TECHNISCHE UNIVERSITÄT DRESDEN

Mobility in IPv6

Thomas Liske

Dresden, 2005

Abstract

Classical IPv6 networks lack native support for mobile nodes. Mobile nodes are nodes which might change their point of attachment to the internet and still are reachable by a somewhat static IP address. With mobility support, higher level communication could be maintained while the mobile node moves around. The mobility extension presented here only takes care of ISO/OSI layer 3 which results in shortcomes on hand-over latency. In the last part of the paper we take a look on approaches to reduce hand-over latency, i.e. by considering layer 2 triggers.

Introduction

C. Perkins and D. Johnson presented in [1] a mobility extension for IPv6. Since nowadays mobile computers become more and more popular, it is import that the upcoming IPv6 takes care about the issues arising by mobile computers. Mobile computers, especially computers equipped with wireless network technology, might change their so called point of attachment to the internet while communicating with other nodes. As a result of changing the point of attachment without any mobility support established communication relations will break.

Terms and Definitions

To describe mobility support, the following terms (Fig. 1) are used. A *mobile node* could be any node which might change its point of attachment to the internet. The mobile node has a so called *home address* which is the node's IP address in its *home subnet*. The mobile node has to be reachable by its home address regardless where it is currently attached to the internet. The *care-of address* is the IP address in the network where the node is currently attached to.

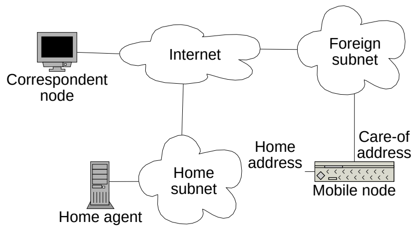

Figure 1: Terms in mobility

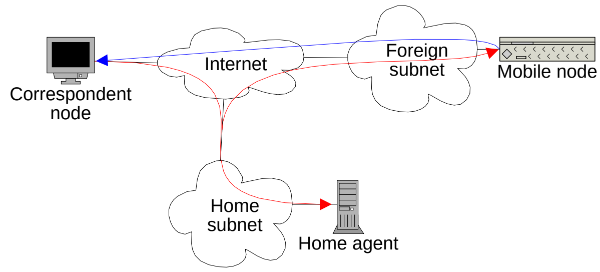

Figure 2: Triangle routing

The association between the home address and the care-of address of a mobile node is called *binding*. The so called *home agent* is located in the home subnet. It is responsible for forwarding packets which arrive for mobile nodes while they are away from their home subnet to the mobile node's actual point of attachment to the internet using the binding information.

A node which communicates with a mobile node is called *correspondent node* and might be itself either mobile or stationary.

Basic Operation

While a mobile node is away from its home subnet and connected to a foreign subnet, it has to maintain at least three different IP addresses, the link-local address and the care-of address of the subnet it is actually connected to and the home address from its home subnet. Each time the mobile node moves its point of attachment, it needs to configure a new link-local and care-of address according to the *IPv6 Neighbor Discovery protocol*[5]. A mobile node might have multiple care-of addresses whenever it is attached to multiple networks simultaneously.

Triangle Routing

Packets arriving for the mobile node at its home subnet while the node is away are forwarded by the home agent to the mobile node's new point of attachment. The mobile node itself could send packets directly to its destination. So we get the so called *triangle routing* problem (Fig. 2). This gives several problems like increased delay, increased network load on the home subnet and lack of scalability. This becomes even worse if two mobile nodes communicating with each other. So every IPv6 node is to be expected to support at least mobility functions for correspondent nodes to avoid all-time triangle routing.

Overview on IPv6

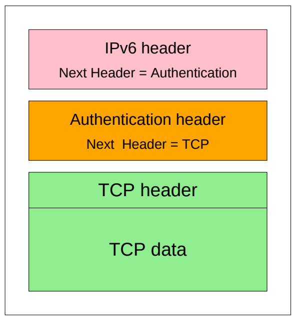

Figure 3: IPv6 packet headers

We will take a short look on some important properties of IPv6 [4] which are needed to understand the mobility extension. The well known change of IPv6 in respect to IPv4 is the increased size of the address space from 32 bits to 128 bits. This address space is separated in ranges like for the old IPv4 address space, the link-local addresses, unicast addresses and multicast addresses. Routing is done prefix based, as it was in IPv4.

