



**ITSSv6**

ITSSv6 - IPv6 ITS Station Stack  
for Cooperative ITS FOTs  
<http://www.itssv6.eu/>



ICT-2009.6: ICT for Mobility,  
Environmental Sustainability  
and Energy Efficiency

## ITSSv6 Deliverable

|                                     |
|-------------------------------------|
| ITSSv6 STREP Grant Agreement 210519 |
|-------------------------------------|

|   |
|---|
| D2.1 Preliminary System Recommendations |
|---|

|   |   |
|---|---|
| <b>DATE</b>                                   | 22nd May 2012                                     |
| <b>CONTRACTUAL DATE OF DELIVERY TO THE EC</b> | M08 (30.09.2011)                                  |
| <b>ACTUAL DATE OF DELIVERY TO THE EC</b>      | M14 (31.03.2012)                                  |
| <b>EDITOR, COMPANY</b>                        | Thierry Ernst, Inria                              |
| <b>DOCUMENT CODE</b>                          | ITSSv6-D2.1-PreliminarySystemRecommendations-v1.1 |
| <b>SECURITY</b>                               | Public  |

Project Coordinated by Thierry Ernst - Mines ParisTech / Inria  
E-mail: [thierry.ernst@mines-paristech.fr](mailto:thierry.ernst@mines-paristech.fr)

---

## Document History

---

| Release | Date     | Reason of change                  | Status | Distribution |
|---------|----------|-----------------------------------|--------|--------------|
| 1.0     | 01/04/12 | Final consolidated version        | Final  | Internal     |
| 1.1     | 01/05/12 | Alignment with other deliverables | Final  | EC           |

|   |           |
|---|-----------|
| <b>Executive summary</b>                                  | <b>6</b>  |
| <b>Contributors</b>                                       | <b>7</b>  |
| <b>1 Introduction</b>                                     | <b>8</b>  |
| 1.1 The ITSSv6 project . . . . .                          | 8         |
| 1.2 Purpose of this deliverable . . . . .                 | 9         |
| 1.3 Structure of the document . . . . .                   | 9         |
| <b>2 Cooperative ITS Context</b>                          | <b>10</b> |
| 2.1 Cooperative ITS definition . . . . .                  | 10        |
| 2.2 Cooperative ITS applications . . . . .                | 11        |
| 2.3 Cooperative ITS communication architecture . . . . .  | 11        |
| 2.4 Cooperative ITS standardization . . . . .             | 13        |
| 2.4.1 ETSI TC ITS . . . . .                               | 13        |
| 2.4.2 ISO TC 204 / CEN TC278 . . . . .                    | 13        |
| 2.5 IPv6 context . . . . .                                | 14        |
| 2.5.1 IP protocol evolution . . . . .                     | 14        |
| 2.5.2 IPv6 deployment . . . . .                           | 14        |
| 2.5.3 IPv6 at the EC level . . . . .                      | 15        |
| 2.5.4 IPv6 for ITS . . . . .                              | 15        |
| 2.5.5 IPv6 contribution from CVIS . . . . .               | 15        |
| 2.5.6 IPv6 contribution from GeoNet . . . . .             | 16        |
| 2.6 Conclusion . . . . .                                  | 16        |
| <b>3 ITS station reference architecture</b>               | <b>17</b> |
| 3.1 ITS station reference architecture overview . . . . . | 17        |
| 3.1.1 OSI-like layered architecture . . . . .             | 18        |
| 3.1.2 Types of ITS stations . . . . .                     | 18        |
| 3.1.3 ITS stations hosts and routers . . . . .            | 19        |
| 3.1.4 ITS stations and IPv6 . . . . .                     | 19        |
| 3.2 ITS station networking and transport . . . . .        | 21        |
| 3.3 ITS station management . . . . .                      | 21        |
| 3.4 ITS station security . . . . .                        | 23        |

|          |   |           |
|----------|---|-----------|
| 3.5      | ITS station access technologies . . . . .                             | 23        |
| 3.6      | ITS station facilities . . . . .                                      | 24        |
| 3.7      | ITS station applications . . . . .                                    | 24        |
| 3.8      | ITS station service access points (SAP) . . . . .                     | 25        |
| <b>4</b> | <b>ITS communication scenarios involving IPv6</b>                     | <b>28</b> |
| 4.1      | Scenario classification . . . . .                                     | 28        |
| 4.1.1    | Communication endpoints . . . . .                                     | 28        |
| 4.1.2    | Communication mode . . . . .  | 29        |
| 4.1.3    | Communication range . . . . .   | 29        |
| 4.2      | Road safety scenario example . . . . .                                | 30        |
| 4.2.1    | Scenario: description . . . . .                                       | 30        |
| 4.2.2    | Scenario: mapping to the classification . . . . .                     | 31        |
| 4.2.3    | Scenario: benefit of IPv6 . . . . .                                   | 31        |
| <b>5</b> | <b>IPv6 protocol stack design goals</b>                               | <b>33</b> |
| 5.1      | Architecture requirements . . . . .                                   | 33        |
| 5.1.1    | Cooperative ITS standards compliance . . . . .                        | 33        |
| 5.1.2    | IETF standards reusability . . . . .                                  | 34        |
| 5.1.3    | Layer separation . . . . .  | 35        |
| 5.1.4    | ITS station types . . . . .   | 35        |
| 5.1.5    | ITS station nodes and internal network . . . . .                      | 36        |
| 5.1.6    | Access technology diversity . . . . .                                 | 36        |
| 5.1.7    | Application type diversity . . . . .                                  | 36        |
| 5.1.8    | Scalability . . . . .   | 37        |
| 5.1.9    | Performance . . . . .   | 37        |
| 5.1.10   | IETF standards backward compatibility . . . . .                       | 37        |
| 5.2      | Communication type requirements . . . . .                             | 38        |
| 5.2.1    | Communication endpoints . . . . .                                     | 38        |
| 5.2.2    | Infrastructure-less and infrastructure-based communications . . . . . | 38        |
| 5.2.3    | Communication range . . . . .   | 38        |
| 5.3      | Functional requirements . . . . .                                     | 39        |
| 5.3.1    | Transparency . . . . .  | 39        |
| 5.3.2    | Internet connectivity . . . . .                                       | 39        |
| 5.3.3    | Transient connectivity . . . . .                                      | 39        |
| 5.3.4    | Multiple access technologies . . . . .                                | 40        |
| 5.3.5    | Providing and getting network connectivity . . . . .                  | 40        |
| 5.3.6    | Adhoc communications . . . . .  | 40        |
| 5.3.7    | Interoperability between IPv6 and IPv4 . . . . .                      | 40        |
| 5.3.8    | ITS station management . . . . .                                      | 41        |
| 5.3.9    | Best communication path selection . . . . .                           | 41        |
| 5.3.10   | Security . . . . .  | 41        |
| 5.3.11   | Access technologies . . . . .   | 41        |
|          | 5.3.11.1 IEEE 802.11p . . . . .                                       | 41        |
|          | 5.3.11.2 Cellular access technologies . . . . .                       | 42        |
| 5.4      | Convergence with non-ITS sectors . . . . .                            | 42        |
| 5.4.1    | Internet of Things . . . . .  | 42        |
| <b>A</b> | <b>List of acronyms</b>   | <b>44</b> |



---

## List of Figures

---

|     |   |    |
|-----|---|----|
| 2.1 | ITS stations communicating using IPv6 via various access technologies . . . . | 12 |
| 3.1 | Simplified ITS Station (ITS-S) Reference Architecture . . . . .               | 19 |
| 3.2 | Detailed ITS Station (ITS-S) Reference Architecture . . . . .                 | 20 |
| 3.3 | Types of ITS stations . . . . .   | 21 |
| 3.4 | ITS station communication management . . . . .                                | 22 |
| 3.5 | ITS Station Service Access Points (SAP) . . . . .                             | 25 |
| 3.6 | MN-Command and MN-Request service primitive . . . . .                         | 26 |
| 3.7 | MN-COMMAND Description . . . . .  | 26 |
| 3.8 | MN-REQUEST Description . . . . .  | 27 |
| 4.1 | IPv6 scenarios . . . . .  | 30 |
| 5.1 | Simplified ITS Station (ITS-S) Reference Architecture - Scope of ITSSv6 . .   | 34 |

This document is a public deliverable (D2.1) of ITSSv6 (IPv6 Station Stack for Cooperative ITS Field Operational Tests), a FP7 European Project, which aims at specifying and developing an enhanced IPv6 protocol stack optimized for Intelligent Transportation Systems (ITS) use cases complying with Cooperative ITS (C-ITS) standards. This document targets more particularly third parties deploying Internet Protocol version 6 (IPv6) in Field Operational Tests (FOTs) of Cooperative Intelligent Transportation Systems (C-ITS) standards. This document provides guidelines for a deployment of IPv6 complying with the set of C-ITS standards under specification within the International Organization for Standardization (ISO) (ISO TC204), the European Committee for Standardization (CEN) (CEN TC278) and the European Telecommunications Standards Institute (ETSI) (ETSI TC ITS) following the European Commission's standardization mandate M/453. At first the C-ITS context is detailed. Then, it is explained why, in which context and how IPv6 shall be deployed for ITS use cases. Then, requirements for the specification of an IPv6 protocol stack complying with C-ITS standards are defined. They will serve for the proper specification of the IPv6 protocol stack which is provided in another deliverable of the ITSSv6 project (D2.2). No specific knowledge on IPv6 is assumed for understanding this document. An updated version of this document entitled *ITSSv6 D2.3: Final System Recommendations* will be provided in July 2013.

The following ITSSv6 members have contributed to this deliverable:

- Thierry Ernst, from Mines ParisTech / INRIA.
- Jong-Hyook Lee , from INRIA.
- José Santa, from University of Murcia.
- Fernando Pereñiguez, from University of Murcia.
- Antonio F. Skarmeta, from University of Murcia.



## 1.1 The ITSSv6 project

ITSSv6 (IPv6 Station Stack for Cooperative **ITS** Field Operational Tests (FOTs) is an European Project (STREP) from the 7th Programme Framework (Grant Agreement 270519), Call 6 (ICT-2009.6: ICT for Mobility, Environmental Sustainability and Energy Efficiency) started in February 2011 and lasting until January 2014. The project is coordinated by Institut National de Recherche en Informatique et en Automatique (**Inria**) and gathers Universidad de Murcia (**UMU**), Institut Mines Telecom (**IT**), lesswire (**LW**), Magyar tudományos akademia szamitastechnikai es automatizalasi kutato intezet (**SZTAKI**), Schalk & Shalk OG (**IPTE**) and Bluetechnix Mechatronische Systeme GmbH (**BT**) (Bluetechnix in short).

The objective of the ITSSv6 project is to deliver an optimized IPv6 implementation of ETSI / ISO ITS station reference architecture. ITSSv6 builds on existing standards from **ETSI**, **ISO** and **IETF** and IPv6 software available from the CVIS and GeoNet projects. The IPv6 ITS station stack provided by ITSSv6 supports at least 802.11p and **2G/3G** media types and is configured differently according to the role played by the ITS station (roadside, vehicle, central). The tasks of ITSSv6 are to:

- Gather third party users into a common User Forum to collect user's requirements;
- Enhance existing IPv6-related ITS station standards and specification of missing features;
- Implement IPv6-related ITS station standards;
- Validate the implementation and assess its performance;
- Port the IPv6 ITS station stack to selected third party platforms;
- Support third parties in the use of the IPv6 ITS station stack.

Publishable material of the ITSSv6 project (public deliverables, newsletters, presentations made at conferences or workshops, information about events) are made available on the project's web site (<http://www.itssv6.eu>) as it becomes available.

