Personal
Internet Draft
Technologies
Document: draft-oneill-mipv6-cao-00.txt
Expires: Mar 2003

A. O'Neill
Flarion

19 Sept 2002

MIPv6 Care of Address Option
<draft-oneill-mipv6-cao-00.txt>

Status of this Memo

Copyright Notice

Abstract

IPv6 and MIPv6 has constrained the HoA to being used within forward and reverse tunnels via the HA. In the unicast case, the MN can then activate
Route Optimisation to bypass the HA in both directions by securely installing
a Binding Cache Entry into the CN. The MN then sends from the CCoA source address to the CN directly into the foreign multicast system, and includes the Home Address Option (HAO) so that the changing CCoA is masked from the transport layer.

This draft defines the Care of Address Option, which carries the current CCoA
of the MN. The CAO can be included in a Hop By Hop Header or Destination header and used instead of the packet source address for unicast ingress filtering and multicast RPF purposes. This enables a MN to potentially use

the HoA as a source address on the foreign network, and to inform the CNs of the evolving MN location.

INDEX

1. Introduction

Mobile IP for IPv4 enables the MN to use its HoA as a source address on the foreign subnet when forwarding to the CN either directly or via the HA using reverse tunnelling. The native forwarding follows the optimal route to the CN but incurs the risk of being discarded by ingress filtering routers due to the topologically incorrect source address. IPv6 and MIPv6 have therefore constrained the HoA to being used as a source address when either at home or within a reverse tunnel from a foreign subnet via the HA of the MN. The CN then returns packets to the MN HoA, via the HA, and the forward HA to MN tunnel based on the CCoA in the HA binding for the MN. In the unicast case, the MN can then activate Route Optimisation to bypass the HA in both directions by securely installing a Binding Cache Entry into the CN. The MN then sends from the CCoA source address to the CN directly via the foreign unicast or multicast system, and includes the Home Address Option (HAO) in the unicast packets so that the changing CCoA is masked from the transport

layer. The CN sends directly to the MN using a routing header. In the multicast case, the persistent HoA cannot be used as a multicast source address because such packets will fail the multicast reverse path forwarding check. The MN must instead use its CCoA on the foreign network as its source address, and a new multicast tree must be built for each new CCoA on each MN hand-off to ensure that the multicast source address is topologically correct. These multicast issues are discussed in detail in [MIP-Multicast].

This draft defines the Care of Address Option, which carries the current location of the MN in the form of the CCoA or the HoA, within either a Hop By Hop or a Destination Header. The Hop By Hop or Destination header based CAO can be used to both redirect ingress filtering / multicast RPF checks so that the MN can use its HoA as a source address from the foreign network directly with the CN. The Destination Header based CAO can in addition be used to inform the CN of the location of the MN when either reverse tunnelling to the HA or on the home network, and hence when ingress filtering checks would already succeed. They also inform the CN of the current location of the MN. This information is stored by the CN in an Inverse Binding Cache Entry, which may be used by high-layer mobility aware processes, and may also be used to improve Route Optimisation procedures.

The CN can reflect a CAO back to the MN in a Destination header either directly or via the HA using a routing header, to close the verification loop so that the MN can be reasonably confident that the CN knows the desired binding between the MN HoA and the MN CCoA.

The CAO, whilst primarily designed for unicast communications, may also be used to enable the HoA to be used as a multicast source address on a foreign subnet to pass multicast RPF checks, and address the efficiency limitations of MIPv6 multicast. The multicast details of this are not covered in this draft but are described at a high-level in [MIP-multicast].

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 [RFC2119].

3. Terminology used in this document

Much of the terminology used in this document borrows from Mobile IPv4 [MIPv4] and [MIPv6] specifications and drafts. This draft introduces and uses the following additional terminology.

Care of Address Option (CAO) - an option included in an IPv6 Hop by Hop or Destination Header that is used to redirect source address checks to the CCoA

rather than the source address (HoA) of the packet and to indicate to the CN the present location of the MN. The CAO may also be reflected back to the MN in a Destination Header to verify the contents of the triggering CAO that was received at the CN.

Inverse Binding Cache Entry - an optional entry in a table at the CN that has the mapping between the MN HoA and its evolving location as well as details of how and when the CAO was received, and if, how and when the CAO was verified. As a result, any IBCE explicitly includes a measure of confidence in the entry for each MN and implied or explicitly stated constraints on its use by the CN.

Option Enforcement Point (OEP) - a node that inspects options within extension headers when the header type would not otherwise have caused this node to process the options, such as with a firewall. A node that is defined by the header type as able to process the option is a Defined node.

4. Motivation

4.1. The Ingress Filtering Problem

MIPv4 MNs can use the HoA as a source address for unicast packets from the foreign subnet without using a reverse tunnel to the HA. In the case of a FA, the MIP binding information between the HoA and the CoA is known and trusted, and therefore the Access Router containing the FA can enable the topologically incorrect source address to be forwarded safely. However, this still risks the packet being discarded by ingress filtering in internal nodes that are not aware of the secure MIP binding information between the HoA and the CoA.

