Mobile Transmission Control Protocol (MTCP) for Mobility Management over IP networks

<Draft-kuangyj-mobile-tcp-00.txt, .PDF>

Yujun Kuang	kuangyj@cqupt.edu.cn
Keping Long	longkp@cqupt.edu.cn
Qianbin Chen	chenqb@cqupt.edu.cn
Yun Li	liyun@cqupt.edu.cn

Special Research Centre for Optical Internet & Wireless Information Networks (COIWIN)
Chongqing University of Posts & Telecommunications
(CQUPT)
Chongqing, China, 400065

August 2004

By submitting this Internet-Draft,
I certify that any applicable patent or other IPR
claims of which I am aware have been
disclosed, or will be disclosed, and any of
which I become aware will be disclosed, in
accordance with RFC3668.

Internet Engineering Task Force
Internet Draft
Expires: February 2005

Yujun Kuang
Keping Long
Qianbin Chen
Yun Li
Special Research Centre for Optical Internet and
Wireless Information Networks (COIWIN)
Chongqing University of Posts & Telecommunications
August 2004

Mobile Transmission Control Protocol (MTCP) for Mobility Management over IP networks

<Draft-kuangyj-mobile-tcp-00.txt, .PDF>

Status of Memo

Abstract

This document defines two types of IP addresses to support mobile TCP - one for routing and location management, the other for host identification. Therefore, the dependency of TCP/UDP socket identification upon the network layer is eliminated, and transmission sessions will be no longer dependent of network layer IP address, that is, location changes of a mobile host result only new network IP address, which has no impact on transmission communications and its continuity.

And two new options are designed for M-TCP to hold IPv4, IPv6 and NAI addresses; and a new protocol, M-UDP is designed to support Transmission Control Layer host mobility.

Table of Contents

1. Introduction and Motivation

As known [1], IP version 4 (IPv4) even IPv6 assumes that a node's IP address uniquely identifies the node's point of attachment to the Internet. Therefore, a node must be located on the network indicated by its IP address in order to receive datagrams destined to it; otherwise, datagrams destined to the node would be undeliverable. When a node needs to change its point of attachment without losing its ability to communicate, it must typically: 1) change its IP address whenever it changes its point of attachment, or 2) recur to host-specific routing scheme – in which route information must be propagated throughout much of the Internet routing fabric to successfully deliver packets to the mobile node. Both of these alternatives are often unacceptable. The first makes it impossible for a node to maintain transport and higher-layer connections when the node changes location. The second has obvious and severe scaling problems, especially relevant considering the explosive growth in sales of notebook (mobile) computers.

Therefore, new, scalable, mechanism is required for accommodating node mobility within the Internet. Currently, there are many approaches to solve this problem, such as Mobile IP[1], HMMP[2][3], Mobile-TCP[4], ROAMIP[5], Cellular IP[6], etc. This draft describes a new framework to support host mobility in TCP/IP networks, by introducing some modifications in Transmission layer to make the TCP/IP stack more delaminated at the borderland between IP layer and Transmission layer.

In the section, we first briefly summarize the current works for host mobility management [1-6] in subsection 1.1. In the following subsections 1.3, 1.4, 1.5, 1.6, we present assumptions upon which the protocol is based, its applicability, and terms used in this document. Then, a general description is given in subsection 1.7.

1.1. Related Works

Thanks to the vast development of microelectronics technology, our PDAs and/or mobile phones become much more intelligent and powerful as they become much smaller and easier to use, which makes us nowadays much more dependent upon the information network: Internet.

To access into Internet at whatever time and anywhere, many challenges must be faced, because IP architecture is not designed for moving freely.

1.1.1. Mobile IP [1]

Mobile IP (MIP) is the most famous solution to introduce host mobility into Internet framework. RFC2002 introduces enhancements to Internet Protocol that allow transparent routing of IP datagrams to mobile nodes in the Internet. Mobile nodes are always identified by their home addresses, regardless of their access point or locations where they are attached to the Internet. When they are away from home, they must obtain temporary care-of-addresses – which are valid with regard to their visited network – and register them to their home agents. In MIP architecture, the home agents intercept and capture datagrams

destined for the mobile node and then forward the datagrams through tunnels (usually IP-in-IP tunnels) to the care-of address. At the end of the tunnel, each datagram is then delivered to the mobile nodes.

1.1.2. Mobility Support for TCP with SIP (HMMP) [2][3]

Host mobility management protocol (HMMP) is a protocol for supporting real-time and non-real-time multimedia applications on mobile terminals of 3G-IP networks, which utilizes as well as extends session initiation protocol (SIP) to provide means of domain hand-off (i.e., roaming), and subnet hand-off (i.e., macro mobility) so that users can access the network from any location using their own mobile terminal. This protocol relies on An advantage of HMMP is that it can spoof constant endpoints for mobile TCP connections and supports mobile TCP applications in a SIP environment without any changes to the TCP.

1.1.3. Mobile TCP [4]

Mobile TCP introduces an asymmetric transport protocol design for mobile systems, where a transport layer connection between a mobile and a corresponding stationary host is partition into two connections, the connection between the mobile host and a local fixed host referred to as Mobil e Gateway and the connection between the local fixed host and the corresponding host. In the first connection, TCP connection is an emulated version by means of L2 link operation or else to reduce computation or other processing cost to save battery power of a mobile terminal.

1.1.4. ROAMIP [5]

ROAMIP is an architecture that uses application layer solutions for global reachability and reuses transparent Mobile IP tunneling mechanisms or SIP message formats to ensure session continuity. ROAMIP eliminates long triangular routes, yet it is compatible with mobility unaware correspondent hosts. It is argued that it applicable to IPv6 as well as IPv4 networks.

