INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2001-2004

STUDY GROUP 13

TD 15 (WP 3/13)

English only

Question(s): 11/13 Geneva, 29 October - 8 November 2002

TEMPORARY DOCUMENT

Source: Rapporteur Q.11/13

Title: Updated Living List of Q.11/13

The following living list structure and procedures are intended to progress the work on Q.11/13 related Recommendations.

1. Structure

A. List of Items

- Title of item

B. Description of each item

- Title
- Description of the problem and possible solutions
- List of documents addressing the issue
- Intermediate agreements

2. Status of proposals

Status of proposals
U - Under study
P - Provisionally agreed
F - Frozen

3. Guidelines

- Insertion of an issue into the Living List is generally based on contributions and requires a general agreement that the issue is important for further consideration within Question 11/13.
- Proposal should include texts conforming to the Recommendation structure and provide for enhancements and/or modifications of the relevant parts of the Recommendation.
- An issue is deleted from the Living List if no contributions addressing the issue have been provided in a long period and there is a general consensus for its removal.
- When an item is added to the living list, its status is U by default.
- Transition from U to P may happen at the next meeting if there is a consensus on the solution proposed in the form of modifications to the current text of the Recommendation and if no contradicting contribution is provided.
- Transition from P to F may happen at the next Q.11/13 meeting if no contribution contradicts the provisionally agreed text and there is consensus.
- When contribution (s) are provided contradicting the existing text with status “P” and no consensus is achieved on the contribution, the status of the existing text is unchanged. Transition from P to U happens only if consensus is achieved on the contradicting contribution.
- Frozen texts are inserted in the updated version of the Recommendation if there is consensus.

4. Operational rules

- All proposed modifications to the Recommendation should be made available to the ITU-T meetings in a PC compatible electronic version.

The first living list item deals with support of Mobile IP service through the MPLS network.
The second living list item deals with an IP Network architecture with out-band signalling.
The third living list item deals with End-to-end Voice over MPLS.
The last living list item deals with Service architecture classification for Layer 1 VPN .

No.	Title of Living Lists	Status
1	Application procedures for support of Mobile IP Service over MPLS	Under Study (July 2002 Chitose)
2	An IP network architecture with out-of-band signalling	Under Study (Jan. 2002 Geneva)
3	End-to-end Voice over MPLS	Under Study (July 2002 Chitose)
4	Service architecture classification for Layer 1 VPN	Under Study (Nov. 2002 Geneva)

Living List #1 of Q.11/13

Title: Application procedures for support of Mobile IP Service over MPLS

Description of the problem and possible solution

This living list item discusses the application procedures of the MPLS network to support the mobile IP service. The relevant control procedures on the MPLS network are required to set up the LSP tunnels, discover the mobile agents (home agent and foreign agent), and register the mobile node, etc. In addition, the hand-over and re-routing scheme through the MPLS network should be analyzed when a mobile node is moving to a distance area. The application procedures are also depending on network architecture and service scenario.

It is requested to investigate the relevant application procedures including tunneling, agent advertisement/solicitation, registration, and hand-over, etc.

1. Application Procedures for Mobility Support

1.1 General Assumptions

The main issues of MPLS network architecture with mobility support are focused on the control procedure such as registration, LSP establishment and LSP Extension, etc. Agent advertisement and discovery procedure is unmodified in the existing Mobile IP protocol.

It is required to program appropriate QoS support for the MN's packets in the intermediate network domains, so that the performance of QoS-sensitive applications running on the MN is maintained at desired level. To achieve this, our model adopts QoS Object to interoperate with CR-LDP/RSVP-TE.

In the MPLS-based Mobile IPv4 Tunneling Scenario, wireless IP communicators will be turned around the clock, ready to receive or initiate services. In fact, the vast majority of subscribers will not be actively communicating most of the time. Rather, wireless IP communicators will be switched on, ready for service, constantly reachable by the wireless Internet. The MN will be in an idle state but passively connected to the network infrastructure. Thus design principle is that only active data are supposed to traverse over QoS guaranteed LSP. This will prevent LSP abusing that can be caused by lots of control packets.

If LSP is established for the datagram IP traffic (the UDP traffic), LSP setup and release repetition would occur because the traffic are generated sparsely. So our model considers only TCP traffic.

There is no additional Message or TLV/Object on existing CR-LDP/RSVP-TE to setup QoS guaranteed LSP between CN's LER and MN's LER. The suggested model adopts data-driven LSP setup.

There requires LSP tunnels to send a stream of mobile IP packets through the MPLS network. The existing LDP specification is well described to establish LSP tunnels for mobility. The address of home agent and foreign agent for LSP tunnels will be given by the Registration and Agent Discovery Procedure within the Mobile IP protocol.

While traditional traffic engineered MPLS are unidirectional, generalized MPLS supports the establishment of bi-directional LSP. In three types of MPLS-based Mobile IPv4 scenarios, bi-directional LSP have the benefit of lower setup latency and lower number of messages required during setup. It takes only one initiator-eliminator round trip time. The LSP with QoS constraints is contained in the CR-LDP or RSVP-TE specification.

1.2 LSP Tunneling Procedures

1.2.1 MPLS-based Mobile IPv4 Tunneling Procedures

There are LSP tunnels in the MPLS-based Mobile IPv4 Tunneling Scenario;

- LSP tunnels between the Ingress LER and home agent
- LSP tunnels between home agent and the Egress LER/FA

In the registration procedure, the mobile node determines whether it is at home or in a foreign network when it receives Agent Advertisement Messages broadcast by the mobility agents. If the mobile node determines that it is in a foreign network, the mobile node acquires a temporary care-of address from foreign agent and sends a Registration Request to foreign agent. Since foreign agent is an edge LER, it will analyze the incoming Registration Request Message and get the destination address of the request. Then, foreign agent updates its routing table with the value of mobile node home address. In addition, it sets the outgoing port value of this entry to be the incoming port number from which it received the registration request. Based on the IP routing table, foreign agent forwards the Registration Request Message toward home agent.

Figure 4 shows LSP tunneling procedures for mobile IPv4 service over MPLS.

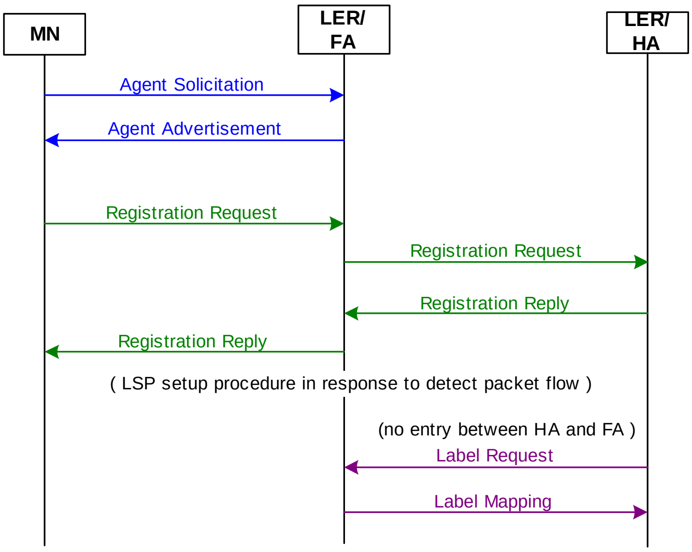


Figure 4. LSP tunneling procedures for mobile IPv4 service over MPLS.

The Registration Request Message is forwarded to home agent using normal IP hop-by-hop routing. When home agent gets the Registration Request Message and learns the care-of address of the mobile node, it sends Registration Reply Message to the mobile node via foreign agent. In the home agent, if long lived message exists between same correspondent node and destination mobile node, then the home agent will send a Label Request/Path Message to foreign agent with the care-of address of the mobile node. A foreign agent replies with an Label Mapping/Resv Message to the home agent. When this Label Mapping/Resv Message arrives at home agent, the LSP would have been established. After that, home agent changes its label information table that contains the home address and the care-of-address of mobile node. It sets the outgoing port entries of the LSP from home agent to foreign agent. In this way, home agent can relay the packets destined to mobile node home address to its current location in the foreign network.

When foreign agent receives packets on the LSP, it records the incoming port number, label value and IP address of the correspondent node of the packet. Therefore, the foreign agent should send user packets through the established bi-directional LSP from the mobile node to the correspondent node because it should know that for which mobile node the LSP is established.

Packets from a correspondent node to the mobile node are addressed to the mobile node home address. If the mobile node is located in a foreign network, packets are intercepted by the home agent. The home agent uses the incoming label value as an index to look up its label table. It inserts the label value in the label table into packet and sends it out through the port indicated in the table. If a mobile node is still in the home network, then outgoing port entries are empty. The packet will be sent to the IP layer and sent out from the port indicated in the corresponding routing table entry. If a mobile node is in foreign network and a LSP is established from the home agent to the foreign agent, then the home agent must send user packets to the foreign agent by using label swapping method.

1.2.2 MPLS-based Mobile IPv4 Route Optimization Tunneling Procedures

There are LSP tunnels in the MPLS-based Mobile IPv4 Route Optimization Scenario;

- Direct LSP tunnels between the Ingress LER and the Egress LER/FA
- LSP tunnel between old foreign agent and new foreign agent (for LSP extension)

The tunneling procedure of this model might be different from that of Scenario 1. When a correspondent node sends packets to a mobile node located in the foreign area, the Ingress LER has to decide the relevant forwarding path depending on routing information.

