,J.Kuthan, J.Rosenberg," MIDCOM Architecture & Framework",
Internet draft, draft-ietf-midcom-framework-01.txt

[RFC2775] B. Carpenter, Internet Transparency

6 Acknowledgments

The author would like to thank the following people for their useful comments and suggestions related to this draft: Patrick Bradd, Matt Broda, Louis-Nicolas Hamer, Mick O'Doherty, Reynaldo Penno, Abdallah Rayhan, Massimo Strazzeri and many others in Nortel Networks.

7 Author's Address

Cedric Aoun
Nortel Networks
33 Quai Paul Doumer
92415 Courbevoie Cedex
FRANCE

Email: cedric.aoun@nortelnetworks.com

8 Intellectual Property Statement

9 Full Copyright Statement