## 1.2 Purpose of this deliverable

This deliverable presents system recommendations for the deployment of IPv6 in Field Operational Tests (FOTs) of Cooperative Intelligent Transportation Systems (C-ITS). It is the output of task *T2.3: System Recommendations*. With a good shared understanding of the output of past projects, FOT needs, specification of IPv6 networking at the standardization level, software availability and its performance, known complexity and unexploited IPv6 potential, ITSSv6 partners issue a public document targeting FOT stakeholders. This initial version (D2.1) is provided early on in order to convince FOTs for making necessary adjustments in existing platforms while a revised version (D2.3) will be produced around the end of the project (July 2013) in order to inform future FOTs and operational deployment stakeholders.

## 1.3 Structure of the document

The present document is structured as follows:

- Chapter 2 presents the context of this study: the concept of Cooperative ITS, the standardization effort, the situation around IPv6;
- Chapter 3 describes the ITS station reference architecture, as currently specified in ISO and ETSI standards;
- Chapter 4 describes some ITS scenarios where IPv6 will contribute to increase road safety, traffic efficiency and road users comfort.
- Chapter 5 defines the requirements for the specification of an IPv6 protocol stack for ITS use cases complying with C-ITS standards
- Appendix A provides the list of acronyms;
- References are provided at the end of this document.

This Chapter presents the context of this study: the concept of Cooperative ITS, the standardization effort, the situation around IPv6 and concludes with the contribution of the ITSSv6 project.

## 2.1 Cooperative ITS definition

The following definition of Cooperative Intelligent Transportation Systems (**ITS**) (Cooperative Intelligent Transportation Systems) has been developed through collaboration between International Organization for Standardization (**ISO**), European Telecommunications Standards Institute (**ETSI**), European Committee for Standardization (**CEN**) and representatives from other standard organizations, and can be found in the *Joint CEN and ETSI Response to Mandate M/453* [[EC-M/453](#)] dated 15 April 2010: *Cooperative ITS is a subset of the overall ITS that communicates and shares information between ITS stations to give advice or facilitate actions with the objective of improving safety, sustainability, efficiency and comfort beyond the scope of stand-alone systems.*

*An essential attribute of Cooperative ITS is that information is shared between the applications providing its services in a single ITS station and those running in different ITS stations. Cooperative-ITS has the following features:*

- *a common reference architecture;*
- *the sharing of information between any ITS station (Vehicle, Roadside, Central and Personal);*
- *the sharing of information between applications in a single ITS station;*
- *the sharing of resources (communication, positioning, security, ...) by applications in an ITS station;*
- *the authorized use of information for purposes other than the original intent; and*
- *the support of multiple applications running simultaneously.*

This definition is currently being developed in a joint technical specification between ISO TC204 WG18 and CEN TC278 WG16 [[ISO-17465](#)].

## 2.2 Cooperative ITS applications

Cooperative ITS applications are generally spread in three categories:

- **Road safety:** this category comprises all applications that are designed to render road traffic safer. These include both applications such as emergency braking or lane departure notification which require short range time-critical for immediate actions from the vehicles, and longer-range applications such as road hazard events (black ice, vehicle in the wrong direction, road work which require non time critical communications (short, medium and long range).
- **Traffic efficiency:** this category comprises all applications that are designed to improve road traffic. These include road itinerary planning, green wave, road diversion, and require constant exchange of informations between vehicles, the roadside infrastructure and some traffic information servers.
- **Other applications:** These are not necessarily ITS-specific applications, but must be supported in other to provide a better transportation experience to the road users. They thus include comfort and infotainment applications. This category is also often referred to as *value added* applications.

The main difference between Cooperative ITS applications and conventional ITS applications is that Cooperative ITS applications rely on a common communication architecture between all connected entities allowing them to exchange all types of information. Such communication peers include:

- **Vehicle equipments** of any type: navigation system, HiFi system, toll payment systems, sensors, ...
- **Roadside equipment** of any type: traffic lights, toll-gate, variable message signs, electric vehicle charging stations, ...
- **Central equipments** of any type: back office systems, traffic control centers, service providers, call centers, remote diagnostic systems, ...
- **Personal equipments** of any type: hand-held devices (smart phones, ...), car keys, ...

Figure 2.1 shows some examples of communication peers exchanging data through IPv6.

As a result of using a common communication architecture, ITS applications can mutually benefit from all information exchanged between all communication peers and become inherently *cooperative*.

## 2.3 Cooperative ITS communication architecture

In an effort towards harmonization, the international ITS community agreed on the definition of a common ITS communication architecture suitable for a variety of communication scenarios (vehicle-based, roadside-based and Internet-based) through a diversity of access technologies (802.11p, infra-red, 2G/3G, satellite, ...) and for a variety of application types (road safety, traffic efficiency and comfort / infotainment) deployed in various continents or countries ruled by distinct policies.

This common communication architecture is known as the *ITS station reference architecture* and is specified by the International Organization for Standardization (ISO) [ISO-21217]

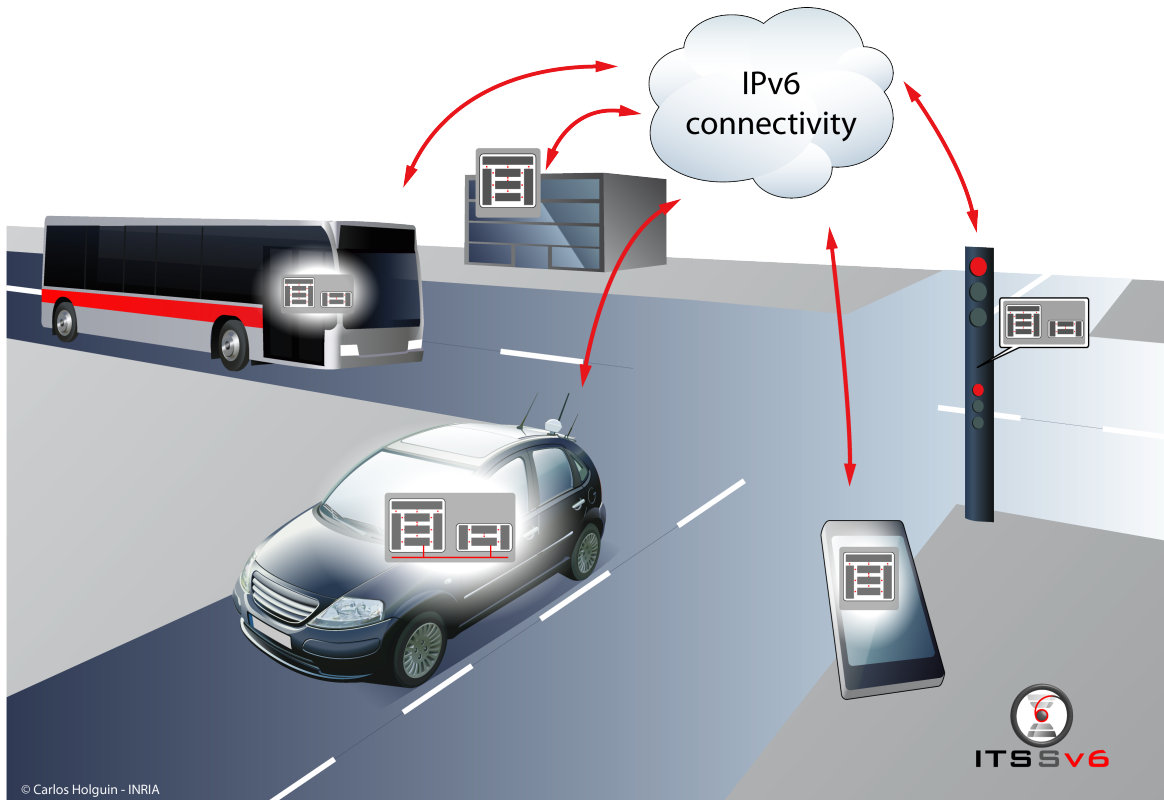


Figure 2.1: ITS stations communicating using IPv6 via various access technologies

and by the European Telecommunications Standards Institute (ETSI) [ETSI-EN-302-665]. It is detailed in Chapter 3 and illustrated on Figure 3.1.

One distinguishable feature of this architecture is the ability to use a variety of networking protocols in order to meet opposite design requirements i.e. fast time-critical communications for traffic safety versus more relaxed communication requirements for road efficiency and comfort / infotainment.

However, for the majority of anticipated ITS applications and services, IPv6 is ideally suited<sup>1</sup>. A particular emphasis was thus put on the use of IPv6 as the convergence layer ensuring the support of the diversity of access technologies, the diversity of applications and the diversity of communication scenarios. This resulted into the FP6 CVIS (Cooperative Vehicle-Infrastructure Systems) European Project taking a leadership on the specification and implementation of *IPv6 Networking* as defined by ISO [ISO-21210], the FP6 SeVeCom (Secure Vehicular Communication) European Project investigating IPv6 security issues (IPv6 addresses based on pseudonyms), the FP7 GeoNet (IPv6 GeoNetworking) European Project specifying and implementing the concepts linking IPv6 networking and geographic addressing and routing (IPv6 GeoNetworking), and the launch of IPv6-related work items at both ETSI TC ITS and ISO TC204. In addition, ETSI is going to provide test suites related to IPv6 and GeoNetworking.

<sup>1</sup>see Section 2.5 for details about what is IPv6 and why it is needed in ITS

## 2.4 Cooperative ITS standardization

In May 2008, the EC published the ITS action plan [EC-COM-886] followed by ITS standardization mandate [EC-M/453] emphasizing the need for more actions in Europe leading to the medium-term deployment of Cooperative ITS solutions. As an answer to this standardization mandate, the European Committee for Standardization (CEN) Technical Committee 278 (CEN TC 278) and the European Telecommunications Standards Institute (ETSI) Technical Committee ITS (ETSI TC ITS) have listed more than 60 standards to be developed or already under development and necessary for the deployment of Cooperative ITS. CEN and ETSI divided the work between the two institutions; CEN work is actually performed jointly with International Organization for Standardization (ISO) Technical Committee 204 (ISO TC204).

### 2.4.1 ETSI TC ITS

Based in Sophia Antipolis (France), the European Telecommunications Standards Institute is officially responsible for standardization of Information and Communication Technologies (ICT) within Europe. Given the prevalent participation of car manufacturers and their equipment suppliers, ETSI TC ITS took over the tasks of defining standards related to time-critical Vehicle ITS station to Vehicle ITS station (V2V) and Vehicle ITS station to Roadside ITS station (V2R) road safety applications. As such, ETSI has so far defined a specific subset of Cooperative Intelligent Transportation Systems standards, including GeoNetworking, IPv6 over GeoNetworking [ETSI-TS-102-636-6-1], Co-operative Awareness Messages (CAM) [ETSI-TS-102-637-2], Decentralized Environmental Notification Messages (DENM) [ETSI-TS-102-637-3].

### 2.4.2 ISO TC 204 / CEN TC278

The European Committee for Standardization TC278 took over the tasks of developing standards related to the system management, regulation and non time-critical applications and more broadly speaking all standards not strictly related to the vehicle part, including Vehicle ITS station to Central ITS station (V2C) (directly between the vehicle and the center using e.g. 3G or via the roadside infrastructure e.g. using IEEE 802.11p and Roadside ITS station to Central ITS station (R2C). As a result, a new working group was established within CEN TC 278 as WG16 *Cooperative Systems*<sup>2</sup>. Given the interest of non-European parties and the ongoing activity at ISO, the *Cooperative Systems* working group was actually established as a joint working group between CEN TC278 and ISO TC204. In line with this, ISO TC204 established this new group as WG18.

