
Ravi Pendse | Electrical Engineering and Computer Science

Mobility and Layer 2 Tunnels

Ravi Bhagavathula
Electrical and Computer Engineering Department at the Wichita State University

Patricia Best
Electrical and Computer Engineering Department at the Wichita State University

Ravi Pendse
Electrical and Computer Engineering Department and the Director of the Center of Research and Teaching

---

Recommended citation
Bhagavathula, Ravi., Best, Patricia and Ravi Pendse. 2006. Mobility and Layer 2 Tunnels. *Wireless Personal Communications*, v. 39, no. 3, 361-380, DOI: 10.1007/s11277-006-9068-z

Mobility and Layer 2 Tunnels

RAVI BHAGAVATHULA[1], PATRICIA BEST[1] and RAVI PENDSE[2]

[1]*Electrical and Computer Engineering Department at the Wichita State University, KS 67260, USA*
[2]*Electrical and Computer Engineering Department and the Director of the Center of Research and Teaching Excellence at Wichita State University*

Abstract. An increase in the size and requirements of a mobile workforce is driving the development of better mobility oriented services in terms of both content and connectivity. Even though traditional Mobile IP has been the primary means of providing mobility to nodes roaming between foreign networks, its extension to support the mobility of entire networks leads to an increase in the encapsulation overheads. In addition, the increasing perception within the mobile workforce as to the inadequacies of Layer 3 connectivity provided by traditional Mobile IP opens up the possibility of considering the mobility problem from a Layer 2 perspective.

This paper presents a Layer 2 extension to the traditional implementation of Mobile IP by replacing the IP-IP tunnels of Mobile IP with L2TPv3 based Layer 2 tunnels. Simulations results obtained from performance evaluation indicate comparable performance of the proposed Layer 2 mobility solution with respect to traditional Mobile IP in terms of real-time and best-effort traffic streams. The proposed Layer 2 mobility solution increases the possible services available to mobile nodes with minimal performance degradation.

Keywords: mobility, mobile IP, encapsulation, tunneling

1. Introduction

With a growing number of portable computing devices like laptops and Personal Digital Assistants (PDA), the need for seamless connectivity to the global Internet is driving the acceptance of different mobility solutions. Identifying this need for remote connectivity by an increasingly mobile workforce, a number of remote access mechanisms have been deployed under the framework of an Access VPN.

The fundamental problem with IP, the most widely deployed protocol in the Internet, is that it associates every address with a specific point of attachment to the Internet. To provide connectivity to mobile nodes, IP needs to be modified such that data can be transferred transparently to the mobile node without regard for the node's current point of attachment to the Internet.

Mobile IP is an extension to the IP protocol that attempts to de-lineate the physical location of a mobile node with its assigned IP address [1]. A MH is defined to be a host that can migrate from one network to another (or between different subnets of the same network) without changing its IP address and yet maintain data connectivity with other nodes, referred to as Correspondent Nodes (CN), on the Internet assuming link-layer connectivity to a point of attachment is available. An HA is a host in the Home Network (HN) of the MH and is responsible for tunneling datagrams to the MH when the MH is away from home. The HA is also responsible for maintaining current location information of the MH. A Foreign Network (FN) is any network other than the HN. Further, a FN that the MH is currently visiting is

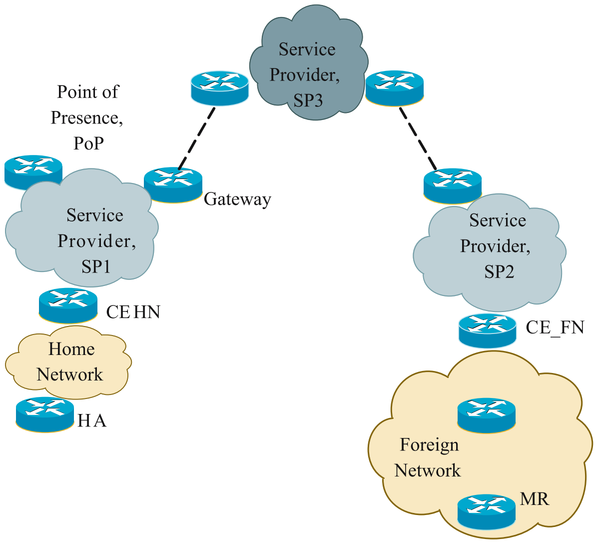


Figure 1. A typical mobility deployment scenario. The Mobile Router (MR) is expected to roam away from its Home Network into a Foreign Network. Service Provider SP3 could represent the global Internet.

referred to as the Visiting Network (VN). A FA is a host in the VN that provides routing functionality to the MH. Since a tunnel is formed between the FA and the HA, a FA is also responsible for forwarding the decapsulated datagrams from the HA to the MH. A typical deployment scenario for Mobile IP is shown in Figure 1. It needs to be borne in mind that SP3 in Figure 1 could represent the global Internet.

When the MH moves from its HN into a FN, it obtains a temporary Care-Of-Address (CoA). The CoA identifies the MH's current point of attachment to the Internet and is valid as long as the MH stays within the specific FN. The CoA could be obtained by either of the following mechanisms:

- Via FA: In this mode of operation (also referred to as FA Decapsulation mode), the MH receives a CoA from the FA through agent advertisements. The CoA is typically the IP address of one of the interfaces of the FA.
- Without the FA: In this mode of operation (also referred to as Mobile Node Decapsulation), the MH obtains an IP address (which is different from its home IP address) via Dynamic Host Configuration Protocol (DHCP) or any other suitable mechanism. This newly acquired IP address is also called a Co-Located CoA

The association between the MH's home address and its CoA is referred to as a mobility binding. Once a MH acquires a CoA, the HA is duly notified (through a sequence of authentication and registration processes) and a tunnel is built from the HA towards the MH's CoA. All packets destined for the MH are forwarded through the tunnel towards the MH. The encapsulation methods supported by Mobile IP are:

- IP-IP encapsulation
- Minimal encapsulation

In IP-IP encapsulation, the datagram is already fragmented prior to encapsulation. The original IP datagram is encapsulated into another IP datagram by attaching an outer IP-header to it. The source and destination addresses in the outer IP header identify the end points of the tunnel (HA and FA). Similarly, the source and destination address in the inner IP header identifies the sender and recipient of the datagram. After decapsulation, the original IP datagram is delivered to the mobile node. An optional header may be included for security reasons. This method of encapsulation is widely used for IP traffic [2].

Minimal Encapsulation (ME) can only be used when the original datagram is not fragmented. The original IP header of the datagram is modified and a minimal encapsulating header is inserted into the datagram after the new IP header. The minimal encapsulating header contains the IP address of the source and the destination. Protocol number 55 for minimal encapsulation protocol replaces the protocol field in the new IP header [3]. The source and the destination fields in the new IP header are replaced by the encapsulating agent and the CoA of the mobile node. When decapsulating a datagram, the forwarding header is removed from the datagram. The advantage of using this method is a reduction in the header size when compared to IP-IP encapsulation.