The MPLS-based Mobile IPv4 Route Optimization Scenario uses the same Registration and Advertisement procedure with the MPLS-based Mobile IPv4 Tunneling Scenario (Scenario 1). The Registration Request Message is forwarded to home agent using normal IP hop-by-hop routing. When home agent gets the Registration Request Message and learns the care-of address of the mobile node, it sends Registration Reply Message to the mobile node via foreign agent.

Figure 5 shows Route optimized LSP tunneling procedure for mobile IPv4 service over MPLS.

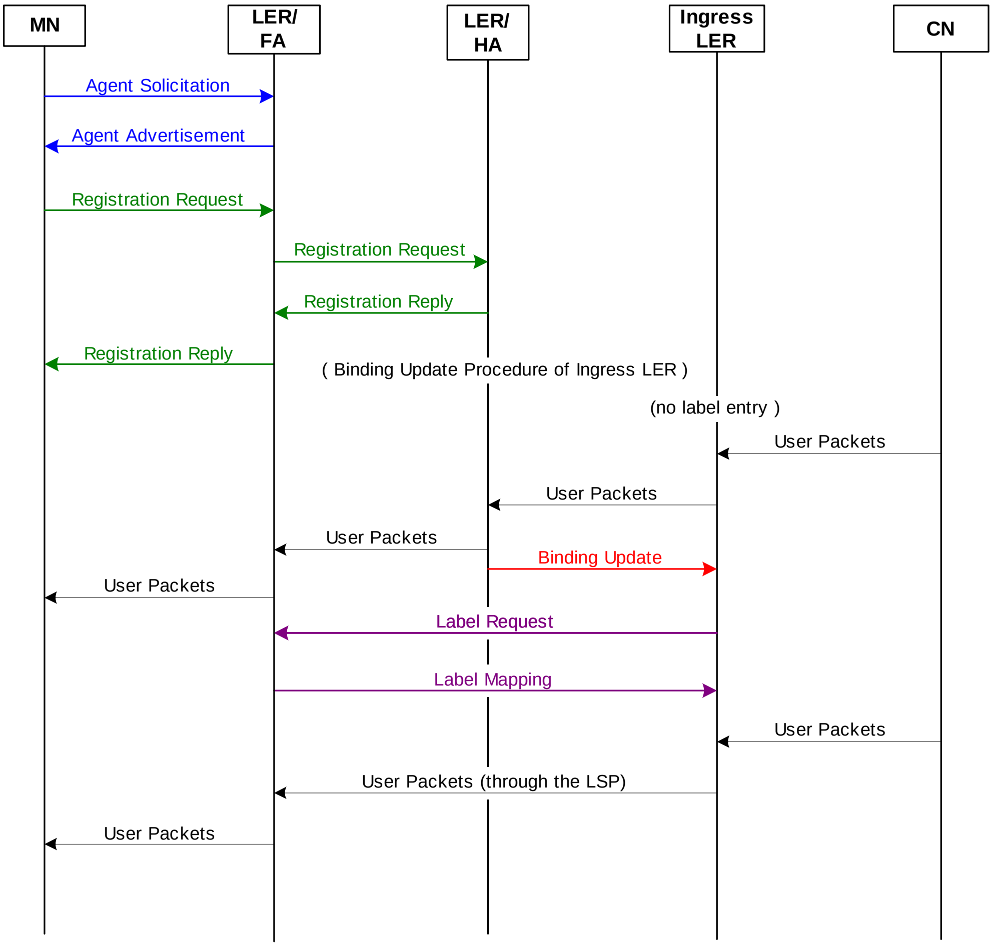


Figure 5. Route optimized LSP tunneling procedure for mobile IPv4 service over MPLS

When a mobile node's home agent intercepts a datagram from the home network and tunnels it to the mobile node, the home agent should then send a Binding Update Message to the Ingress LER of correspondent node, informing it of the mobile node's current mobility binding. The binding update procedure is defined in [5]. There are four message types used for management of binding cache entries; Binding Warning message, Binding Request message, Binding Update message, and Binding Acknowledge message. For a Binding Update to be authenticated by the Ingress LER of original correspondent node, the Ingress LER and the home agent must have established a mobility security association. The detail procedure for security association is for further study.

When any foreign agent receives a tunneled datagram, if it has a binding cache entry for the destination mobile node and thus has no visitor list entry for this mobile node, the node receiving this tunneled datagram may deduce that the tunneling node has an out-of-date binding cache entry for this mobile node. In this case, the receiving node should send a Binding Warning Message to the mobile node's home agent, advising it to send a

Binding Update message to the Ingress LER that tunneled this datagram. As in the case of a Binding Update sent by the mobile node's home agent,

Ingress LER may maintain a binding cache to optimize mobile node's communication with mobile nodes. An Ingress LER may create or update a binding cache entry for a mobile node only when it has received and authenticated the mobile node's mobility binding. As before, each binding in the binding cache also has an associated lifetime, specified in the Binding Update Message in which the node obtained the binding. After the expiration of this time period, the binding is deleted from the cache.

For the matters of QoS and traffic control, it should investigate whether the bandwidths between the Ingress LER and the Egress LER are available or not. With these concerns, the CR-LDP or RSVP-TE may be useful to take a relevant forwarding path. The detail scenarios on MPLS-based Mobile IPv4 Route Optimization require for further study.

In the absence of any binding cache entry, datagrams destined for a mobile node will be routed to the mobile node's home network in the same way as any other IP datagram, and then tunneled to the Egress LER via the mobile node's home agent. With Binding information received from home agent, Ingress LER initiates the label binding process to the Egress LER/FA to a mobile node. After that, Ingress LER updates the label information table that contains the Egress LER address and the care-of address of a mobile node. It sets a label value and outgoing port entries.

When a correspondent node sends IP packets to Ingress LER, the Ingress LER searches forwarding label entries to the destination mobile node. If a label entry found, it sends IP packets to the Egress LER with the care-of address of a mobile node through the LSP. If not found, Ingress LER should send IP packet to the Egress LER via home agent.

1.2.3 MPLS-based Mobile IPv6 Binding Update Tunneling Procedures

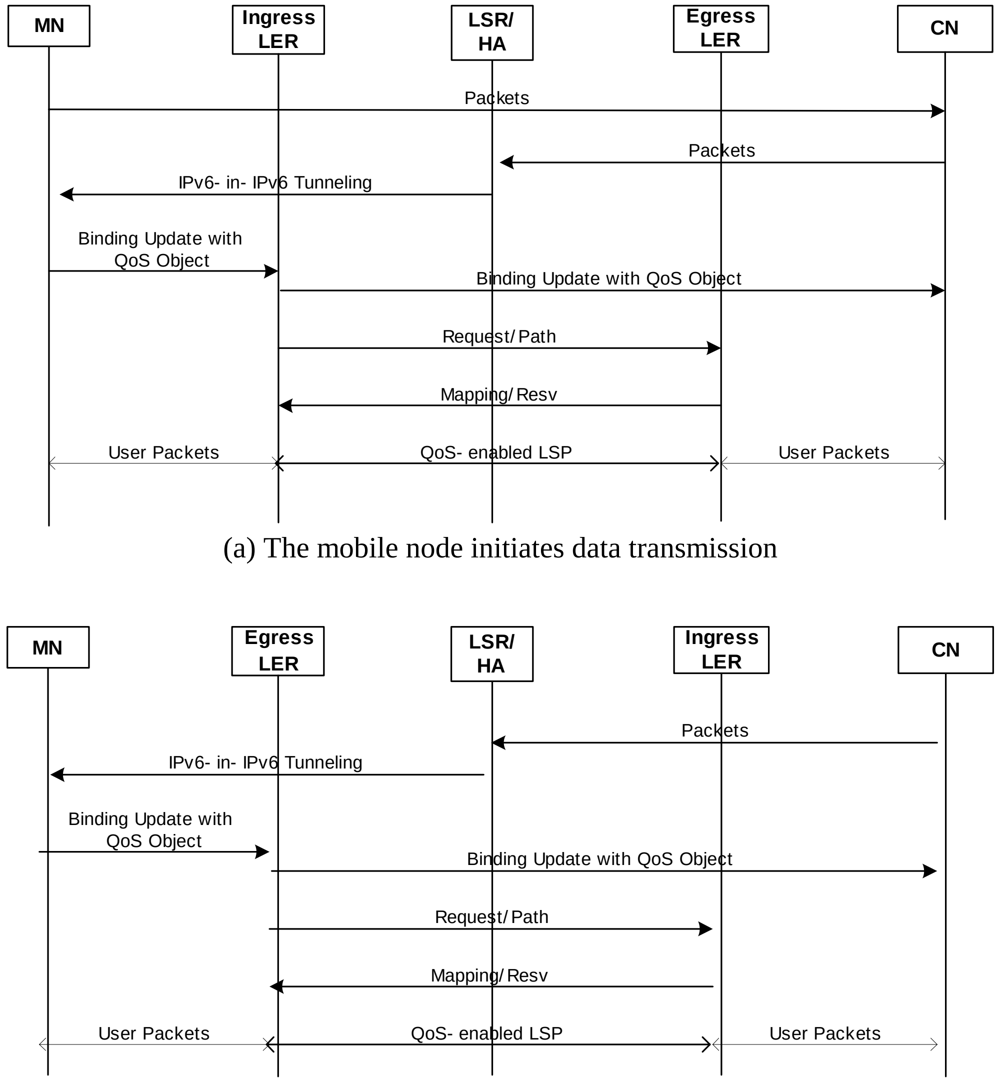
There are LSP tunnels in the MPLS-based Mobile IPv6 Binding Update;

- Direct LSP tunnels between the Ingress LER and the Egress LER/FA

When the MN sends packets to any other correspondent node, it sends packets directly to the destination. The MN sets the source address of this packet to the care-of-address and includes a 'Home Address' destination option. Then the correspondent node must process the option in a manner consistent with exchanging the Home Address field from the Home Address option into the IPv6 header. Since the home address is static (in contrast to the care-of-address), this allows every correspondent node the transparent use of the care-of-address for layers above the Mobile IPv6 support. Higher layers including applications do not recognize the care-of-address. They only notice the home address. Then the packets from the correspondent node are routed to the HA and tunneled to MN by IPv6-in-IPv6. This routing is called Triangle Routing.