In MIPv6, the use of the HoA as a unicast source address when sending direct to the CN is prevented and the MN must instead only use the HoA when reverse tunnelling packets to the CN via the HA. Route Optimisation can then be used to securely install a Binding Cache Entry (BCE) in the CN so that the CN and MN can then directly communicate using the CCoA of the MN as a network address. The Home Address Destination Option and the Type 2 Routing Header is then used to enable the network layer to forward packets whilst maintaining the HoA as the transport layer view of the MN address. Unfortunately, Route Optimisation has significant security issues and places a significant burden on the MN during hand-off. For this reason it is likely to be inappropriate in many circumstances and a lightweight method of optimising one leg of the path might therefore be useful.

One potential mechanism is to use the MN HoA as a source address on a foreign network, but add the CCoA of the MN into the CAO within a Hop By Hop Header, to affect all routers that wish to undertake ingress filtering. All such routers must first check for the existence of the CAO. Its presence informs the router that the ingress filtering should be performed on the address in the CAO option rather than on the packet source address. In addition, the MN must only issue such packets from the network on which the CCoA is valid. All IPv6 Access Routers MUST implement ingress filtering on the source address but MAY, along with any other IPv6 router, be enhanced to

support redirected ingress filtering checks on the CAO in the Hop By Hop header. Routers implementing CAO based ingress filtering MUST check the validity of the address in the CAO within the Hop By Hop Header and discard any packet with an incorrect Option value. In the absence of the CAO in the Hop By Hop Header, the ingress filtering is performed on the packet source address. An incorrect CAO / source address is an IPv6 unicast address that is received on the wrong interface according to unicast routing.

An alternative mechanism is to once again use the MN HoA as a source address but this time include the CAO within a Destination Header. This requires that unicast ingress filtering and multicast RPF checks in routers need to occur independently of the IPv6 header processing rules. This is reasonable given

that a MN cannot be trusted to request its own packets to be policed and therefore offers a potentially lightweight alternative to the Hop By Hop Header.

An ingress access router that supports a redirected ingress filtering check, using the CAO, SHOULD advertise this capability in its router advertisement. This is so that a MN can avoid trying to send packets directly from a foreign network that does not support the CAO. A MN SHOULD NOT include a CAO unless this capability has been advertised. In addition, an access router MAY indicate if the whole visited domain supports the CAO option throughout that domain so that the MN can aggressively use the CAO at each new access router in an operator's domain during hand-off.

4.2. The Mobile Source Tracking Problem

A MN that uses its HoA as a source address might also wish to inform appropriate CNs of its current CCoA, and of CCoA changes, for a range of reasons. This is true whether the MN is at home, sending natively from a foreign network or reverse-tunnelling from that foreign network to its home network. The CN can then maintain an Inverse Binding Cache Entry for the MN that tracks its movement and address details of its locations. The IBCE can be built in multiple ways and with different levels of confidence in the binding information.

Applications can then have an API with the IBCE and hence subscribe to mobility events or to CCoA specific information. For example, the presence of an unchanging CAO provides the CN with a very good reason to support RO with this MN due to the likely low rate of binding updates from such a slow moving / stationary MN. In addition, being optionally informed of the new CCoA by the MN enables the CNs to automatically track the movement of the MN through the topology. Applications might also wish to delay sending new packets for a short time whilst the MN is undertaking a hand-off, or receivers might wish to perform less aggressive buffer management for real-time applications. Sessions with specific MNs might also be scoped such that service would only be provided to MNs when either at home, or when they are at CCoAs under specific prefixes such as the home or local domain. This draft does not motivate the new mechanisms on the above specific examples but instead is using them simply to indicate the potential usefulness of the API to the location information.

5. High-level Processing Rules for the CAO

5.1. Option Enforcement Points and Ingress Filtering

IPv6 header processing rules state that the header options within an extension header are processed by nodes according to 'defined' rules of that header. So Hop By Hop Header options, for example, are processed by all hops.

In addition, header processing rules state that such processing nodes must process the options according to the three most significant bits of the option type, where for example, code 110 means that the packet should be dropped if the option is unrecognised and the option cannot be modified on route.

Clearly though a router that wishes to police the contents of packets, for policy and firewall reasons, cannot rely on a MN creating packets with suitable header types that will enable the enforcement point to check out all the options in a defined manner according to the extension header processing rules. For an arbitrary enforcement point to be fully capable of correctly checking extension header options, every packet from every node would need to carry all options within a Hop By Hop header, with the option type code at '111'. This would naturally result in an arbitrarily located option enforcement point discarding packets with options that it did not understand, and whose threats it cannot assess, as well as modifying options it did not like. This however is clearly not practical as it removes much of the functionality of option processing.

Therefore an arbitrary option enforcement point must be able to examine packet options both by ignoring extension header processing rules that would normally prevent it from examining all options, as well as ignoring the option type code and instead treating all options as '110' by default. The likely exception is for end to end options that are within a Destination Header, and either below any routing header that itself is not end to end (ie type 2 ok), or absent a routing header. Only if the option enforcement point fully understands the option will it likely apply additional enforcement processing, including rewriting the option value (as if option code 'XX1') and recalculating the CRC to match. This draft neither requests nor recommends such behaviour by a general OEP on behalf of the CAO, whose requirements are instead detailed below.