In a mobile environment, two distinct instances of mobility can be formulated. In the first instance, mobility on a host specific basis could be considered that would correspond to the movement of a single MH from one network to another. The second scenario would correspond to an entire network migrating from one point of attachment to another [4]. An example for the second scenario would be an airplane providing mobility to all the passengers. A router that provides connectivity to such a mobile network is referred to as a Mobile Router (MR). A MR, therefore, could be envisioned to be a router containing a Roaming Interface (RI) and a Non-Roaming Interface (NRI). Since a MR provides mobility to an entire network, it would need to run a Mobile IP compatible TCP/IP stack.

A MH does not need to participate in any routing processes since these aspects are handled by the HA and the FA. When the MR is in its HN, it behaves like a normal router running an ordinary routing protocol. As the MR roams into an FN, it is required to provide connectivity to its RI and to the networks attached to its NRI. As packets would still need to be forwarded between the RI and the NRI, the MR would need to continue running a routing protocol. When the MR is in an FN, the RI is made passive (for all supported routing protocols) to avoid flooding the FN with localized routing updates. Hence, routing of packets to the networks connected to the NRI of the MR needs to be handled by an external agent. It is unreasonable to expect the FA to handle these routing issues since the FA would not have the required information related to the size and nature of the networks connected to the NRI of the MR. Since the HA keeps track of the mobility of the MR, it handles the task of providing connectivity to the networks attached to the NRI of the MR.

Connectivity to the networks attached to the NRI of the MR is provided through a tunnel that extends from the HA to the RI of the MR (in addition to the tunnel created between the HA and the FA of the MR [4]) leading to an increase in the encapsulation overheads. As shown in Figure 2, the size of a packet captured between the HA and the FA with the usage of traditional Mobile IP to provide mobility to mobile networks is equal to $(N + 60)$ bytes where N is the size of the data.

Prior to formulating an analytical model of Mobile IP, the following assumptions are made:

- The cost of transferring data along a path is directly proportional to the distance being traversed by the particular datagram. In other words,

$$\text{Cost} = \delta_T.\text{distance} \tag{1}$$

Tunnel 1 (*FA* to *HA*) ***IP* header** **(20 bytes)**	**Tunnel 0** (*MR* to *HA*) ***IP* header** **(20 bytes)**	**Original** ***IP* Header** **20 bytes**	**Original** ***IP* Payload** ***N* bytes**

Figure 2. Packet format of a typical packet with the usage of traditional Mobile IP for providing mobility to entire networks.

where, δ_T is defined to be the cost scaling factor. Distance between the mobility agents is defined as the number of nodes along the path connecting them

- Since wireless links are more susceptible to transmission errors, it is assumed that the wireless link connecting the MR to the FA is m times more expensive than its wired counterpart.
- The cost of encapsulating a datagram is equal to the cost of decapsulating a tunneled datagram.

The registration cost associated with a mobile node in a foreign network employing IETF Mobile IP is given by,

$$\text{L3MIP}_{\text{MNRC}} = 2.C_{\text{hf}} + 3.C_A + 2.C_{\text{fm}} \tag{2}$$

where, C_{hf}, C_A, and C_{fm} represent the cost of the path connecting the HA with the FA, the processing costs on the mobility agents, and the cost of the path connecting the mobile node with the FA respectively. The first and the last terms in (2) represent the manner in which the registration request (and the registration reply) is transported between the MR and the HA. The second term in (2) accounts for the processing of the registration messages on the HA, the FA and the MR.

Similarly, the cost associated with the transport of datagrams between the mobile node and the HA is given by

$$\text{L3MIP}_{\text{MNTC}} = 2.C_{\text{IP}-\text{IP}} + C_{\text{hf}} + C_{\text{fm}} \tag{3}$$

where, $C_{\text{IP}-\text{IP}}$ represents the encapsulation-decapsulation costs associated with an IP-IP tunnel. The first term in (3) is multiplied by a factor of 2 to account for the encapsulation and decapsulation operations that are associated with the tunnel between the HA and the FA.

The deployment of a MR requires the usage of 2 tunnels (one between the HA and the FA, and another between the HA and the MR). The presence of two tunnels instead of the one tunnel in the case of a mobile node increases the cost associated with the transportation of datagrams via the MR.

As shown in Equation (4), the transportation cost associated with a MR is given by,

$$\text{L3MIP}_{\text{MRTC}} = 4.C_{\text{IP}-\text{IP}} + C_{\text{hf}} + C_{\text{fm}} \tag{4}$$

since the datagram needs to be encapsulated (and decapsulated) twice.

Once a handoff has been initiated, the time taken to complete the registration processes and resume the transfer of datagrams is considered next. The time taken to commission the connection between the mobile node and the HA after a handoff has been initiated is given by,

$$T_{\text{comm}} = T_{\text{trans}} + T_{\text{proc}} + T_{\text{tun}} \tag{5}$$

where, T_{trans} accounts for the time taken for the transmission of the registration requests within the framework of Mobile IP, T_{proc} is the time taken by the various mobility agents to process the registration requests, and T_{tun} corresponds to the time taken for the appropriate tunnels to be constructed between the mobility entities.

Since the transmission time is directly proportional to the distance that the registration requests (and the registration replies) need to travel, T_{trans} is given by,

$$T_{\text{trans}} = 2.\tau.[m.d_{\text{fm}} + d_{\text{hf}}] \tag{6}$$

where, τ is defined to be the time scaling factor. The first term in Equation (6) accounts for the wireless link connecting the FA with the mobile node while the second term accounts for the transmission time between the HA and the FA respectively.

Assuming the case of a mobile node, $T_{\text{proc}} = 2.\ T_{\text{MA}}$ (T_{MA} is the processing time at each mobility agent). For the sake of clarity, the processing time is assumed to be the same on any mobility agent. Further, $T_{\text{tun}} = T_{\text{ip-ip}}$ where $T_{\text{ip-ip}}$ denotes the time taken to construct an IP-IP tunnel. Therefore, T_{comm} will be given by,

$$T_{\text{comm-MN}} = 2.\tau[m.d_{\text{fm}} + d_{\text{hf}}] + 2.T_{\text{MA}} + T_{\text{ip-ip}} \tag{7}$$

In case of a MR, T_{comm} would need to account for the additional tunnel begin constructed between the HA and the MR in addition to the tunnel between the HA and the FA. Therefore,

$$T_{\text{comm-MN}} = 2.\tau.[m.d_{\text{fm}} + d_{\text{hf}}] + 3.T_{\text{MA}} + 2.T_{\text{ip-ip}} \tag{8}$$

It can be observed from the above equations that the deployment of a MR not only increases the transportation costs but also increases the corresponding commissioning times with respect to those for a mobile node. In addition, the availability of Layer 3 connectivity to network resources within the HN is increasingly being perceived as being insufficient to cater to the connectivity needs of a mobile workforce. For example, there is an increasing demand for remote file system access based on (a) Microsoft's Common Internet File System (CIFS), an extension of Server Message Block (SMB), (b) Network File System (NFS) or (c) Andrew File System (AFS). In addition, many resources within a corporate intranet are made available to users based on their Media Access Control (MAC) addresses and the presence of Layer 3 only connectivity to mobile users does not scale well with these requirements.