To avoid triangle routing a MN sends Binding Update that may be together with QoS Object to correspondent node. The MN's LER receiving the Binding Update message should determine whether to initiate REQUEST/PATH message or not. If the Binding Update message has zero H bit, the LER initiates REQUEST/PATH for a destination address (FEC). Now the correspondent IPv6 node receiving the Binding Update message is able to send packets to MN directly. Newly established QoS guaranteed LSP provides tunnel for packets to traverse.

Figure 6 shows LSP tunneling procedures for mobile IPv6 service over MPLS.



(a) The mobile node initiates data transmission

(b) CN initiates data transmission

Figure 6 LSP tunneling procedures for mobile IPv6 service over MPLS

We assume a MN has already done new default router finding, Address auto-configuration, Registration, and Biding Acknowledgement reception as Mobile IPv6 procedures. Before a CN sends any packet to the MN, the CN should examine its Binding Cache for an entry for an entry for the destination address (Home address) to which the packet is being sent. If the CN has a Binding Cache entry for this address, the CN should use a Routing header to route the packet to the MN by way of the care-of-address in the binding recorded in that Binding Cache entry. We assume that a CN has no Binding Cache entry for the MN in this part. The packet sent by the CN will be intercepted by the MN's HA and tunneled (using IPv6-in-IPv6 encapsulation) to the MN's current primary care-of-address.

To avoid triangle routing a MN sends Binding Update that may be together with QoS Object to correspondent node. The MN's LER receiving the Binding Update message should determine whether to initiate REQUEST/PATH or not. If the Binding Update message has zero H bit, the LER initiates REQUEST/PATH for a destination address (FEC). Now the correspondent IPv6 node receiving the Binding Update message is able to send packets to MN directly. Newly established QoS guaranteed LSP provides tunnel for packets to traverse.

1.2.4 MPLS-based Hierarchical Mobile IP Tunneling Procedures

There are LSP tunnels in the MPLS-based Hierarchical Mobile IPv4 Tunneling Scenario;

- LSP tunnels between the Ingress LER and home agent
- LSP tunnels between home agent and GFA
- LSP tunnels between GFA and RFA
- LSP tunnels between RFA and the Egress LER/FA

The address of GFA, RFA and the Egress LER/FA for LSP tunnels will be given by the Registration Procedure within the Mobile IP Regional Registration.

A foreign agent advertises addresses of hierarchical foreign agent in order between its own address (first) and the GFA address (last) in the Agent Advertisement. If the mobile node determines that it is in a foreign network, the mobile node sends a Registration Request, with the care-of address set to the GFA address announced in the Agent Advertisement. When the foreign agent closest the mobile node receives the Regional Registration, because the foreign agent is a LER, it will analyze the incoming Registration Request message and relays the Registration Request to the next RFA in the hierarchy toward the GFA.

The next RFA that is a LSR receives the Registration Request. For each pending or current registration, an RFA maintains a visitor list entry. RFA stores mobile node entry its mobile node table, and insert its own address to the registration packet. This procedure is repeated to the GFA. When the GFA receives the Registration Request, it cashes information about the next lower-level RFA in the hierarchy. It then relays the Registration Request to the home agent. For each pending or current registration, the GFA maintains a visitor list entry. The request message is forwarded to home agent hop-by-hop using normal IP routing.

When home agent gets the Registration Request message and learns the care-of address of GFA within the packet, the home agent sends a Registration Reply to the GFA. When GFA receives the Registration Reply message, GFA can recognize what the Registration Reply is come from the specific mobile node that is registered. GFA can know the lower-level RFA of a registered mobile node by reading the information of the mobile node entry corresponding to a received Registration Reply packet. And then GFA sends a Registration Reply to the RFA. This procedure is repeated in every FA in the hierarchy, until the Registration Reply message reaches the FA closest to the mobile node. When the lowest-level FA receives Registration Reply, it should check its cached information and relays the Registration Reply to the mobile node.

Figure 7 shows LSP tunneling procedures of mobile IP service over hierarchical MPLS.

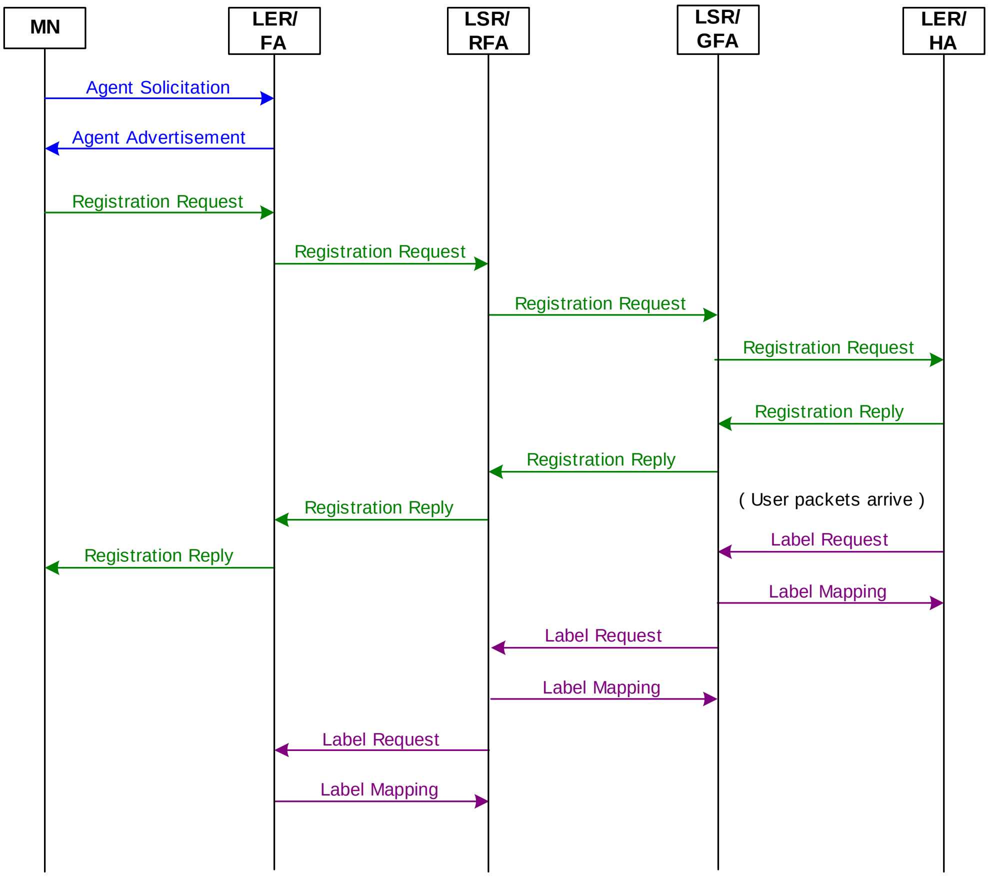


Figure 7. LSP tunneling procedures of mobile IP service over hierarchical MPLS.

When home agent gets user packets to the mobile node, it will send a Label Request/Path Message to GFA with the care-of address of the mobile node. GFA replies with a label mapping/Resv message to home agent. GFA should assign labels and keep the Home address of a mobile node and binding table of a specific label about being registered mobile nodes. When this Label Mapping/Resv Message arrives at home agent, the LSP would have been established. Figure 7 shows the registration and LSP establishment procedure. After that, a home agent changes its label information table that contains the home address and the care-of-address of mobile node. It sets the empty out label and outgoing port entries to the values of out label and outgoing port. In this way, home agent can relay the packets destined to mobile node home address to its GFA in the foreign network. Finally, home agent sends user packets to GFA along the LSP from home agent to GFA.

When GFA receives the labeled user packets, GFA can recognize what the Registration Reply is come from the specific mobile node that is registered after the operation of label pop. GFA writes the label value attached to user packets on an incoming value of corresponding mobile node. GFA can know the lower-level RFA of a registered mobile node by reading the information of the mobile node entry corresponding to a received user packets. GFA will send a label request/Path message to next RFA with the care-of-address of the mobile node. RFA replies with an Label Mapping/Resv Message to the home agent. RFA should keep the information of binding table and the Home address by assigning a Label about the registered whole mobile nodes. When this Label Mapping/Resv Message arrives at GFA, the LSP would have been established.