The link-local addresses are non-routable and guaranteed to be unique on each network. They are used for direct host-to-host and multicast communication on the local network only. The link-local address is derived from the MAC address and some pseudo random number. Since this does not guarantee the address to be unique on the network, there is the IPv6 Duplicate Address Detection[5] protocol which must be performed by an IPv6 node before beginning to use a link-local address.

In change to IPv4, IPv6 has a fixed size header with aligned fields. The fixed size and the aligned fields increases the processing speed of IPv6 packets comparing to IPv4 packets in each hop. Additional there are optional extension headers which might occur in a defined order. For mobility support there are two important extension headers: the authentication header and the routing header.

The authentication header authenticates that the package really originates from a certain source node and was not altered during transmission using cryptography methods. The routing header is used to do loosely source routing. Loosely source routing means the sender could define hops the packet has to pass but not the whole route.

Mobile Node

The home agent forwards packets to the mobile node using IPv6 encapsulation. So mobile nodes must support IPv6 decapsulation. To inform the home agent about the actual binding between home address and care-of address the mobile node must be able to send so called *binding updates* and receive *binding acknowledgements*.

Binding Updates

A binding update tells the receiver the association of the senders home and care-of address. So the mobile node has to send a binding update whenever it changes its point of attachment to the internet to its home agent.

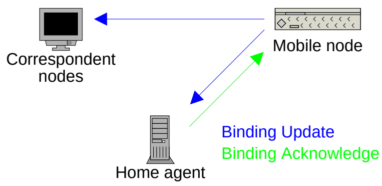

Figure 4: Binding updates

To prevent the triangle routing problem, it also should send binding updates to correspondent nodes when it receives the first encapsulated packet forwarded by the home agent. Although this is needed to prevent triangle routing, it is not necessarily needed if the mobile node wants to hide its actual point of attachment to a correspondent node.

When the mobile node changes its point of attachment, it has at first to configure a new link-local and a new care-of address. After doing so, it must update its binding at the home agent by sending binding updates. The mobile node will request a binding acknowledgement by the home agent to detect packet losses. The mobile node additionally sends binding updates to any correspondent nodes it is communicating with. Requesting correspondent nodes for sending binding acknowledgements is optional.

Correspondent Node

Since every IPv6 node might become a correspondent node, any IPv6 node must be able to process binding updates (and so sending binding acknowledgements if requested) and maintain a *binding cache*.

Before a node sends a packet, it has to check its binding cache looking for existing bindings between the destination address of the packet and the binding's home address. If there is an entry found, the node has to add an IPv6 routing header to the packet to route it via the mobile node's care-of address.

Home Agent

The home agent additionally needs to support IPv6 encapsulation used to tunnel packets to the mobile node's care-of address. When the home agent intercepts a packet with a mobile nodes home address as destination address, the home agent could not add an IPv6 routing header like a correspondent node since this would invalidate the IPv6 authentication header. Only the original sender is able to build a valid authentication header which authenticates the sender and the integrity of the packet.

So the home agent uses IPv6 encapsulation which means building an IPv6 packet around the packet which is to be forwarded. After the mobile node has arrived the encapsulated packet, it could decapsulate it and get the original packet back. Since this leads to triangle routing, it should only happen for the first few packages until the binding update sent by the mobile node has reached the correspondent node.

When a mobile node registers the binding at its home agent the first time, the home agent must send *Neighbor Advertisements*[5] for the mobile node's home address associating it with the home agent's link-local address. All nodes on the home subnet receiving the advertisements will update their destination cache entries accordingly. Since their may be correspondent nodes on the home subnet already using the mobile node's link-local address, the home agent needs to send additional *Neighbor Advertisements* for the mobile node's link-local address.

Additional the home agent should act as a proxy for the mobile node by replying to any received *Neighbor Solicitation*[5] messages for the mobile node's home address or link-local address.