To overcome the issues listed above, an alternative connectivity mechanism based on Layer 2 tunnels instead of the IP-IP tunnels employed by the traditional Mobile IP implementations is proposed in this research. The organization of the paper is as follows. In Section 2, a discussion of Layer 2 tunneling mechanisms is carried out while in Section 3, the integration of a Layer 2 tunnel into the framework of Mobile IP is presented. Section 4 presents the details of the test-bed employed for evaluating the proposed L2MIP and Section 5 presents the results obtained from simulations carried out in the SRL for evaluating the performance of L2MIP in the presence of real-time and best-effort traffic streams.

2. Layer 2 Tunneling

In sharp contrast to Layer 3 tunneling mechanisms, the endpoints of a Layer 2 tunnel natively transport Layer 2 frames. Therefore, the Layer 2 connection is transparent to Layer 3 services (including routing and QoS deployment) leading to considerable improvement in the scalability of the tunnel endpoints.

Depending upon the available transport, a Layer 2 connection could be deployed using either Any Transport over MPLS (AToM) [5, 6] or Layer 2 Tunneling Protocol version 3 (L2TPv3) [7]. The Pseudo-Wire Emulation Edge-to-Edge (PWEEE or PWE3) working group aims at providing Ethernet, Frame Relay, ATM, Point-to-Point Protocol (PPP), Time Division Multiplex (TDM) and High level Data Link Control Protocol (HDLC) services over a GRE, MPLS or Layer 2 Tunneling Protocol (L2TP) [8] transport mechanisms.

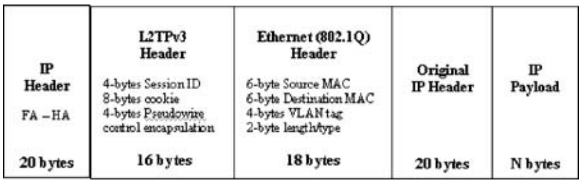
The various mechanisms involved in setting up Layer 2 tunnels based on a MPLS transport mechanism are described in two IETF drafts: draft-Martini [5] and draft-Kompella [6]. The primary difference between the two drafts emanates from the protocol employed for setting up the parameters for the establishment of a Virtual Circuit (VC). Draft-Martini specifies the usage of Label Distribution Protocol (LDP) for setting up a VC while draft-Kompella requires the usage of route-target attributes within Border Gateway Protocol (BGP) for the construction of a Layer 2 tunnel.

Unlike the MPLS based layer 2 tunneling mechanism, L2TPv3 employs IP as the primary transport mechanism [7]. As in the case of draft-Martini based Layer 2 tunneling mechanism, L2TPv3 based tunnels employ the concept of a VC which is associated with a unique VC Identifier (VC-ID). Instead of the usage of LDP for the negotiation of parameters between tunnel endpoints (as done in the case of draft-Martini based Layer 2 tunnels), L2TPv3 based Layer 2 tunnels employ the control plane associated with the Layer 2 Tunneling Protocol (L2TP).

Each L2TPv3 packet contains an IP delivery header, an L2TPv3 header that includes Session Identifiers (S-ID) (of size 4 bytes), a session Cookie whose length needs to be negotiated prior to setting up the session, and the PseudoWire Control Encapsulation (PWCE) (of size 4 bytes). The session Cookie can consume 0, 4 or 8 bytes depending upon the cookie length supported by a particular decapsulating end-point. The format of an L2TPv3 packet is shown in Figure 3.

Consider the network shown in Figure 4. R1 and R5 are two routers that are connected onto the same VLAN. Since the connectivity between R5 and R1 is at Layer 2, R4 and R2 need not maintain any routing table entries for these nodes. Figure 5 shows the configurations of R2, R4 and R1 while Figure 6 shows the details of the Layer 2 tunnel constructed between R4 and R2. Figure 7 shows the IP routing table and the ARP table on R5. Figure 7 also shows the result of a ping operation from R5 to R1. As can be seen from Figure 5, the configuration of R2 (Layer 2 PE router) does not include any Layer 3 information on the link connected to R3.

The primary advantage of constructing an L2TPv3 based Layer 2 Pseudo Wire Service (PWS) is the high speed interconnection of physically disjoint network components. Setting up a Virtual Leased Line (VLL) based on L2TPv3 for emulating end-to-end Ethernet, Frame



IP Header	**L2TPv3 Header**	**Ethernet (802.1Q) Header**	**Original IP Header**	**IP Payload**
FA – HA	4-bytes Session ID 8-bytes cookie 4-bytes Pseudowire control encapsulation	6-byte Source MAC 6-byte Destination MAC 4-bytes VLAN tag 2-byte length/type		
20 bytes	**16 bytes**	**18 bytes**	**20 bytes**	**N bytes**

Figure 3. Packet format of a typical L2TPv3 packet.

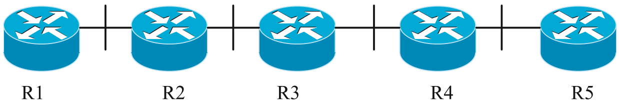


Figure 4. Network employed for illustrating the deployment of a Layer 2 tunnel.

```
R2#sh run
hostname R2
l2tp-class class1
        authentication
        password 0 secret
pseudowire-class vlan-xconnect
        encapsulation l2tpv3
        protocol l2tpv3 class1
        ip local interface Loopback0
interface Loopback0
        ip address 1.1.1.1 255.255.255.255
interface GigabitEthernet2/0.1
        encapsulation dot1Q 1000
       xconnect 3.3.3.3 123 pw-class vlan-xconnect

R4#sh run
hostname R4
l2tp-class class1
        authentication
        password 0 secret
pseudowire-class vlan-xconnect
        encapsulation l2tpv3
        protocol l2tpv3 class1
        ip local interface Loopback0
interface Loopback0
        ip address 3.3.3.3 255.255.255.255
interface GigabitEthernet1/0.2
        encapsulation dot1Q 1000
        xconnect 1.1.1.1 123 pw-class vlan-xconnect

R1#sh run
hostname R1
interface GigabitEthernet1/0.1
        encapsulation dot1Q 1000
        ip address 100.10.10.1 255.255.255.0
```

Figure 5. Configurations employed for the Layer 2 tunnel.

```
R4#sh l2tun session all
 Session Information Total tunnels 1 sessions 1

Session id 47446 is up, tunnel id 9152
Call serial number is 1957200000
Remote tunnel name is vxra
        Internet address is 1.1.1.1
        Session is L2TP signalled
        Session vcid is 123
        Session Layer 2 circuit, type is Ethernet Vlan, name is
GigabitEthernet1/0.2:1000
        Circuit state is UP
Remote session id is 23139, remote tunnel id 33127
       DF bit off, ToS reflect disabled, ToS value 0
```

Figure 6. Details of the Layer 2 tunnel.

```
R5#sh ip route
    100.0.0.0/24 is subnetted, 1 subnets
C       100.10.10.0 is directly connected, GigabitEthernet4/2.2

R5#sh arp
Internet  100.10.10.1  0005.0091.041c  GigabitEthernet4/2.2
Internet  100.10.10.2   00b0.8e40.d602  GigabitEthernet4/2.2

R5#ping 100.10.10.1
Sending 5, 100-byte ICMP Echos to 100.10.10.1: !!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/1/4 ms
```

Figure 7. IP routing table, ARP table on R5.