1.1.5. Cellular IP [6]

Cellular IP defines local and wide area mobility to improve the performance of existing mobile host protocols (e.g. Mobile IP). In Cellular IP, networks are divided into service domains where local mobility is invisible to home agents – Cellular IP maintains distributed cache for location management and routing purposes – thus reduces frequent registration messages or binding updates between home agents and the mobile host. In local visited domain, distributed paging cache coarsely maintains the position of "idle" mobile hosts in a service area, which are used to quickly and efficiently pinpoint "idle" mobile hosts that wish to engage in "active" communications. This approach is beneficial because it can accommodate a large number of users attached to the network without overloading the location management system.

1.2. Specification Language

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [8]

1.3. Assumptions

Like MIP, this document places no additional constraints on the assignment of IP addresses. That is, a mobile node can be assigned an IP address by the organization that owns the machine.

No additional constraints or modifications are placed on routers along the datagram path during the communication between the Mobile Host and Correspondent Host.

The protocols defined in this document focus interests on unicast service only and support of multicast services is for further study (See Section 3).

Moreover, the protocols described in this document are not assumed to implemented only in IPv4, though examples or illustrations for IPv4 are given. IPv6 support is under further study.

The protocols defined in this document assume that each mobile host may be equipped with more than one network interface, but each of them can own only one permanent IP address, though the protocols are applicable for multiple permanent IP addresses.

This document strictly assumes that the routers are reliable or credible, while the mechanism to ensure reliability is out of scope of this document.

1.4. Applicability and Goals

The protocols aim at mobility management for mobile hosts that roam frequently resulting frequent hand-offs as well as fixed Internet nodes that occasionally change their attach point to Internet.

The protocols defined here are suited for both "macro" mobility management and "micro" mobility management.

In the proposed framework IP network layer is treated as purely routing layer to deliver datagrams to where they are destined. And the sessions created by transmission control layer are in principle independent of the IP layer below, though IP address is still an indispensable element to ensure the uniqueness of a socket, i.e., a session between processes on peer hosts. More details will be presented in "Protocol Overview" (Section 1.7) and Section 2.

The proposal here aims to make transmission layer more independent of network layer, thus sessions will not be broken when Internet nodes changes their IP addresses, which is applicable not only to intelligent mobile terminals, PDAs etc, but also to primarily fixed Internet nodes such as ponderous apparatus requiring Internet access service all the time.

1.5. New Architectural Entities

Actually, no new architectural entities are introduced in this document.

However, to make it easy to state and for comparison purpose, we redefine some architectural entities in Mobile IP [1].

Mobile Node (MN), or **Mobile Host** (MH)

Mobile Node is a host or router that changes its point of attachment from one network or subnetwork to another. In our architecture, a mobile node MUST has two different type of IP addresses (See Section 1.7, "Protocol Overview"), it may change the temporary address because of location change or for other reasons even if it is still on home network, while it may continue to communicate with other Internet nodes at any location using its (constant) IP address, assuming link-layer connectivity to a point of attachment is available. An MN CAN deliver redirection messages by ICMP datagrams or else.

Native Router (NR) acts almost alike **Home Agent** (HA) in Mobile IP.

A Home Router is a router on a mobile node's home network which functions like HA in Mobile IP, but rather than tunnels datagrams in IP-in-IP encapsulation it just forwards them for delivery to the mobile node when it is away from home, and maintains current location information for the mobile node.

Foreign Router (FR) is a router on a mobile node's visited network (foreign network) that provides routing services to the mobile node. An FR here is not the same as Foreign Agent in Mobile IP because it MAY have no capacity to handle IP-in-IP packets. Moreover, an FR MUST have functionalities to handle ICMP messages generated by MH in order to delivery subsequent datagrams destined to MH correctly. For datagrams sent by a mobile node, the foreign agent may serve as a default router for registered mobile nodes.

1.6. Terminology

This document frequently uses the following terms:

Permanent Address, **PA**, is an identification of the Mobile Host. The prefix of PA MUST be the same as that of its home network. In the document, its alias, **Home Address** may be used frequently.

Unique Network Identifier, **UNI**, or **Network Access Identifier**, **NAI**, is a globally unique identifier used to locate an Internet node’s home network or user’s service agent, usually in USER@DOMAIN form [9][10].

Dynamic Address (**DA**), or **Temporary Address** (**TA**). Each node in our architecture MUST obtain manually or automatically by some auto-configuration protocol an IP address valid to its attached network even at home network. TA plays a similar role of Care-of-Address in Mobile IP, but in quite different manner.

Redirect ICMP Message (**RMSG**), MAY be an existing ICMP message or some extended version of existing ICMP message used to tell the router (HR or FR) to deliver messages to a new location, i.e., a new

TA.

Agent Advertisement is an advertisement message constructed by attaching a special Extension to a router advertisement [11] message.

Correspondent Node (**CH**) or **Correspondent Host** (**CH**) is a peer with which a mobile node is communicating. A correspondent node may be either mobile or stationary.

Foreign Network (**FN**) is any network other than the mobile node's Home Network. In this document, its alias **Visited Network** may be frequently used.

Native Network (**NN**) or **Home Network** (**HN**) is a network, possibly virtual, having a network prefix matching that of a mobile node's home address. Note that standard IP routing mechanisms will deliver datagrams destined to a mobile node's Native Address to the mobile node's Native Network.

Link is a facility or medium over which nodes can communicate at the link layer. A link underlies the network layer.

Link-Layer Address is the address used to identify an endpoint of some communication over a physical link. Typically, the Link-Layer address is an interface's Media Access Control (MAC) address.

Node is a host or a router.

Nonce is a randomly chosen value, different from previous choices, inserted in a message to protect against replays.

Security Parameter Index (**SPI**) is an index identifying a security context between a pair of nodes among the contexts available during the Mobility Security Association between the MH and its NR.

Redirection Nodes Table (RNT) is a database on the NR with mobility management information, for example, about which TA is associated with its MH.