Many of the new standards under the responsibility of CEN TC278 WG16 / ISO TC204 WG18 are indeed elaborated in cooperation with existing ISO/CEN working groups. In particular:

Current standards relevant to C-ITS under development include:

- The definition of C-ITS (see Section 2.1) is developed together with ISO TC 204 WG1 (Architecture).
- Standards related to networking (in particular IPv6 [ISO-21210, ISO-16788, ISO-16789]), access technologies [ISO-21218] and communication management [ISO-24102] are under the responsibility of ISO TC204 WG16, known as CALM.

<sup>2</sup>The denomination Cooperative Intelligent Transportation Systems (C-ITS) is now taking over the former denomination known as *Cooperative Systems*

- Standards related to the exchange of information between the roadside infrastructure and control centers and from the roadside infrastructure to the vehicles are specified within CEN TC278 WG16 / ISO TC204 WG18, and include [ISO-17429] (pre-processing and transfer between the roadside infrastructure and the control center of information collected by passing-by vehicles), [ISO-17425] (variable message signs indicated by the roadside infrastructure) and [ISO-17426] (contextual speeds indicated by the roadside infrastructure).

## 2.5 IPv6 context

### 2.5.1 IP protocol evolution

The first widely deployed protocol allowing packet based communications between computers located in various networks was the Internet Protocol version 4 (IPv4) [rfc791]. This protocol defines addresses of a fixed 32-bit length. This allows approximatively 4 billions IP addresses to be used on the Internet. This figure appeared sufficient for the expected use of the protocol at that time. But the emergence of the commercial use of the Internet in the 90's decade led to an exponential use of IP addresses. To prevent the shortage of IP addresses, the IETF decided two measures: the specification of private IPv4 address spaces [rfc1918], to be used with Network Address Translation (NAT) and the design of a new version of the IP protocol: IP version 6 (IPv6).

The specification of this new protocol was finalized in 1998 [RFC2460]. This protocol defines addresses of a fixed 128-bit length. This allows a very large address space that is considered sufficient for most ambitious deployment scenarios (there would be enough addresses to identify every grain of sand on Earth). In addition to the address space, IPv6 defines new protocols to ease the management of the layer-3 protocol stack, such as Neighbor Discovery [rfc2461] that allows auto-configuration of IPv6 addresses.

While IPv6 is entering in its deployment phase, the depletion of the IPv4 address space is ongoing, despite the measures taken by the IETF. The global IPv4 address pool is exhausted since February 2011 and several regions such as Asia and Europe are facing shortage of IPv4 addresses. The exhaustion for the European region may happen in August 2012. After this date, Internet Service Providers (ISPs) and hosting services will not be able to get new IPv4 addresses. The deployment of IPv6 is therefore critical to ensure the future growth of the services of these stakeholders.

### 2.5.2 IPv6 deployment

To this date, IPv6 deployment is ongoing in most network backbones. All major operating systems (Windows, Linux, BSD variants, Mac OS X), most network equipments and services (routers, DNS, etc.) can support IPv6 once IPv6 is activated in the network they are located in. However there are still few ISPs (Internet Service Providers) in Europe offering IPv6 and support of IPv6 in applications (web and email servers, etc) is still lacking, although those issues are of limited importance in vertical segments such as ITS. It must nevertheless be acknowledged that IPv6 deployment is taking momentum and that soon IPv6 will become the rule rather than the exception. Certainly the expansion rate of IPv6 is not fast enough, but the depletion of the IPv4 address space is now going to boost it.

### 2.5.3 IPv6 at the EC level

In their common answer to the ITS standardization mandate [EC-M/453] from the European Commission, CEN TC 278 and ETSI TC ITS lists a number of items for which IPv6-related standards are needed while the European Commission's standardization work programme [EC-ICT-Standardization] includes actions turing around IPv6. IPv6 is in itself a topic that requires and is attracting a lot of attention from the European Commission. The Work Programme 2010 [EC-COM-5893] Section 3.7 *Encouraging the use of Internet Protocol version 6* follows the *IPv6 Action Plan* issued by the European Commission published in May 2008 [EC-COM-313, EC-IPv6-web] given the fast coming ultimate depletion of the IPv4 address space and a number of alerting reports published in 2008, including from the OECD. In its IPv6 Action Plan, the European Commission (DG INFSO) set an objective of a penetration rate of 25% of European Internet users and servers able to use IPv6 by 2010. This target is followed by some European nations.

### 2.5.4 IPv6 for ITS

By the time ITS services requiring the use of the public IP addresses appear on the market, there won't be enough public IPv4 address available. The use of this version of IP scales to meet the addressing needs of a growing number of vehicles and connected devices, and provides the added functionality necessary in mobile environments. By relying on IPv6 in their ITS communication architectures, ISO followed by ETSI, COMeSafety and the Car-to-Car Communication Consortium have thus taken the right decision to guarantee sustainable deployment of C-ITS.

Furthermore, IPv6 has the potential to decrease accident rates by enabling transmission of safety critical information. Here we don't indulge ourselves in demonstrating this would be the case for the time critical type of applications since the automotive industry and the SDOs - at this time - are not considering IPv6 for fast V2V communications. However, it is simple to note that not all data is time critical. There is no question that IPv6 could be a media-agnostic carrier of such non time critical but safety essential information. An example of the benefit of IPv6 for time critical application has been demonstrated by FP7 GeoNet in the traffic hazard detection and notification scenario during its final demonstration [GeoNet-D7.1]. Once the safety benefit of IPv6 is acknowledged, there are classical ways of calculating the economic impact of reducing road fatalities. E. g. an estimate by Safety Forum 2003 Summary Report estimated the cost of accidents at 160 billions euros. A 1% reduction would reduce these costs by 1.6 billion euros annually. And of course, this does not take into account the reduction of pain and suffering experienced by surviving family members and friends of accident victims that may not be adequately reflected in the method used to estimate the economic costs of traffic fatalities.

### 2.5.5 IPv6 contribution from CVIS

By being the first project of its kind in the ITS to base itself on IPv6, CVIS (Cooperative Vehicle-Infrastructure Systems, a FP6 Integrated European Project [url-CVIS]) has advanced tremendously the experimental knowledge and has developed sufficient skills to encourage forthcoming ITS-related projects to do the same. The conclusions of CVIS on IPv6 are that a communication system based of ISO standards (known as CALM) and IPv6 is definitely feasible [CVIS-D3.4, Ernst2009, Moe2010]. IPv6 networking as specified by ISO [ISO-21210] has thus been somewhat validated though CVIS has also acknowledged that improvements



are necessary for operational use of IPv6 <sup>3</sup>.

### 2.5.6 IPv6 contribution from GeoNet

GeoNetworking is a geographic addressing and routing protocol originally defined by the Car-to-Car Communication Consortium (C2C-CC) and allowing non-IP multi-hop communications between vehicle and roadside ITS stations attached to the same vehicular ad-hoc network. It can maintain a path between two ITS stations over intermediate ITS stations. It particularly allows an ITS station to broadcast time-critical safety informations to all ITS stations located in a given geographic area, either immediately located around the sending ITS station (e.g. a vehicle ITS station sending information about emergency braking to all vehicles immediately located behind) or located in a remote area defined by geographical coordinates (e.g. a roadside ITS station informing approaching vehicles located at some distance that there is black ice).

In a situation where a roadside ITS station reachable from a vehicle ITS station via intermediate ITS stations by means of GeoNetworking is connected to the Internet, or in a situation where two ITS stations can reach one another via intermediate ITS stations by means of GeoNetworking, it is possible to transmit IPv6 packets over the GeoNetworking path therefore extending the reach of the GeoNetworking capabilities. This combination is referred to as IPv6 GeoNetworking and allows to perform IPv6 communication over a multi-hop network made of forwarding vehicle and roadside ITS stations. It requires the encapsulation of IPv6 packets within GeoNetworking packets.

The combination of IPv6 with GeoNetworking into a single protocol stack has been defined by the GeoNet (IPv6 GeoNetworking) FP7 European Project (2008-2010). The work realized within the C2C-CC was assumed as the starting point and led to the architecture defined by the GeoNet project in [GeoNet-D1.2, GeoNet-D2.2]. These documents are publicly available and can be found on the GeoNet project web site [url-GeoNet]. In its final demonstration, the GeoNet project demonstrated the use of IPv6 combined with GeoNetworking for a typical road safety and traffic efficiency applications where a control center is able to report road traffic hazards directly to the vehicles located in a pre-determined geographic area (end-to-end, i.e. without processing of the information by roadside ITS stations which act as simple relayers) [GeoNet-D7.1].

IPv6 GeoNetworking capabilities have partly been standardized [ETSI-TS-102-636-6-1]. New work items at ISO TC204 have being proposed to complement the ETSI standard.

## 2.6 Conclusion

IPv6 is a protocol necessary for many ITS use cases and is part of the set of C-ITS standards under definition by ISO, CEN and ETSI. The European know-how on IPv6 networking for ITS (conventional ITS or Cooperative ITS) remains limited and belongs to a handful of expert parties, though it is taking momentum. As a result, little effort has been put into bringing together in an IPv6 stack all the needed features for the operational use of IPv6 for ITS.

The objective of the ITSSv6 project is to fulfill this gap; the objective of this document is to help prospective ITS users to feel more confident in deploying IPv6 as it will be necessary in the short run. Late deployment of IPv6 will only bring additional costs that could be avoided if IPv6 deployment is being considered in a stepwise approach.

---

<sup>3</sup>The objective of ITSSv6 is to provide the necessary improvements, both in terms of standard specification and actual implementation

In this chapter, we describe the *ITS station reference architecture* as currently defined in standards from the International Organization for Standardization (ISO) (Technical Committee 204) and the European Telecommunications Standards Institute (ETSI) (Technical Committee ITS).

### 3.1 ITS station reference architecture overview

In an effort towards harmonization, the European ITS community (EC's funding programs FP6 and FP7, the Car-to-Car Communication Consortium) and international standardization bodies (ISO TC204 WG16 and ETSI TC ITS) have invested significant effort into the specification of a communication architecture suitable for a variety of C-ITS needs. This harmonization effort, initially conducted by COMeSafety in 2010 (European FP6 Specific Support Action), considered early work performed by ISO TC204 WG16 and other stakeholders from various FP6 and FP7 European Projects (CVIS, SafeSpot, Coopers, GeoNet, SeVeCom) and organizations (e.g. C2C-CC).

This has led to the definition of the *ITS station reference architecture* at both ETSI TC ITS [ETSI-EN-302-665] and ISO TC 204 [ISO-21217]. This architecture is illustrated on Figure 3.1. Both ISO and ETSI architecture standards are based on the same terminology and tend to converge although there are still remaining differences between the two. This lack of consistency shall disappear as standards are revised (revision is undergoing as of February 2012).

The design principle of this communication architecture is to support simultaneously a diversity of applications of all types (road safety, traffic efficiency and comfort / infotainment) and to offer them a diversity of access technologies including cellular (2G, 3G), microwave (5 GHz IEEE 802.11p vehicular WiFi, 2.5 GHz IEEE 802.11n urban WiFi), satellite, infrared, 60 GHz millimeter-wave and possibly others, for a variety of communication scenarios (vehicle-based, roadside-based and Internet-based). These access technologies provide wired and wireless broadcast, unicast and multicast communications between mobile stations, between mobile and fixed stations and between fixed stations.

A fundamental advantage of this design concept over currently deployed systems is that applications are abstracted from the access technologies and the networks that transport the

information from the source to the destination(s). This means that ITS stations applications are not limited to the availability and characteristics of a single access technology and networking protocol stack. Communication management functions make optimal use of all these resources transparently to the applications.

ISO TC204 WG16, also known as **CALM** (Communications Access for Land Mobiles) and established at ISO in 200, is the birth place of many of the concepts behind the communication architecture before it was harmonized by COMeSafety.

