Project designation

VDL Mode 4 Network Sweden

Document title

POINT-TO-POINT SYSTEM ARCHITECTURE

DOCUMENT CHANGE RECORD

Revision	Changes	Date	Responsible
A	For NEWSKY	2009-04-21	Lars Gustafsson

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.

TABLE OF CONTENTS

1 SCOPE 4

1.1 SYSTEM OVERVIEW 4
1.2 REFERENCES 4
1.3 TERMS AND ABBREVIATIONS 4

2 SYSTEM ARCHITECTURE 7

2.1 FUNCTIONAL OVERVIEW 7
2.2 DEPLOYMENT VIEW 7
2.3 VDL 4 COMMUNICATION SERVICE 8
2.4 VME 9
2.5 GROUND IPV6/VDL 4 TUNNEL FUNCTION 10
2.6 MOBILE IPV6/VDL 4 TUNNEL FUNCTION 11
2.7 IPV6 COMMUNICATION SERVICE 12
2.7.1 HoA assignment 12
2.7.2 Mobility 12
2.7.3 Security 18
2.7.4 Network design 18

3 APPENDIX A - IPSEC/IKE IMPLEMENTATION 19

3.1 INTRODUCTION 19
3.2 ASSUMPTIONS 19
3.3 GENERAL 19
3.4 GROUND-GROUND 19
3.5 AIR-GROUND 19
3.6 APPLICATION-LEVEL END-TO-END 20
3.7 MOBILITY ACCESS 20

LIST OF FIGURES

FIGURE 1. FUNCTIONAL OVERVIEW 7
FIGURE 2. DEPLOYMENT VIEW 8
FIGURE 3. VDL 4 COMMUNICATION SERVICE 9
FIGURE 4. VME 10
FIGURE 5. GROUND IPV6/VDL4 TUNNEL FUNCTION 11
FIGURE 6. MOBILE IPV6/VDL4 TUNNEL FUNCTION 12
FIGURE 7. MS CONNECTED TO SUBNETWORK ANNOUNCED AT GS1 13
FIGURE 8. MS CONNECTED TO SUBNETWORK ANNOUNCED AT GS2 BEFORE BU IS COMPLETED 14
FIGURE 9. MS CONNECTED TO SUBNETWORK ANNOUNCED AT GS2 AFTER BU IS COMPLETED 14
FIGURE 10. APPLICATION DATA EXCHANGE 15
FIGURE 11. MNW CONNECTED TO ROUTER AT GS1 16
FIGURE 12. MNW CONNECTED TO ROUTER AT GS2 BEFORE BU IS COMPLETED 16
FIGURE 13. MNW CONNECTED TO ROUTER AT GS2 AFTER BU IS COMPLETED 17
FIGURE 14. APPLICATION DATA EXCHANGE 18
FIGURE 15. NETWORK DESIGN 18

LIST OF TABLES

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.

TABLE 1-1. TERMS.....5
TABLE 1-2. ABBREVIATIONS.....5

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.

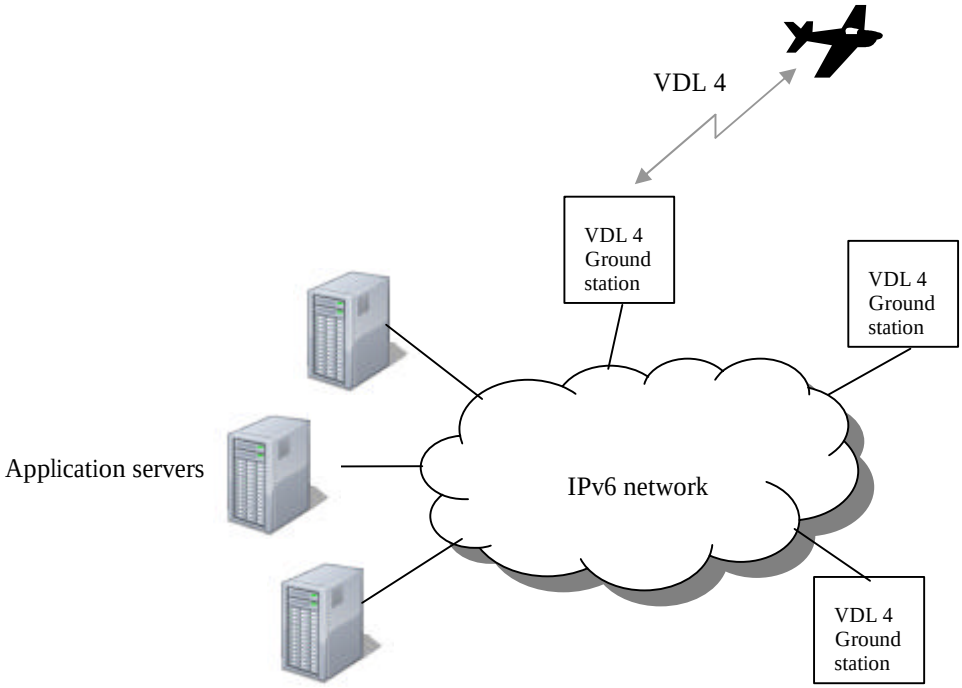
1 SCOPE

This document describes the architecture of the point-to-point communication functionality in the Swedish VDL Mode 4 network.

1.1 System Overview

The point-to-point communication service is based on IPv6 with support for node mobility. The node mobility is supported according to both the Mobile IPv6 standard and the Network mobility extension.

The VDL Mode 4 (VDL 4) communication standard, see [2] and [3], provides the link layer functions for ground-air communication with mobile stations.



1.2 References

[1] Manual for the ATN using IPS Standards and Protocols, Draft Doc 9896, version 15, September 17, 2008.
[2] Electromagnetic compatibility and Radio spectrum Matters (ERM); VHF air-ground Digital Link (VDL) Mode 4 radio equipment; Technical characteristics and methods of measurement for ground-based equipment; Part 4: Point-to-point functions, EN 301 842–4, V1.2.1
[3] Electromagnetic compatibility and Radio spectrum Matters (ERM); VHF air-ground and air-air Digital Link (VDL) Mode 4 radio equipment; Technical characteristics and methods of measurement for aeronautical mobile (airborne) equipment; Part 4: Point-to-point functions, EN 302 842–4, V1.2.1
[4] RFC3775 - Mobility Support in IPv6
[5] RFC2460 - Internet Protocol, Version 6 (IPv6) Specification
[6] RFC3963 - Network Mobility (NEMO) Basic Support Protocol

1.3 Terms and Abbreviations

The terms and abbreviations used in this document are defined in Table 1-1.

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.

Table 1-1. Terms.