Visitor List is a database on one of the foreign routers on the visited network for management purpose, which contains at least a list of mobile nodes visiting a foreign agent.

Transmission Control Protocol (**TCP**) refers to both TCP and UDP in this document except for cases where clearly declared to mean pure TCP.

Mobile-TCP (**MTCP**) is extended transmission layer protocol defined in this document, which supports transmission layer mobility over traditional IP layer. In this document, **M-TCP** is used to refer mobile transmission control protocol only and **M-UDP** for mobile user datagram protocol only.

MTCP message refers to transmission layer message or payload of IP datagrams compatible with MTCP.

Mobile-TCP compatible Node (**MTN**) is a node that implements necessary protocols defined by this document.

Scheme A refers implementation of M-TCP by extending traditional TCP to include PA information (see Section 2.1.1).

Scheme B refers implementation of M-TCP by adding a new TCP protocol to TCP/IP stack (see Section 2.1.2).

Non-Triangle Mode refers to an operation mode when the CH knows where the MH locates and sends data directly to its current TA, which involves no triangular route.

1.7. Protocol Overview

1.7.1. References Network Model

In the proposed architecture, we introduces some modifications to the existing TCP/IP stack to make Transmission Control Layer more independent from Internet Protocol Layer, thus an MTN MUST be configured with two IP addresses.

One is **Permanent Address** (**PA**), or called **Home Address**. The PA resides on the transmission layer, which can be passed down to network layer for particular purpose. The permanent address may be configured as home network compatible IP address or even a unique network identifier – it is up to transmission layer to interpret the PA and associate to sockets for communication session. Only IP address format is considered in this document, and the PA is carried along with the TCP payload as an option.

The other is **Dynamic Address** (**DA**), or **Temporary Address** (**TA**). A node's TA can be obtained from a DHCP server (which is usually on the attached network) or manually configured. TA functions quite like the traditional IP address used to route datagrams and to locate the Mobile Node, but is no longer a tag associated to a session, which is represented by a socket. However, it may have the same value of PA when PA is an IP address and the MH is on the home network.

Figure 1 illustrates the new network model of the proposed architecture.

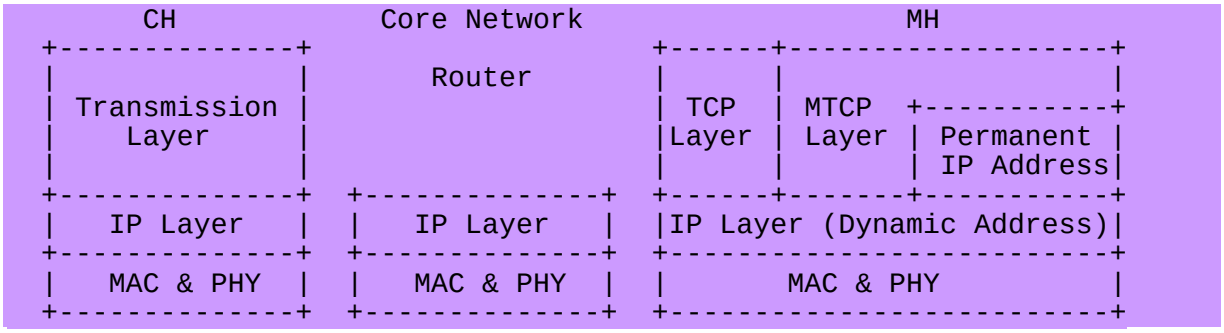


Figure 1. Reference Model

1.7.2. Protocol Overview

Based on above reference model we defined:

1) Two schemes for M-TCP
   a) Two new TCP options to upgrade TCP to M-TCP, and
   b) A new TCP protocol: M-TCP, and
2) A new UDP protocol: M-UDP.

In M-TCP and M-UDP, three kinds of permanent address can be used for transmission control layer

session identification, IPv4, IPv6 and NAI addresses that are independent of network layer address, which are dynamic even when the MH is on home network. By contrast, the network address is used only for location management and datagram routing function by router to deliver datagrams correctly.

In the proposed architecture, changes of network addresses result no impaction on its upper layer function.

Therefore, the transmission control layer is mobile in nature, which means that no IP-in-IP tunneling needed, routers remain unchanged except that they are mobile as mobile nodes. Moreover, IPv4 and IPv6 nodes are essentially compatible on the TCP layer. By introducing NAI in identification of TCP layer sessions, some high-level services can be supported by transmission layer such as per-bill tolling.

1.7.3. Sockets and Addressing

1.7.3.1. Definition of Sockets

In TCP/IP stack, a socket is a unique identifier for a TCP layer conversation. There are five distinct elements that make a TCP layer connection unique:

IP address of the server
IP address of the client
Port number of the server
Port number of the client
Protocol (UDP, TCP/IP, etc...)

In our proposed MTCP, a socket is also a combination of the above five elements, i.e.,

<socket> := <protocol, local address, local process, foreign address, foreign process>.

For half associations, a socket address is the triple: {protocol, local-address, local-process}, often referring to service interface on a server, i.e.,

<half-socket> := <protocol, local address, local process>.

The address in above mentioned socket identifier should be permanent address that is the only notation for identity of the host or the node.

1.7.3.2. Addressing

Both PA and TA can be configured manually or by auto-configuration mechanism such as DHCP. However, they reside on different layers with different function.

In our architecture, PA and TA may belong to different address family. And for auto-configuration progress, the configuration servers may or may not reside on the same host/node.

Particularly for NAI address, the process to map NAI to its associated permanent and/or temporary address may be complicated, but it should be kept intact in the TCP/UDP header for reasons not mentioned in this text, or it should use its associated permanent address unless the account information is configured not to so.

When a CH needs to communicate with a MH, it destined its datagrams to the MH's home address.