### 3.1.1 OSI-like layered architecture

As shown on Figure 3.1, the *ITS station reference architecture* is layered. At the top sits the *application layer*, immediately below the *facilities layer* (middleware providing a set of standard services to the applications), below it the *networking and transport layer* and at the bottom the *access technologies layer* (providing the physical communication media).

This ITS station reference architecture differs from conventional OSI layered architectures by the addition of vertical entities providing cross-layer management (ITS station management) and security functions (ITS station security) and the new middle layer (ITS facilities) providing common services to the applications (maps, positioning, time stamping, etc). The network layer itself also comprises a variety of networking protocols, including IPv6 (for Internet-based communications), GeoNetworking of FAST (for roadside-based and vehicle-based communications), a combination of both (IPv6 GeoNetworking) and possibly other protocols.

The particular novelty from a design view point, compared to a typical OSI 7-layer architecture, are the two vertical entities, i.e. the ITS station management entity and the ITS station security entity performing a number of cross-layer functions. Cross-layer functions are not new in the literature (ITS no less than other use cases), but it is the first time this is explicitly shown on architecture diagrams.

The main difference between ETSI and ISO documents lies in the specification of the ITS station management entity. So far, ISO CALM has concentrated its effort on the cross-layer functions to ensure a given communication flow is matched to a particular communication interface (CI) according to application needs and current network conditions. ETSI is not too much concerned about this issue because the current ETSI work is largely focused on the used of the 802.11p access technology whereas the focus of the ISO work (CALM) has always been the simultaneous support of a variety of access technologies.

### 3.1.2 Types of ITS stations

Historically, the terms On-Board Unit (**OBU**), Road Side Unit (**RSU**) and Application Unit (**AU**) are used in the automotive industry. However, these terms were not defined with a networking view in mind and have therefore become obsolete in Cooperative ITS. In addition, the ITS station reference architecture doesn't use these terms either because they were confusing the discussion. This led to the definition of the ITS station (**ITS-S**) and a distinction of the supported functions according to the type of environment or network where it is be located. As such, four types of ITS stations are currently defined, as described on Figure 3.3:

- vehicle ITS station (**V-ITSS**): ITS station located in a vehicle
- roadside ITS station (**R-ITSS**): ITS station located in the roadside infrastructure
- central ITS station (**C-ITSS**): ITS station located in the central infrastructure

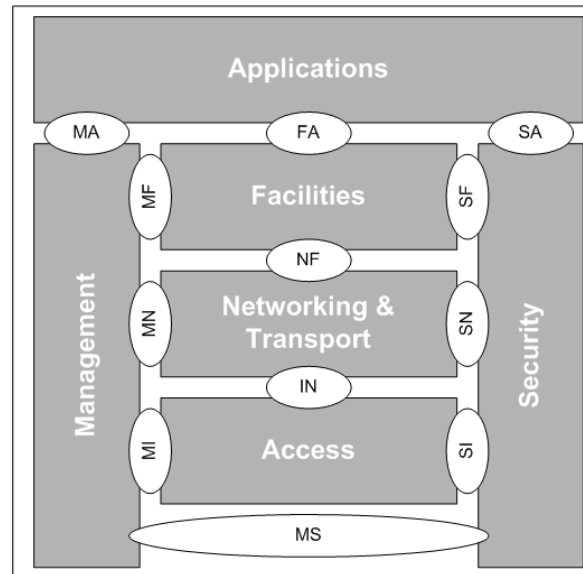


Figure 3.1: Simplified ITS Station (ITS-S) Reference Architecture

- personal ITS station (**P-ITSS**): ITS station located in a hand-held device

More ITS station types may be added in the future, if needed (e.g. for buses, trains, emergency vehicles, tramways, bicycles, motorbikes, truck, ...).

### 3.1.3 ITS stations hosts and routers

The ITS station is defined as a *bounded secured managed domain*. In the most general case the functions of an ITS station (**ITS-S**) are split into a router (ITS-S router) and hosts (ITS-S host) attached to the ITS-S router via some ITS station internal network. The router and hosts functions may also be merged into a single entity.

### 3.1.4 ITS stations and IPv6

In most cases, an ITS station will be linked to other ITS stations and networked entities via IPv6, either a legacy IPv6 network or a proprietary IPv6 network. In some very specific cases like for instance direct communication between neighbor vehicle ITS stations using 802.11p, IPv6 may be replaced by some ITS-specific networking protocol like GeoNetworking or a legacy cellular network. Considering the different types of ITS stations shown on Figure 3.3, the following ITS-S IPv6 nodes could exist:

- In the vehicle ITS station, the nodes executing the ITS-S router functions are the ITS-S IPv6 vehicle routers (**VRs**). The ITS-S host functions may be implemented by the ITS-S IPv6 router, or by ITS-S IPv6 hosts. Vehicle ITS-S IPv6 routers and hosts are also known as mobile routers (**MRs**) and mobile network nodes (**MNNs**) when continuous Internet connectivity is supported.
- In the roadside ITS station, the nodes executing the ITS-S router functions are the ITS-S IPv6 roadside routers (**RRs**) and the ITS-S IPv6 border routers (**BRs**). Roadside ITS-S IPv6 routers are also known as the ITS-S IPv6 access router (**AR**) when they provide access to ITS-S IPv6 mobile router (**MR**). border routers (**BRs**) are the ITS-S

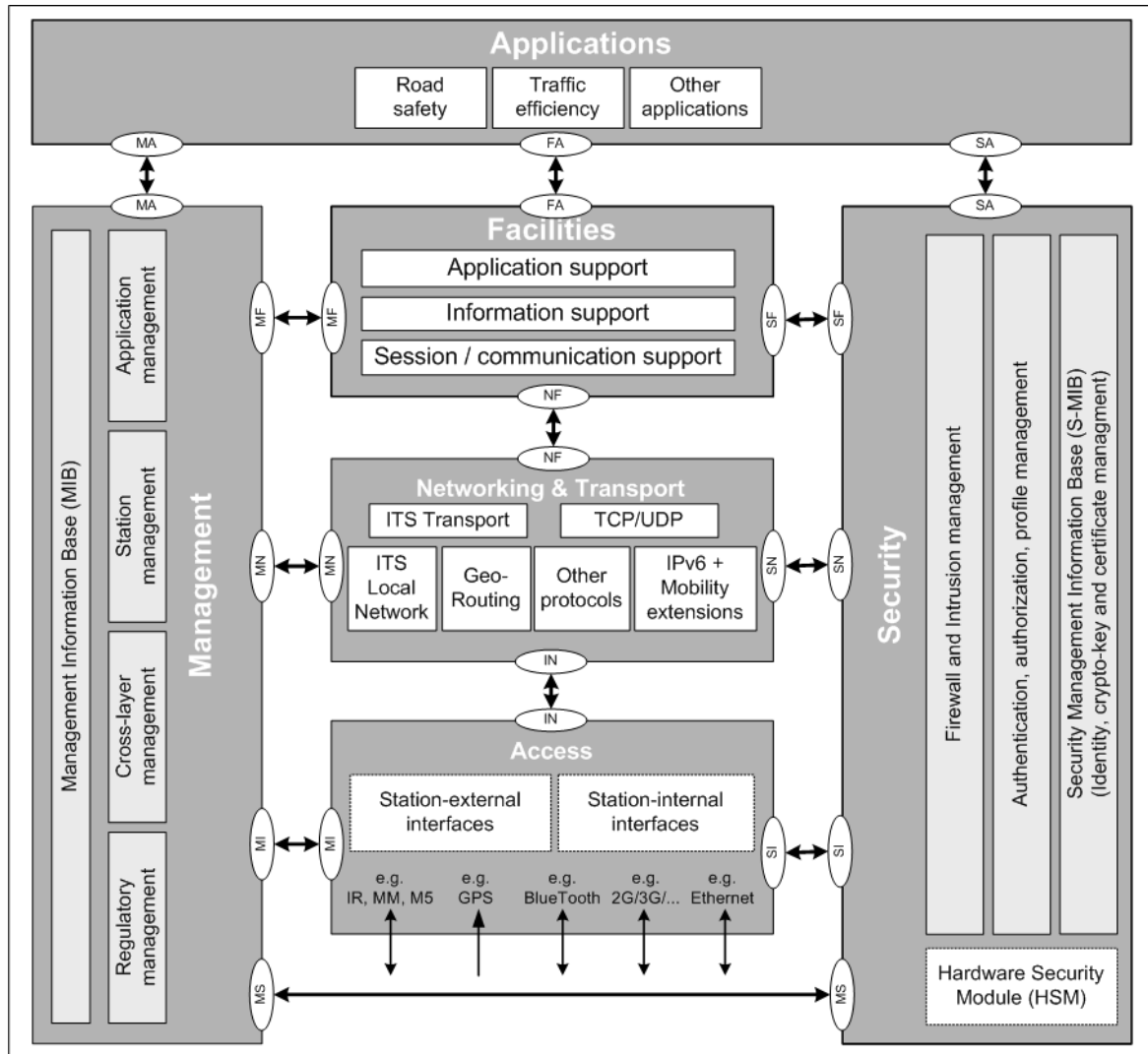


Figure 3.2: Detailed ITS Station (ITS-S) Reference Architecture

IPv6 routers connecting the ITS station to the Internet or other ITS stations. The ITS-S host functions may be implemented by an ITS-S IPv6 router, or by ITS-S IPv6 hosts.

- In the central ITS station, the nodes executing the ITS-S router functions are the ITS-S IPv6 border routers (**BRs**) connecting the ITS station to the Internet or other ITS stations and the ITS-S home agents (**HAs**) for supporting IPv6 mobility. The ITS-S host functions may be implemented by an ITS-S IPv6 router, or by ITS-S IPv6 hosts.

In this document, the terms On-Board Unit (**OBU**), Road Side Unit (**RSU**) and Application Unit (**AU**) are meant for IPv6 mobile router (**MR**), IPv6 access router (**AR**) and IPv6 node, respectively.