Now the option type for the CAO, given the above, is also '110' so that the option will be discarded by a Defined processor of the option, if that node does not understand the option. At an option enforcement point, the option processing will also discard the packet by default if the CAO is not understood. The discarder, whether a Defined processor of the option, or an OEP, must generate an ICMP message back to the sender in the case of a unicast packet, including the CAO and the reason for the discard, so that the sender can distinguish between a node that does not support the CAO, and a node that has explicitly discarded the packet due to a range of CAO errors such as 'topologically incorrect (ingress filtering)' or incorrect binding (in a HA). The option MUST not be modified by a Defined option processor, but an enforcing processor such as an option enforcement point MAY modify the CAO if it fully understands the CAO semantics.

The following is then the expected behaviour through nodes such as access routers and other general OEPs;

If a legacy node is neither CAO-aware nor a Defined option processor, then it will pass the CAO unless it is an Option Enforcement Point in which case the packet will be dropped.

If the legacy node is a Defined option processor but is not CAO-aware then it will drop the packet as a result of normal CAO processing rules.

If the router is CAO-aware but not a Defined option processor, then it is an option enforcement point that may undertake CAO-aware ingress filtering. If it does so, then the packet will be passed or dropped based on the topological correctness of the CAO contents. Other option enforcement rules might also be applied to the CAO to decide on the

packets fate including passing it if the legacy ingress filtering process succeeds on the packet source address. Given that the CAO is only used to bypass the ingress filtering check, passing a packet on this check should be safe for any OEP.

If the router is CAO-aware and a Defined option processor then the node can also support CAO-based ingress filtering. The packet will then be discarded on the topological correctness of the CAO and other such rules in this draft, and the option will not be modified by the node as indicated by the option type.

If any node is a legacy ingress filtering node, which means it does not support CAO-aware ingress filtering, then the arriving packet might also be dropped or passed as a result of an incorrect source address.

The use of the CAO within a Destination Header is preferred to its use within a Hop By Hop Header because the latter will require all nodes on the path to be CAO aware for the packet to be correctly forwarded. In contrast, the use of the Destination Header requires only the 'Destinations' to be CAO-aware, along with any Option Enforcement Points on the path. Henceforth, this draft will only discuss the CAO in the Destination Header but in all cases the Hop By Hop Header can also be used. The Destination Header may be utilised above or below the Routing Header. When above the routing header it will be inspected by all destinations visited according to the routing header. When below the Router header and optionally below an ESP header, only the ultimate destination will process the CAO in the Destination Header. The appropriate choice by the MN is to by default place the CAO within a Destination Header above any routing header and ESP header. Specific situations do exist however when the CAO can be safely encrypted. If the Destination Header is below any ESP header then only the MN can verify that the CAO is correct and the existence of the ESP header ensures the CAO has not been modified on route.

It is a minimum expectation of this draft that all IPv6 access routers undertake ingress filtering on the packet source address and will discard topologically incorrect source addresses. It is recommended by this draft that all IPv6 access routers support CAO based ingress filtering. It is required by this draft that all such access routers indicate their support for CAO in their Router Advertisements, to avoid a MN attempting that which is unavailable and as a result risking packet discard. It is recommended by this draft that the Router Advertisement indicate whether or not the operators domain supports CAO processing so that the MN can aggressively use the MN HoA as a source address. It is also required by this draft that a HA advertise its capability to support CAO processing to the MN through Router

Advertisements on the home network, and through suitable advisory and error messages during MIP signalling. The details of these messages are for further study.

5.2. Existing MIPv6 Processing Rules for the HoA Source Address

The following nomenclature is used to describe the supporting figures in this draft when describing the use of the CAO.

MN - Mobile Node
CN - Correspondent Node
HA - Home Agent
HoA - Home Address from HA
CCoA - Co-located Care of Address from foreign network
HAR - Home Access Router (default router on the home network)
FAR - Foreign Access Router (default router on the foreign network)
OEP - A general Option Enforcement Point that passes CAO packets.
R - A general core router on the path of the packet..

^ - the destination node according to the current destination address
> - a node traversed by that packet
[- an encapsulating node
] - a decapsulating node
I - a node that undertakes a legacy ingress filtering check on source address.
E - an option enforcement point that supports enhanced CAO-based ingress filtering.
H - a Defined node that supports enhanced CAO-based ingress filtering
X - a node that discards a packet due to an incorrect source address
S - an option enforcement point that snoops and passes the CAO unaffected.

Figure 1 shows a schematic of the possible forwarding paths between the MN and the CN, when the MN is on its home or a foreign network, and the MN uses its HoA as a source address. The FAR, HAR and HA are at least option enforcement points but may also be Defined option processors. The FAR and HAR are CAO aware ingress filtering nodes.