Term	Definition
Application processor nodes	These are standard computers connected to the IPv6 network.
Binding	Association between a Home address and a Care of address for a Mobile node
Care of address	The IPv6 address of the Mobile node while visiting a foreign network
Correspondent node	A peer node with which a Mobile node is communicating. The Correspondent node may be either mobile or stationary
Home address	An IPv6 address out of the Mobile node's home network
Home agent	A router on the home network which represents the Mobile node while it is not attached to the home network
Mobile network	A network segment or subnet that can move and attach to arbitrary points in the routing infrastructure
Mobile node	An IPv6 network node that can change its point of attachment while still being reachable via the Home address
Mobile router	A Mobile network can only be accessed via specific gateways called Mobile routers that manage its movement
Mobile station	This is a VDL 4 transceiver and a processor (EFB) for executing mobile applications. The EFB's IPv6 stack implements a Mobile node
VDL 4 Ground station	This is a computing node connected both to an IPv6 and an IPv4 network. The ground stations are equipped with a VDL 4 transceiver.
VME processor node	This is a standard computer connected to the IPv4 network

Table 1-2. Abbreviations.

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.

Term	Definition
ANSP	Air Navigation Service Provider
CoA	Care of address
CN	Correspondent node
CDPLC	Controller Pilot Data Link Communications
DLS	Data Link Service, the protocol layer entity providing the point-to-point communication protocol in VDL 4
EFB	Electronic Flight Bag (a computer adapted to the avionics environment)
HA	Home agent
HoA	Home address
ICAO	International Civil Aviation Organization
IPsec/IKE	Internet Protocol security (IPsec) and the Internet Key Exchange (IKE) protocol
IPS	Internet Protocol Suite
IPv6	Internet Protocol version 6
IPv4	Internet Protocol version 4
LME	Link Management Entity, the protocol layer entity providing link management functions
MAC	Media Access Control
MN	Mobile node
MNW	Mobile network
MPLS	Multiprotocol Label Switching
MR	Mobile router
MSP	Mobility Service Provider
NEMO	Network Mobility
NSCOP	Network Setup Connection Protocol
VDL	VHF (Very High Frequency) Digital Link
VME	VDL Management Entity
VPN	Virtual private network
WiFi	Certification applied to products compatible with the IEEE 802.11 standards, also known as WLAN

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.

2 SYSTEM ARCHITECTURE

2.1 Functional overview

The point-to-point communication function in the VDL Mode 4 network is based on the principles specified in [1].

The end-to-end addressing and routing of application data, are according to the Mobile IPv6 communication standard specified in [4]. The VDL 4 communication service, see [2], is used as a link layer in the communication with the airborne part of the IPv6 network. The VDL 4 link layer provides a bi-directional tunnel for IPv6 packets destined to and arriving from the mobile IPv6 nodes in the network.

The VDL 4 air-ground links are managed by the VDL Management Entity (VME).

The functional blocks and their relationships are presented in Figure 1.

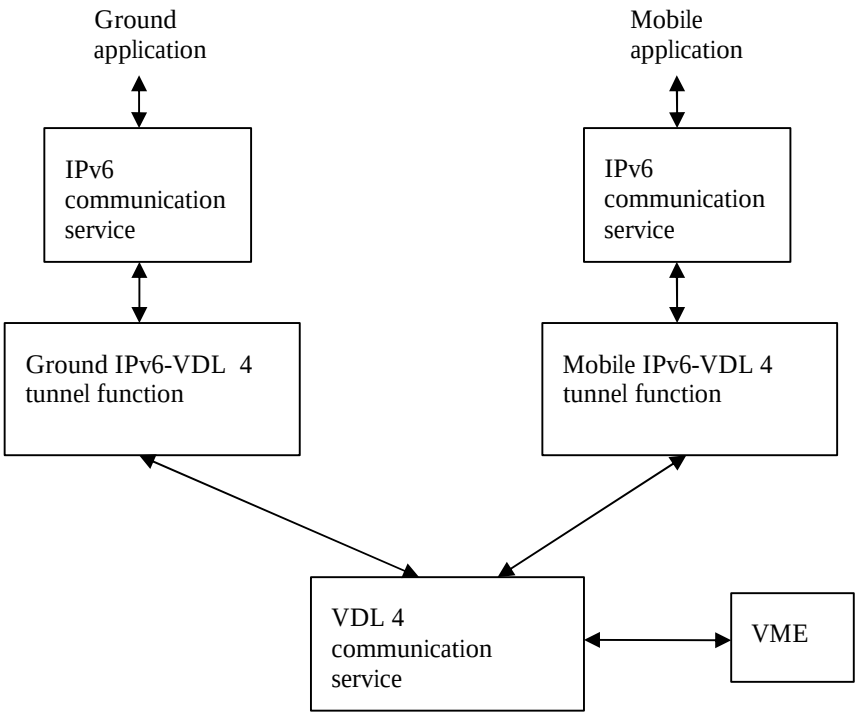


Figure 1. Functional overview

2.2 Deployment view

The communication functions described in the previous chapter are deployed to a network of computing nodes, see Figure 2.

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.

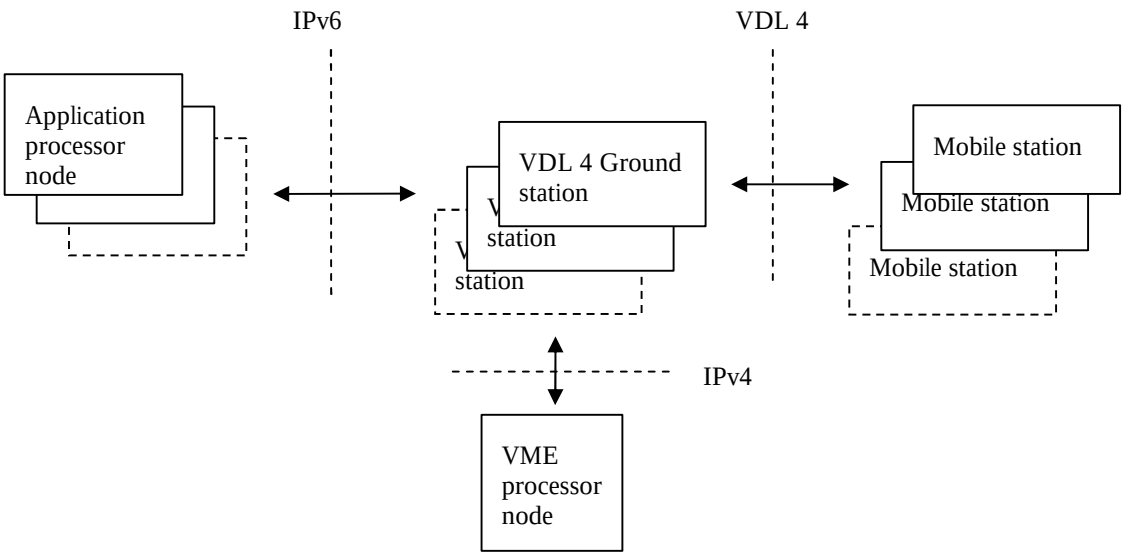


Figure 2. Deployment view

The computing nodes are:

- VDL 4 Ground stations - connected both to an IPv6 and an IPv4 network. The ground stations are equipped with a VDL 4 transceiver.
- Application processor nodes – this is standard computers connected to the IPv6 network.
- The VME processor node – this is a standard computer connected to the IPv4 network
- Mobile station – this is a VDL 4 transceiver and a processor (EFB) for executing mobile applications.