The home agent or native router of the MH intercepts the datagrams destined to MH, and redirects to MH's TA where MH is. And the proposal makes it possible for MH to tell CH its present TA by replacing the source address field with its current TA, which may be useful to eliminate triangle routes – but this is prohibited when the TA is changed at the same time, because it may confuse the receiver and announce an error and abort this connection.

When a MH needs to communicate with a CH, it can decide to use either PA or TA as source address. Actually, when TA is used as source address, the triangle routing issue will not occur.

Security issues involved in the above addressing mechanism are under further consideration. However, some authentication means are already available.

2. Mobile Transmission Control Protocol (MTCP)

2.1. Mobile TCP

2.1.1. Scheme A

In scheme A, M-TCP is implemented as an extended version of TCP by introducing new options to TCP header format. However, because UDP header is not extendable, so a new UDP header is designed and assigned a new value for the protocol field of the IP header.

Basically, the TCP header format remains unchanged (see Figure 2), and the protocol value in IP header remains as 06 (HEX).

But two new options must be introduced to carry source address and destination address in the TCP header. Moreover, in the new TCP header, the calculation of checksum MUST not be based upon the pseudo header, because the source address and destination address are already included in the M-TCP header.

Although, the TCP header seems overstaffed, at most 16 bytes are introduced for IPv4 – which is less than that by IP-in-IP encapsulation in Mobile IP [1].

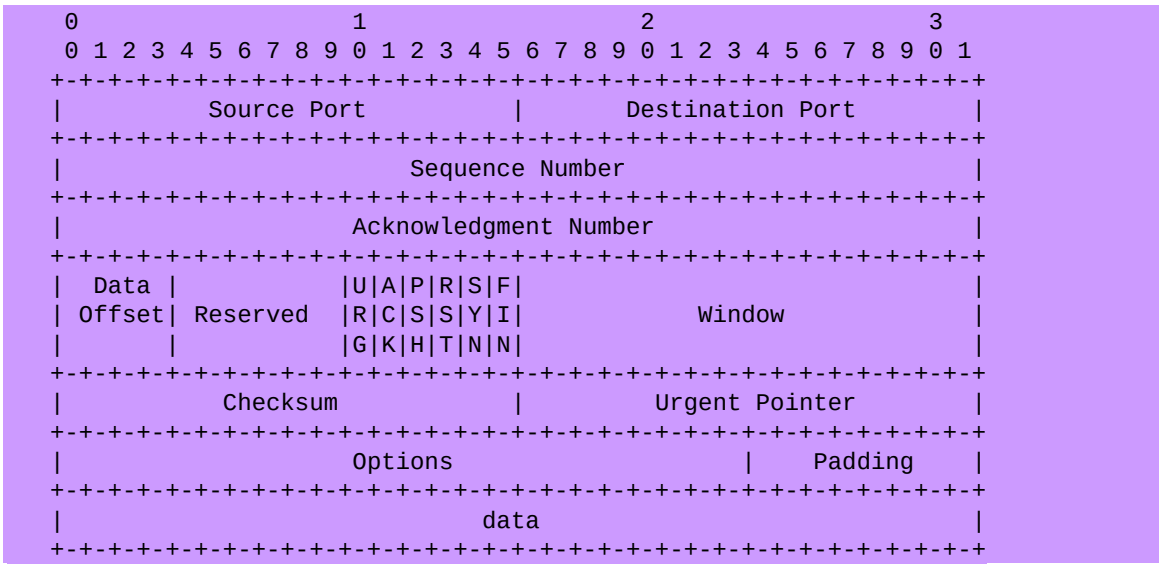


Figure 2. TCP Header Format (Note that one tick mark represents one bit position.)

2.1.1.1. Options for Mobile TCP

The new options MUST be compatible for three cases**:** 1) **PA is in IPv4 address format**; 2) **PA is in IPv6 address format**; 3) **PA is in NAI format**. Therefore, we have designed two types of options in type-length-value (TLV) format.

The first one is used for source permanent address; the second is used for destination permanent address. The format is show in Figure 3 and Figure 4. Either one goes first is of no importance.

The option length is variable, and its value depends on the type of address chosen.

The address type can be one of the following three values; others are reserved for further study:

```
<Address-Type>    := 1; for IPv4 address.
                  := 2; for IPv6 address.
                  := 3; for NAI address.
```

The address length can be determined according to the address type in octets, but for NAI addresses, it stands for the length of the NAI ASCII string, and may be variable:

```
<Address-Length> := 4; for IPv4 address.
                 := 16; for IPv6 address.
                 := Variable; for NAI address.
```

The length of the padding bits used to make the header size 32-bit aligned is calculated as:

```
<Padding-Length> := Ceil(Option-Length/4) * 4 - Option-Length
```

"Ceil (value)" rounds <value> to the nearest integers towards infinity.

By convention, the Most Significant Bit of the permanent address is sent first, i.e., in MSB first sequences.

The address length for IPv4 and IPv6 address can be zero to tell the receiver to infer it from network layer, but this mode is not support yet for NAI address.

When M-TCP is assumed, at least one of defined option must be included. However, for both options, the permanent address may be not present by setting address length to zeros – When this is true, the transmission control layer should use the corresponding network layer address, in which case NAI addresses will not be supported.