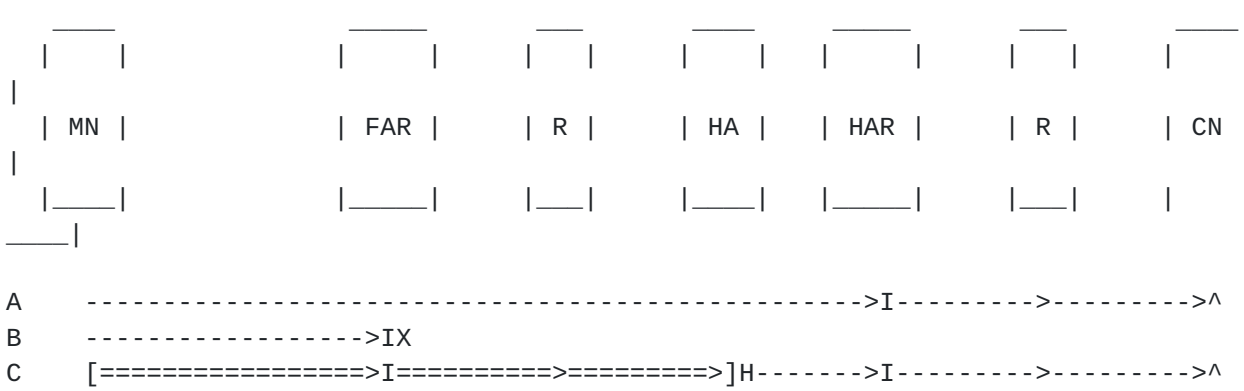


Figure 1: Existing processing Rules

In flow A, the HAR examines the packet source address and because it is valid

will be forwarded to the CN.

In flow B, the FAR examines the packet source address and because it is invalid on the foreign network (not from a prefix on the FAR) then the packet will be dropped.

In flow C, the MN is reverse tunnelling so the MN will encapsulate in the CCoA which will pass source address ingress filtering examination in the FAR. The HA decapsulates, checks the CCoA source address against the registered binding, and forwards the successful packet to the CN. The HAR examines the packet source address which again passes because it is the MN HoA.

5.3. Modified Processing Rules for the Foreign Network

In figure 2 we examine the basic changes brought about by this draft.

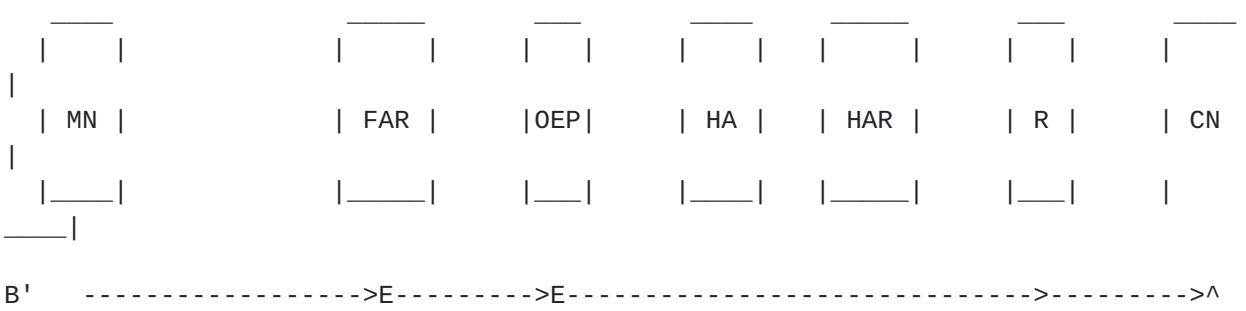


Figure 2: Modified processing Rules from the Foreign Network.

In case B', the MN is again on the foreign network but this time uses the Destination Header to carry the CAO containing the MN CCoA. This means that only a router on the path that chooses to enforce options (as an OEP) can undertake CAO based ingress filtering. Any such router, that does not understand the CAO, will drop the packet by default, but may pass the packet if the CAO is topologically correct. Therefore, if all the Option Enforcement Points between the MN and the CN are all CAO aware then this will ensure that the MN can send directly to the CN and avoid reverse tunnelling to the HA. The FAR MUST advertise its support for the CAO enhanced ingress filtering in the Router Advertisement and the MN should only use the HoA source address directly with the CN if this advertisement is received.

5.4. MN Location Exchange

Figure 3 illustrates the different forms of communication that a MN can now undertake as a result of this draft, and illustrates how the MN can in addition provide the CN with its location. The MN needs to set a flag, the filter flag (F), in the CAO to indicate whether or not the CAO or the source address is to be used for ingress filtering. If the filter flag is set then the ingress filtering is on the contents of the CAO whilst if it is not set then the ingress filtering is on the source address. The diagram also includes the cases when the MN tries to lie about its location to illustrate the level of confidence that the CN can place in the contents of the CAO.

Note that the CAO need only contain a topologically correct address. A MN can choose to set the P bit in the CAO, include only the access router prefix (most significant 64 bits) and hide the MNs current EUI-64. This is useful

if
   the MN HoA does not itself include that EUI-64, the MN therefore wishes to hide its terminal information from the CN, and/or the MN wishes to deny the CN reachability to its CCoA, yet reveals its topological location and share its movement history and mobility events with the CN. When the P bit is not set, the CN is informed that the contained CCoA is a valid communications address. The P bit setting must therefore be policed by the HA and access routers whilst also policing the CCoA contents and the other CAO flags. The MN may include the address of its default router whilst also setting the P Bit whereas if just the prefix is included then the lower 64 bits are zeroed.