The ground applications execute on the Application processor nodes. The applications communicate with mobile applications, executing on the Mobile stations, over the IPv6 communication service.

The IPv6 communication service is executing on the Application processor nodes, the VDL 4 Ground stations and on the Mobile stations.

The VDL 4 communication service executes on the VDL 4 Ground stations and on the Mobile stations. It provides the link layer functions that interconnect the ground part of the IPv6 network with the mobile part.

The Ground and Mobile IPv6/VDL 4 tunnel functions provide the link layer interfaces for the IPv6 communication service on the VDL 4 Ground stations and on the Mobile stations.

The VDL 4 air-ground links are managed by the VME function executing on the VME processors node. The VME communicates with the VDL 4 Communication service, executing on the ground stations, over IPv4.

2.3 VDL 4 communication service

The VDL 4 communication service is responsible for providing the following communication services for applications executing on the VDL 4 Ground stations and on the Mobile stations:

- VDL 4 broadcast communication at the DLS level, see [2]
- Air-ground (NSCOP) point-to-point communication at the DLS level, see [2].

Ground station and Mobile station applications access the broadcast and point-to-point communication services in the VDL 4 Transceiver.

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.

The VDL 4 Communications service is also responsible for providing an interface to the VME, based on IPv4, for link management, see chapter 2.4.

The deployment of the VDL 4 Communication service (shaded circles) and important interfaces are presented in the figure below.

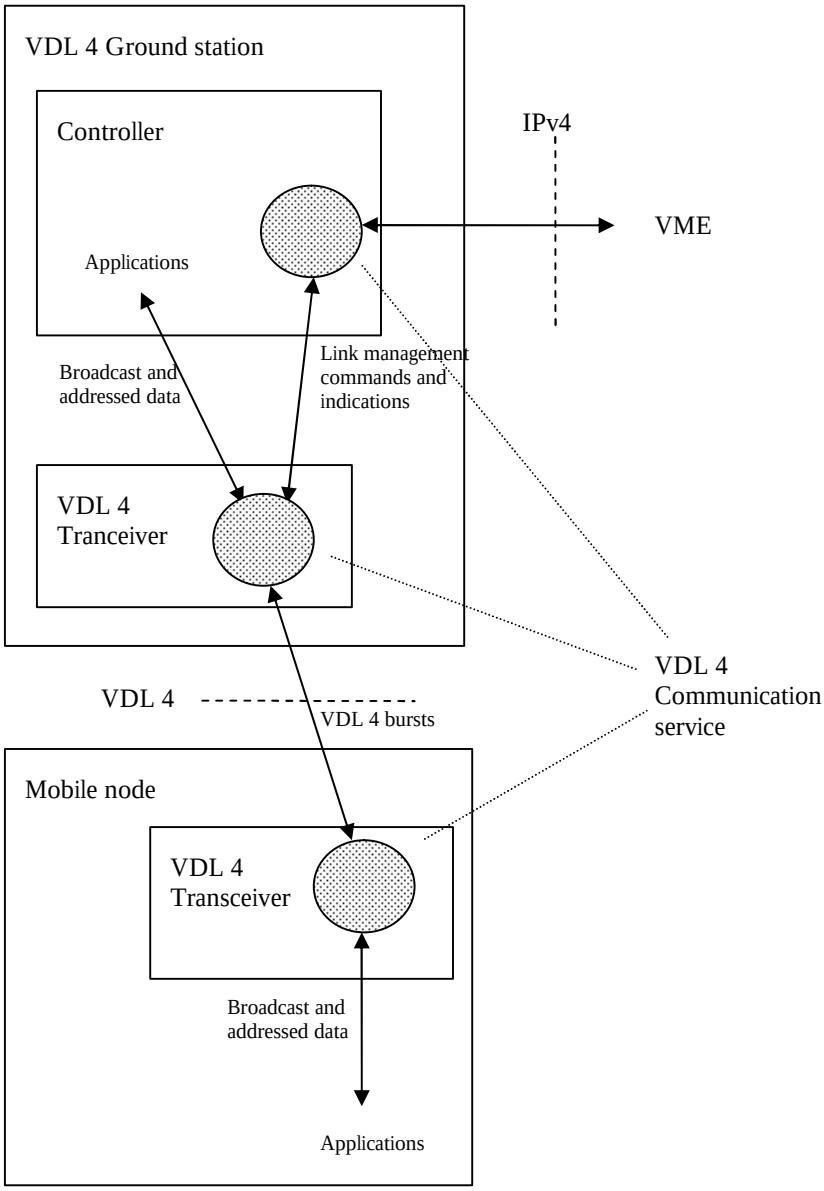


Figure 3. VDL 4 Communication service

2.4 VME

The following definitions from the ETSI standard for VDL 4, see [2], are used in this chapter:

- Ground system - a network of VDL 4 Ground stations.

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.

- Mobile system - a mobile VDL 4 station.
- NSCOP – Network Setup Connection Protocol, the point-to-point link between a Mobile system and a Ground system

The VME is responsible for the VDL 4 link management functions for a single Ground system.

The purpose of the VME is to ensure reliable link-layer connectivity between a Mobile system and the Ground system, while the mobile is in coverage of an acceptable VDL 4 Ground station.

The VME continuously monitors alternative VDL 4 Ground stations for the Mobile system's NSCOP links. The VME shall move the link, i.e. initiate a handoff, if a "significantly better" ground station becomes available.

The definition of "significantly better" is implemented in the VME's Handoff decision algorithm.

The VME consists of the following components:

- VDL4 Link Management Entity (LME) – This component manages the link state of all NSCOP links in the Ground system and provides access to the link management functions in the VDL 4 Communication service.
- Handoff decision function (HO) – This component continuously monitors the contents of the HO decision information base and ensures that each Mobile system is connected to the VDL 4 Ground station with the "best" prerequisites to handle communication.
- HO decision information base – This component manages the information, e.g. ADS-B information, which provides the basis for the handoff decision.

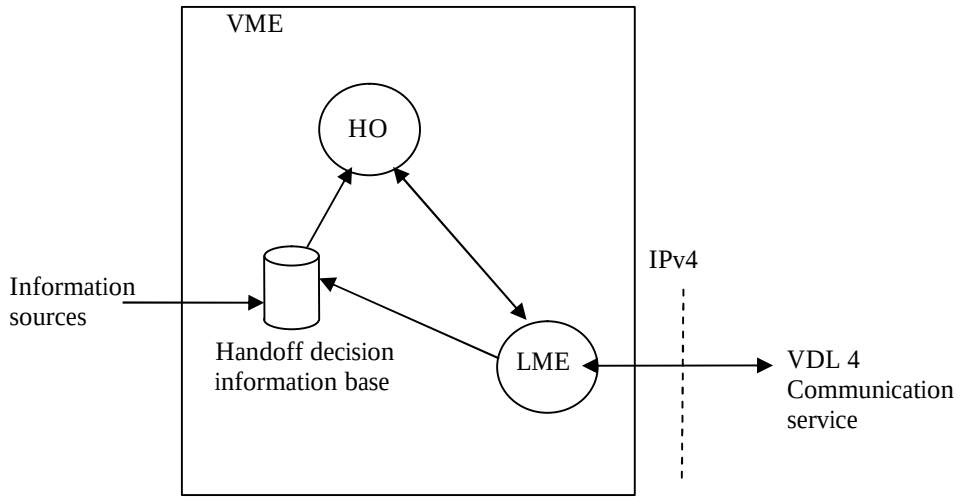


Figure 4. VME

2.5 Ground IPv6/VDL 4 tunnel function

The Ground IPv6/VDL 4 tunnel function interfaces the link layer, provided by the VDL 4 Communication service, to the IPv6 communication service on the VDL 4 Ground station.