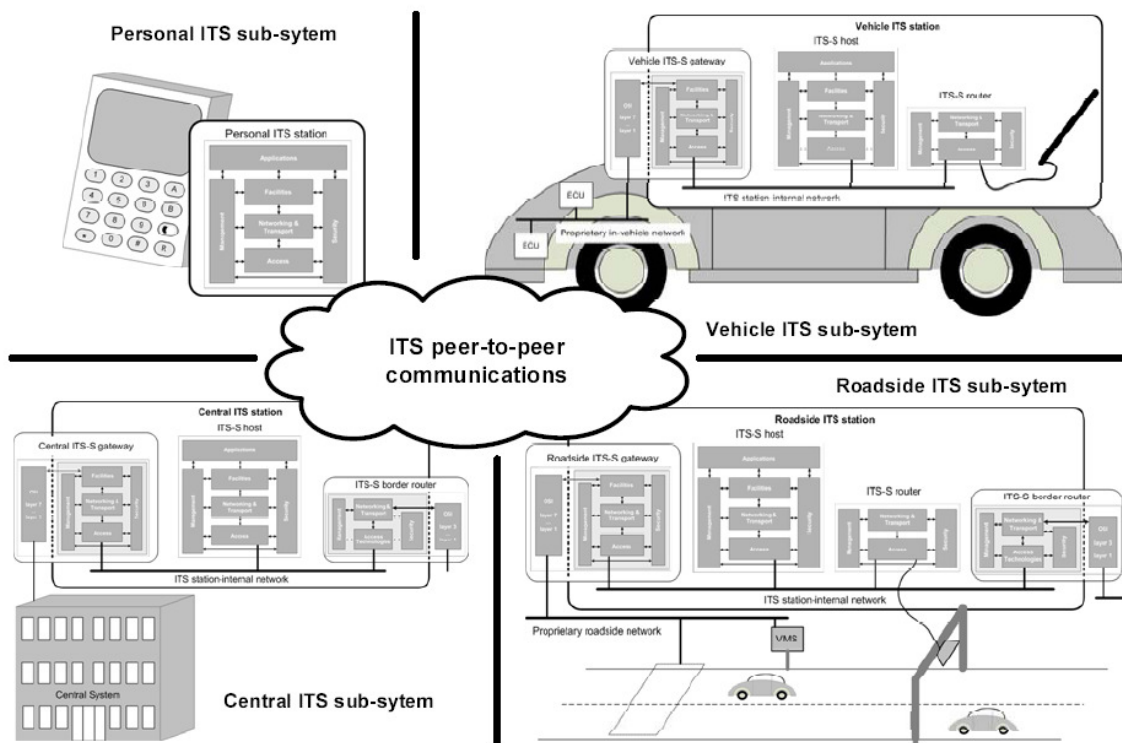


Figure 3.3: Types of ITS stations

### 3.2 ITS station networking and transport

As shown on Figure 3.2, the horizontal ITS station networking & transport layer (**SNT**) can support a variety of networking protocols. Currently, IPv6 Networking and the newly developed FNTP protocol (Fast Networking & Transport layer Protocol, previously known as FAST) are specified at the ISO TC204 level, respectively in ISO 21210 [ISO-21210] and [ISO-29281-2], whereas GeoNetworking (media-dependent [ETSI-TS-102-636-6-1] and media-independent [ETSI-TS-102-636-4-1]) and IPv6 over GeoNetworking adaptation layer [ETSI-TS-102-636-4-2] are specified by ETSI. More networking protocols could be added if needed.

The terms *Mobility Extensions* indicated in the *IPv6 + Mobility Extensions box* of the **SNT** is misleading as these are extensions of IPv6 only needed for mobile ITS stations such as vehicle or personal ITS stations. This is a detail that should not appear on this figure describing the architecture of a generic ITS station.

### 3.3 ITS station management

The vertical ITS station management entity (**SME**) is in charge of all cross-layers functions including path selection based on pre-set policies, regulations, static and dynamic capabilities of the different access technologies. The **SME** is responsible for the selection of the best communication path (communication interface and end-node) according to the flow requirements expressed by the ITS station applications, the access technologies characteristics and the current network conditions. The ITS station management entity must thus interact with the

horizontal layers in order to make this determination and more particularly with the ITS station networking & transport layer (SNT) that must update its forwarding tables according to rules provided by the SME. This is illustrated on Figure 3.4 [ETSI-EN-302-665, ISO-24102-1].

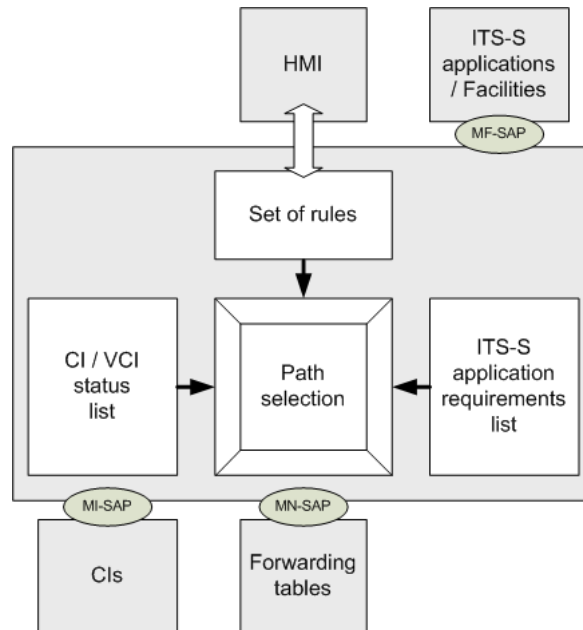


Figure 3.4: ITS station communication management

To exploit the availability of multiple access technologies, the SME supports different types of handover, including:

- those involving a change of the point of attachment to the network without a change of access technology;
- those involving a change of the point of attachment to the network with a change of access technology;
- those involving reconfiguration or change of the network employed to provide connectivity; and
- those involving both a change of the point of attachment to the network and network reconfiguration.

The SME functions are under specification by ISO TC204 WG16 [ISO-24102]. New ISO work items have been launched and published ISO standards are under revision. In addition, ETSI TC ITS has also opened work items related to cross-layer functions and the ITS station management, in order to comply with the ITS standardization mandate M/453 from the European Commission. Existing ETSI work items include Cross-layer architecture [ETSI-TS-102-723-1], MI interface [ETSI-TS-102-723-3], MN interface [ETSI-TS-102-723-4]. These work items should actually simply refer to the existing ISO TC204 standards, otherwise ISO and ETSI standards would diverge.

The interactions between the ITS station management entity and the horizontal layers is performed via Service Access Points (SAPs) (see Section 3.8).

### 3.4 ITS station security

The vertical ITS station security entity provides common security functionalities to all the horizontal layers and maintains security credentials used by these [ETSI-TS-102-731]. The ITS station security entity does not perform any particular security mechanism or protocol. Protocol dedicated security mechanisms and security protocols are implemented at each layer. For instance, IPv6 dedicated security mechanisms and protocols, which are subject to modifications or replacement, shall be implemented at the IPv6 protocol block, not at the ITS station security entity [Lee2011b, Lee2012a]. This provides more modularity and minimizes development complexity of the ITS station security entity.

The common security functionalities provided by the ITS station security entity include:

- Firewall and intrusion detection management;
- Authentication, authorization, and profile management; and
- Identity, cryptographic key, and certificate management.

Security credentials such as cryptographic keys, authorization tickets, and certificates are stored and maintained at the security entity with other security related parameters and status information. Upon request from horizontal layers, atomic security operations are provided by the security entity. The atomic security operations include:

- Arbitrary bit generation (for the pseudonym service);
- Hashing;
- Signing and verification; and
- Encryption and decryption.

The interactions between the ITS station security entity and the horizontal layers is performed via Service Access Points (SAPs) (see Section 3.8).

### 3.5 ITS station access technologies

A variety of access technologies can be used for the communication with other ITS stations, with ITS station internal network nodes, and other legacy ITS nodes. These access technologies can be used simultaneously, and vary according to the type of ITS station and its purpose. In order to support any given access technology, a new standard must specifying the parameters and functions so that the access technology could be recognized by the ITS station. Currently, the support of several wireless access technologies (infrared [ISO-21214], microwave [ISO-21215], millimeter wave, 2G/3G [ISO-21212, ISO-21213]) and wired access technologies (Ethernet) is already specified, in either ISO or ETSI standards. More access technologies could be supported in the future, without any impact on the other layers of the ITS station reference architecture. It is of course not required for a given deployment to implement neither all these access technologies nor to implement the specific functions required to support all these access technologies. So, the purpose of the standard is to specify how a given access technology, if needed, can be integrated into the ITS station.



### 3.6 ITS station facilities

The ITS station facilities is an intermediate layer between the ITS station networking & transport layer (**SNT**) and the applications, offering them access to information collected by other ITS stations (vehicles, roadside) and freeing them from the necessary message signaling to transmit and process data exchanged between ITS stations in a broadcast fashion. The immediate benefit is the sharing of data between various application which would otherwise have broadcast potentially similar information, therefore increasing consumption of network resources and processing power. The current facilities include **CAM** (Co-operative Awareness Messages) [ETSI-TS-102-637-2] 1-hop broadcast messages transmitted in the immediate vicinity mainly for time-critical road safety purposes, and Decentralized Environmental Notification Messages (**DENM**) (Decentralized Environmental Notification Messages) [ETSI-TS-102-637-3] multi-hop broadcast messages transmitted in a given geographical area. Information collected by **CAM** and **DENM** are recorded in a Local Dynamic Map (**LDM**) [ETSI-TR-102-863] together with other information.

### 3.7 ITS station applications

As shown on Figure 3.2, applications supported by the ITS station reference architecture are generally spread in three categories:

- **Road safety:** this category comprises all applications that are designed to render road traffic safer. These include both applications such as emergency braking or lane departure notification which require short range time-critical for immediate actions from the vehicles, and longer-range applications such as road hazard events (black ice, vehicle in the wrong direction, road work which require non time critical communications (short, medium and long range).
- **Traffic efficiency:** this category comprises all applications that are designed to improve road traffic. These include road itinerary planning, green wave, road diversion, and require constant exchange of informations between vehicles, the roadside infrastructure and some traffic information servers.
- **Other applications:** These are not necessarily ITS-specific applications, but must be supported in other to provide a better transportation experience to the road users. They thus include comfort and infotainment applications. This category is also often referred to as *value added* applications.

These applications rely partly on services offered by the ITS station facilities layer. As a result of the messages processed by the ITS station facilities, applications may for example display messages on the navigation system in the vehicle.

These applications may also issue messages to other ITS stations without subsequently involving the ITS station facilities. For example, as a result of receiving a service notification by the ITS station facilities, of a charging spot for electric vehicle charging spot, the application may directly contact a server to enquire about the availability of the charging spot and book it. In addition, some ITS station applications may be completely standalone, i.e. not taking benefit of the ITS station facilities at all.

All applications have specific communication requirements<sup>1</sup>. These application requirements must be provided to the ITS station management entity in order to determine the capability of the ITS station to transmit the information and to determine the communication path (e.g. the access technologies) that should be used to route the packets given the requirements provided by the application.

### 3.8 ITS station service access points (SAP)

The functional blocks of the ITS station communication architecture are interconnected via Service Access Points (SAPs) as presented in Figure 3.2.

|                | SAP       | Description   |
|----------------|-----------|---|
| Management     | <i>MI</i> | SAP allowing the interaction between the ITS station management entity (SME) and the ITS station access technologies layer (SAT)    |
|                | <i>MN</i> | SAP allowing the interaction between the ITS station management entity (SME) and the ITS station networking & transport layer (SNT) |
|                | <i>MF</i> | SAP allowing the interaction between the ITS station management entity (SME) and the ITS station facilities layer (SF)              |
|                | <i>MA</i> | SAP allowing the interaction between the ITS station management entity (SME) and the ITS station applications                       |
| Security       | <i>SI</i> | SAP allowing the interaction between the ITS station security entity (SSE) and the ITS station access technologies layer (SAT)      |
|                | <i>SN</i> | SAP allowing the interaction between the ITS station security entity (SSE) and the ITS station networking & transport layer (SNT)   |
|                | <i>SF</i> | SAP allowing the interaction between the ITS station security entity (SSE) and the ITS station facilities layer (SF)                |
|                | <i>SA</i> | SAP allowing the interaction between the ITS station security entity (SSE) and the ITS station applications                         |
| Between layers | <i>IN</i> | SAP allowing the interaction between the ITS station access technologies and the ITS station networking & transport layer (SNT)     |
|                | <i>NF</i> | SAP allowing the interaction between the ITS station networking & transport layer (SNT) and the ITS station facilities layer (SF)   |
|                | <i>FA</i> | SAP allowing the interaction between the ITS station facilities layer (SF) and the ITS station applications                         |

Figure 3.5: ITS Station Service Access Points (SAP)

<sup>1</sup>To be clearer, all application have specific communication flow requirements as there could be various flows with different flow characteristics, for instance a voice flow and a video flow when considering a video-conferencing application

According to the ISO specifications [ISO-24102-1], the following types of services, illustrated in Figure 3.6 must be used for the MN-SAP:

- MN-COMMAND: Sending a command to the ITS station networking & transport layer (SNT) , using the following primitives:
  - MN-COMMAND.request: this management service primitive allows the ITS station management entity (SME) to trigger an action at the ITS station networking & transport layer (SNT), using the following function parameters:
  - MN-COMMAND.confirm: this management service primitive reports the result of a previous MN-COMMAND.request.
- MN-REQUEST: Receiving a request (command) from the ITS station networking & transport layer (SNT), using the following primitives:
  - MN-REQUEST.request: this management service primitive allows the ITS station networking & transport layer (SNT) to trigger an action at the ITS station management entity (SME).
  - MN-REQUEST.confirm: this management service primitive reports the result of a previous MN-REQUEST.request.