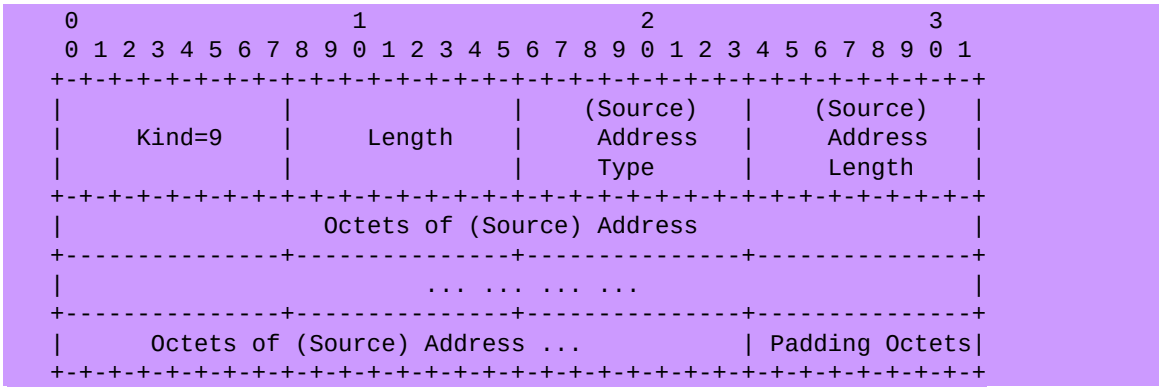


Figure 3. Option definition for source permanent address

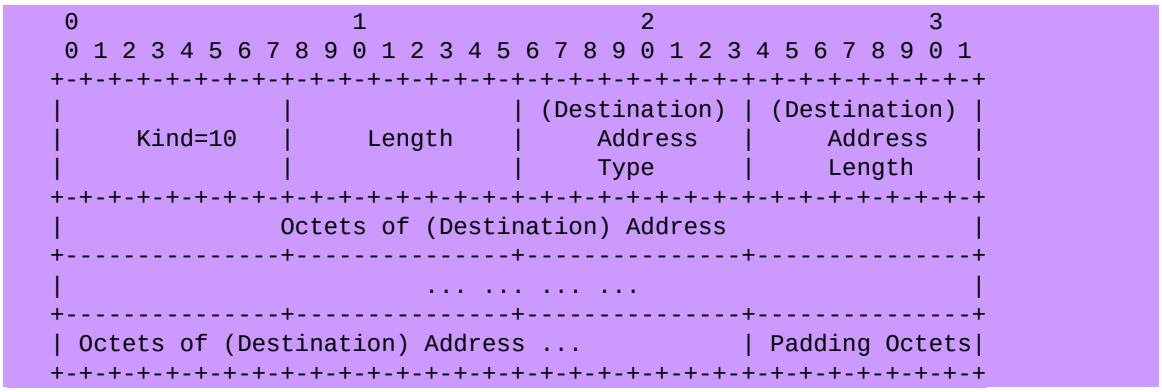


Figure 4. Option definition for destination permanent address

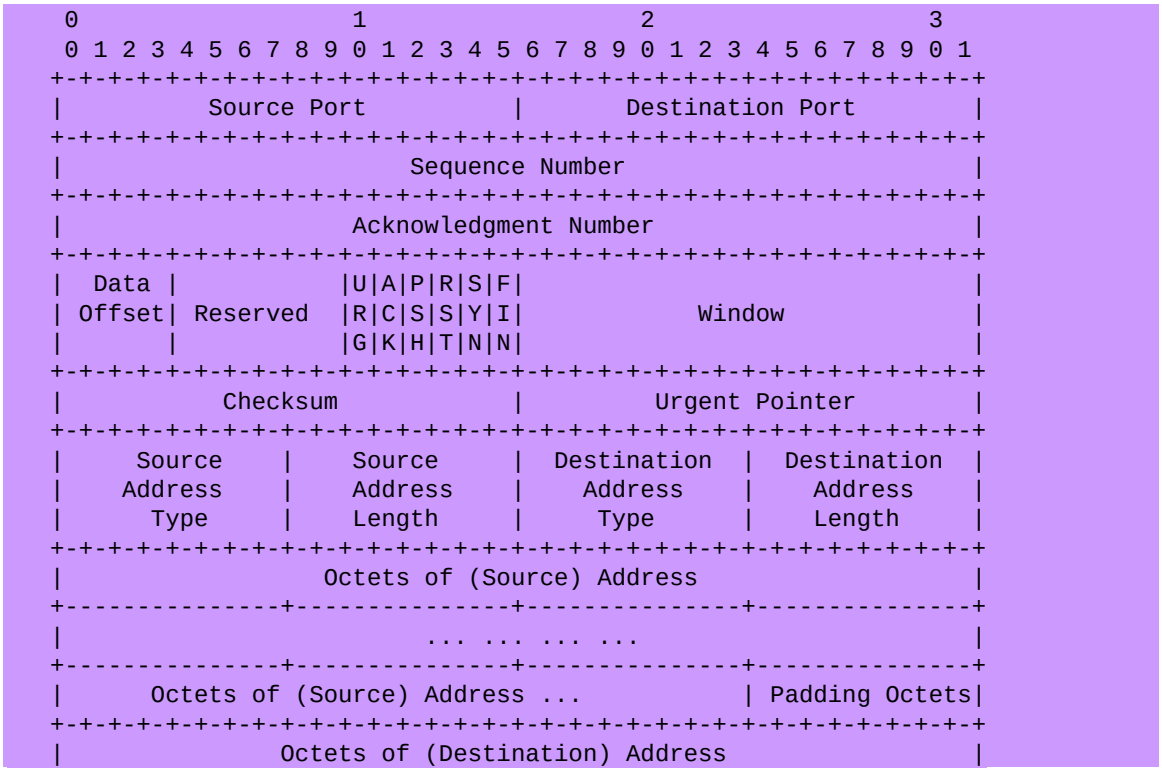
2.1.2. Scheme B

In this scheme, M-TCP is implemented as a new protocol (to be specified by IANA) that coexists with TCP, which is preferred by this document.

In this case, the source and destination permanent addresses are included as essential elements in the M-TCP header (see Figure 5) that go ahead of options.

Like that in TCP, when either of both addresses can be absent, but the address length must be present and set to zero. When this is true, the receiver should obtain the corresponding address from network layer. But for the checksum calculation, the pseudo TCP header is not used for the addresses are already included in M-TCP header.