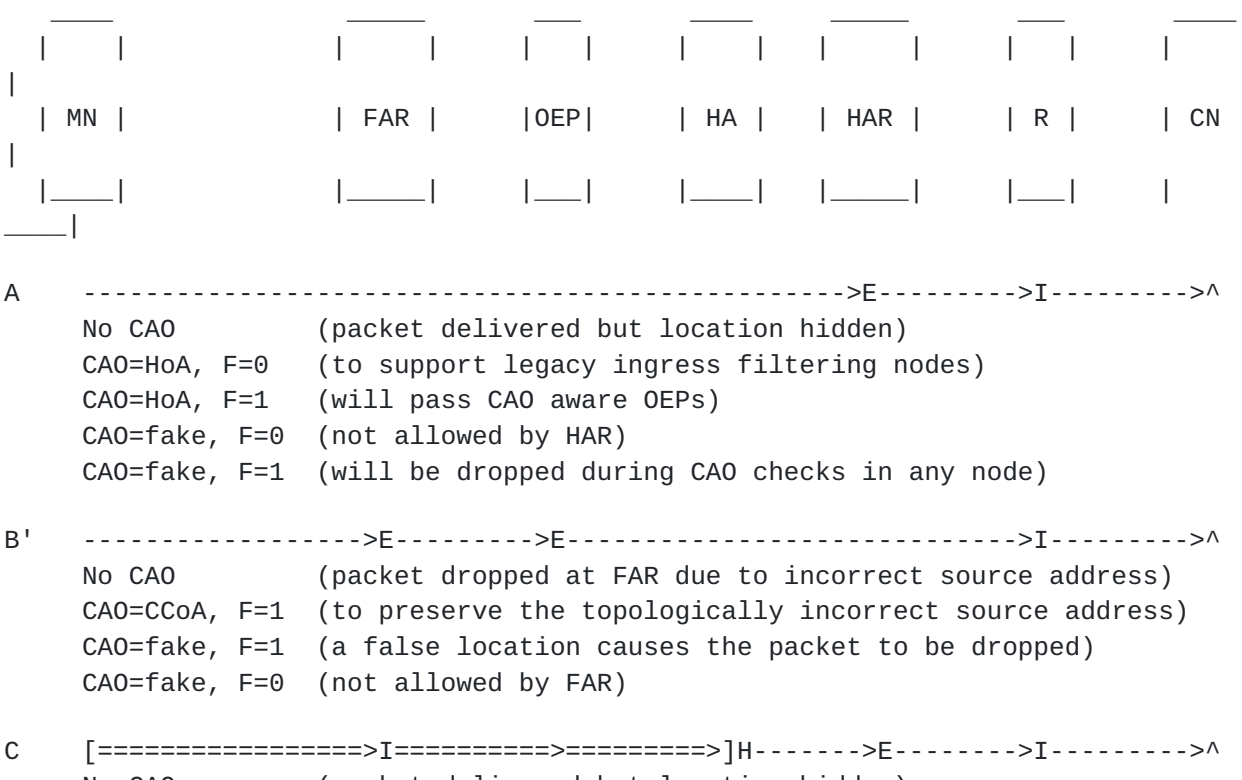


Figure 3: MN location exchange

In case A, the MN is at home and can optionally put a CAO into a Destination Header containing the HoA of the MN. The filter flag is best set to F=0 but MAY be F=1. The HAR MUST be able to check and recognise either a source address or a CAO that contains an address that is not from the home network.

In case B', similar processing rules apply except that the omission of the CAO is no longer possible and hence the CN always learns the CCoA and the EUI-64 of the MN. The FAR must be able to check and recognise a CAO that contains an address that is not from the foreign network.

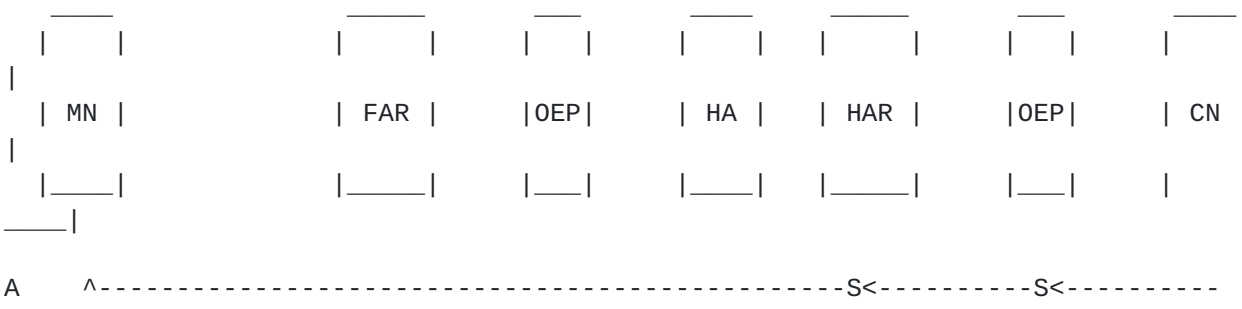
In case C, the MN is reverse tunnelling and the HA is used to assist the HAR in being able to distinguish between a packet from a foreign MN that can have a CAO=(CCoA=foreign, F=0) and a home MN that cannot (i.e. MN is lying about its location). The HAR can distinguish between packets from a MN and those from the HA due to the link-layer addresses and the RA from the HA. However,

if this link-layer information is not considered sufficient for all cases, then the MN MUST use a type 0 routing header containing the CN address and set the inner packet destination address to that of the HA. The HA is then a Defined processor of the CAO and after swapping the CN address into the destination address, the HA address will remain in the RH which will be received by the HAR. The HAR must be configured with, or learn securely the HA addresses on the home network, so that packets checked by the HA can be distinguished at L3, from those that have been sent directly by MNs or indirectly via MNs pretending to be HAs. The HAR then discards packets where the CAO=(CCoA=foreign, F=0) except if received via a trusted HA.