Relay or ATM networks could be used effectively within the framework of traditional Mobile IP in an effort to provide Layer 3 mobility as compared to the Layer 3 mobility offered by traditional Mobile IP. This is considered in the next section.

3. Mobile IP and Layer 2 Tunnel

The network considered in the previous section (Figure 4) illustrates the advantages of a Layer 2 tunnel over a traditional Layer 3 tunnel. In this section, a Layer 2 extension to traditional Mobile IP is proposed in an effort to provide a scalable connectivity option for mobile nodes. In order to differentiate the proposed Layer 2 extended Mobile IP from the traditional Mobile IP implementations, the proposed mobility solution is referred to as Layer 2 Mobile IP (L2MIP) in the rest of this paper.

The network shown in Figure 8 illustrates a typical scenario for the deployment of L2MIP. The registration of the MR with the HA is assumed to follow the same procedure as that for traditional Mobile IP. However, instead of constructing an IP-IP tunnel between the FA and the HA, an L2TPv3 tunnel is employed to construct a Virtual Circuit (VC) between the HA and the FA.

Once a VC is constructed between the FA and the HA, the HA and the MR communicate with each other through an XConnect Ethernet interface using an L2TPv3 session over the configured VC. Ethernet frames arriving on the FA's interface from the MR are transported transparently to the interface connecting the HA to VG1. This is in sharp contrast to the usage of an IP-IP tunnel wherein the Ethernet frames are stripped of their Layer 2 headers and the IP payload is encapsulated into the IP-IP tunnel.

For the network shown in Figure 8, Internet connectivity to the nodes within the MN using Mobile IP is provided via two tunnels: one tunnel between the FA and the MR, and another tunnel between the MR and the HA. The need for a second tunnel emanates from the requirement of traditional Mobile IP to provide Layer 3 connectivity between the HN and the non-RI of the MR. By configuring L2MIP between the HA and the FA, Layer 2 services could be provided to the MR thereby eliminating the need for a second tunnel between the MR and the HA.

Considering the network shown in Figure 8, a Layer 2 VPN could be constructed between the FA and the HA to provide Layer 2 connectivity between the wireless link connecting the FA with the MR and the network connecting the HA with VG1. Due to a Layer 2 connection between the RI of the MR and the HN, routing IP packets from the non-RI of the MR towards

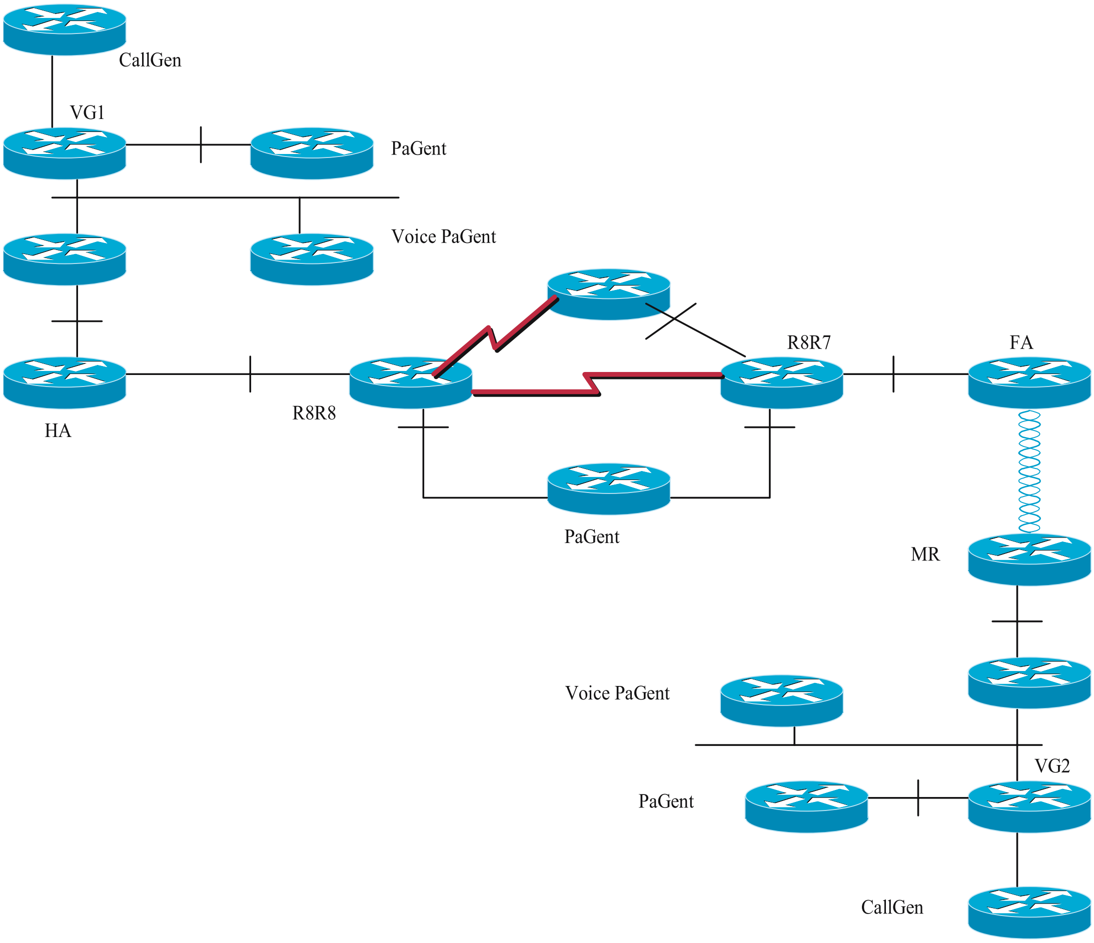


Figure 8. Network configured in the SRL to evaluate the performance of IP-IP tunnel based Mobile IP and L2TPv3 based Mobile IP.

the global Internet is carried out transparently over the network connecting the FA to the HA. In other words, since the MR is seemingly connected to the same Layer 2 network irrespective of its geographical location, there does not exist any need for special provisioning to account for Layer 3 connectivity due to mobility.