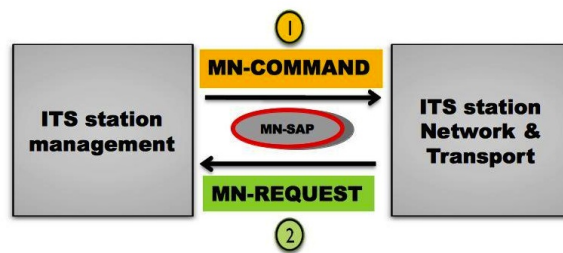


Figure 3.6: MN-Command and MN-Request service primitive

ISO 24102 [ISO-24102-1] indicates that both MN-COMMAND and MN-REQUEST supports up to 256 possible SAP functions. For MN-COMMAND five functions are currently defined; for MN-REQUEST, seven functions are currently defined. This is described in Table 3.8:

| MN-COMMAND Number | Description                      |
|-------------------|----------------------------------|
| 0                 | Reserved for future use.         |
| 1 to 5            | Used                             |
| 6 to 224          | Reserved for future use.         |
| 225               | For private non-standardized use |

Figure 3.7: MN-COMMAND Description

| MN-REQUEST Number | Description                      |
|-------------------|----------------------------------|
| 0                 | Reserved for future use.         |
| 1 to 7            | Used                             |
| 8 to 224          | Reserved for future use.         |
| 225               | For private non-standardized use |

Figure 3.8: MN-REQUEST Description

---

## ITS communication scenarios involving IPv6

---

This Chapter describes **ITS** scenarios where IPv6 will contribute to increase road safety, traffic efficiency and road users comfort. A typical road safety use case is presented in Section 4.2, then is given a classification of the scenarios.

### 4.1 Scenario classification

Communication scenarios can be classified according to three levels of distinction. The first one is the type of communication endpoints (vehicle, roadside, central, personal). The second is the communication mode i.e. whether some infrastructure is involved or not. The third is the communication range i.e. whether the destination is a single communication endpoint or a set of communication endpoints.

A quality discrimination factor is the type of flow: road safety, traffic efficiency, infotainment or signaling (control information).

The number of hops (e.g. Single hop or Multi-hop) is not a discrimination factor since single-hop may be considered as a special case of multi-hop. Performance requirements (e.g. latency and reliability) are not considered in the classification. However, it has to be noted that different communication flows under the same communication mode may have totally different requirements on performance, which may have an important influence on the protocol design. This is why we introduce flow type as a quality discrimination factor.

#### 4.1.1 Communication endpoints

Communications between ITS stations typically involve a sending ITS station and a receiving ITS station. Most scenarios usually involve:

- **V2R**: communication between a vehicle ITS station and a roadside ITS station;
- **V2V**: communication between a vehicle ITS station and a vehicle ITS station;
- **V2C**: communication between a vehicle ITS station and a central ITS station;
- **V2P**: communication between a vehicle ITS station and a personal ITS station.

- **V2L**: communication between a vehicle ITS station and a legacy node (not an ITS station).
- **R2C**: communication between a roadside ITS station and a central ITS station.

Packets may be transmitted either directly, via multiple nodes without infrastructure, via multiple hops with a roadside infrastructure (e.g. V2R2V) or via multiple hops with an Internet infrastructure (e.g. V2C2V) or with both roadside and Internet infrastructure (e.g. V2R2C2V).

#### 4.1.2 Communication mode

Communications may or not involve some infrastructure:

- **Infrastructure-less communication**: direct IPv6 communication between endpoints without involving any infrastructure;
- **Roadside-based communication**: IPv6 communications between endpoints via the roadside infrastructure;
- **Internet-based communication**: IPv6 communications between endpoints via the Internet infrastructure.

The *Infrastructure-less communication* is an ad-hoc mode of communication usually taking place using WiFi (vehicular WiFi based on IEEE 802.11p) between vehicle ITS stations (**V2V**) and possibly involving personal ITS stations (**V2P** (urban WiFi based on IEEE 802.11a/b/g/n)).

The *roadside-based communication* is an infrastructure-based communication mode using a dedicated ITS infrastructure. It mostly covers **V2R** and **R2C** communications, and also **V2V** when such communication is performed via the roadside infrastructure (i.e. V2R2V).

The *internet-based communication* is an infrastructure-based communication mode using infrastructure not dedicated to ITS. It mostly covers **V2L**, **V2C**, **R2C**.

#### 4.1.3 Communication range

Communications could be point-to-point, and point-to-multipoint. In the latter case, communications could involve destination in a given geographical area:

- **Unicast communication range**: between any IPv6 node (ITS station IPv6 node or legacy IPv6 node) or a given ITS station IPv6 node located at a given position in the network topology
- **Multicast communication range**: from any IPv6 node (ITS station IPv6 node or legacy IPv6 node) to a set of ITS stations IPv6 nodes or legacy IPv6 nodes located at various positions in the network topology.
- **Anycast communication range**: from any IPv6 node (ITS station IPv6 node or legacy IPv6 node) to an undefined ITS station IPv6 node or an undefined legacy IPv6 node located at a given position in the network topology.
- **GeoUnicast communication range**: from any IPv6 node (ITS station IPv6 node or legacy IPv6 node) to an ITS station located at a given geographic position.

- **GeoBroadcast communication range:** from any IPv6 node (ITS station IPv6 node or legacy IPv6 node) to a set of ITS stations located within a given geographic area.
- **GeoAnycast communication range:** from any IPv6 node (ITS station IPv6 node or legacy IPv6 node) to an undefined ITS station located within a given geographic area.

Unicast, multicast and anycast are legacy communication means in IPv6. Geocast (i.e. GeoUnicast, GeoAnycast and GeoBroadcast) are communications means defined for non-IP communications (using GeoNetworking). These communication ranges can be implemented in IPv6 using IPv6 multicast combined with GeoNetworking (see Section 2.5.6)

## 4.2 Road safety scenario example

### 4.2.1 Scenario: description

Figure 4.1 illustrates a typical road safety use case where IPv6 is applied.

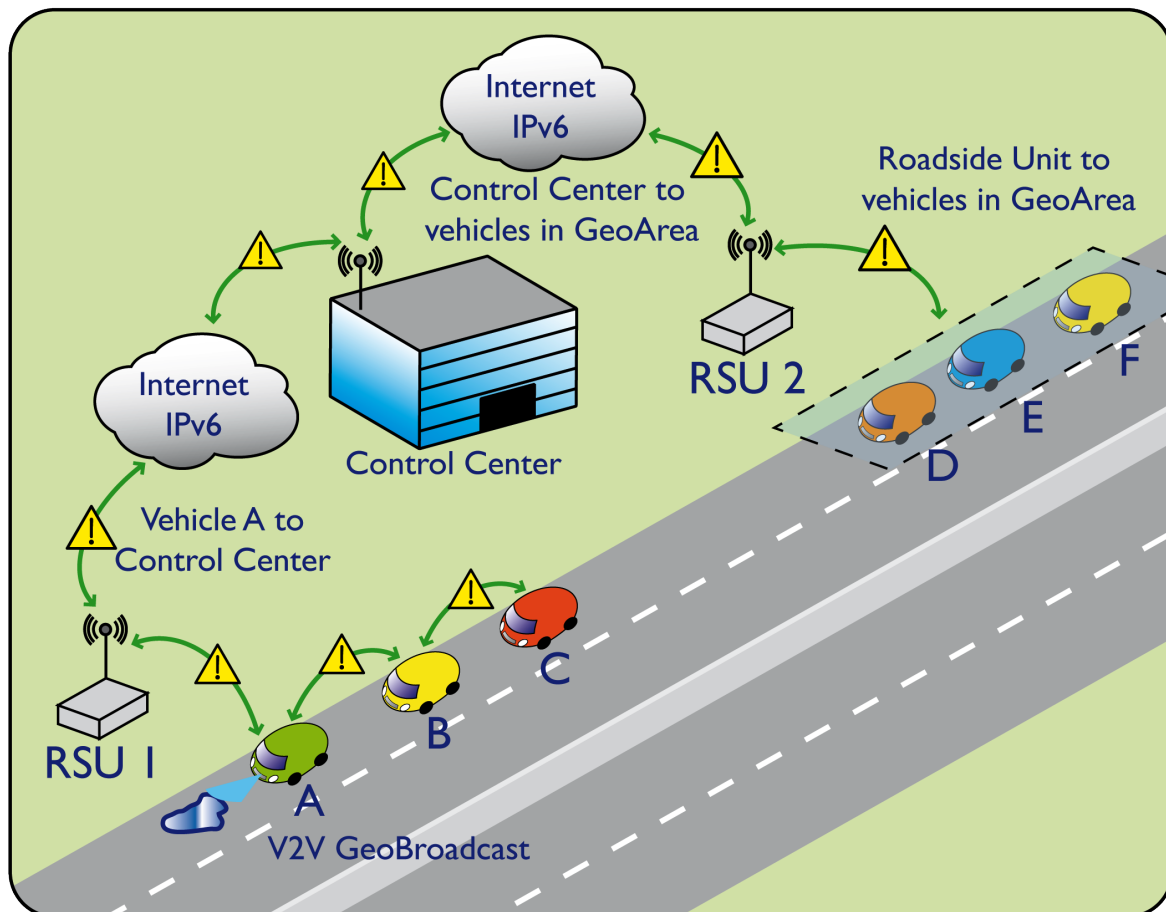


Figure 4.1: IPv6 scenarios

- Vehicle A detect black ice on the road. As an immediate action, the traffic hazard application running on Vehicle A informs all the vehicles driving immediately behind

it about this traffic hazard and the information is broadcasted (GeoBroadcast) from vehicle to vehicle within a limited geographical area. As a result the message reaches Vehicle B which further broadcast the same message to other vehicles and the message reaches vehicle C.

- This road hazard information is going to be valid for some time and vehicles not immediately following but heading to the same spot could benefit from this information too. Vehicle A would thus send this information to a traffic control center server located in the Internet, through the Internet access provided by a roadside ITS station (RSU1 on the Figure)<sup>1</sup>. IP - thus IPv6 - must be used in such a case. Vehicle A transmits this information using IPv6 unicast through RSU1, either directly as shown on the figure, or through intermediate vehicles in case Vehicle A is not anymore in RSU1's radio range. In this latter case, the notification would be forwarded from vehicle to vehicle until it reaches a node connected to the Internet.
- The traffic control center server receives this information and consolidates it with information received from various sources. If appropriate, it periodically transmits road hazard information to all vehicles in some specific geographic area. The black ice report only concerns vehicles heading to a specific point on a specific road. The server would thus send an IP packet using IPv6 multicast to a roadside ITS station (RSU2 on the Figure) known to serve the geographic area where the information should be distributed. Once this information is received, RSU2 would in turn broadcast (GeoBroadcast) it to all vehicles in the specific geographic area. Vehicle E would get the packet first and would retransmit it to other vehicles (i.e. Vehicles D and F).