The link layer is represented as a virtual network interface configured in the ground station's IPv6 stack. The Ground IPv6/VDL 4 tunnel function is responsible for providing the routing information that allows the IPv6 stack to route packets to this network interface. Only packets destined to IPv6 nodes on Mobile stations with an NSCOP link to this ground station will be routed.

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.

The Ground IPv6/VDL 4 tunnel function handles packets received from the virtual network interface differently depending on which type of IPv6 addressing that is used:

- In addressed packets, the VDL 4 station address of the Mobile station's VDL 4 Transceiver, is included as a part of the Home Address, see chapter 2.7. The packet is sent to the mobile with this station address on the corresponding NSCOP link managed by the VDL 4 Communication service.
- The multicast packets are broadcasted using the broadcast function of the VDL 4 Communication service.

The IPv6 packets received on the managed NSCOP links are sent directly to the virtual network interface for routing and delivery by the IPv6 communication system.

The NSCOP links available at a particular ground station is provided by the VME.

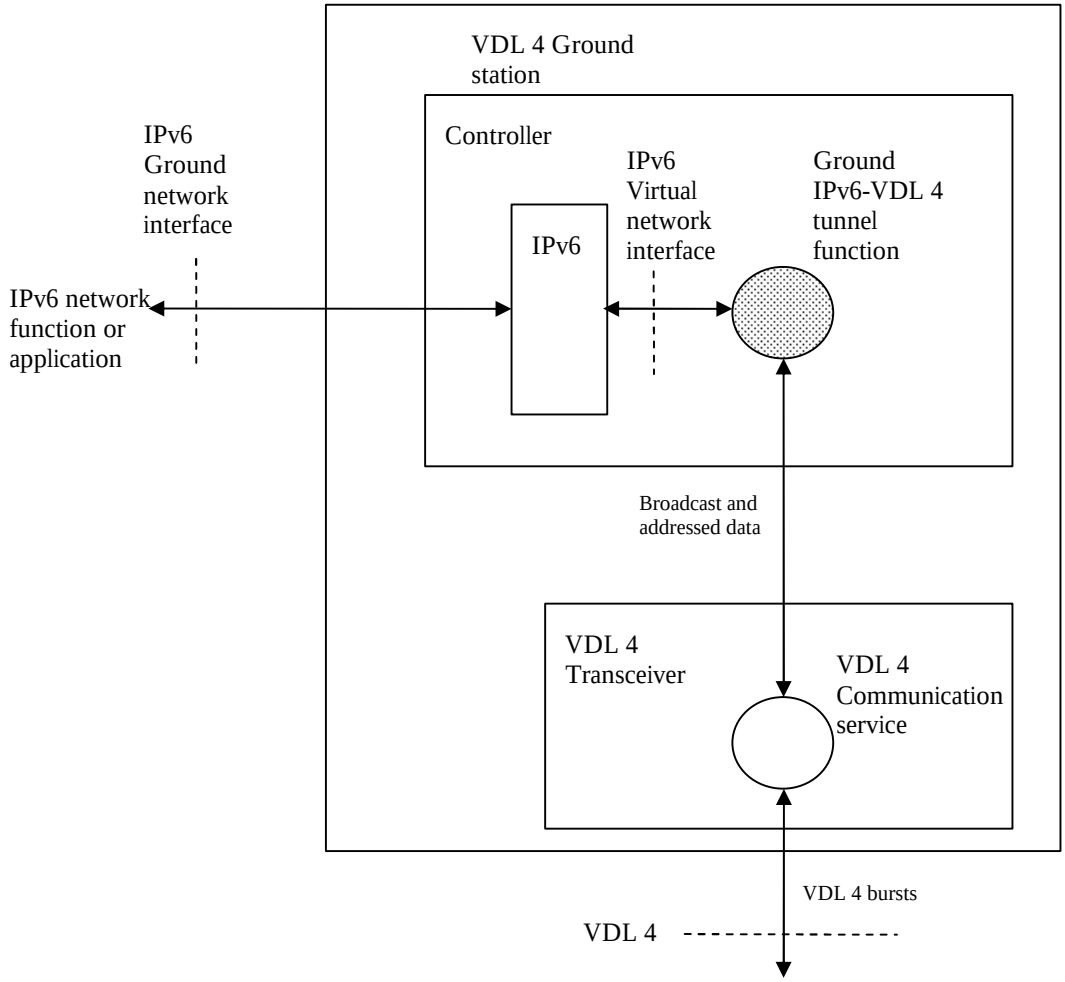


Figure 5. Ground IPv6/VDL4 tunnel function

2.6 Mobile IPv6/VDL 4 tunnel function

The Mobile IPv6/VDL 4 tunnel function interfaces the link layer, provided by the VDL 4 Communication service, to the IPv6 communication service on the Mobile station.

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.

The link layer is represented as a virtual network interface in the EFB's IPv6 stack. The Mobile IPv6/VDL 4 tunnel function is responsible for providing the routing information that allows the IPv6 stack to route all packets, destined to IPv6 nodes in the ground network, to this network interface.

The Mobile IPv6/VDL 4 tunnel function passes all packets received from the virtual network interface directly to the NSCOP link managed by the VDL 4 Communication service.

The IPv6 packets received from the VDL 4 Communication service either on the NSCOP link or broadcasted from the VDL 4 Ground station at the other end of the NSCOP link, are sent directly to the virtual network interface for routing and delivery by the IPv6 communication system.