The usage of a Layer 2 tunnel instead of two Layer 3 tunnels could lead to savings in the transportation costs and in the connection commissioning times. The registration costs associated with L2MIP is given by,

$$\mathrm{L2MIP}_{\mathrm{RC}} = 2.C_{\mathrm{hf}} + 3.C_{\mathrm{A}} + 2.C_{\mathrm{fm}} \tag{9}$$

while the transportation costs are given by,

$$\mathrm{L2MIP}_{\mathrm{TC}} = 2.C_{\mathrm{L2Tun}} + C_{\mathrm{hf}} + C_{\mathrm{fm}} \tag{10}$$

where C_{L2Tun} represents the encapsulation and decapsulation costs associated with a Layer 2 tunnel. Since the usage of a Layer 2 tunnel does not affect the manner in which the basic Mobile

IP processes work, the registration costs and transportation costs associated with IETF Mobile IP enabled mobile node (Equations (2) and (4)) would be comparable (if not more) than that in the case of L2MIP (Equations 9 and 10) provided the encapsulation and/or decapsulation costs associated with an IP-IP tunnel are similar to those of a Layer 2 tunnel. It needs to be borne in mind that unlike the implementations of IP-IP (and GRE) tunnels, L2TPv3 and EoMPLS were designed to be more hardware "friendly". While the encapsulation and decapsulation procedures for both Layer 3 and Layer 2 tunnels could be sped up with appropriate hardware assistance, the authors do not believe that a Layer 2 tunnel would entail more overhead than a Layer 3 tunnel. An important characteristic of L2MIP is the fact that mobility of a network is handled in exactly the same manner as the mobility of a single node. The advantages accrued in the deployment of a L2MIP based MR emanate from this characteristic since the Layer 2 tunnels are built on a per-HN basis rather than on a per-MR basis. In other words, multiple nodes (or networks) from the same HN connected to a FA will utilize a single Layer 2 tunnel as opposed to multiple Layer 3 tunnels employed by IETF Mobile IP. This feature would improve the scalability of the mobility agents to a great extent.

The commissioning time with L2MIP would be given by,

$$T_{\text{comm}-\text{L2MIP}} = 2.\tau[m.d_{\text{fm}} + d_{\text{hf}}] + 2.T_{\text{MA}} + T_{\text{L2TPv3}} \tag{11}$$

A comparison of the commissioning times associated with traditional Mobile IP and L2MIP (as shown in Equations (8) and (11)) shows that,

$$T_{\text{comm}-\text{MN}} - T_{\text{comm}-\text{L2MIP}} = T_{\text{MA}} + 2.T_{\text{ip}-\text{ip}} + T_{\text{L2TPv3}} \tag{12}$$

A discussion on the comparative commissioning times of both L2TPv3 based Layer 2 tunnels and IP-IP based Layer 3 tunnels is carried out in Section 5.

As a brief digression, the interaction of L2MIP with the many micro-mobility protocols is considered. Since L2MIP does not change the basic processes involved in the operation of Mobile IP (other than the form of the tunnel being employed), any micro-mobility protocol that is compliant with the IETF Mobile IP implementation should interoperate with L2MIP. However, Layer 2 tunnels could be employed for the practical deployment of a particular micro-mobility protocol described in [12]. The authors of [12] propose the usage of a special Media Access Control (MAC) learning bridge to facilitate the bridging of datagrams between the old FA and the new FA even before the mobile node has registered itself with the new FA. An efficient way of constructing the MAC learning bridge to facilitate its practical deployment would be to use the concept of Virtual Private LAN Service (VPLS) employing Layer 2 tunnels.

The transportation of Ethernet frames transparently over the network connecting the FA with the HA leads to Layer 2 connectivity between the network connected to the MR and the HN. The presence of Layer 2 connectivity leads to a richer set of network resources being made available to mobile users since many of the file/print sharing protocols are by nature non-routable.

The enhanced set of services afforded by L2MIP are achieved at the expense of an increase in the size of the payload being transported across the IP network between the MR and its HA. It can be observed from Figures 2 and 3 that the size of the captured packet in the case of an L2MIP is larger than that of Mobile IP due to the native transport of Ethernet frames over the IP network.

It needs to be borne in mind that even though an Ethernet frame is being natively transported over the network connecting the MR with the HA, the Ethernet Preamble, Start Frame Delimiter, Padding and Frame Check Sequence (FCS) are stripped of the Ethernet header before being inserted into the L2TPv3 frame. Considering the size of the original IP payload to be N bytes, the total size of the encapsulated packet on the serial link connecting R8R8 and R8R7 (Figure 8) would be equal to (N + 60) bytes for the case of Mobile IP and (N + 74) bytes in the case of L2TPv3 based L2MIP. Hence, the usage of an L2TPv3 based L2MIP results in an overhead of 14 bytes associated with every datagram being forwarded between the MR and the HA.

An increase in the packet length associated with L2TPv3 based L2MIP leads to issues with the Maximum Transmission Unit (MTU) corresponding to the XConnect Interface. As implemented by Cisco Systems, an option exists for setting the MTU size for every L2TPv3 session through the ip pmtu which lets the L2TPv3 control channel participate in path MTU discovery. Further, by setting the Discard Frame Bit (DFBit), any frame which exceeds the MTU associated with an L2TPv3 session will be dropped [9].

Since the usage of IP Precedence bits is a more common means of providing preferential treatment to traffic streams in an IP network, the deployment of QoS within the framework of an L2TPv3 based L2MIP could be achieved by

- Copying the IP Precedence values from the inner IP header on to the outer IP headers of the L2TPv3 encapsulated IP packet. This operation is also referred to as ToS Byte Reflection.
- Static assignment of IP Precedence values to all traffic flowing between the MR and the HA
- Classification of incoming traffic into appropriate classes before manipulating the IP Precedence values

While L2MIP is assumed to be implemented using L2TPv3, the usage of EoMPLS within the framework of Layer 2 mobility is equally valid. In terms of overheads, a typical packet associated with an EoMPLS based L2MIP would be (N + 46) bytes as compared to (N + 74) bytes with an L2TPv3 based L2MIP implementation. However, the requirement of MPLS connectivity between the FA and the HA is a major concern in the widespread deployment of an EoMPLS based L2MIP implementation.

In the next section, a discussion of the simulation test bed employed for evaluating the performance of the proposed L2MIP solution is presented.

4. Test Bed

In order to evaluate the practical deployment of Mobile IP within a typical corporate infrastructure, simulations were carried out to evaluate two distinct characteristics of the proposed L2MIP: (a) the commissioning times associated with L2TPv3 based Layer 2 tunnels, and (b) the performance of real-time and best-effort traffic streams in the presence of the proposed L2MIP.