After that, GFA changes its label information table that contains the home address and the care-of-address of mobile node. It sets the empty out label and outgoing port entries to the values of out label and outgoing port. In this way, GFA can relay the packets destined to mobile node home address from home agent to RFA. Finally, GFA sends user packets to RFA through the LSP. This procedure is repeated in every FA in the hierarchy, until the user packets reach the FA closest to the mobile node. When the lowest-level FA receives user packets, it should remove its labels and checks its cached information and relay the user packets to the mobile node.

If a packet is arriving at the Ingress LER from a corresponding node, the Ingress LER certifies the destination IP address and finds the mapped label in a label information base (LIB). If a mapped label is found, the Ingress LER attaches the label at the header of a packet and tunnels it to the Egress LER via relevant LSRs. But if the mapped label is not found, the Ingress LER should set up the relevant LSP using LDP before transmitting packets. The Ingress LER transmits the Label Request Message to the Egress LER (that is the foreign agent corresponding to the destination IP address).

The home agent, which receives the Label Request/Path Message about a mobile node by using Proxy ARP or gratuitous ARP, transmits the Label Mapping message about home IP address of a mobile node to a upstream LSR instead of the mobile node. At this time home agent should be able to recognize the home IP address of corresponding mobile node using label value that is received from a upstream LSR by the recorded table that is consist of home IP addresses and mapped label. A home agent records the label about a GFA and a mobile node in label table, which consists of the upstream LSRs and incoming labels that are mapped into outgoing labels. The table is composed to be transmitted to a GFA by swapping the packet about conveyed a mobile node from the Ingress LERs through intermediate LSRs. The Ingress LER that receives a packet from a correspondent node recognizes the destination IP address of the packet and transmits a labeled packet through corresponding LSP. In the case of the destination IP address is mobile node, labeled packet is transmitted to a home agent through a LSP.

1.3 Agent Discovery

The agent discovery procedure includes both agent discovery and agent solicitation. Same agent advertisement and solicitation procedures with mobile IP are used at the MPLS network since mobile agents are located at the MPLS node. Mobile agents (i.e., foreign agents and home agents) advertise their presence via Agent Advertisement messages. A mobile node may optionally solicit an Agent Advertisement message from any locally attached mobility agents through an Agent Solicitation message. A mobile node receives these Agent Advertisements and determines whether it is on its home or a foreign location.

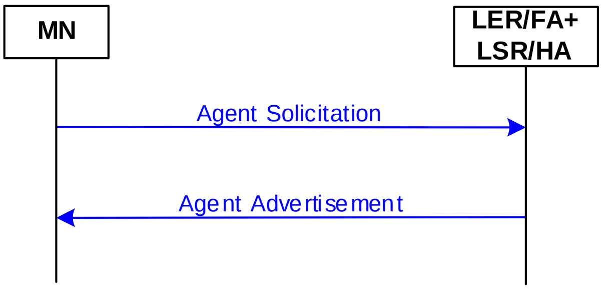


Figure 8. Agent discovery of mobile node over the MPLS Network

If sent periodically, the nominal interval at which Agent Advertisements are sent should be 1/3 of the advertisement Lifetime given in the MPLS shim header. This allows a mobile node to miss three successive advertisements before deleting the agent from its list of valid agents.

1.4 LSP Re-Routing Procedures during Handover

In the MPLS-based Mobile IPv4 Tunneling Scenario (Scenario 1), when mobile node moves from one foreign agent to another, the registration procedure is repeated once between the home agent and new foreign agent. The existing LSP should be changed to the new foreign agent. The following issues are further considered on the MPLS network.

- LSP rerouting
- LSP extension

We imagine that wireless IP communicators will be turned around the clock, ready to receive or initiate services. In fact, the vast majority of subscribers will not be actively communicating most of the time. Rather, wireless IP communicators will be switched on, ready for service, constantly reachable by the wireless Internet. In essence, MN will be in an idle state but passively connected to the network infrastructure. Thus design principle is that only active data are supposed to traverse over QoS guaranteed LSP. This will prevent LSP abusing that can be caused by lots of control packets. Thus an LSP is established only between MN's router and CN's router other than LSP via HA. This would be efficient scheme to save bandwidth on network and to reduce end-to-end delay.

There are two goals in term of handoff; the first, to reduce the latency or interruption due to handoffs; and second, to reduce the signaling load. Mobile IPv6 is considered as optimal solution for those needs. Use of more than on care-of-address by a MN may be useful to improve smooth handoff when the MN moves from on wireless link to another. Our suggested model supports the smooth handoff scheme of Mobile IPv6 and gives solution to QoS consideration with providing QoS guaranteed multiple LSP for the number of MN's care-of-address.

1.4.1 LSP Extension

IP datagrams intercepted by the home agent after the new registration are tunneled to the mobile node's new foreign agent (that is the new Egress LER), but datagrams in flight that had already been intercepted by the home agent and tunneled to the old foreign agent (that is the old Egress LER) when the mobile node moved are likely to be lost.

Route Optimization provides a means for the mobile node's previous foreign agent to be reliably notified with the mobile node's new binding update information, allowing datagrams in flight to the mobile node's previous foreign agent to be forwarded to its new foreign agent.

When old foreign agent received Binding Update Message from the new foreign agent to notify the mobile node's new location, it looks up its forwarding information base (FIB) to find a label of mobile node. If forwarding information base has a label of that mobile node, old foreign agent set up label switched path with existing traffic parameters for the mobile node to the new foreign agent. Therefore existing label switched path from an Ingress LER to an old foreign agent should be extended to the new foreign agent.

After signaling messages should be exchanged between old foreign agent and new foreign agent, it extends the current LSP by establishing a LSP between current foreign agent and new foreign agent by using above LSP extension method. During that time, old foreign agent buffers all the packets from and to the mobile node. Once the LSP is established, packets are sent along the new path to the mobile node.

Any tunneled datagrams for the mobile node that arrives at its previous foreign agent after the extended LSP has been created can then be re-tunneled to the mobile node's new foreign agent through the extended LSP. If there isn't any label to the destination mobile node at the old foreign agent, the old foreign agent should send user packets which are received from correspondent node to the new foreign agent by using IP-in-IP tunneling method.

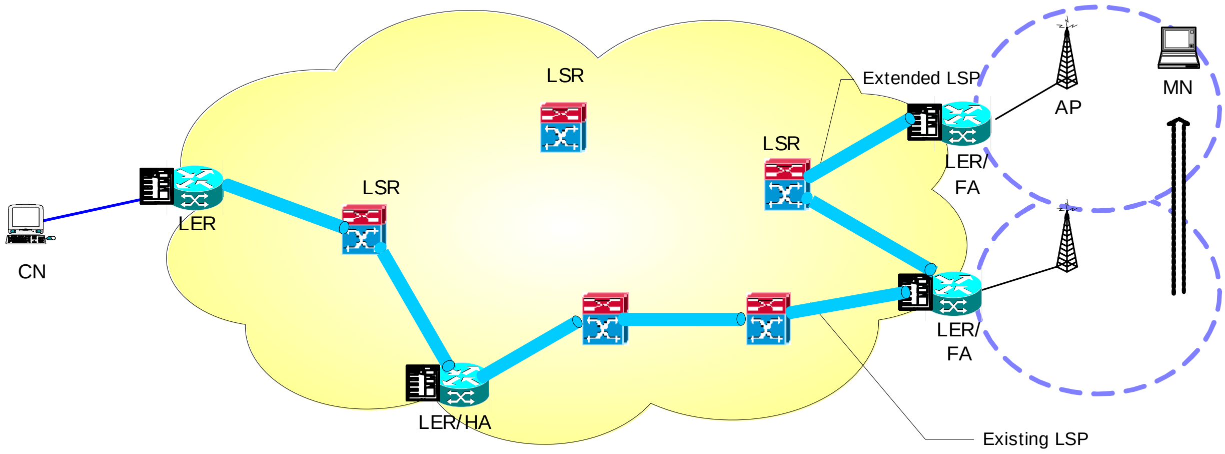


Figure 9. LSP Extension for mobile IP service for a time of handover

Whenever a mobile node migrates to an adjacent subnet, existing LSP from the Ingress LER to the old foreign agent is extended to the new foreign agent. When the Ingress LER receives a Binding Update Message in response to a Binding Warning Message or Binding Request Message, the Ingress LER should recognize that a destination mobile node migrate the new foreign agent. However, whenever a destination mobile node migrates, the Ingress LER shouldn't set up new LSP to the new foreign agent.

When the QoS of LSP tunnel is temporarily degraded, LSP re-establishment is triggered by the Ingress or Egress LERs. After LSP re-establishment, the route between the Ingress LER and new foreign agent can be optimized. Old path is torn down and new path is set up. If performance degradations are detected by comparing with the negotiated Forwarding Equivalence Classes, the LSP re-establishment message is initiated by the Ingress or Egress LERs. The detail measurement and judgment scheme of performance degradation are for further study.