#### 4.2.2 Scenario: mapping to the classification

The example scenario presented in the above sections actually combines three types of communication:

- The first part from Vehicle A to all vehicles immediately behind is a typical non-IP *infrastructure-less V2V GeoBroadcast* time critical active safety transmission.
- The second part from Vehicle A to the traffic control center is a typical IPv6 *Internet-based V2C Unicast* non time critical safety transmission.
- The third part from the traffic control center to vehicles in a geographic area is a typical IPv6 *Internet-based V2C Multicast* non time critical safety transmission.

#### 4.2.3 Scenario: benefit of IPv6

The benefit of IPv6 over legacy systems not using IPv6 is that the proper delivery of this information is not relying on the availability of dedicated ITS equipment along the road, either at the emitter vehicle side, or the receiver vehicle side, or both. First, other available access technologies could be used (in particular 3G) to notify from the vehicle to the control center and from the control center to the vehicles. Second, IPv6 communications are by nature media agnostic, so the information could be delivered via intermediate vehicles in a situation where the concerned vehicle(s) doesn't have the appropriate access technology. This will necessarily happen due to the penetration rate of any new technology.

<sup>1</sup>Vehicle B could also transmit this information through e.g. a 3G media or a WiFi hot spot, whatever media is available



A second benefit of IPv6 over legacy systems is that IPv6 offers a large set of features available from day 1 and applicable to any scenario and use case while legacy systems are actually restricted to perform the limited set of scenarios that have been implemented. IPv6 therefore offers greater flexibility.

---

## IPv6 protocol stack design goals

---

The purpose of this Chapter is to define what are the requirements for an IPv6 protocol block designed to meet ITS use cases. As such, we present the requirements applying to the IPv6 protocol block of the ITS station networking & transport layer (SNT) of the ITS station reference architecture described in Section 3.1. These requirements are defined according to the scenarios highlighted in Chapter 4 and taking into account lesson learned from past projects related to Cooperative Intelligent Transportation Systems (C-ITS), more particularly the GeoNet (IPv6 GeoNetworking) project [GeoNet-D1.2], and the CVIS (Cooperative Vehicle-Infrastructure Systems) project [CVIS-D3.4], and communication requirements expressed by delegated from C-ITS European Field Operational Tests (FOTs), in particular DriveC2X (Connecting vehicles for safe, comfortable and green driving on European roads), FOTsis (Field Operational Test on Safe, Intelligent and Sustainable Road Operation) and SCORE@F (Système COopératif Routier Expérimental Français).

In the following sections, by mobile ITS station it is meant an ITS station which is changing its point of attachment to the network. This could more frequently apply to vehicle ITS stations and personal ITS stations. The design goals are classified into *Architecture Requirements* (Section 5.1), *Communication type requirements* (Section 5.2) and *Functional Requirements* (Section 5.3). These design goals served as guidelines for ITSSv6 partners for the selection of IPv6 features (see Deliverable D2.2 for the specification of the IPv6 protocol stack) and the development of the IPv6 stack.

### 5.1 Architecture requirements

#### 5.1.1 Cooperative ITS standards compliance

The IPv6 protocol stack shall comply with the set of C-ITS standards specified by ISO TC204, CEN TC278 and ETSI TC ITS. As such, it shall comply with the common communication architecture known as the *ITS station reference architecture* specified by ISO [ISO-21217] and ETSI [ETSI-EN-302-665] (see Sections 2.3 and 3.1).

With respect to IPv6, some features require cooperation between layers (e.g. interface management, security). These are key aspects of the level of performance and the main challenges. As highlighted on Figure 5.1, the IPv6 networking horizontal layer, the management cross-layer, the security cross-layer entities and the interfaces linking these layers (Service

Access Points (SAPs)) together (i.e. the IN-SAP, the NF-SAP, the MN-SAP and the SN-SAP) must be covered by the specification of an efficient IPv6 protocol block complying with the set of C-ITS standards:

- The standard *ITS – CALM – IPv6 Networking* [ISO-21210] shall be assumed as a basis although this standard must be completed by a number of other features. New work items have already been proposed at ISO, in particular *ITS – CALM – IPv6 Networking Security* [ISO-16788] and *ITS – CALM – IPv6 Networking Optimization* [ISO-16789] while other are being proposed.
- For efficient management of IPv6 communication flows (deciding on which interface a given flow of packets should be routed according to application flow requirements, characteristics of currently available access technology and current network availability), the IPv6 protocol stack shall comply with *ITS station management* standards [ISO-24102].

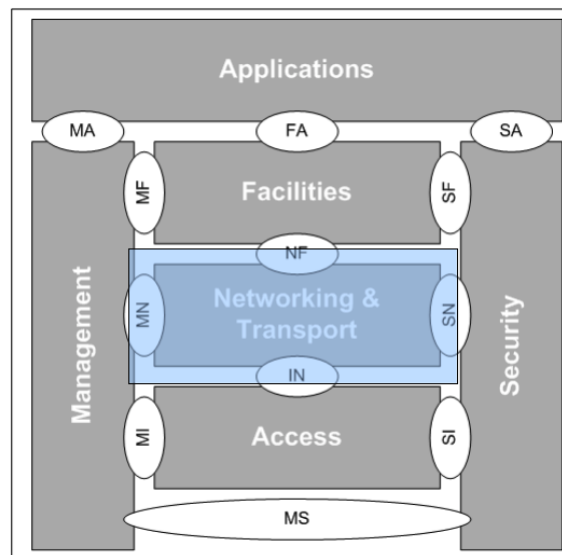


Figure 5.1: Simplified ITS Station (ITS-S) Reference Architecture - Scope of ITSSv6

### 5.1.2 IETF standards reusability

The IPv6 protocol stack shall reuse existing IPv6 protocols specified by the Internet Engineering Task Force (IETF) as long as existing protocols are able to cope with ITS requirements. Otherwise, extensions of existing IETF standards should first be sought. New IPv6 features should only be defined for C-ITS if existing IETF protocols are unable to cope with requirements applying to C-ITS.

The IETF is in charge of the design and the standardization of the protocols of the Internet, from Layer-3 protocols (Internet Protocol) to application protocols (SIP, HTTP, etc.). In addition to IPv6, which has been standardized by the IETF back in 1998[RFC2460], IETF protocols are part of the ITS architecture providing 3 features: Network Mobility, IPv4/IPv6 interoperability and Security.

Based on IPv6 Host Mobility[rfc3775], the design of the Network mobility feature was addressed by the IETF inside the nemo working group created in 2003. This working group

issued the NEMO Basic Support specifications in [rfc3963] in 2005. This group continued working on informational documents before it was concluded in 2008. Host an Network Mobility protocols were extended in the `mext` and `monami6` working groups and now, as these working groups are concluded, are considered as stable protocols.

As IPv6 was standardized, its deployment on existing networks became a big concern in the IETF. First the IETF believed that IPv6 will be deployed by simply replacing IPv4. But the need of continuous operations in IPv4 and the lack of IPv6 connectivity leads the IETF to develop a great variety of solutions to solve the interoperability problem in the great variety of situations in the Internet. First solutions were developed in the `ipv6` working group and, as it was concluded in 2005, now in the `6man` working group. In 2006, the `softwire` working group was assigned with the problem of IPv6 deployment in IPv4 access networks known as the *last-mile problem* faced by network operators. This effort ended up with the standardization of the Softwire Hub and spoks solution specified in [?] in 2009. As the Internet is facing IPv4 addresses depletion, this working group is now working on solutions for the use of residual IPv4 addresses over IPv6 networks.

Security at the Layer-3 level was an early concern of the IETF. This problem was addressed to the `ipsec` working group which designed the IPsec solution back in 1995. This feature was integrated in the new IPv6 protocol. Security is a key feature for IP mobility, as deploying a non-secured solution can lead to major problems. The integration of IPsec with mobility was part of the work done for [rfc3775]. But the proposed solution was not satisfying operational requirements as it was based on pre-shared keys. The IETF the worked on the integration of Internet Key Exchange protocol version 2 (IKEv2)[?] in mobility mechanisms. This effort ended up with the standard [rfc4877] specifying Mobile IPv6 operation with IKEv2.

### 5.1.3 Layer separation

The ITS station reference architecture follows the OSI layered architecture principles, where packets are transmitted between two communication endpoints in a transparent and end-to-end manner without transformation of the content of the packet. Layers are clearly separated which means that the payload of a packet filled up at a certain layer shall be carried transparently by the layers below. No information contained in the payload shall be used at the IPv6 layer to perform any specific operation.

In the context of ITS station reference architecture, parameters necessary by the IPv6 protocol block to take decisions on a per IPv6 packet basis shall be transmitted through theService Access Points (**SAPs**) linking the IPv6 protocol block and the cross-layer ITS station management entity.

### 5.1.4 ITS station types

The IPv6 protocol stack shall support all types of ITS station (vehicle, roadside, central, personal and forthcoming new ones) and shall be configured according to the role played by the ITS station. For instance, a roadside ITS station connected to the Internet via optic fiber may provide Internet access to vehicle ITS stations, while a roadside ITS station connected to a control center via 2G would most likely not. They are playing a different role and the IPv6 stack would be configured differently in terms of requested features, communication security support, etc.

### 5.1.5 ITS station nodes and internal network

An ITS station may be composed of several ITS station nodes (hosts and routers) linked by an ITS station internal network. As such the IPv6 protocol block shall thus support:

- ITS stations where the functions of the ITS stations are deployed in multiple ITS station IPv6 nodes
- all types of ITS station nodes, i.e. ITS station hosts, ITS station routers and ITS station gateways. ITS station routers include border router (**BR**), access router (**AR**), mobile router (**MR**) and home agent (**HA**).
- a (reasonably) unlimited number of IPv6 nodes within an ITS station

### 5.1.6 Access technology diversity

The ITS station reference architecture supports a variety of access technologies of different characteristics, which allows great flexibility to connect ITS stations to one another and to connect ITS station to the Internet, at any given moment or any given location (ubiquitous connectivity). Since no single access technologies can be deployed everywhere for numerous reasons (deployment rate, national policies, vendor policies, technical characteristics, population density, ...), it is important for mobile ITS station (i.e. most particularly vehicle ITS stations) to be able to use whatever access technology is available in a certain area (nation, city, ...).

IPv6 shall be supported through any available access technology supported by the ITS station reference architecture and the IPv6 protocol stack should thus support a variety of access technologies.

It shall be possible to use multiple access technologies either sequentially or simultaneously to transmit IPv6 communication flows. One communication flow may be transmitted on a given available access technology while another would be transmitted over another access technology.

### 5.1.7 Application type diversity

The ITS station reference architecture supports a variety of applications ranged into:

- **Road safety**
- **Traffic efficiency**
- **Infotainment / comfort**

Applications shall be access technology agnostic so that the best available access technology can always be used. However, some application provider or some central authority may prefer or request the use of a specific access technology for a given or set of applications. For doing so, applications shall provide their communication requirements so that the IPv6 protocol block can always select the best communication path (in particular the access technology).

### 5.1.8 Scalability

The IPv6 protocol stack shall be defined so that an unlimited number of ITS stations (vehicles, roadside, central, personal), an unlimited number of ITS station IPv6 nodes and an unlimited number of ITS station internal subnetworks can be supported, in both scarce and dense population of IPv6 nodes.

The IPv6 protocol stack shall limit its signaling and the impact of numerous and mobile ITS stations on the Internet routing table entries.

### 5.1.9 Performance

IPv6 communications shall be realized in such a way that latency, processing overhead, packet overhead, routing inefficiencies are minimized. Performance requirements shall be set by application flow type: end-to-end latency, priority, transmission rate, etc. It is particularly relevant within the context of security, due to the high processing requirements and packet overhead usually required by security operations (e.g. cryptography).