The commissioning times associated with L2TPv3 based Layer 2 tunnels were evaluated using the network shown in Figure 9. Routers R3 and R4 were configured to act as tunnel end-points while pagent, configured to run a specialized IOS image from Cisco Systems, was configured to generate test-traffic at a rate of 500 packets per second (pps). The generated data traffic was routed via router R3 towards R4 and eventually terminated on pagent. The

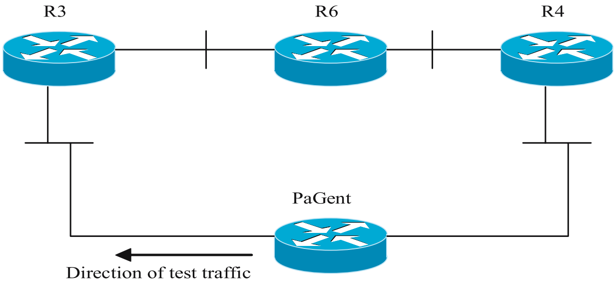


Figure 9. Network employed for estimating the commissioning times associated with IP-IP and L2TPv3 tunnels.

following were the steps involved in the estimation of the commissioning times of Layer 2 and Layer 3 tunnels;

1. Force the tunnel to be inactive at the start of the simulation thereby making the loopback interface on router R4 unreachable from router R3.
2. Activate the tunnel interface and start the data traffic generation (and measurement) utility
3. Since data traffic was generated at a rate of 500 pps, a measurement of the difference between the number of packets transmitted to the number of packets received would indicate the effective time taken to commission a tunnel.

In order to evaluate the practical deployment of Mobile IP within a typical corporate infrastructure, a variety of real-time and best-effort traffic was introduced into the network shown in Figure 8. Real-time traffic, in terms of voice calls, was introduced using CallGen while best-effort traffic was introduced through PaGent.

CallGen is a Cisco IOS-based call generator. Voice calls are originated by the CallGen router shown in Figure 8 and the voice packets pass through the VG2 router towards the VG1 router. The VG2 router was connected to the CallGen router through a T1 link uses an appropriate codec for transmitting voice packets across the IP network. The voice packets were routed from the VG2 router towards the VG1 router via the MR router. In the network considered for the current work, a 3640-series Cisco router running an appropriate CallGen image was configured to be the CallGen router. Since a T1 interface supports 24 DS0 channels, the maximum number of calls that could be placed simultaneously by the CallGen router in the current network setup was limited to 24. One important feature of CallGen is the ability to measure the quality of voice in terms of end-to-end voice delay, end-to-end voice jitter and Perceptual Speech Quality Measurement (PSQM) scores. In order to measure voice quality in terms of PSQM scores, CallGen requires the usage of a PSQM server. In this case, while CallGen connects and disconnects voice calls, the actual computation of the PSQM score is left to the PSQM server.

PaGent is another Cisco IOS-based application that was used for generating data traffic. While CallGen is capable of generating only voice calls, PaGent can be configured to generate a variety of packets based on different layer 2, layer 3 and layer 4 parameters. In addition, PaGent could be used to measure the packet end-to-end latency and the number of in-transit lost packets within the IP cloud.

The performance of the real-time and the best-effort traffic introduced into the network shown in Figure 8 was evaluated based upon the following parameters:

- End-to-end voice delay
- End-to-end voice jitter
- PSQM scores [10]
- End-to-end data delay
- Number of lost voice packets
- Number of lost data packets

The end-to-end voice delay and end-to-end voice jitter values were obtained from CallGen and indicate the delay and jitter values computed with respect to the voice waveform rather than the voice packets themselves. Therefore, these statistics include the effects of the de-jitter buffer and reveal a stronger correlation to the actual voice quality as compared to traditional end-to-end packet delay and end-to-end packet jitter values.

Since the primary aim of the current work was not to evaluate the handoff scenarios in the Mobile IP deployment scenario, the MR was assumed to be connected to the FA for the entire duration of the simulation runs. The link connecting the MR to the FA was configured to support a bandwidth of 5.5 Mbps. Default queuing was employed on all the concerned interfaces such that all the serial links were configured for Weighted Fair Queuing (WFQ) while all the Ethernet links were running First-In First-Out (FIFO). The number of voice calls was limited to 20 while the maximum data rate generated by PaGent was restricted to 100 packets per second (pps). The codec employed was G.711 [11]. With the size of each datagram generated by PaGent set to 1000 bytes, the maximum bandwidth consumed by the PaGent traffic was contained to within 750 kbps. The maximum bandwidth consumed by voice traffic was restricted to 1.6 Mbps. The serial links within the network shown in Figure 8 were configured to support a bandwidth of 1.544 Mbps and all the other parameters were set to their defaults.

Depending upon the Mobile IP implementation being employed (L2MIP or the traditional Mobile IP), the tunnel extending between the FA and the HA could be either an IP-IP tunnel or an L2TPv3 tunnel. In the case of traditional Mobile IP, a second IP-IP tunnel is configured between the MR and the HA. With L2MIP, the presence of Layer 2 connectivity between the MR and the HN obviates the need for a second tunnel between the HA and the MR.

Since the L2TPv3 feature set was not available on the standard IOS images for the routers available in the Wichita State University Student Routers Lab (SRL), a special image was compiled to include the required features to run on the 3620 series Cisco routers used to implement the functionalities of a HA and a FA.

In the next section, a discussion of the results obtained from simulations carried out in the SRL to evaluate the performance of traditional Mobile IP and L2MIP is presented.

5. Simulation Results

5.1. TUNNEL COMMISSIONING TIMES

The primary advantage of L2TPv3 tunnels over IP-IP tunnels lies in the fact that an IP-IP tunnel is considered to be a logical Layer 3 interface thereby making it mandatory for its registration into the router's forwarding/control plane. Cisco System's IOS, for example, employs a specific set of Interface Descriptor Blocks (IDB) for a Layer 3 tunnel which increases their corresponding commissioning times. Since a Layer 2 tunnel (like L2TPv3 tunnel) is not

Table 1. Commissioning times for IP-IP and L2TPv3 tunnels

Tunnel	Commissioning Times (ms)
IP-IP	3155.6
L2TPv3	1151.8

Table 2. Performance of voice and data traffic streams for mobile IP with default mobility and QoS options for G.711 codec

Call volume	Data rate (pps)	Voice delay (ms)	Lead voice Jitter (ms)	Lag voice jitter (ms)	Max. PSQM score	Disconnects	Lost voice Packets (%)	Data packet delay (sec)	Lost data packets (%)
3	0	89	4	4	0.613	0	0.0108	0	0
3	50	89	5	6	0.616	0	0.0322	0.0159	0.1639
3	100	102	11	12	3.706	1	19.593	0.0159	16.712
10	0	89	4	5	0.689	0	0.0510	0	0
10	50	92	12	12	3.139	4	26.978	0.0161	25.742
10	100	108	15	16	3.463	4	47.199	0.0162	47.379
20	0	98	12	15	1.581	3	45.213	0	0
20	50	102	12	29	2.465	5	51.043	0.0169	76.99
20	100	110	16	16	2.465	7	52.322	0.0165	79.586

involved in any routing functionality, its commissioning times are expected to be lesser than those for Layer 3 tunnels.

For the network shown in Figure 9, Table 1 shows the tunnel commissioning times for IP-IP and L2TPv3 tunnels. The tunnels were commissioned (and de-commissioned) 1000 times and the average commissioning time is shown in Table 1. As can be seen from Table 1, the commissioning times associated with IP-IP tunnels are greater than those for L2TPv3 tunnel. Since $T_{\mathrm{ip-ip}}$ (= 3.1556 sec) is greater than T_{L2TPv3} (= 1.1516 sec), from Equation (12) the commissioning times associated with L2TPv3 based mobility solution is lesser than that of traditional Mobile IP.