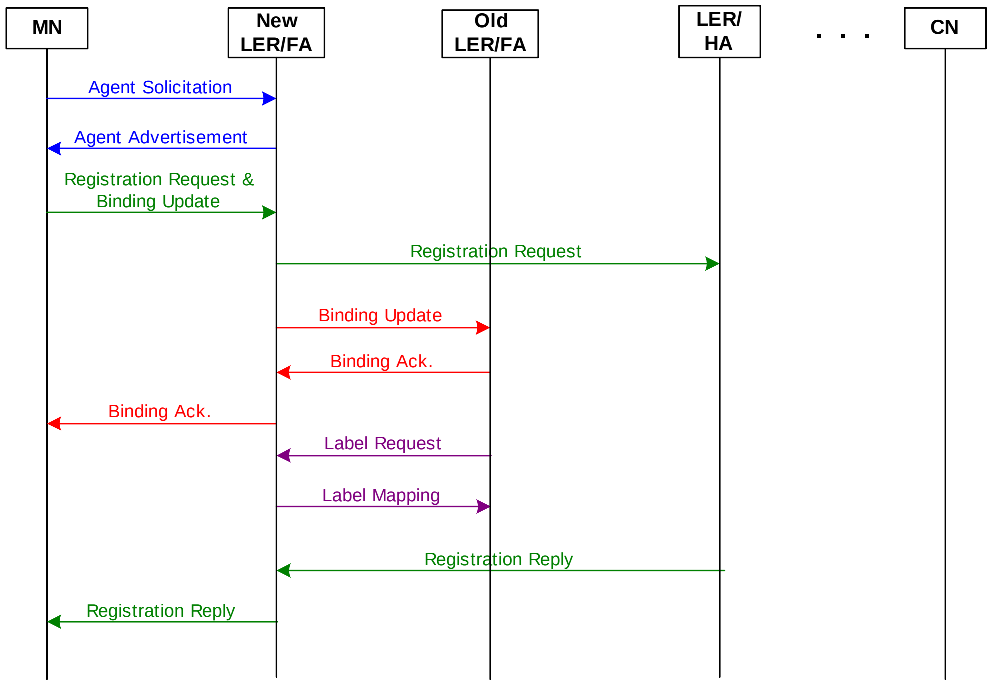


Figure 10. Message sequence chart for LSP extension

The LSP extension procedures in Figure 10 are as follows.

- A mobile node moves to a new foreign agent and sends a Registration Request and Binding Update message to new foreign agent.
- New foreign agent sends a Registration Request message to home agent and sends a Binding Update Message to the old foreign agent.
- When the old foreign agent received Binding Update Message, it responses with Binding Acknowledgement Message to the mobile node via the new foreign agent. And old foreign agent may send Label Request Message to the new foreign agent.
- A LSP is established between old foreign agent and new foreign agent when old foreign agent receives Label Mapping/Resv message.
- Then, a home agent sends Registration Reply message in response to the Registration Request.

1.4.2 LSP Optimization

Use of more than on care-of-address by a MN may be useful to improve smooth handoff when the MN moves from on wireless link to another. If each of these wireless links is connected to the Internet through a separate base station, such that the wireless transmission range from the two base stations overlap, the mobile node may be able to remain connected to both links while in the area of overlap. In this case, the MN could acquire a new care-of-address on the new link before moving out of transmission range and disconnecting from the old link. The MN may thus still accept packets at its old care-of-address while it works to update its HA and CNs, notifying them of its new CoA on the new link.

When a MN acquires new CoA while communicating with CN over legacy LSP, The MN sends Binding Update along with QoS Object to the CN for Route Optimization. The MN's LER receiving the Binding Update message will initiates REQUEST/PATH. Now the correspondent IPv6 node receiving the Binding Update message is able to send packets to MN directly while previous flow have been traversed over the legacy LSP. Which supports smooth handoff scheme over both legacy LSP and newly established QoS guaranteed LSP. The old LSP will be released automatically as time goes by because no more data transmitted over the LSP.

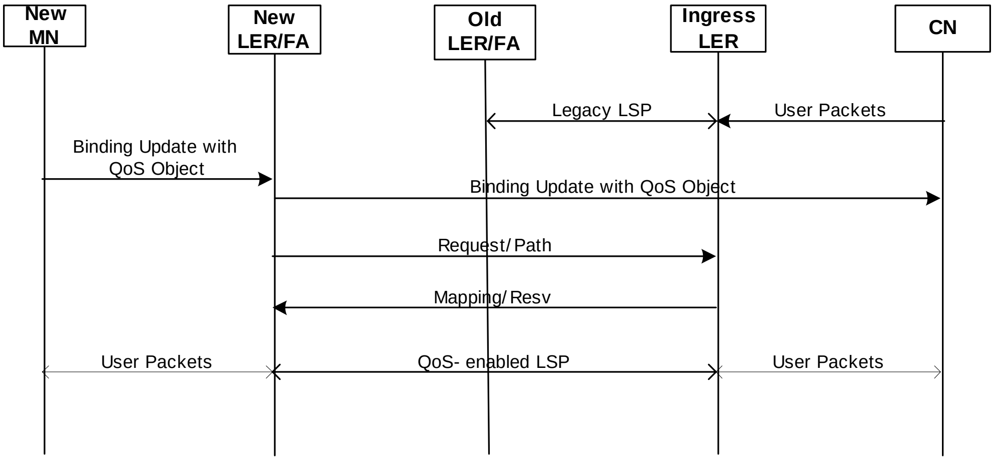


Figure 11. LSP optimization procedure

There are still lots of discussion to adopt appropriate handoff scheme. Our document keeps an eye on those emerging handoff algorithm and will adopt some of them to establish LSP between CN's LSR and MN's one. Thus above handoff support LSP scheme may change. For example, If a Handoff scheme use tunnel method between Old Access Router (AR) and New AR, Our scheme may evolve to setup extended LSP between Old AR and New AR. In this case MN can receive data through old LSP and extended LSP as well as newly established LSP associated new CoA.

1.4.3 LSP Optimization for Hierarchical MPLS

In a Mobile IPv4 Regional Registration, when a handover occurs, mobile node compares the new vector of care-of address with the old one. It chooses the lowest-level foreign agent that appears in both vectors, and sends a Regional Registration Request to that anchor foreign agent. Any higher-level agent need not be informed of this movement since the other end of its forwarding LSP tunnel still points to the current location of the mobile node.

A Registration Request is forwarded to the GFA by way of one or more intermediate RFA. When the Registration Request message arrives at the first FA, the foreign agent checks its visitor list to see if this mobile node is already registered with it. If it is not, the foreign agent checks which next higher-level RFA to relay the Registration Request to. The next RFA checks its visitor list to see if the mobile node is already registered with it. If it is not, the RFA relays the message to the next higher-level RFA in the hierarchy toward the GFA. This process is repeated in each RFA in the hierarchy, until an RFA recognizes the mobile node as already registered. This RFA may be the GFA, or any RFA beneath it in the hierarchy.

If the mobile node is already registered with this RFA, it will transmit the Registration Reply toward the lower-level RFA. When the lower-level RFA receives the Registration Reply, the RFA is able to point out the received Registration Reply so that the packet is associated with which mobile node. The RFA reads the information about mobile node entry equivalent to received Registration Reply, and recognizes the mobile node as the registered lower-level one. RFA will send Registration Reply message to the lower RFA. Above sequence is repeated up to the new FA of network that mobile node is moved to.

If there is an established LSP about the mobile node to the anchor RFA, it will send a Label Request/Path Message to the next lower-level RFA in the hierarchy. The lower-level RFA replies with an Label Mapping/Resv Message to the upper-level. The foreign agents should keep the binding table information of a label and home address of a mobile node about registered whole mobile nodes by assigning Label. On the all mobile nodes registered to foreign agent, it is necessary to assign label, and to maintain the binding table of home address and label of mobile node. When a Label Mapping/Resv Message from lower-level RFA arrives at upper-level RFA, the LSP would have been established. After RFA received the label from the lower-level one, it is necessary to modify the label mapping/Resv entry on the associated mobile node in the label table. The incoming label value of label mapping/Resv entry is unchanged as the received label value form the upper-level RFA, and outgoing label value is changed into new acquired label value from the new lower-level RFA through the Regional Registration method. And then, RFA will send a Label Request/Path Message to next RFA with the care-of address of the mobile node. When this Label Mapping/Resv Message arrives at RFA, the LSP would have been established. Above sequence is repeated up to the new foreign agent of network that mobile node is moved to. In this way, the LSP is newly established from anchor foreign agent to new foreign agent. In this LSP partial re-establishment method, since the LSP is maintained from home agent to anchor foreign agent and a new LSP is established from anchor foreign agent to new foreign agent, the LSP setup time is reduced compared with the MPLS-based Mobile IPv4 Tunneling Scenario (Scenario 1).

Packet is delivered from home agent to new foreign agent along the LSP by label swapping. New foreign agent receives the packet and looks up its label table. Since it is the egress point of the LSP from home agent to new foreign agent, new foreign agent strips off the label header and sends the packet to the IP layer. Finally new foreign agent as a border gateway router within the corresponding local domain forwards the packet to mobile node based on the newly added routing table. A mobile node receives the packet sent by correspondent node.

Figure 12 shows a example of Regional Registration and LSP optimization process for mobile IP service over hierarchical MPLS when the mobile node moves to new LER/FA.