5.5 CAO Specific Processing Rules at the CN

The inclusion of a Care of Address option within either a Hop by Hop or a Destination Header does not affect the destination node's processing of this single packet but can create or modify state in the correspondent node in the form of an Inverse Binding Cache Entry (IBCE). The CN MAY inspect the evolving contents of the CAO and as a result MAY build an Inverse Binding Cache Entry (IBCE). This IBCE can be used by the CN to track the location of the MN in the topology if the MN so desires and for the networking stack and high-layer processes to be aware of hand-off activity and MN location. Specifically, the CAO can contain flags, that signal mobility events to the CN such as the M flag (movement) when a hand-off is starting on the old CCoA.
However, the presence of a Care of Address option in a received packet MUST NOT alter the contents of the receiver's Route Optimisation Binding Cache and MUST NOT cause any changes in the routing of subsequent packets sent by this receiving node without additional activity.

The contents of the CAO in an Hop By Hop option header has been fully verified by the routing infrastructure as being topologically correct. The contents of the CAO in a Destination header has been partially verified by the routing infrastructure and fully verified by the home or foreign network.
In either case, this does not prevent a 'man in the middle' attacker within the infrastructure or on the access link of the CN from modifying the contents of the CAO and replacing it with a topologically correct CAO at that location, which henceforth will still pass CAO based ingress filtering on route to the CN. Additional security processes are therefore required for the CN to fully trust the MN location for Route Optimisation purposes, which are not the subject of this draft. In all other cases, the IBCE is simply used for MN location tracking and provides little incentives for an attacker to go to great expense just to affect the contents of the IBCE.



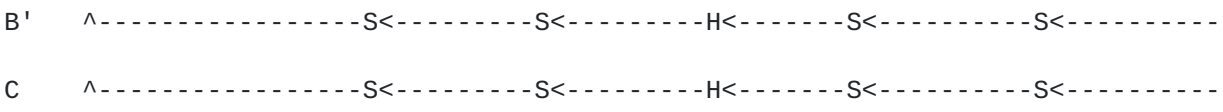


Figure 4: CAO reflection.

In the absence of an SA to authenticate or encrypt the CAO within a Destination Header, the CN can acquire additional confidence in the contents of the CAO through the reflection process (figure 4). The CN MAY reflect back the contents of a received CAO to a MN, using a Destination Header, within session response packets, or when those are not available, MIP signalling packets. This reflection MUST be undertaken immediately on receipt of a triggering CAO to avoid the contents of the CAO becoming stale, which would result in a failed verification and a discarded response packet. The receipt of a reflected CAO informs the MN that the CN is maintaining an IBCE for the

MN, as well as the current location of the MN contained in that IBCE at that CN. The MN can therefore detect whether the CN has an incorrect location created through an attack or simply as a result of a CN bug. The MN SHOULD discard packets containing an incorrect CAO entry and return an ICMP message back to the CN, reporting the failure of the CAO. The ICMP message MUST include the erroneous CAO and the reason for the failure. The MN MAY alternatively process the packet and send a new CAO to the CN immediately. The CN may also use a reflected CAO entry of 'all 0' to autonomously request a CAO update from the MN. The reflection process ensures that an attacker must be on both paths to be able to modify both the inbound and the outbound CAO. The Reflected CAO is also ameniable to end to end security, whilst the use of the triggering CAO for ingress filtering and RPF redirection generally prevents this. However, the CN may well prefer to have both the MN and its HA verify the reflected CAO as Defined processors, which then requires the CN to use a routing header and place the Destination Header above that routing header.

The combination of a triggering CAO in an extension header followed by a reflected CAO in a Destination Header, enacted periodically during a session, gives the CN a high level of confidence that its IBCE does indeed contain the current and evolving location of the MN. In both these cases, and potentially in other cases, the IBCE may assist with subsequent installation of Route Optimisation between the MN and the CN. A session in which the MN and CN are periodically and mutually verifying the MN location (HoA/CoA binding) may provide significant levels of confidence in advance of the Route Optimisation procedure and in so doing potentially reduce the additional message exchanges presently envisaged in the base MIPv6 spec. Essentially, the CAO is a proactive binding tracking mechanism whilst the COT(I)/HOT(I) sequence is a reactive mechanism enacted at the point of hand-off.