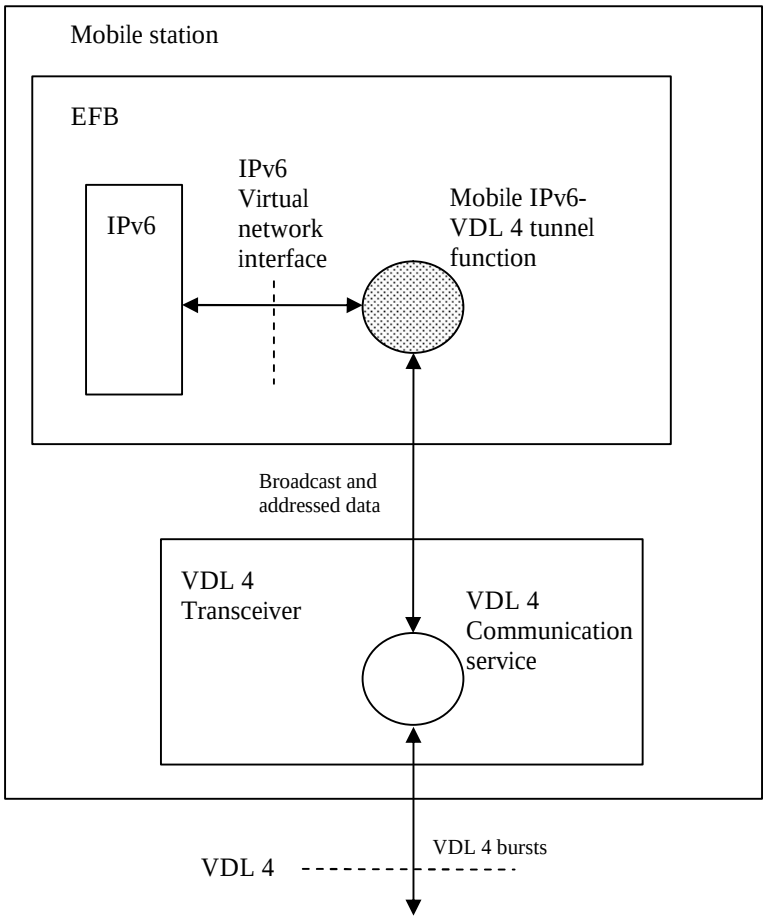


Figure 6. Mobile IPv6/VDL4 tunnel function

2.7 IPv6 communication service

The specification of the IPv6 communication service is in [5].

2.7.1 HoA assignment

Mobile nodes are assigned HoAs according to [1] and the description in chapter 2.7.4.

2.7.2 Mobility

Two types of mobility mechanisms will be supported:

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.

- Node-based mobility (Mobile IPv6) - the mobility management signalling is performed by the node requiring mobility itself, the principles are specified in [4].
- Network mobility (NEMO) – the mobility management signalling is performed by a Mobile router on behalf of a Mobile network, the principles are specified in [6]. This is an extension of Mobile IPv6.

The NEMO extension is backward compatible with Mobile IPv6, i.e. a NEMO-compliant Home Agent can operate as a Mobile IPv6 Home Agent.

2.7.2.1 Node-based mobility

The Mobile node is responsible for determining when its Binding is invalid, i.e. when the VME has moved the NSCOP link to another VDL 4 Ground station, and to perform a Binding update with the Home Agent.

The IPv6 stack in the VDL 4 Ground stations are each assigned a unique IPv6 subnet, a Care-of-address network, which is announced in periodic Router advertisements multicasted to that subnet.

The Mobile nodes use this information to trigger a Binding update with a CoA assigned by the Mobile node.

The CoA is composed from the subnet id, provided by the Router advertisement, and a unique identity managed by the EFB, e.g. the MAC address of one of its physical network interfaces.

2.7.2.1.1 Mobility scenario

The scenario is illustrated in the sequence of pictures below.

In Figure 7 the Mobile station (MS) is connected at the link layer (VDL 4 NSCOP) with the VDL 4 Ground station GS 1. The link layer connection is used to tunnel IPv6 packets, see chapter 2.5 and 2.6.

The MS has initiated a Binding update associating its Home address with a Care-of-address on the subnet announced with Router advertisements by GS 1 (1).

The MS is approaching GS 2 which is announcing its subnet (2).

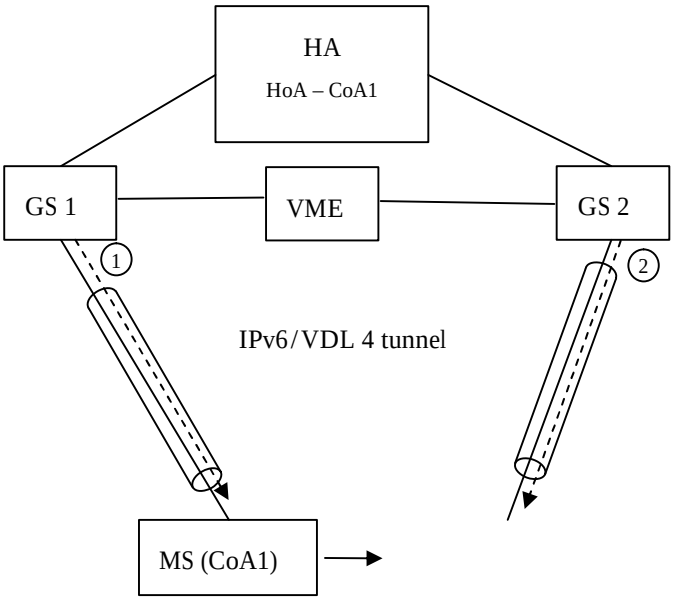


Figure 7. MS connected to subnetwork announced at GS1

In Figure 8, the VME has moved the NSCOP link to GS2 (3). The Router advertisements from GS 2, announcing its subnet, are received by the MS. The MS detects that it has been moved to a new subnet and triggers a Binding update (4).

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.

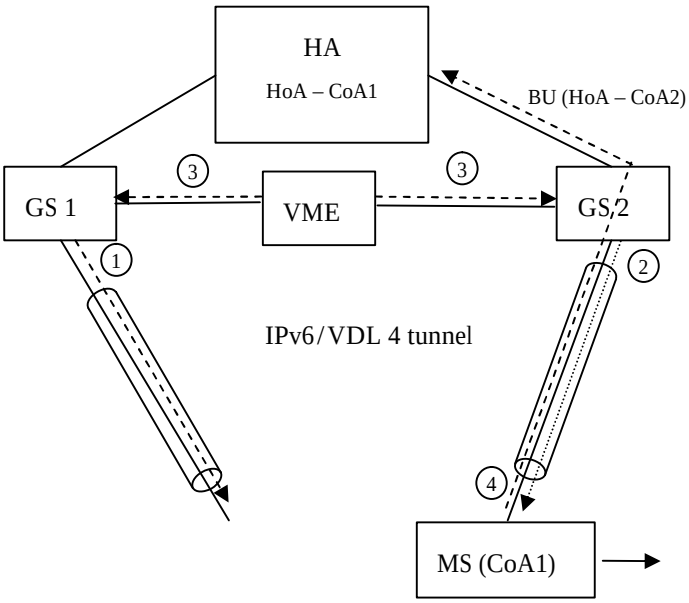


Figure 8. MS connected to subnetwork announced at GS2 before BU is completed

In Figure 9, the BU has been completed and the Home Agent has associated the MS' Home address with a Care-of-address on the subnet announced by GS 2.