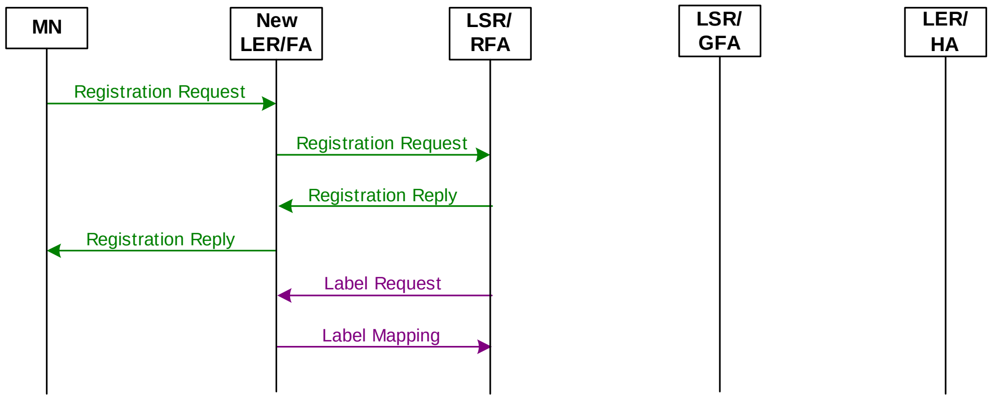


Figure 12. LSP optimization procedure at mobile IP over hierarchical MPLS during handover

In MPLS-based Hierarchical Mobile IPv4 network, additionally, it is necessary to clear the registration information on the old foreign agent and the upper-level RFA, and to release the LSP. If old locations are not deregistered, it is possible that tunnels are not correctly redirected when a mobile node moves back to a previous foreign agent.

The anchor RFA should send a Binding Update with a zero lifetime and Label Release Message to the previous care-of address it had registered for the mobile node. Each foreign agent receiving the Binding Update removes the mobile node from its visitor lists. And the LSP that is assigned between Upper-level foreign agents is released. The Binding Update and Label Release Message are relayed down to the new foreign agent and old foreign agent, respectively. Old foreign agent in the hierarchy receiving this notification removes the mobile node from its visitor list. A LSP that is established to old foreign agent is released by receiving Label Release Messages.

1.4.4 Other Considerations

- **Consideration of idle mobile nodes**

It notes that the most of wireless subscribers will not be actively communicating most of the time. Rather, wireless IP communicators will be switched on, ready for service, constantly reachable by the wireless Internet. The mobile nodes will be in an idle state but passively connected to the network. Thus LSP tunnel procedure is done that only active conditions of high layer applications are supposed to traverse over QoS guaranteed LSP. This will prevent LSP abusing that can be caused by lots of control packets.

- **QoS service interruption**

At the time of handover, interruption in QoS would occur if the packets sent by or destined to the mobile node arrive at the intermediate node without the information about their QoS forwarding requirement. Such QoS interruption must be minimized.

We consider two schemes, which should minimize the interruption in QoS. One is the scheme using multicast LSP. In this method, an anchor LSP establishes a LSP to the current LER/FA and all LER/FAs in the neighborhoods of the serving LER/FA. When data arrives for that mobile node, the anchor LSR multicast the data to all the MN's multicast group. If the mobile node moves to one of the neighboring location, data is immediately available.

The other is the method using bi-directional LSP tunnel between the FA/LER. In this scheme, LER/FA will establish bidirectional LSP to the neighbor LER/FA in advance. If the mobile node moves to the neighbor subnet, packets to the MN can be sent via bidirectional LSP tunnel between the LER/FA.

Related contributions

- D 172, WD11_CTS_31, WD11_CTS_32

Relevant Recommendation(s)

Status : Under study (July 2002, Chitose)

Living List #02 of Q.11/13

Title: An IP network architecture with out-of-band signaling

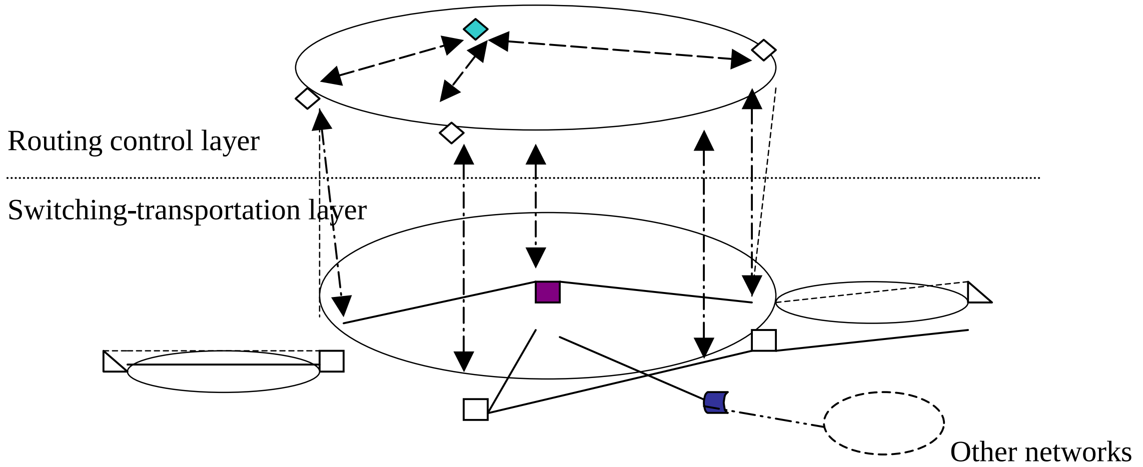
Description of the problem and possible solution

In order to solve or mitigate the problems of security, QoS and shortage of address space in Internet, a new IP routing and transport architecture is proposed. A description of the architecture is given, and then the advantages of the proposal are discussed. Some practical considerations are also mentioned.

The present IP networks are facing three problems: security, QoS and shortage of address space (IPv4). There is variety of proposals/solutions to solve these problems, but they are all problem specific until now. Here we offer a proposal to solve or mitigate all these problems with an architecture change of IP transport networks.

The proposed architecture can be described as follows:

- We are going to use out-band signaling instead of in-band signaling, i.e. the L3 IP packet will be separated, the user data (maybe also with a segmentation indicator) will be directly put into the lower layer (e.g. $L2^+$ MPLS layer) for switching / transportation. And the routing information in the IP header will be exchanged/delivered with appropriate signaling used to control the lower switching / transportation layer mentioned above.
- Together with out-band signaling, a two layer architecture is proposed for data transportation (see figure 1), including an end-to-end MPLS switching - transporting layer and a routing control layer. The former one consists of end-users, edge MPLS switches, transit MPLS switches and all the links to link them, which is controlled by the latter one. The routing control layer may be centralized with only one control server and signaling links linking to the switching-transporting layer; or distributed, consisting of a series of routing control servers (e.g. edge control servers and transit control servers) and signaling links.
- MPLS is going to be extended to user terminal, user network gateway or a LAN/community network gateway. In the access links, MPLS labels will be used to distinguish / identify user-data, signaling, OAM information, they are also going to be used to identify different users, different QoS and different IAPs/ISPs to access.
- In the public network access, only point-to-point and multipoint-to-point types of network structures between the user and the local switch are allowed, so that the users (information senders or callers) can be identified by the physical wire positions and/or ports. We can use this identification in user network access control / authentication to make the access control/authentication much more reliable. In case of mobile access, instead of physical wire/port identification, we can use a SIM card to identify user, and know the user's service profile with VLR-HLR signaling.
- With the control layer and out-band signaling, a service of calling line identification presentation (similar to CLIP of ISDN) or information sender identification presentation could be provided to remote hosts, so that the remote host can use them in user remote access control / authentication.
- Addressing is an important function of signaling. In this architecture, the address fields of the signaling could be various. If necessary, an addressing type sub-field and/or address length sub-field could be put into the signaling messages.



Legend:

□	Edge MPLS switch
■	Transit MPLS switch
◇	Edge routing controller
◆	Transit routing controller
◺	User terminal/user network
◖	Interworking function (IWF)
—·—·—·-	Switching control signaling
---------	Controller-controller signaling
--------------	User-network signaling
———	User data flow
—··—··—	Interworking connection

Figure1 – An IP Network with out-band signaling

Using this architecture and the identified functions mentioned above, the following results can be expected:

- The public network infrastructure, including all the switches and controllers will be controlled only by related signaling messages and OAM information, and managed by Administration. They are all non-accessible for ordinary user. So the safety of the public network infrastructure is guaranteed.
- The user identification could be used to replace or enhance the access authentication, and make the access control much more reliable. Besides, more security services, such as user behavior monitoring, user security credit data-base, etc. could also be provided for the security of end-to-end communication.
- In user plan, only two layers, i.e. MPLS and physical layer are needed. Lesser overhead and lesser processing could be expected, resulting better QoS.
- With out-band signaling, the problem of address space will also be solved. Because here the length of address is just a parameter of a signaling information element, it has nothing to do with the protocol. We can use whatever type of addressing needed, and whatever address length needed. In this case, IPv6 is no longer needed.
- With the separation of controlling and forwarding, more flexibility could be achieved with regard to the network organization and service providing. We can use one controller to control two or more switches, or partition one switch into several sub-switches to be controlled by several controllers. These are useful for the VPNs creation, switching capability renting service and/or trusteeship service.

Not only the new architecture can support connection-oriented services, but also connectionless services. In case of connectionless services, like a connection-oriented one, a signaling session should go first before the sending of each packet. But there is no need to have a connection finite state machine for the connectionless services.

The architecture can use all the developing MPLS technology, routing algorithm, and other existing technology and protocols. Some signaling protocols should be developed, but most of them can be created based on existing ones. The architecture has no effects to the upper layers above L3.

The interworking with the present IP network is needed, but not difficult. In the direction of the new one to the present one the job should be done by the IWF is just to merge the routing control information with the user data to create IP packets; And separating each IP packet in the opposite direction. Also we can use some specific LSPs in the new architecture, similar to a tunnel, to connect two separate IP networks of present type, or use a tunnel in the present IP network to connect two new IP networks with out-band signaling.
If this architecture is going to be considered, a work plan will be proposed for on-going jobs.