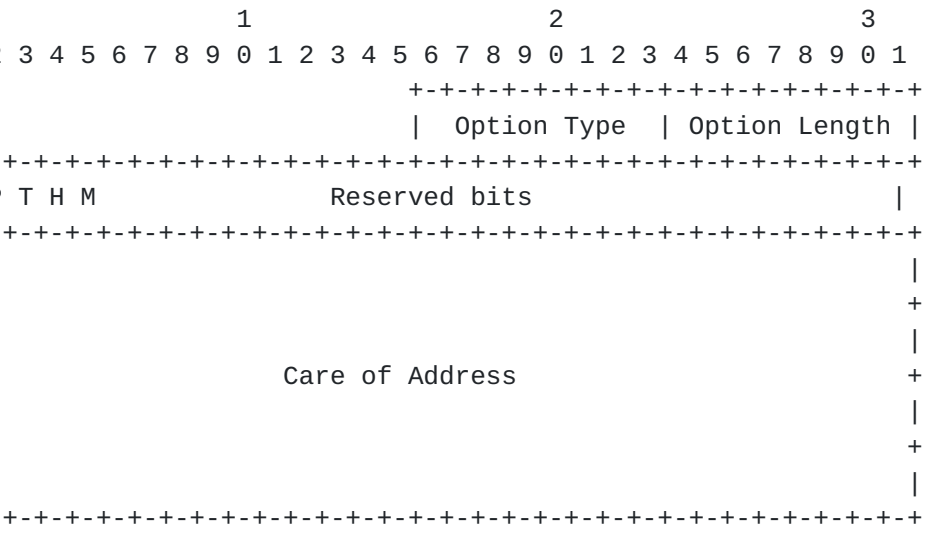
The IBCE contents might also be useful for identifying candidate sessions for the installation of route optimisation because a MN with a stable or slow moving location is preferable to one with high-mobility dynamics due to the significant security and signalling load (bandwidth/latency costs) required with RO each time the MN undertakes a hand-off. Finally, the movement information of the MN in the IBCE can be used for policy and application control of sessions that are affected by either location, roaming or mobility events.

The specific additional security requirements necessary to complement the

CAO
   processing for its use in Route optimisation is not covered by this draft.

6. Format and Usage Rules for the Care of Address Option

The Care of Address option is encoded in type-length-value (TLV) format as follows:



Option Type
TBA

Option Length
This field MUST be set to 16.

R bit
When unset this indicates that this is the CAO of the sender.
When set this indicates that this is the CAO of the receiver and the CAO has been reflected.

F bit
When set it indicates that the ingress filtering MUST be undertaken on the address in the CAO.
When unset it means that the ingress filtering MUST be conducted on the packet source address.

P bit
When set, this indicates that the Care of Address field includes the prefix of the MN only.

H bit
When set this indicates that the CAO will be verified by the MN HA and may be used by a CN to indicate that the location may be fake.

M bit
When set this indicates that the MN is starting a hand-off from the location address included in the CAO.

Care of Address
The present Care of Address (location) of the mobile node, which can be

either the MN CCoA or the HoA. It can be either the full address of the location, the prefix of the access router or a fake address.

A CAO with the R bit unset can appear in either the Hop By Hop or Destination Headers in a packet, but not both at the same time. Within the same packet, a reflected CAO with the R bit set MAY also be included in a Destination Header. A CAO with the R bit set SHOULD NOT appear in a Hop By Hop Header. Therefore, the Care of Address Option with the same R bit setting, MUST NOT appear twice in the same packet header. A CAO with the R bit unset can appear at most N times within a N-fold encapsulated packet. A CAO with the R bit set can also appear at most N times within a N-fold encapsulated packet.

IPv6 requires that options appearing in a Hop-by-Hop Options header or Destination Options header be aligned in a packet so that multi-octet values within the Option Data field of each option fall on natural boundaries (i.e., fields of width n octets are placed at an integer multiple of n octets from the start of the header, for n = 1, 2, 4, or 8) [11]. The alignment requirement [11] for the Care of Address option is 8n+6.

The Care of Address Option MAY be included in a Hop by Hop Header when;

- the MN is at home, or at a foreign network and either sends directly to the CN or reverse tunnels to the CN via its HA, and
- the MN uses its HoA as the source address

The Care of Address Option MAY be included in a Destination Header when;

- the MN is at home, or at a foreign network and either sends directly to the CN or reverse tunnels to the CN via its HA, and
- the MN uses its HoA as the source address.

The Care of Address Option MAY be reflected in a Destination Header when;

- the CN has received a CAO from the MN,
- the CN has created an IBCE for the MN, and
- the CN is sending to that MN HoA either directly, or
- the CN is sending to that MN HoA via its HA.

Multicast addresses, link-local addresses, loopback addresses, IPv4 mapped addresses, and the unspecified address, MUST NOT be used within a Care of Address option.

The Care of Address option in the Hop By Hop Header MUST be placed as follows:

- Before the Destination Header, if that header is present

- Before the Routing Header, if that header is present

- Before the Fragment Header, if that header is present

- Before the AH Header or ESP Header, if either one of those headers is present

The Care of Address option in the Destination Header SHOULD be placed as follows:

- After any Hop By Hop Header
- Before the Routing Header, if that header is present
- Before the Fragment Header, if that header is present
- Before the ESP /AUTH Header, if this header is present

This enables the Routing Header to formally control which nodes, such as the HA and MN, process the CAO in the Destination Header but means that the CAO cannot be encrypted. The HA and any other OEP MAY also snoop the CAO in unencrypted packets that pass through it as part of existing MIP operations.