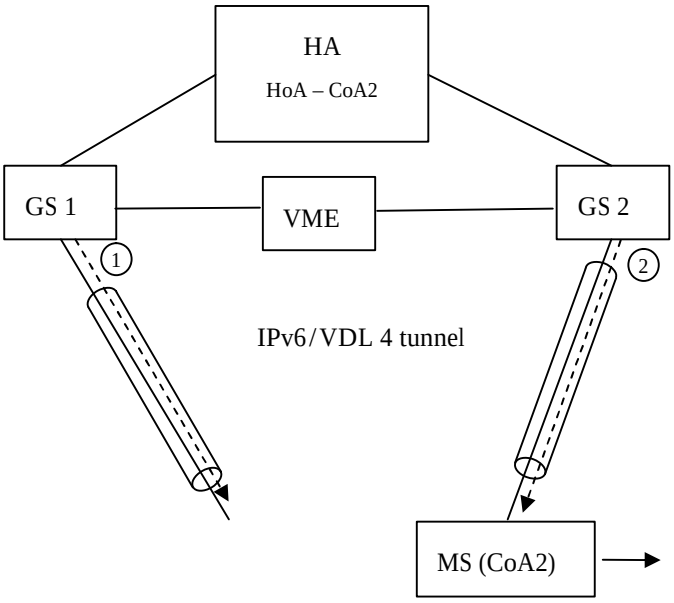


Figure 9. MS connected to subnetwork announced at GS2 after BU is completed

2.7.2.1.2 Application data forwarding scenario

The data originating from the Correspondent node, i.e. an Application processor node in chapter 2.2, is addressed to the Mobile node's HoA, Assuming that a Binding is available, the HA intercepts and forwards packets that arrive for the MN via an IPv6/IPv6 tunnel to its CoA.

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.

The Mobile station (MS) is connected at the link layer (VDL 4 NSCOP) with the VDL 4 Ground station GS. The link layer connection provides a second layer of tunnelling.

Traffic in the reverse direction follows the same path through the tunnel to the HA for forwarding to the CN via standard routing.

The principles are presented in Figure 10.

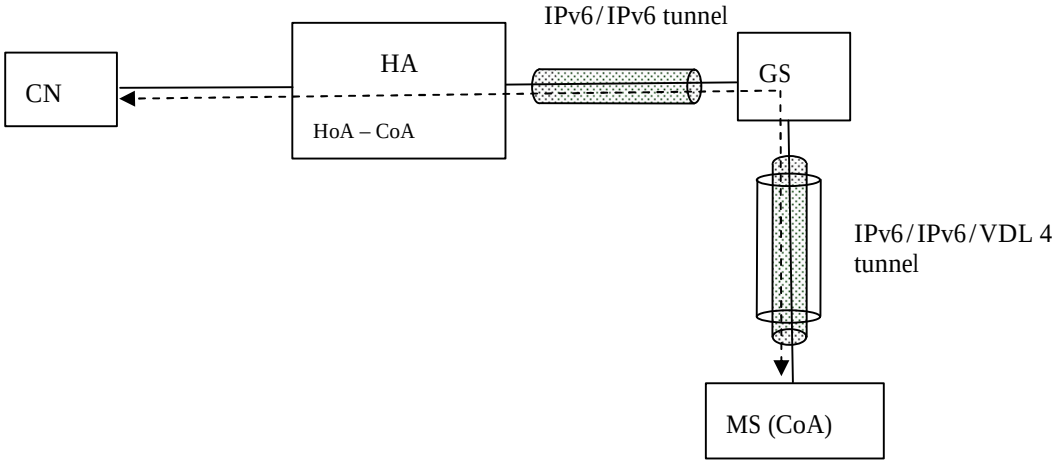


Figure 10. Application data exchange

2.7.2.2 Network mobility

When the Network mobility extension is used, the IPv6 stack in the VDL 4 Ground stations serves as a router to multiple Mobile networks (MNWs), each represents the EFB's IPv6 stack in a Mobile station. The Ground IPv6/VDL4 tunnel function, see chapter 2.5, is responsible for adding or removing routing information, to reflect the current set of Mobile networks connected with NSCOP links to the ground station.

The VDL 4 Ground station takes over the role from the Mobile node as responsible for the Binding update. The Binding is in this case valid for an entire Mobile network, rather than an individual node, c.f. chapter 2.7.2.1. The router sends a Binding update that includes the address prefixes for the connected Mobile networks. The set of address prefixes are provided by the Ground IPv6/VDL4 tunnel function. A Binding update is triggered when the set of Mobile networks connected to the VDL 4 Ground station is changed.

2.7.2.2.1 Mobility scenario

The scenario is illustrated in the sequence of pictures below.

In Figure 11 the Mobile network (MNW) is connected at the link layer (VDL 4 NSCOP) with the VDL 4 Ground station GS 1. The link layer connection is used to tunnel IPv6 packets, see chapter 2.5 and 2.6, addressed to nodes in the MNW.

The router at GS 1 has associated the address prefix of the MNW with its own address at the Home Agent. The bi-directional IPv6/IPv6 tunnel, responsible for forwarding data to and from the nodes on the MNW, has been established between the HA and the router at the ground station.

The MNW is approaching GS 2.

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.

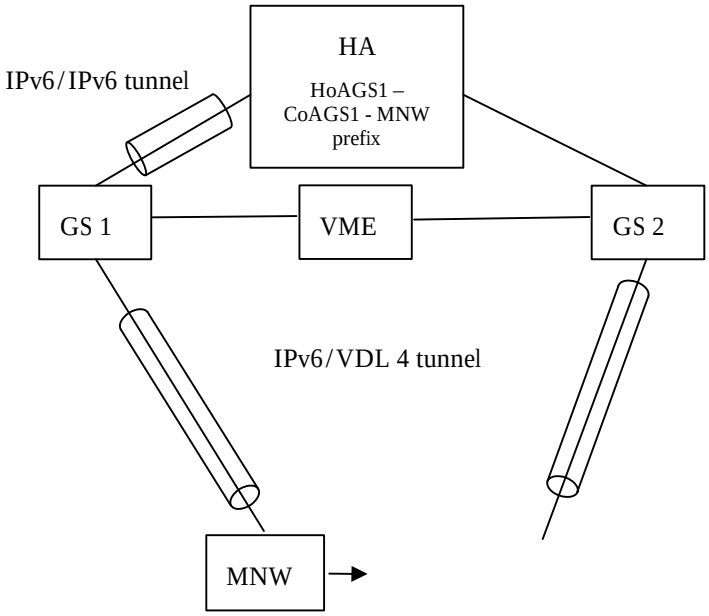


Figure 11. MNW connected to router at GS1

In Figure 12, the VME has moved the NSCOP link to GS2 and informs the Ground IPv6/VDL 4 tunnel functions at GS 1 and GS 2 of the change (1).

The Ground IPv6/VDL 4 initiates a Binding update (2) that associates the MNW prefix with GS 2.