5.2. NETWORK PERFORMANCE

The network shown in Figure 8 was configured in the SRL for evaluating the performance of L2MIP and traditional Mobile IP. For traditional Mobile IP, default queuing and QoS options were configured on all the interfaces. Table 1 shows the performance of voice and data traffic for varying call volume and data rates with G.711 as the codec.

From Table 2, it can be observed that the quality of voice, as indicated by the voice delay, the voice jitter and the PSQM statistics, deteriorates with increasing amount of voice and data traffic in the network. The delay associated with data traffic is also seen to increase with increasing voice and data traffic.

In order to evaluate the performance of voice and data traffic (originating from the MN) in the presence of congestion from external sources between the FA and the HA, simulations

Table 3. Performance of voice and data traffic streams for mobile IP with default mobility and QoS options for G.711 codec in the presence of congestion from external data sources

Call volume	Data rate (pps)	Voice delay (ms)	Lead voice jitter) (ms)	Lag voice jitter (ms)	Max. PSQM score	Disconnects	Lost voice packets (%)	Data Packet delay (sec)	Lost Data packets (%)	Lost data packets (%) TGN3
3	0	89	5	5	0.613	0	0.0269	0	0	0.1067
3	50	89	5	7	1.086	0	0.3652	0.0161	0.3459	0.1679
3	100	92	12	12	1.724	1	18.572	0.0159	16.793	0.1362
10	0	89	4	4	0.787	0	0.0528	0	0	0.0848
10	50	93	12	12	3.334	2	27.037	0.0161	26.251	0.1408
10	100	101	16	16	3.463	4	46.597	0.0161	47.782	0.1054
20	0	98	9	16	1.581	7	41.92	0	0	0.094
20	50	116	11	12	2.465	7	51.464	0.0165	71.067	0.1401
20	100	97	13	14	2.465	5	51.164	0.0168	84.207	0.112

were carried out in the SRL using the network shown in Figure 8 with the only addition being that of a second PaGent router configured between R8R8 and R8R7. Since OSPF would pick the shortest path connecting the FA and the HA to include the serial link connecting R8R8 and R8R7, congesting this serial link would reflect the behavior of voice and data traffic in the presence of congestion in the global Internet. The data rate of TGN3 was set to 200 pps with each packet configured to be of size 1000 bytes.

Table 3 shows the variation in delay values associated with the voice and the data traffic emanating from the MN in the presence of congestion. The results in Table 3 follow a similar pattern as those shown in Table 2, wherein increasing voice and data traffic leads to deteriorating voice and data quality. Table 3 also reveals a considerable increase in the percentage of lost data packets with increasing voice and data traffic while the delay statistics for both voice and data traffic are comparable with those shown in Table 2.

While the scenario considered in this section represents the interaction of Mobile IP with different traffic streams within a network, its practicality is limited by (a) the lack of traffic shaping on the FA to ensure that the traffic from the MR does not overwhelm the FA's Service Level Agreement (SLA) with its Service Provider (SP), (b) the usage of different IP Precedence values for different traffic streams emanating from the MR and (c) the usage of TE capabilities in the network so as to provide guaranteed services to the MR. These additional constraints are imposed on the network shown in Figure 8 and the obtained simulation results are discussed next.

While the simulations in the previous section used a maximum call volume of 20 calls in conjunction with a maximum data rate of 100 pps and a packet size of 1000 bytes/packet, the FA was not configured with any traffic shaping features to rate-limit the traffic originating from the MR. Since the FA typically connects to the HA via a SP and its interaction with the SP is regulated by a specific SLA, an increase in the traffic from the MN could potentially result in packet drops in the traffic streams originating from the FN itself. In addition, the lack of traffic-shaping capabilities on the FA places several constraints on the billing and accounting policy applicable on the FA.

To overcome this practical limitation of the network scenario considered earlier, the FA was configured to drop traffic exceeding 750 kbps originating from the MR. In practice, the actual

Table 4. Performance of voice and data traffic streams for mobile IP with traffic shaping and different IP Precedence values in the presence of congestion from external data sources. Codec used was G.711

Call volume	Data rate (pps)	Voice delay (ms)	Lead voice Jitter (ms)	Lag voice Jitter (ms)	Maximum PSQM score	Disconnects	Lost voice packets (%)	Data packet delay (sec)	Lost data packets (%)	Lost data packets (%) TGN3
3	0	89	4	4	0.612	0	0.0161	0	0	0.1413
3	50	89	5	5	0.843	0	0.3272	0.0161	0.3081	0.1399
3	100	101	12	12	2.233	1	19.139	0.0159	16.799	0.1516
10	0	89	4	4	0.775	0	0.0387	0	0	0.0916
10	50	94	11	12	3.792	3	27.411	0.0161	25.482	0.1399
10	100	109	13	13	2.465	5	46.865	0.0161	47.651	0.0838
20	0	100	14	15	1.581	4	45.319	0	0	0.0565
20	50	99	12	12	2.465	2	50.756	0.0169	77.904	0.1122
20	100	111	14	15	2.465	7	51.776	0.0167	78.325	0.0902

rate-limiting traffic volume would be decided by a negotiation between the MR, the FA and the Bandwidth Broker (BB) configured in the FN. In order to provide preferential treatment to real-time traffic streams, voice traffic emanating from the MN was configured with an IP Precedence value of 5 while data traffic was configured with an IP Precedence value of 0.

Table 4 shows the performance of voice and data traffic for traditional Mobile IP with traffic shaping on the FA and different IP Precedence values for best-effort and real-time traffic streams. As can be seen from Table 4, an increasing number of calls clubbed with increasing data traffic leads to a deterioration in the end-to-end statistics of both voice and data traffic. Considering the cases without any data traffic from the MN, an increase in the number of calls is seen to result in a large number of voice packet drops due to the presence of the traffic shaping feature on the FA. For the case of 20 calls with no data traffic, the percentage of dropped voice packets is seen to reach about 45% which translates approximately to about 750 kbps of voice traffic that was allowed to flow into the FN. With increasing data traffic, the percentage of dropped voice and data packets is seen to be increasing. It needs to be pointed out that even though the voice and data packets emanating from the MN were configured for different IP Precedence values, the traffic shaping feature on the FA does not provide preferential treatment to these flows since traffic shaping is enforced irrespective of the IP Precedence values associated with packets presented for shaping. To reap the benefits of different priorities associated with real-time and best-effort traffic streams, the QoS provisioning needs to be carried out within the MN.

In an effort to evaluate the performance of real-time and best-effort traffic streams in the presence of an L2MIP, simulations were carried out in the SRL using the network shown in Figure 8. In order to compare the end-to-end performance accrued due to L2MIP with those obtained from Mobile IP, the simulation test-bed employed for the previous end-to-end performance simulations was retained with a few L2MIP specific modifications to them.