Home Agent Discovery

The mobile node must know the IP address of the home agent. Since having one dedicated home agent gives a single point of failure and administrative effort on network reconfiguration, a possibility for dynamic home agent discovery is needed.

This is done by sending binding updates to a *IPv6 anycast address* of the home subnet. Nodes in the home subnet could register for anycast addresses. Whenever a packet for an anycast arrive on a border router, it is forwarded to one of the registered nodes of the address with the least routing cost. Since there is no guarantee that multiple packets to an anycast address arrives on the same node, the anycast address can not be used directly (else there might be multiple home agents maintaining bindings for the same home address with different care-of addresses at the same time).

Since the mobile node needs the actual home agent's IP address, the home agent rejects the binding update by sending a binding acknowledgement (there is a special flag in the binding acknowledgement indicating that the mobile node rejects the binding update). Since the home agent uses its normal unicast IP address for the binding acknowledgement, the mobile node gets aware of the home agent IP address and can proceed as normal.

Hand-over Procedure

The mobile node detects changes of its point of attachment by IPv6 router advertisements[5]. The node first has to generate a new local-link address. It has to do IPv6 duplicate address detection which takes at least one second. Next it has to configure a new care-of address using stateful or stateless address auto-configuration and might do an additional duplicate address detection. The last step is to send binding updates to the home agent and the corresponding nodes.

Router-Assisted Smooth Hand-offs

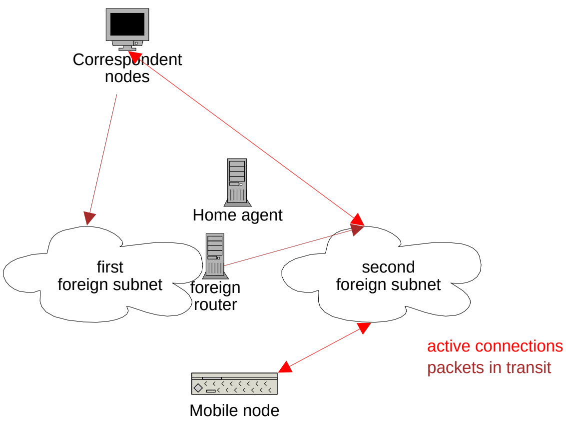

Figure 5: Smooth hand-offs

Today's 802.11 wireless lan technique can only maintain one link simultaneously. To reduce the packet loss when switching to another foreign subnet a mobile node could request a router in its old foreign subnet to act as a temporary home agent for it's old care-of address. So any packet still arriving to its old care-of address after the temporary home agent has been set up could be forwarded to the new care-of address. The binding might only has a small timeout since it is only important for packets still in transit to the old care-of address.

Hierarchical Mobile IPv6

The internet is divided in regions of local mobility, i.e. on the campus of an university. The region is managed by one administrative authority and may span over several subnets.

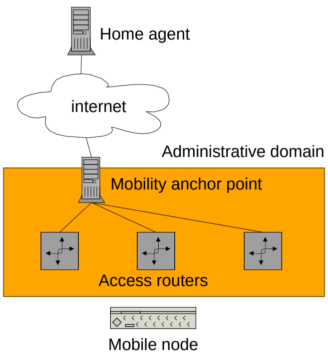

Figure 6: Hierarchical mobile IPv6

Such regions have only single or a small number of connections to the rest of the internet, so while the mobile node moves around inside the region packets are routed over the same external links. The idea of *hierarchical mobile IPv6* is to place so called *mobility anchor points* at the external links to reduce external signalling load while the mobile node moves only internally.

The mobile node detects the availability of hierarchical mobile IPv6 by *agent advertisements* sent to the networks. If such an advertisement is detected, the mobile node can do a *regional registration* to its home agent in two different modes.

Basic Mode

In *basic mode*, each mobile node acquires two care-of addresses. The on-link care-of address is an IP address from the subnet behind the *access router* the mobile node is connected to. The regional care-of address is taken from the mobility anchor point's subnet. The mobility anchor point acts as a home agent for the regional care-of address. This solution does not scale for the regional care-of addresses, so it is not suitable for larger setups.