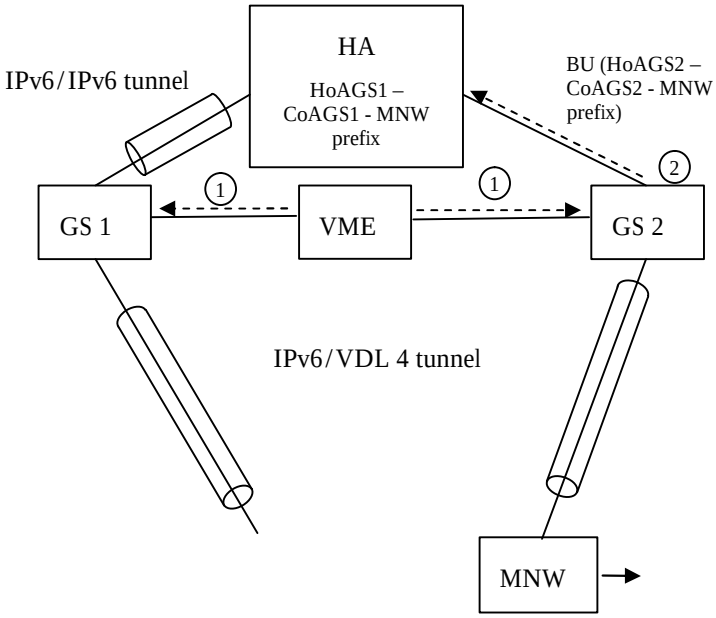


Figure 12. MNW connected to router at GS2 before BU is completed

In Figure 13, the BU has been acknowledged and the Home Agent has associated the MNW prefix with the address of GS 2 and established the bi-directional IPv6/IPv6 tunnel with the router at GS 2. The Ground IPv6/VDL 4 tunnel function at GS 2 has provided the IPv6 stack with routing information for MNW.

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.

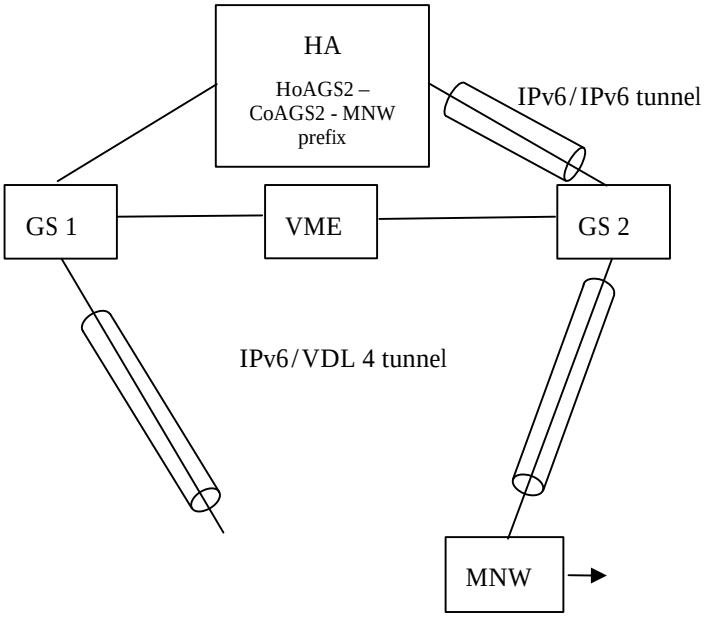


Figure 13. MNW connected to router at GS2 after BU is completed

2.7.2.2.2 Application data forwarding scenario

The data originating from the Correspondent node, i.e. an Application processor node in chapter 2.2, is addressed to a node in the MNW. Assuming that a Binding to the MNW prefix is available, the HA forwards packets that arrive for the MNW to the MN via an IPv6/IPv6 tunnel to the router specified by the Binding, i.e. the router at GS.

The router removes the outer IPv6 encapsulation and routes the packet (1) according to the destination address of the inner IPv6 encapsulation and the routing information set up by the Ground IPv6/VDL 4 tunnel function, see chapter 2.7.2.2.1.

The MNW is connected at the link layer (VDL 4 NSCOP) with the VDL 4 Ground station GS. The Ground IPv6/VDL 4 tunnel function forwards the packet across the NSCOP link to the MNW

Traffic in the reverse direction is forwarded to the Mobile-station end of the tunnel. When a packet with a source address belonging to the MNW prefix is received by the ground station, the router reverse-tunnels the packet to the Home Agent (1) through the IPv6/IPv6 tunnel mentioned earlier. The Home Agent removes the outer IPv6 encapsulation and forwards the packet to the IPv6 network. The packet is then routed to the CN via standard routing.

The principles are presented in Figure 14.

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.

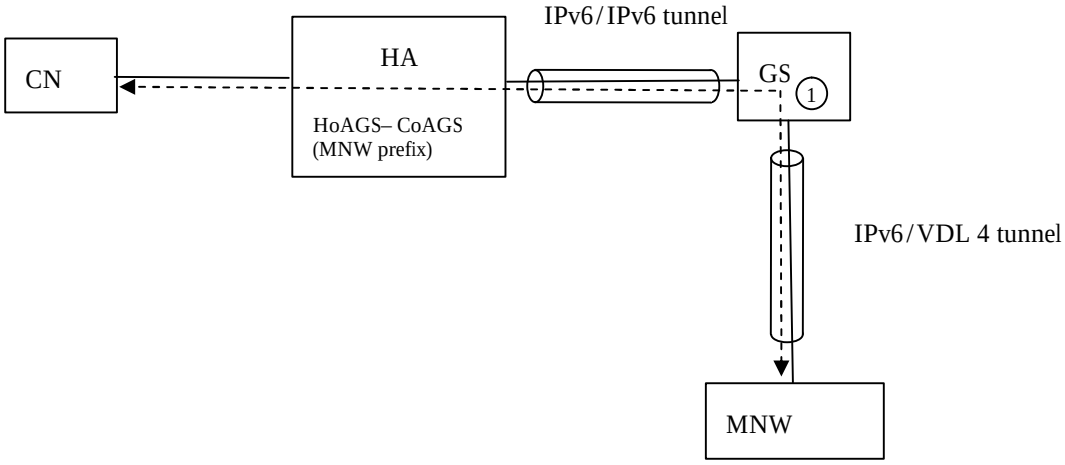


Figure 14. Application data exchange

2.7.3 Security

See Appendix A.

2.7.4 Network design

The network design is presented in Figure 15.