Moreover, when NAI address (for either source or destination address) is used, proper length of padding octets must be added to make address body with 32-bit length, though the padding octets will not be included in the address length calculation.



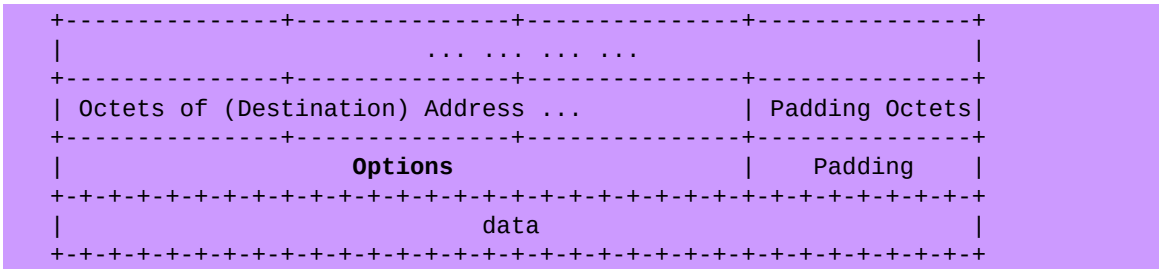


Figure 5. M-TCP Header Format (Note that one tick mark represents one bit position.)

Note that the most significant bit of the address is sent first, i.e., in MSB first sequences.

2.2. Mobile UDP

Since UDP header cannot be extended to hold source address and destination address, a new UDP format must be designed with a new protocol value (to be specified by IANA) in IP header.

Figure 6 illustrates the new UDP header format. The source and destination permanent address type and length are piggybacked to the original UDP header, and then follow the source address and destination address.

Like that in UDP, when either of both addresses can be absent, but the address length must be present and set to zero. When this is true, the receiver should obtain the corresponding address from network layer.

Moreover, when NAI address (for either source or destination address) is used, proper length of padding octets must be added to make address body with 32-bit length, though the padding octets will not be included in the address length calculation.

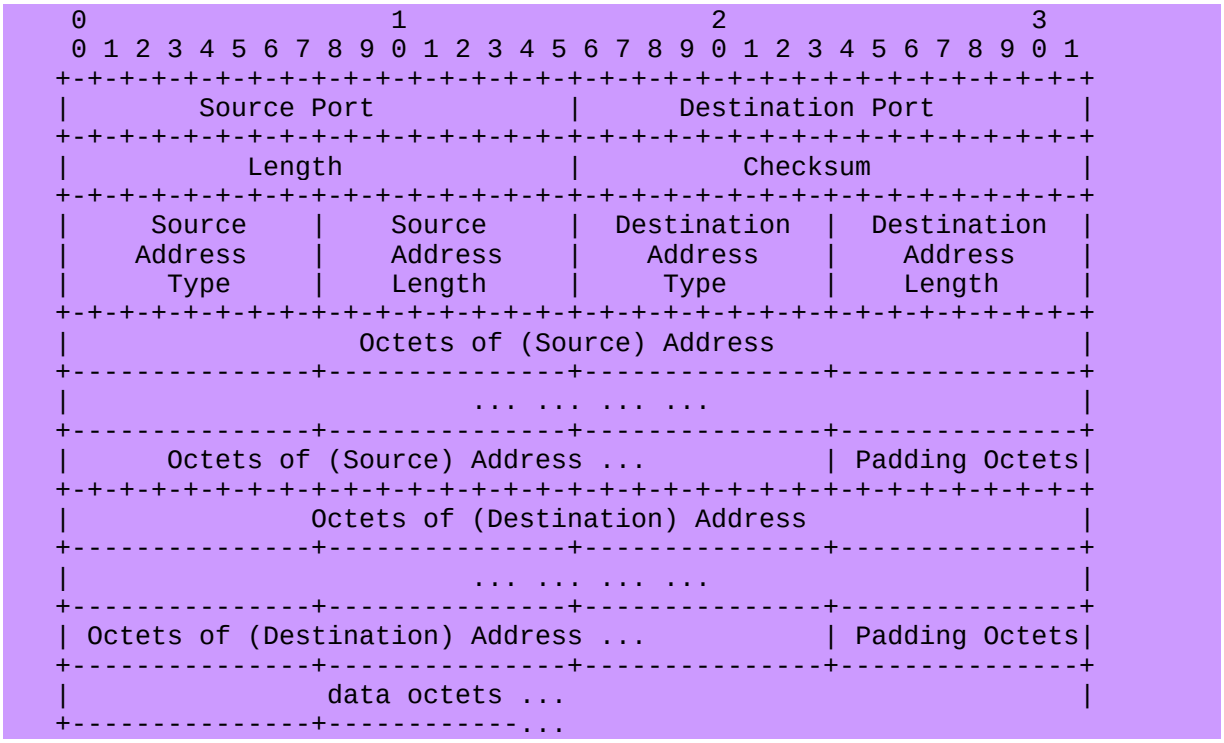


Figure 6. Header format of Mobile UDP

2.3. Redirect ICMP Message (RMSG)

When an MH is attached to a network – whether it is home network or foreign network – the MH may change its temporary address (TA). If so, it is MH that is responsible to inform the router that it has changed its (TA). We call it a Redirection Operation. The redirect message in RFC792 is not suitable for our case, for it is designed for gateway use only, a non-router node is not assumed to generate that message.

Here, we design a new ICMPv4 redirection – that for IPv6 is under further discussion – for this purpose. See Figure 7.