List of document addressing the issue

- D 162

Relevant Recommendation(s)

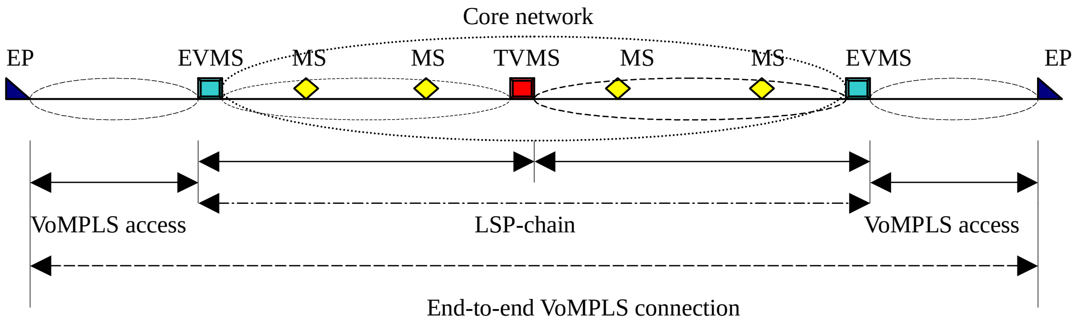
Status: Under study (Jan. 2002, Geneva)

Living List #3 of Q.11/13

Title: End-to-end Voice over MPLS

1 End-to-end Voice over MPLS Architecture

It says in the draft Y.vompls that "VoMPLS can be applied in both the core and access networks." But the access parts of the network are not shown clearly in Fig. 6.1. Here it is proposed to add a complete end-to-end VoMPLS connection in the draft, which consists of two access parts and a core LSP/LSP-chain.



Legends:

EP	End point
MS	Normal MPLS switch
EVMS	Edge MPLS switch with voice functions
TVMS	Tandem MPLS switch with voice functions

Figure 1- End-to-end VoMPLS connection

2 MPLS access /VoMPLS access

First of all, the concept of MPLS access should be made clear. But it is not the intention of this document to define the MPLS access. Here it is only assumed that the idea of MPLS could be similarly be used in access networks. It means that similar MPLS frame formats with labels could be used for packets delivering in the access. The number of the labels needed in a frame could be 0, 1 or more.

Based on this assumption, it is proposed to use similar formats of VoMPLS defined in Protocol X in the access networks. Several voice channels could be multiplexed onto one LSP, which connects a CPN/EP to an edge MPLS switch.

3 Function needed for MPLS switches to support VoMPLS

When VoMPLS frames, each of which consists of a number of channels going to different destinations, come to an edge MPLS switch, the switch should de-multiplex the frames and re-construct new VoMPLS frames according to their destinations of channels. We can call this frame re-construction (FRC).

FRC function can be equipped in an edge MPLS switch with voice handling capability, which is called as EVMS in Fig. 1, and also in a tandem VoMPLS switch, which is called as TVMS (See Fig. 1).

4 New control payload type for the control sub-frame

In order to support the FRC function, a new type of control payload of VoMPLS control sub-frames: "Label-Info" could be added, which is to carry the label information of a LSP to EVMS or TVMS for a relevant channel. This type of VoMPLS control sub-frame should send to the relevant EVMSs / TVMSs during the call establishment to tell the switches which output LSP is to be used for the relevant call/channel of a input VoMPLS frame with the same CID.

5 Control layer aspects

In order to support VoMPLS, some kind of call control and connection control functions and signalling capabilities should also be provided. The mechanism proposed in point 4 could well fit in with the architecture proposed in D.162. And it can also be used in other architectures.

6 Conclusion

In order to support end-to-end VoMPLS, an end-to-end voice over MPLS architecture, including the access, the FRC function for switches, and a new control payload type for FRC are proposed. It is hoped to be used to improve the draft recommendations: Y.vompls and Y.protocolx.

List of document addressing the issue

- WD11_CTS_02

Relevant Recommendation(s)

Status: Under study (July 2002, Chitose)

Living List #4 of Q.11/13

TITLE: SERVICE ARCHITECTURE CLASSIFICATION FOR LAYER 1 VPN

1. INTRODUCTION

This is not an agreed material at this Q11 meeting , but proposes enhancements to the architecture section in Y.l1vpnsdr.

2. SERVICE ARCHITECTURE CLASSIFICATION FOR LAYER 1 VPN

In order to support needed functions, the L1 VPN providing network must perform the following functions. Some of the functions can be optional.

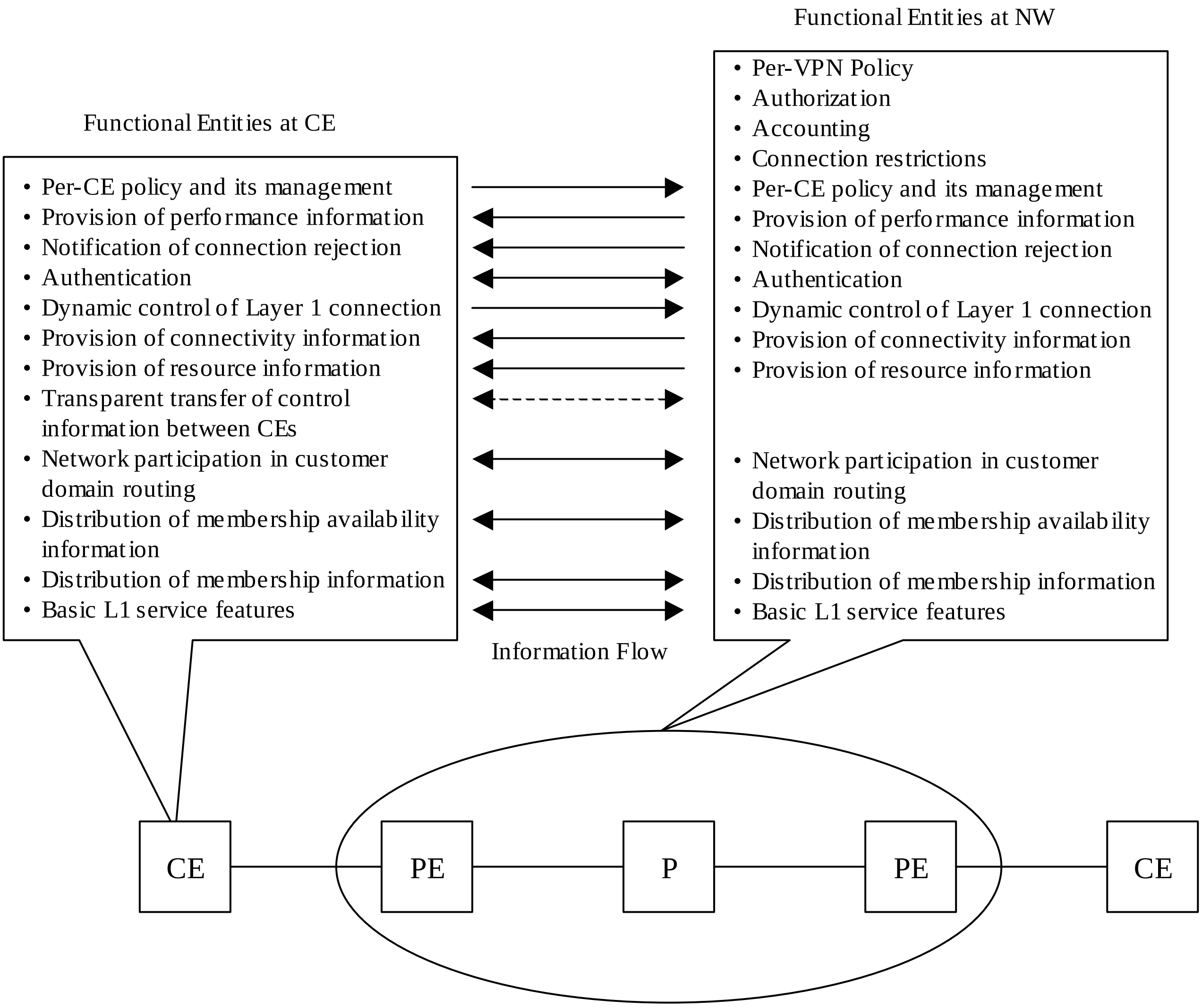

Functional Entities at NW
Per-VPN Policy
Authorization
Accounting
Connection restrictions
Per-CE policy and its management
Provision of performance information
Notification of connection rejection
Authentication
Dynamic control of Layer 1 connection
Provision of connectivity information
Provision of resource information
Network participation in customer domain routing
Distribution of membership availability information
Distribution of membership information
Basic L1 service features
Functional Entities at CE
Per-CE policy and its management
Provision of performance information
Notification of connection rejection
Authentication
Dynamic control of Layer 1 connection
Provision of connectivity information
Provision of resource information
Transparent transfer of control information between CEs
Network participation in customer domain routing
Distribution of membership availability information
Distribution of membership information
Basic L1 service features
Information Flow
CE
PE
P
PE
CE

Figure 1.1 L1 VPN reference model with functional entities

Based on functional implementations, the service functional architectures are classified into three categories in general. Note that an annex to this recommendation indicates example layer 1 specific implementation scenarios based on G.805 terminology.