Extended Mode

In *extended mode* the mobile node only acquires an on-link care-of address. The mobility anchor point keeps a binding between the home address and the on-link address and must encapsulate arriving for the mobile node.

Fast Hand-over

The mobility extension for IPv6 does only take care about ISO/OSI layer 3. To reduce the time needed for hand-over there are the fast hand-over approaches which additional looks on layer 2 to anticipate and detect changes of the point of attachment.

We introduce three different *L2 triggers*. There are the *link up* and *link down* trigger which occur whenever a link becomes available or not. Additional there is the *L2 hand-over start* trigger. On wireless links this trigger might occur whenever the signal strength drops below a given threshold.

Anticipated Hand-over

In the *anticipated hand-over* mode the mobile node begins to negotiate a new care-of address when a L2 hand-over start trigger occurs (steps 1 and 2, Fig. 7). When the trigger is forwarded to the current access router it must contain an identification of the target access router. After the current access router has received the trigger, it assigns an IP address for the mobile node in the new subnet and sends this information to both the mobile node (step 3a) and the target access router (step 3b). The target access router has to check if the address is unique on the subnet and send the validation result to the current access router. If the address is valid, the current access router sends a confirmation into both subnets (step 5). So when the mobile node switches to the target subnet it can immediately use the new care-of address and send binding updates to its home agent and correspondent nodes. To reduce packet loss, the old access router should act like a temporary home agent for the old care-of address for a short time.

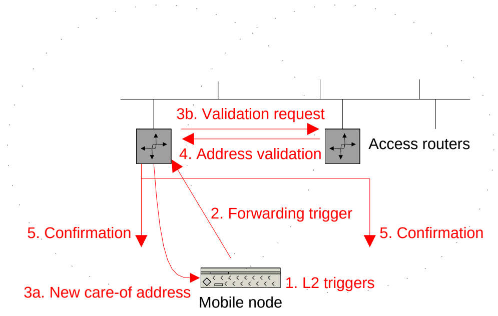

Figure 7: Anticipated hand-over

Tunnel Based Hand-over

In the *Tunnel Based Hand-over* mode the assignment of a new care-of address is delayed when the mobile node moves to a new access router. The mobile node only performs a L2 hand-over and continues to use its old care-of address in the new subnet.

Therefore the old and the new access router need to set up a bidirectional tunnel from the L2 triggers. Packets sent in the new subnet but originating from the old care-of address of the mobile node are captured and forwarded to the old access router. Packets arriving for the mobile node on the old subnet take the reverse path from the old to the new access router. The mobile node will later register a new care-of address in parallel with its normal communication. If the L2 triggers occur on the access router side, the mobile node movement can be detected without exchanging any packets with the mobile node but between the access routers. Since sending packets on wireless networks is more expensive than sending on wired networks, this is an interesting issue.

Conclusions

The presented mobility extension for IPv6 is as lightweight as possible and uses only a minimized control traffic. But it must be deployed into all IPv6 nodes to prevent triangle routing.

Since the mobility extension only looks on ISO/OSI layer 3, the hand-over latency is just to high for real-time application. So using hierarchical mobile IPv6 inside administrative domains or fast hand-over could help to reduce the hand-over latency.

References

[1] C. Perkins and D. Johnson
Mobility Support in IPv6
Proceedings of MobiCom'96, 1996

[2] C. Perkins, D. Johnson and J. Arkko
Mobility Support in IPv6
Network Working Group, RFC 3775, Jun 2004

[3] N. Montavont and T. Noël
Handover Management for Mobile Nodes in IPv6 Networks
IEEE Communications Magazine, pages 38–43, Aug 2002

[4] S. Deering and R. Hinden
Internet Protocol, Version 6 (IPv6) Specification
Network Working Group, RFC 2460, Dec 1998

[5] T. Narten, E. Nordmark and W. Simpson
Neighbor Discovery for IP Version 6 (IPv6)
Network Working Group, RFC 2461, Dec 1998