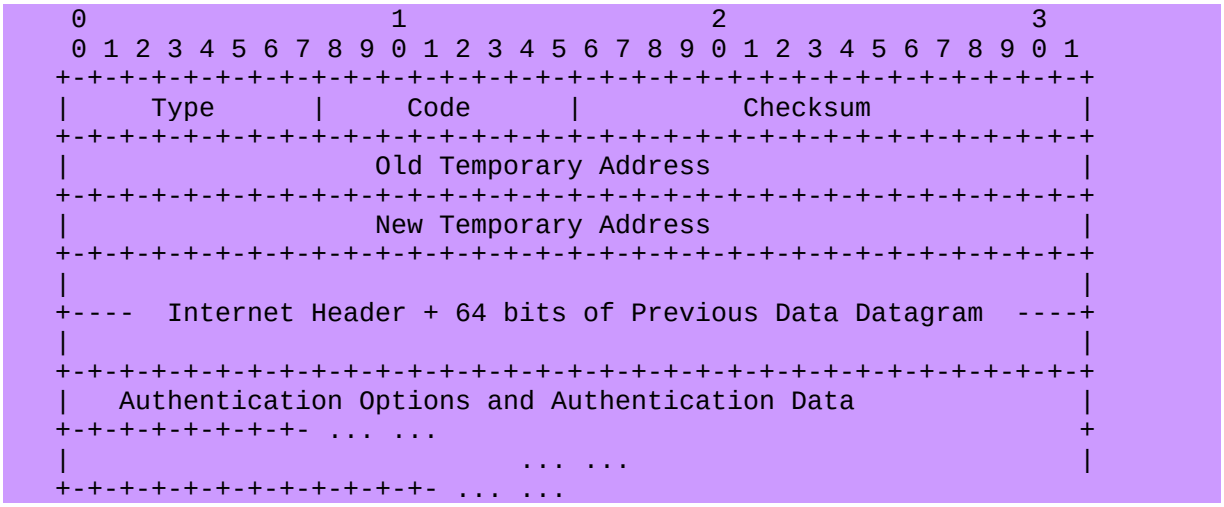


Figure 7. Redirection message format for Mobile TCP

Type. Type is to be specified by IANA.

Code. 1 for no authentication in IP layer; 2 for authentication attached; others reserved.

Checksum. The checksum is the 16-bit 1's complement of the one's complement sum of the ICMP message starting with the ICMP Type. For computing the checksum , the checksum field should be zero. This checksum may be replaced in the future.

Old TA and New TA. When MH moves to a new location associated with a new TA or it changes its TA by any method, the old TA and new TA should be included here.

Authentication Options. The authentication option may be used for ICMP integrity checking and authentication purpose against cheating or faking. The actual operation is out of scope of this document and under further study.

Internet Header + 64 bits of Data Datagram is the Internet header plus the first 64 bits of the original datagram's data, which is used by the host to match the message to the appropriate process. If a higher-level protocol uses port numbers, they are assumed to be in the first 64 data bits of the original datagram's data.

Description.

When the MH's TA is changed, it should use this message to alert the router on the previous network the old TA belongs informing that all following datagrams destined to the old TA should be diverted to the new TA. If the message is proved valid, the destined router unconditionally accepts the redirection command to following datagrams for MH. At the same time, the MH sends a similar redirection command to its home router, but the old

TA will be replaced by its home PA. This functions like a rebinding operation. Additionally, when in non-triangular mode, the MH sends the ICMP redirection command to the CH too.

For safety, multiple redirections should be sent against failure of packet losses. The routers or CH shall drop the subsequent redirection quietly, when a successful redirection is received. The interval between successive redirection is implementation dependent, but should be adaptable to the traffic status.

2.4. Requirements for Mobile Hosts

A MH may fall into two types of mobile nodes:

1) MN to be addressed by CHs according to its known address and its Home address is permanent in form of IPv4, IPv6 or NAI address. In this case the MH MAY work as a server known to some CHs. We call it is a PASSIVE host.
2) MH never to be addressed by others and always acts as a client to initiate conversions. Its home address may or may not be permanent; it may be configured by dynamic IP assignment schemes or manually. We call it an ACTIVE host.

At the same time, a MH may be in two statuses when it is changing its TA whether at home or abroad:

1) It maintains at least one communication session active with one or more CHs. We call it is talking.
2) No active communication session or connection involved. We call it is quiet.

The term "communication" here means an active connection or a running TCP/UDP process bound to a port number, whether or not data stream transferring through it.

For an active host, when it is quiet, it changes TA quietly, without informing the foreign router or native router; when it is talking, it should inform the previously attached router and the corresponding host to update its new TA.

For a passive host, when it is quiet, it should inform the foreign router and its home router about new TA; when it is talking, it may also inform the CH if non-triangular mode is set.

When MH is powered on and configured with permanent home address, it should obtain its TA by DHCP or manually, and report it to its home router regardless of whether it is at home or abroad by send redirect message to its home router.

For more reliable binding of TA with PA, an MH may send RMSG periodically or it can use Mobile IP registration messages if the router supports Mobile IP. However, interoperation of M-TCP with MIP needs further study.

2.5. Requirements for Correspondent Hosts

If CH is mobile TCP compatible, it should work as MH described above.

If not, that is CH cannot understand Mobile TCP headers or options, it should report error to the MH when it decides to reject the connection requests.

When an MH decides to make its location known to one of its CH it should send more than one

redirection command messages to the CH, and the CH should drop redundant redirections quietly.

And if it cannot handle the redirection messages from its corresponding MH it should drop it quietly.

2.6. Requirements for Routers

Routers on the native network should be able to handle redirection messages and maintain a redirection nodes table (RNT). The RNT may be a part of routing table or a routing cache.

When an NR received a valid RMSG from a MH wherever it is, it should update the corresponding entry.

When an NR receives a datagram destined to a node belonging to its domain, it simply searches the NR. If there is a matched entry, it forwards it to the TA of that entry.

If there is more than one native router on the same domain, it is the native routers' responsibility to share the NR information; therefore home agent discovery in MIP is not necessary in this architecture.