Table 5 shows the performance of voice and data traffic streams with L2TPv3 based L2MIP for G.711 codec. It can be observed that an increasing in the traffic between the MR and the HA leads to considerable number of voice call disconnects in addition to a significant portion of dropped data packets.

Since the L2TPv3 based L2MIP implementation virtually extends the LAN segment that exists between the HN and the FN, the issue of ensuring the proper sequencing of Ethernet

Table 5. Performance of voice and data traffic streams with L2TPv3 based L2MIP and default QoS options for G.711 codec

Call volume	Data rate (pps)	Voice delay (ms)	Lead Voice jitter (ms)	Lag voice jitter (ms)	Maximum PSQM score	disconnects	Lost Voice packets (%)	Data packet delay (sec)	Lost data packets (%)
3	0	90	4	5	0.591	0	0	0	0
3	50	90	5	5	0.584	0	0	0.0167	0.0063
3	100	92	5	5	0.591	0	0	0.0168	0.0064
10	0	90	5	6	0.591	0	0.007	0	0
10	50	90	5	5	1.281	0	0.0023	0.0175	0.0063
10	100	90	3	3	2.912	0	0.0023	0.018	0.0221
20	0	91	4	4	1.973	9	0	0	0
20	50	101	4	4	1.973	12	0.1313	0.0184	16.148
20	100	98	5	5	1.973	13	0.1126	0.0201	22.156

frames becomes a major challenge. Traditionally, Ethernet has been a LAN protocol that does not account for frames being delivered in an out-of-order fashion. With the extension of a LAN segment over an IP network, the frames being transported over the L2TPv3 pseudowire interface could be received at the PE routers in an out-of-order fashion. This is due to the fact that IP allows for packets to be re-ordered or re-sent resulting in their out-of-sequence delivery. Since Ethernet does not support sequencing operations, out-of-sequence packet arrivals at the PE router need to be re-ordered. The implementation of L2MIP considered for the current performance evaluation dropped any out-of-sequence frames thereby resulting in considerable number of disconnected voice calls.

The increase in the number of dropped data packets and an increase in the number of voice call disconnects shown in Table 5 can be accounted for by the lack of sequencing support within the configured L2MIP. However, the end-to-end statistics in terms of delay and jitter values associated with voice and data traffic are observed to be comparable with those obtained due to traditional Mobile IP.

Table 6 shows the voice and data statistics with the usage of ToS bit reflection and rate-limiting on the FA. Considering the results obtained for a call volume of 20 and no data traffic originating from within the MN, the very large number of disconnected voice calls emanating from less than 1% of dropped voice traffic highlights the issues related to out-of-sequence frames associated with the configured pseudowire interface.

6. Conclusion

With the need for providing mobility to entire networks, two factors are driving the transformation of the mobility problem from Layer 3 to Layer 2. The first driving factor is the increasing perception among the mobile workforce that Layer 3 connectivity is not enough in terms of supported mobile services. Secondly, the need for a second IP-IP tunnel that exists between the MR and the HA leads to an increase in the encapsulation overheads not only in the size of the tunnel headers, but also in the number of tunnel encapsulation/decapsulation operations being performed on the packet.

Table 6. Performance of voice and data traffic streams for L2TPv3 based L2MIP with traffic shaping on the FA and different IP Precedence values for voice and data traffic. G.711 is the codec being employed

Call volume	Data rate (pps)	Voice delay (ms)	Lead voice jitter (ms)	Lag voice jitter (ms)	Maximum PSQM score	Disconnects	Lost voice packets (%)	Data packet delay (sec)	Lost data packets (%)	Lost data packets (%) TGN3
3	0	90	4	5	0.591	0	0	0	0	0.0615
3	50	90	5	6	0.591	0	0	0.0169	0.0063	0.0715
3	100	92	6	7	1.121	0	0.0053	0.0176	0.0031	0.0797
10	0	90	7	7	2.247	0	0.0023	0	0	0.0721
10	50	90	5	5	1.849	0	0.0047	0.0188	0.0063	0.0932
10	100	92	3	3	2.178	0	0.007	0.0197	0.0188	0.1055
20	0	92	5	5	2.711	100	0.0563	0	0	0.0953
20	50	91	4	5	2.711	8	0.1102	0.0222	25.144	0.1049
20	100	200	6	7	2.711	2	3.5248	0.1162	23.654	25.618

With the introduction of the concept of a VLL, the mobility problem could be resolved at Layer 2 obviating the need for additional provisioning to account for mobile networks. This research presented the fundamental procedures involved in considering the mobility problem as a Layer 2 connectivity issue.

Simulations results obtained from performance evaluation tests indicate similar performance for both the traditional Mobile IP and the proposed L2MIP solutions, with the exception of the issue related to out-of-sequence frames in the Layer 2 mobility solution.

Due to the relatively "experimental" nature of the L2MIP implementation, the authors were not able to report the performance of the proposed L2MIP solution with support for out-of-sequence frames or the scalability of the proposed L2MIP solution compared to that of traditional Mobile IP. These topics are the focus of future work.

References

1. Charles Perkins, IP Mobility Support for IPv4, RFC 3220. [Online] Available: http://www.ietf.org/rfc/rfc3220.txt
2. Charles Perkins, IP Encapsulation within IP, RFC 2003. [Online] Available: http://www.ietf.org/rfc/rfc2003.txt
3. Charles Perkins, Minimal Encapsulation within IP, RFC 2004. [Online] Available: http://www.ietf.org/rfc/rfc2004.txt
4. J. Kim, K. Leung, K. Echols, D. Shell, and M. Denny, *Demonstration of Static Network Mobile Router for Mobile Platforms*, MILCOM 1999.
5. Luca Martini et al., "Transport of Layer 2 Frames over MPLS", IETF Draft. http://www.ietf.org/internet-drafts/draft-martini-l2circuit-trans-mpls-10.txt
6. Vach Kompella et al., "Requirements for Virtual Private LAN Services (VPLS)", IETF draft. http://www.ietf.org/internet-drafts/draft-ietf-ppvpn-vpls-requirements-01.txt.
7. Lau, M. Townsley, A. Valencia, G. Zorn, I. Goyret, G. Pall, A. Rubens, and B. Palter, "Layer Two Tunneling Protocol a.k.a. L2TPv3", Work in Progress. draft-ietf-l2tpext-l2tp-base-03.txt
8. W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, and B. Palter, "Layer 2 Tunneling Protocol", RFC 2661. http://www.ietf.org/rfc/rfc2661.txt
9. "Dynamic Multipoint VPN", Cisco Systems IOS Documentation. http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftgreips.pdf
10. "*Objective Quality Measurement of Telephone Band (300-3400 Hz)*", ITU-T Recommendation P.861, ITU-T. August 1996
11. "*Pulse Code Modulation for Voice Frequencies*", ITU-T Recommendation G.711, ITU-T. November 1988
12. H. Yokota, A. Idoue, T. Hasegawa, and T. Kato, "*Link Layer Assisted Fast handoffs for Mobile IP*," MOBICOM 2002. Atlanta, GA. September 23–26, 2002.