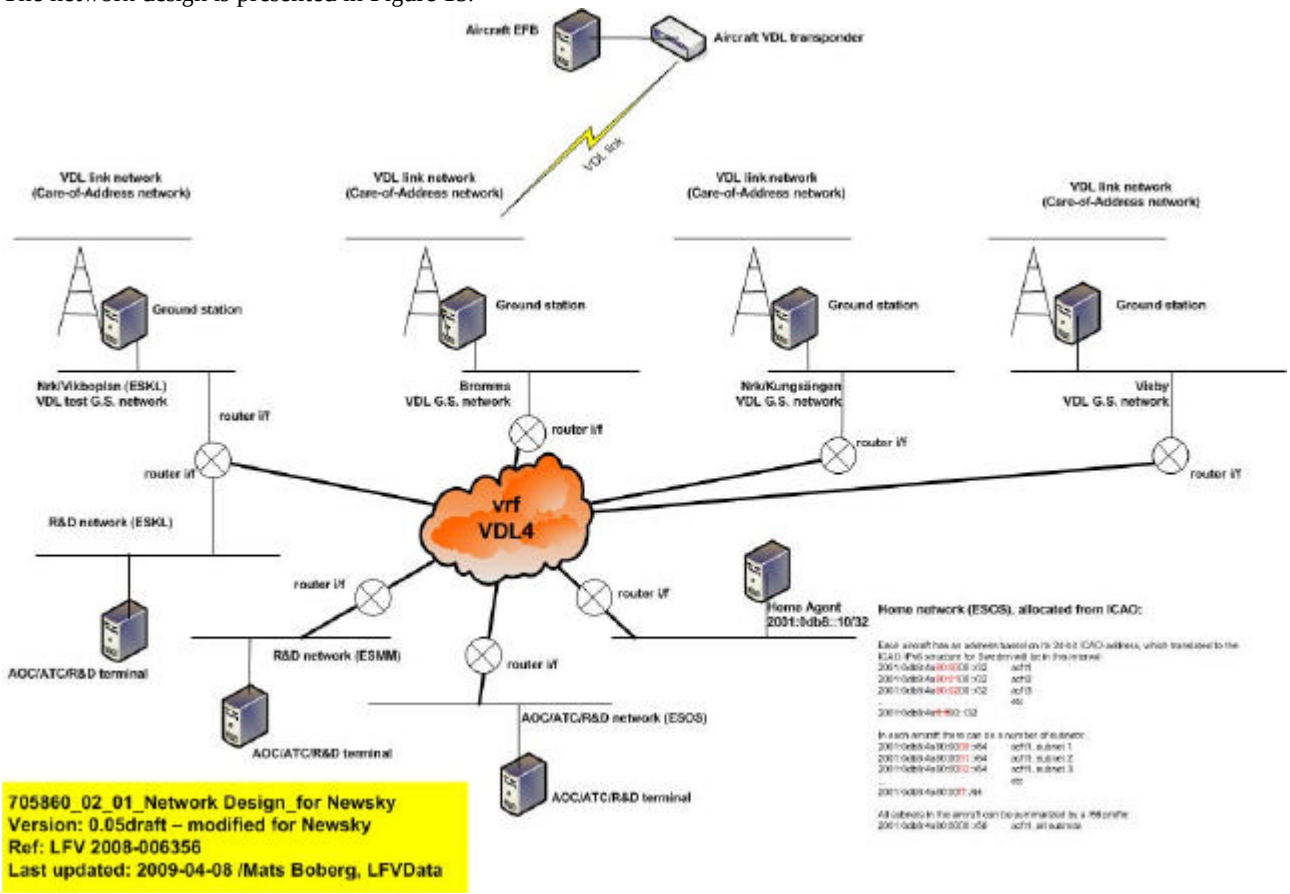


Figure 15. Network design

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.

3 APPENDIX A - IPSEC/IKE IMPLEMENTATION

3.1 Introduction

There are some ambiguities in the ICAO Doc 9896 regarding the requirements for IPsec/IKE which makes it open to different interpretations. Different scenarios exist which are briefly described here along with our interpretations and some issues involved. For a more detailed description of requirements and scenarios the ICAO doc 9896 is the reference.

This document is very much evolving as the project develops and the ICAO doc 9896 gets clearer and technical tests shows what is feasible and what is not.

3.2 Assumptions

Despite what can be inferred from 9896 and what can not, we assume that the objective is to secure the mobility access and to secure the transport of data across all the links. How that is achieved might be debated but the whole purpose of it seems quite clear.

3.3 General

In Part III 5.1 we find that all nodes are required to implement IPsec/IKE but the actual use is based on a system threat and vulnerability analysis.

We interpret this to mean that the IPsec/IKE functionality must exist in all nodes, but if we actually turn that functionality on and really use it will be based on the results of a risk assessment.

3.4 Ground-ground

This can be implemented as a VPN between gateways, and it is most suitable between regions, states or organizations.

We interpret this to mean that we implement IPsec/IKE VPN between LFV and other ANSPs and other MSPs, not within the LFV ground-ground network.

In Part III 5.2.3 we find that it may be appropriate to implement other alternatives in certain operating environments. In the case of traffic within the LFV ground-ground network we consider this to be the case, the CDPLC network within LFV is implemented by a separate MPLS/VPN with one (1) entrance/exit point which is protected by firewalls and IPS. If/when this MPLS/VPN should have a connection to another ANSP and/or MSP this connection will be implemented by a IPsec/IKE VPN.

3.5 Air-ground

The IPsec/IKE requirement is understandable but when it comes to real implementation and actual use things get really tricky. What is actually meant by this section is not clear but we interpret that the radio datalink should be encrypted at the IP layer. And that this means something similar to the gateway model described above in the ground-ground section.

I.e. a VPN between (a gateway on board) the aircraft and the ground station at the MSP, or a VPN between (a gateway on board) the aircraft and a gateway within the MSP ground network.

This brings up the issue of VPN endpoints and key exchange and interoperability when the aircraft leaves its ”home MSP” and moves to another MSP.

A VPN device on board the aircraft most likely has a configured address to a VPN gateway which also most likely will be within its ”home MSP” and therefore the VPN will be from the aircraft through the visited MSP network and into its ”home MSP” network. In this case, the ground-ground scenario above do not need any IPsec/VPN connection between the two MSPs, the traffic will be encrypted anyway. We interpret this to be the most likely case.

If a VPN device on board the aircraft should set up a VPN connection to an unknown VPN gateway in a visited MSP network, how does it find the IP address of that VPN gateway? It must have a means to know what address to connect to in

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.

order to actually be able to set up the VPN connection and in a mobile dynamic environment where it never knows in advance which gateway it will use, this has to be solved.

In general, today the datalink may not have enough bandwidth to facilitate all the extra overhead implied by an IPsec/IKE connection. Impact on performance will be notable, a trade-off must be made somewhere between security and performance until higher capacity datalinks are available.

3.6 Application-level end-to-end

This is a straight-forward and normal way of implementing security over a medium considered unsecure. An example is people working from public hotspots where a IPsec/IKE VPN is set up between their PC (or application) and their home office central gateway (or application server) across the Internet.

It is the most standard and recommended way to implement security and if this is used both the ground-ground and air-ground scenarios above become obsolete. A combination of end-to-end and the other scenarios leads to an unnecessary amount of overhead which will degrade the performance of the datalink considerably.

3.7 Mobility access

In Part III 5.3.4 is discussion is raised regarding security and mobility which seem to stem from more security-evolved mobility designs than VDL (?) like WiFi/WLAN. In particular, a combination of access security described in 5.3.4.2 and application-level end-to-end security is very common in the WiFi/WLAN community. An implementation similar to that would mean:

- implementing authentication and encryption over the link level protocol (between the aircraft transponder and the ground station), thereby securing the air-ground part. This usually speeds up handover between ground stations and the IP level considerably.

- implementing mobile IP binding updates authentication, thereby securing the mobile IP access part.

- implementing application-level end-to-end, thereby securing the actual data transfer regardless of any intermediate MSP ground networks.

This document and attachments shall remain our property. They may not without our written consent, either in their original state or with any changes, be copied or reproduced, disclosed to or delivered to anyone unauthorized nor used for other purposes than what has been confirmed by Com 4 Solutions AB in writing.