(1) Distributed functional architecture

At least, some of the required functions are implemented and performed in a distributed manner. Like a layer 3 NB VPN example shown in Y.1311.1, where membership information and routing information distributed among PEs, this is an example of distributed functional architecture. As for the membership information, the entity having no direct connection with CEs, i.e., P, may not be aware of each VPN membership explicitly, but rather P must be able to distinguish VPNs by identifying VPNs. These functional requirements further differentiate categories of intra-VPN entities into PE and P. In this case, the figure 1.2 describes a functional architecture for the distributed model.

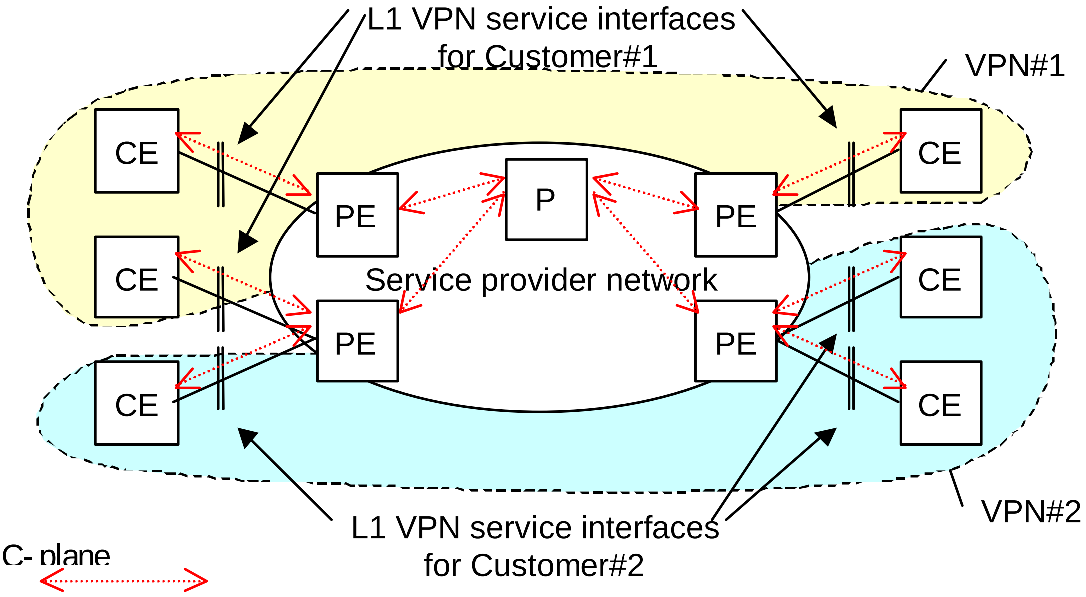


Fig 1.2 Distributed L1 VPN functional architecture

Editor's note: What functions are to be distributed requires further study.

(2) Centralized functional architecture

On the other hand, most of the functions can be performed by a single centralized entity within the L1 VPN providing network. The entity directly connecting the CE, if defined again as PE, then passes all the functional information from CE to the centralized entity and vice versa. This centralized entity can be called as the centralized provider entity, or CP. The figure 1.3 shows a functional architecture in the centralized manner.

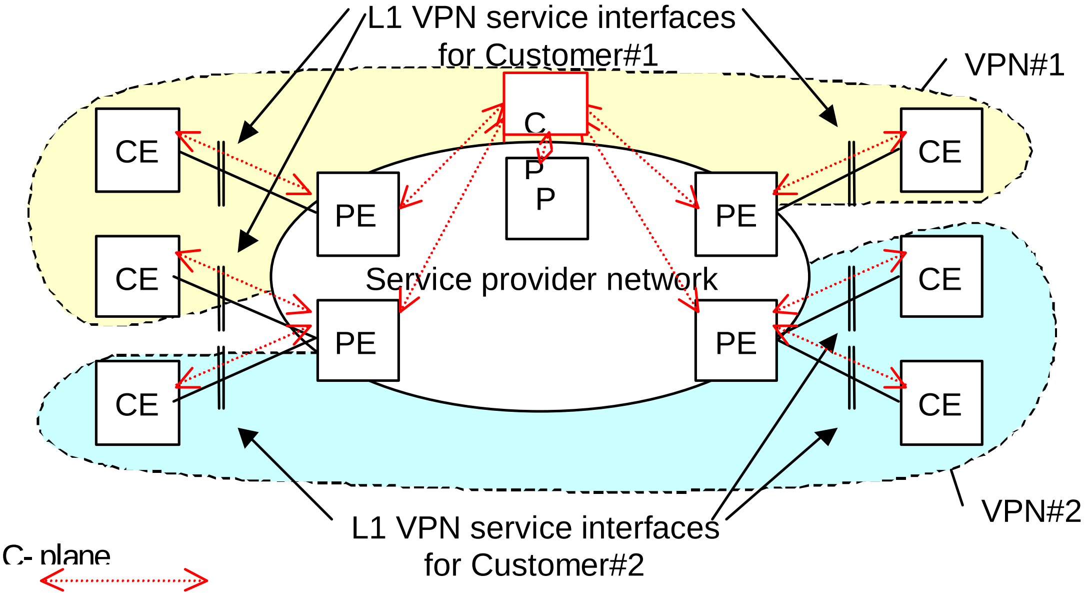


Figure 1.3 Centralized functional architecture for L1 VPN

Editor's note: What functions are to be centralized requires further study.

(3) Further functional architecture considering internal architectural possibility within CE

In addition, further decomposition can be possible when internal functional architecture is centralized for a single L1 connection at the CE-PE boundary. This is a special case because multiple CEs are connected to the network over a single L1 connection. In other words this is only valid for the U-plane shared case.

A typical example is that a centralized entity performs control functions required on behalf of more than one CEs connecting to the L1 VPN using a single L1 connection.
In some cases, this centralized (CE side) control entity, called as a centralized customer controller or CC, only transfers control information between CEs and the L1 VPN. In other cases, CC can participates in control functions but CEs are always controlled by the CC, the typical example of which is that these CEs are only for receiving connections from other CEs such as servers receiving access from active CEs.
Figure 1.4 shows this functional architecture with the distributed L1 VPN network functional architecture.

Editor's note: Text in paragraph 3 needs further work for concise and clearer description.

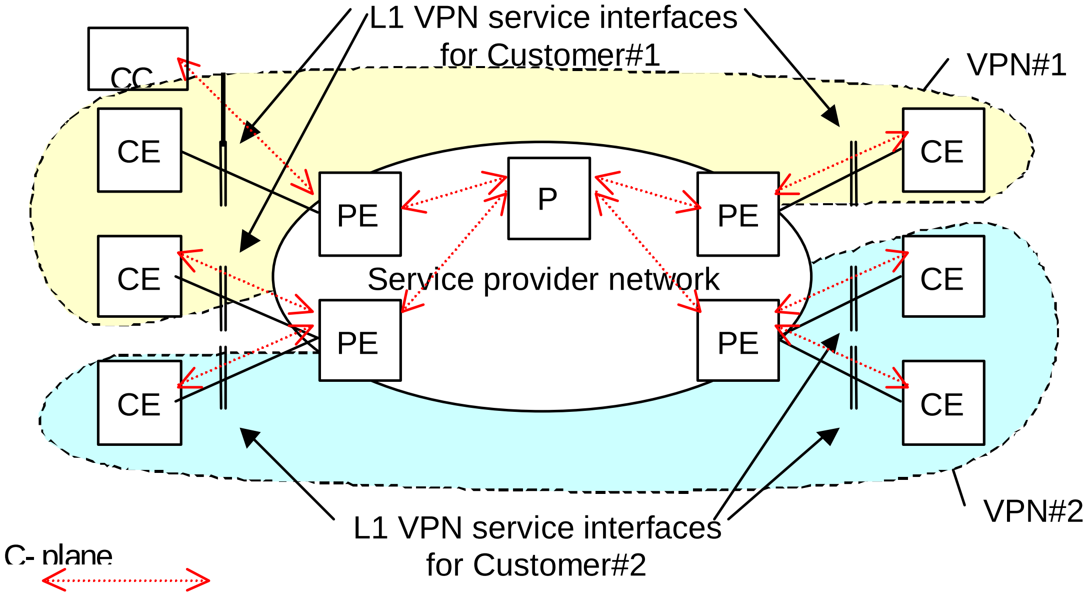


Figure 1.4 Hybrid functional architecture for L1 VPN

(Editor's note) Since this categorization is high level and generic, the number of categories should be kept as small as possible. In addition, various implementations can be slightly different from each other, but fundamental aspect can be the same. Therefore the draft recommendation should keep minimum required variety of service architectures. If needed annexes and appendices should be considered for further detailed examples and distinctions.

Editor's note: Next version will further clarify the functions.

Appendix I

Three implementations examples corresponding to three functional architectures

The appendix I shows example implementations for the three functional architectures.
(1) Implementation example for the distributed architecture
To be provided
(Editor's note) Some IETF drafts propose BGP/GMPLS based optical VPN where the distributed functional architecture can fit well.

(2) Implementation example for the centralized architecture
To be provided
(Editor's note) A classical network management architecture where a centralized OPS controls network entities can fit into this model.

(3) Implementation example for the decomposed CE type architecture
To be provided
(Editor's note) CR and CU examples corresponding to SG15 study may be needed for this case

List of document addressing the issue

Relevant Recommendation(s)

Y.l1vpnsdr

Status: Under study (Nov. 2002, Geneva)