The Care of Address option in the Destination Header MAY be placed as follows:

- After any Hop By Hop Header
- After the Routing Header, if that header is present
- After the Fragment Header, if that header is present
- After the ESP Header, if this header is present

This enables the CAO contents to be encrypted and ensures only the CN can process the CAO. The appropriate rules for the AH header have not been included merely for simplicity reasons but it is clear that ESP and the Auth header can be used to authenticate the contents of the CAO and build trust in the IBCE at the CN.

7. Security Considerations

The Care of Address Option provides an optional facility for the MN to send directly to the CN yet still potentially pass ingress filtering, and /or to inform the CNs of its topological movement. This draft does not specifically recommend, nor suggest standardisation of, the usage of such information by the CN network and higher layers.

The source address of such packets is the HoA of the MN, and the HoA also serves as the return address. The MN can include the CAO in such packets but this option does not in any way affect the routing of subsequent packets. The
packet source address and the returned packets destination address are

always
the same, being equal to the MN HoA. Packets containing the CAO do not therefore offer the redirection threats that were originally offered by MNs originating packets from the CCoA, and including the Home Address Option (HAO). This redirection threat resulted is such packets being banned in the base spec unless the MN/CN have securely installed a BCE in the CN, and this ban forces a MN to have to reverse tunnel packets to the HA in the absence of RO.

If the MN wishes to hide its location it can simply not include a CAO. Packets are not being rerouted based on the CAO and even if they were, it would only affect its own communication so the MN has little incentive to lie about its location and its mobility events.

The CAO processing rules ensure that the MN cannot abuse the CAO system and significantly mislead the CN. The access routers on both home and foreign networks must specifically prevent a MN from including an address into the CAO that is not its own and that has not been policed by the HA, but is valid at the access router and hence would have passed CAO based ingress filtering checks. An attacker on the same network as the MN can potentially try to send packets using the HoA and CCoA of another MN but clearly cannot otherwise intercept, or interfere with, the communications between the MN and the CN. This is true whether or not the CAO is added and is simply an additional requirement on the access router to be able to deny such opportunities to attackers.

Ongoing communications between a MN and a CN based on the HoA, provides the CN with confidence that the MN is reachable at the HoA at some arbitrary subnet via the HA. The inclusion of the CAO in a subset of packets from that MN provides the CN with a reasonable level of confidence that the MN is at that CCoA. A man in the middle attacker can at best modify the CAO and the CRC of a packet, but in doing so can neither hijack communications nor reroute packets. This is because return packets are still routed via the HA and will be correctly delivered to the MN at its presently registered CoA. The attacker could install an invalid CAO into a packet that might well fail upstream ingress filtering checks. This would cause the packet to be discarded but such an attacker could have removed the packet itself, so the addition of the CAO simply opens more subtle ways of discarding packets at significant expense to the attacker. The attacker can add a topologically correct address into the CAO from its location on the path to the CN, and then change it back on the return path but this offers nothing directly to the attacker at significant cost to itself. Additional security processes are however clearly needed to enable the IBCE to be used for Route Optimisation.

The use of the IBCE for Route Optimisation is not covered in this draft in detail and therefore a detailed security analysis of this has not been undertaken in this document.

8. Notice Regarding Intellectual Property Rights

Flarion's submissions will conform with RFC 2026. Flarion may seek patent

protection on some or all of the technical information submitted by its employees in connection with the IETF's standards process. If part(s) of a submission by Flarion is (are) included in a standard and Flarion owns patent(s) and/or pending patent application(s) that are essential to implementation of such included part(s) in said standard, Flarion is prepared to grant a license on fair, reasonable, reciprocal (license back) and non-discriminatory terms on such included part(s).

9. Acknowledgements

Many thanks to George Tsirtsis for reviews of this document and for motivating improvements in the design of CAO enhanced ingress filtering.

10. References

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

[MIPv4] C. Perkins, Ed., 'IP Mobility Support for IPv4', RFC 3344, August 2002.

[MIPv6] D. Johnson, C. Perkins, ``Mobility Support in IPv6", Internet-Draft, draft-ietf-mobileip-ipv6-18.txt (work in progress), 22 March 2002.

[MIP-multicast] A. O'Neill, 'Mobility Management and IP Multicast', Internet-draft, draft-oneill-mip-multicast-00.txt (work in progress), 5 July 2002.

Appendix A: CAO based RPF Check

In general, all routers in a network will be multicast enabled and as such will undertake multicast RPF checks. A CAO based RPF check uses the contents of the CAO rather than the multicast source address for the RPF check. This requires either that all multicast routers must be option enforcement points and to enable them to process the CAO option, or that the Hop By Hop Header be mandated for all multicast packets issued by MNs when away from home. The latter is not unreasonable given all modes are likely to be multicast routers, and any that are not will be tunnelled over and hence such nodes will also not see the Hop By Hop header.

Author's Addresses

Alan O'Neill
Flarion Technologies
Phone: +1 908 947 7033
Email: oneill@flarion.com