2.7. Route Optimization Consideration

In the proposed architecture, any route optimization scheme may be used, because the network layer remains hardly touched.

Moreover, the MH takes the responsibility to share its location information with its CHs. When it is necessary to use non-triangular mode for route optimization purpose, it may send RMSG to CH, or it may replace the source PA in TCP/UDP header to tell the CH to directly send datagrams to that TA.

3. Multicast Support

Multicast support in foreign domains is left for further study, but current multicast solicitation and association schemes can be used without or with little changes.

4. Security Consideration

The proposed architecture may have security problems as Mobile IP – whose solution may or may not be the same – and other security issues under further study. Any problem or solution found will make part of the following updates.

5. Conclusion

This document proposes a framework to implement mobile TCP by introducing two type of IP address – one for routing and location management, the other for host identification, thus transmission sessions will no longer dependent of network layer IP address, and location changes of a mobile host result only new network IP address, which has no impact on transmission communications and its continuity. The new architecture involves no IP-in-IP tunneling, and no changes on intermediate routers; it is almost an End-to-End solution to implement host mobility management, and applicable for both "macro-" and "micro-" mobility.

Then two new options are designed for M-TCP to hold IPv4, IPv6 and NAI addresses; and a new

protocol, M-UDP is designed to support Transmission Control Layer host mobility. Both the designed M-TCP and M-UDP are IPv4 and IPv6 compatible and extensible.

For future high-level host or personal mobility management, NAI may also be used to support M-TCP, which benefits much easier mobility management and per-bill services and so on.

6. Acknowledgements

This research is funded by the National High Technology Research and Development Program of China (863 Program), Grant No. 2003AA121540.
The authors would like to express great thanks for simulation and programming works done by LIU Lei and LIU Xingqian.

7. References

[1]. C. Perkins (Ed.), "IP Mobility Support", RFC2002, October 1996

[2]. F. Vakil, A. Dutta, J-C. Chen, M. Tauil, S. Baba, N. Nakajima, H. Schulzrinne, "Supporting Mobility for TCP with SIP", draft-itsumo-sipping-mobility-tcp-00.txt, June 2001

[3]. F. Vakil, A. Dutta, J-C. Chen, S. Baba, and Y. Shobatake, "Host Mobility Management Protocol: Extending SIP to 3G-IP Networks", Internet Draft, <draft-itsumo-hmmp-00.txt>, work in progress

[4]. Zygmunt J. Haas. "Mobile-TCP: an asymmetric transport protocol design for mobile systems". Proc. IEEE ICC'97, Montreal, 2:1054-1058, 8-12 June 1997

[5]. Zoltán R. Turányi, Csanád Szabó, Eszter Kail, "Global Internet Roaming with ROAMIP", ACM SIGMOBILE Mobile Computing and Communications Review, 4(3): 58-68, July 2000

[6]. A. Valk′ o, "Cellular IP: A New Approach to Internet Host Mobility", ACM SIGCOMM Computer Communication Review, Vol. 29, No. 1, pp. 50-65., January 1999.

[7]. A.C. Snoeren, H. Balakrishnan, "An End-to-End Approach to Host Mobility", 6th ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom ’00), Boston, MA, August 2000.

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

[9]. B. Aboba, M. Beadles, "The Network Access Identifier", Internet RFC 2486, January 1999.

[10]. P. Calhoun, C. Perkins, "Mobile IP Network Access Identifier Extension for IPv4", Internet RFC 2290, March 2000.

[11]. Deering, S., Editor, "ICMP Router Discovery Messages", RFC 1256, September 1991

[12]. Vinton Cerf, Yogen Dalal, Carl Sunshine, "Specification Of Internet Transmission Control Program", RFC 675, December, 1974

[13]. J. Postel, "Transmission Control Protocol", RFC 793, September 1981

[14]. S. Glass, T. Hiller, S. Jacobs, C. Perkins, "Mobile IP Authentication, Authorization, and Accounting Requirements", Internet Draft, draft-ietf-mobileip-aaa-reqs-04, Work in Progress, June 2000.

[15]. Perkins, C., "IP Encapsulation within IP", RFC 2003, October 1996.

[16]. Johnson, D., and C. Perkins, "Route Optimization in Mobile IP", Work in Progress.

[17]. Atkinson, R., "IP Authentication Header", RFC 1826, August 1995.

[18]. Atkinson, R., "IP Encapsulating Security Payload", RFC 1827, August 1995.

[19]. J. Postel. "Internet Control Message Protocol", RFC0792, Sep-01-1981

[20]. A. Conta, S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 2463, December 1998

8. Authors' Addresses

Questions about this memo can be directed to:

Yujun Kuang
Special Research Centre for Optical Internet & Wireless Information Networks (COIWIN), Chongqing University of Posts & Telecommunications Chongqing, 400065 P.R. China
Phone: +86 23 6246 0223
Fax: +86 23 6246 0220
E-Mail: Kuangyj@cqupt.edu.cn

Keping Long
Special Research Centre for Optical Internet & Wireless Information Networks (COIWIN), Chongqing University of Posts & Telecommunications Chongqing, 400065 P.R. China
Phone: +86 23 6246 0218
Fax: +86 23 6246 0220
E-Mail: Longkp@cqupt.edu.cn

Qianbin Chen
Special Research Centre for Optical Internet & Wireless Information Networks (COIWIN), Chongqing University of Posts & Telecommunications Chongqing, 400065 P.R. China
Phone: +86 23 6246 0219
Fax: +86 23 6246 0220
E-Mail: Chenqb@cqupt.edu.cn

Yun Li
Special Research Centre for Optical Internet & Wireless Information Networks (COIWIN), Chongqing University of Posts & Telecommunications Chongqing, 400065 P.R. China
Phone: +86 23 6246 0222
Fax: +86 23 6246 0220
E-Mail: Liyun@cqupt.edu.cn

9. Full Copyright Statement