The following performance design goals shall be addressed:

- **Prioritization:** ability to process packets with different priorities, with the highest priority for safety related packets;
- **Reliability:** ability to effectively deliver packets to the destination, with the highest reliability for safety related packets;
- **Latency:** ability to deliver packets to the destination with the lowest transmission delay, with bounded latency for safety related packets;
- **Efficiency:** ability to transmit packets with minimum overhead and minimum network resource consumption, i.e. minimizing packet size and the number of packets, the number of hops between the two communication end points and state in the network, for both payload and signaling packets;
- **Fairness:** ability to be fair among ITS stations with respect to network resources usage (e.g. bandwidth);
- **Robustness:** ability to be robust against security attack and malfunction.

It is usually agreed that not all performance issues can be addressed at once, so there exist a tradeoff. As such, the tradeoff should be subject to the application communication requirements and current environment on a per flow basis and not subject to the capabilities of the ITS station.

### 5.1.10 IETF standards backward compatibility

Backward compatibility with established **IETF** standards is necessary for communication with IPv6 nodes which are not subject to modifications contrary to ITS station IPv6 nodes. The IPv6 protocol block defined for **C-ITS** shall thus allow ITS station IPv6 nodes to communicate with legacy IPv6 nodes and shall allow legacy IPv6 nodes to attach to the ITS station.

## 5.2 Communication type requirements

### 5.2.1 Communication endpoints

The IPv6 protocol stack shall provide means for supporting communications involving on one side an ITS station node endpoint, for any ITS station type, and on the other side i) any other ITS station node endpoint, or ii) a legacy node endpoint. In other words, it shall be possible for:

- a vehicle ITS station IPv6 node to communicate with any other ITS station (roadside, vehicle, central or personal ) IPv6 node or with legacy IPv6 node;
- a roadside ITS station IPv6 node to communicate with any other ITS station (roadside, vehicle, central or personal ) IPv6 node or with legacy IPv6 node;
- a central ITS station IPv6 node to communicate with any other ITS station (roadside, vehicle, central or personal ) IPv6 node or with legacy IPv6 node;
- a personal ITS station IPv6 node to communicate with any other ITS station (roadside, vehicle, central or personal ) IPv6 node or with legacy IPv6 node;
- a legacy IPv6 node to communicate with any ITS station (roadside, vehicle, central or personal ) IPv6 node.

### 5.2.2 Infrastructure-less and infrastructure-based communications

ITS stations may form a self-organized ad-hoc communication network without infrastructure coordination (e.g. using GeoNetworking, see in Section 2.5.6) and the network may or may not be connected to the roadside or Internet infrastructure. In such a situation, the IPv6 protocol stack shall thus provide for:

- **Infrastructure-less communication:** direct IPv6 communication between endpoints without involving any infrastructure;
- **Roadside-based communication:** IPv6 communications between endpoints via the roadside infrastructure;
- **Internet-based communication:** IPv6 communications between endpoints via the Internet infrastructure.

### 5.2.3 Communication range

Routing functions must efficiently support point-to-point, and point-to-multipoint communication modes. As such, the IPv6 protocol stack shall provide means for supporting the following types of IPv6 data transmission:

- **Unicast communication range:** between any IPv6 node (ITS station IPv6 node or legacy IPv6 node) or a given ITS station IPv6 node located at a given position in the network topology
- **Multicast communication range:** from any IPv6 node (ITS station IPv6 node or legacy IPv6 node) to a set of ITS stations IPv6 nodes or legacy IPv6 nodes located at various positions in the network topology.

- **Anycast communication range:** from any IPv6 node (ITS station IPv6 node or legacy IPv6 node) to a undefined ITS station IPv6 node or an undefined legacy IPv6 node located at a given position in the network topology.
- **GeoUnicast communication range;** from any IPv6 node (ITS station IPv6 node or legacy IPv6 node) to an ITS station located at a given geographic position.
- **GeoBroadcast communication range:** from any IPv6 node (ITS station IPv6 node or legacy IPv6 node) to a set of ITS stations located within a given geographic area.
- **GeoAnycast communication range:** from any IPv6 node (ITS station IPv6 node or legacy IPv6 node) to an undefined ITS station located within a given geographic area.

## 5.3 Functional requirements

### 5.3.1 Transparency

The IPv6 protocol stack shall provide transparent IPv6 access, i.e. any available access technology supported by the IPv6 protocol block or available IPv6 communication paths can be used to transmit IPv6 flows without involving the application layer.

### 5.3.2 Internet connectivity

ITS station nodes may need to communicate with peer nodes reachable through the Internet and may also need to be reachable from the Internet. Communication with nodes in the Internet require the use of a global IPv6 address. The IPv6 protocol block shall thus:

- allocate at a minimum a globally unique IPv6 address to each ITS station IPv6 node that must be reachable from the Internet;
- ensure that an ITS station IPv6 node actually connected to the Internet is reachable at a globally unique IPv6 address (reachability).

### 5.3.3 Transient connectivity

ITS stations may change their point of attachment to the network. As a result, IPv6 connectivity may be transient or may be maintained through distinct access technologies or via multiple access technologies in parallel. The IPv6 protocol stack shall thus:

- quickly detect any loss of Internet access and resume communications as soon as connectivity is restored.
- maintain ongoing sessions while an ITS stations is changing its point of attachment to the network (session continuity). This shall be provided whether the same access technology is used from the former access point to the new one (horizontal handovers) or different access technologies are used from the former access point to the new one (vertical handovers).

Session continuity over distinct access network (whether they offer access through the same access technology or not) is usually provided by a *global mobility support* mechanism, while *local mobility support* mechanisms are useful to improve handover delay when the change of attachment point is realized between points of attachment from the same access network.



### 5.3.4 Multiple access technologies

ITS station may be equipped with multiple access technologies, and multiple technologies may be available simultaneously. The IPv6 protocol stack shall thus:

- provide capabilities to realize simultaneous use of multiple access technologies;
- transfer an IPv6 flow from an access technology to another one without breaking on-going session (vertical handovers);
- dynamically change routing policies to be applied to a given IPv6 communication flow.

### 5.3.5 Providing and getting network connectivity

ITS stations may get network connectivity through other ITS stations, either to realize certain local operations (e.g. connecting a vehicle ITS station to a roadside ITS station acting as a charging spot for electric vehicles) or to connect to the Internet (e.g. a roadside ITS station deployed in a service area may provide Internet access to vehicle ITS stations). Personal ITS station brought to the vehicle may also benefit from the network connectivity of the vehicle ITS station.

The IPv6 protocol block shall thus:

- provide capabilities for an ITS station to provide access to other ITS stations;
- provide capabilities for an ITS station to obtain access to other ITS station.

### 5.3.6 Adhoc communications

ITS stations may form a self-organized ad-hoc communication network without infrastructure coordination (e.g. using GeoNetworking, see in Section 2.5.6 and IEEE 802.11p). In such a situation, the IPv6 protocol stack shall thus:

- provide capabilities to realize direct IPv6 communication between neighbor ITS stations without infrastructure coordination;
- allow to perform IPv6 communication over a multi-hop network made of forwarding vehicle and roadside ITS stations;
- allow the combination of GeoNetworking capabilities with IPv6 networking capabilities (at a minimum it shall support [ETSI-TS-102-636-6-1]).

### 5.3.7 Interoperability between IPv6 and IPv4

ITS station IPv6 nodes may need to communicate with legacy IPv4-only nodes providing established ITS services (e.g. traffic efficiency) or non-ITS services (e.g. comfort, infotainment) that will continue to operate in the Internet for some years. In addition, as the IPv4 address depletion is driving a continuous but slow shift to IPv6 connectivity, some access networks may still provide IPv4-only connectivity.

The IPv6 protocol stack shall provides IPv4-IPv6 interoperability means for:

- ITS station IPv6 nodes to establish connectivity with communication peers over IPv4-only access networks,
- ITS station IPv6 nodes to communicate with IPv4-only communication peers

### 5.3.8 ITS station management

A large number of ITS stations will be deployed and will need to be managed remotely. The IPv6 protocol stack itself may need to be reconfigured, for instance every time a vehicle is sold or every time new regulations must be enforced. The IPv6 protocol stack shall allow remote management of the IPv6 parameters.

In addition, since in some implementations the functions of the ITS station may be split into several IPv6 nodes<sup>1</sup>, the IPv6 protocol block shall allow ITS station internal management of all IPv6 nodes composing an ITS station

### 5.3.9 Best communication path selection

Two communication end-points may be able to communicate by various means when multiple access technologies are available at once. In this situation, the most optimal communication path (i.e. which access technologies, and where the packets should be routed to) must be selected according to the application flow requirements and current network characteristics. It is thus necessary to determine what are the communication requirements in terms of QoS, security, etc. for each existing application flow and what are the available communication paths to reach a given party.

### 5.3.10 Security

Securing communication between ITS stations is not an optional feature for Cooperative ITS. Without security protection, unauthorized actions might easily break down the entire communication capabilities of ITS stations and would undermine road safety, traffic efficiency and user confidence in comfort applications. Securing communications requires the definition of needed security services, and the identification of the relevant security mechanisms and protocols that can implement the security services.

The IPv6 protocol block shall provide a level of security equivalent or higher than legacy IPv6 standards (i.e. it shall not create new threats). It shall ensure protection of IPv6 control flows and allow the protection of IPv6 payload flows according to the needs of the applications (the level of protection depends on the use case) . Protection includes authentication of the sender, authorization to perform the action, confidentiality of the data contained in the messages, anti-replay of messages, location privacy, etc.

Communications involving mobile ITS station (i.e. most particularly vehicle and personal ITS stations) are particularly concerned with the ability to communicate while providing location privacy. The IPv6 protocol stack shall thus not expose information allowing unauthorized third parties to track the location of mobile ITS stations.

### 5.3.11 Access technologies

At a minimum, the IPv6 stack shall be able to transmit IPv6 packets over IEEE 802.11p, IEEE 802.a/b/g/n and 2G/3G when such access technologies are available in a given implementation of an ITS station.

#### 5.3.11.1 IEEE 802.11p

The 5.9 GHz radio range has been allocated for vehicular communications in various regions in the world, including Europe, USA and Japan. It allows direct communication between

---

<sup>1</sup>It is indeed envisioned that in most cases an ITS station will actually be implemented into several IPv6 nodes

vehicles ITS stations, and between vehicle and roadside ITS stations. In Europe, IEEE 802.11p is known as ETSI G5 and as the name stands for, is specified by ETSI TC ITS [ETSI-TS-102-636-4-2]. The European IEEE 802.11p provides multiple channels, one of which is reserved for control traffic and on which IPv6 traffic shall not be used. On the other hand, IPv6 could be transmitted over the other channels. The IPv6 stack shall allow the transmission of IPv6 packets on the appropriate 11p channel.

### 5.3.11.2 Cellular access technologies

The usage of 3GPP networks in cooperative systems is evident in current ISO and ETSI communication architectures for ITS. GPRS (2.5G) and, above all, UMTS (3G) can be found as access technologies to be used in vehicular communications systems in both the CALM and European ITS Architecture proposals. It is, of course, envisaged that LTE will be also included when it is available. One could think that continuous IP connectivity could only be achieved nowadays by means of 3GPP communication technologies, thanks to current deployments of mobile telephone operators.

What remains an issue these days is the support of IPv6 by operators, since the support of 3GPP specifications is a reality since Release 5 (2003) of UMTS. The reasons why telephone operators do not offer IPv6 service right now are the same that maintain Internet service providers to still provide IPv4 connectivity: need to update systems, required support for users, lack of staff training, low perception of current IPv4 problems and so on.

Concretely, the current IPv6 support in 3GPP is as follows [Draft3GPPv6]:

- For 2G/3G access to pre-Release-9 (2010) UMTS networks there are two possible connection types: IPv4 or IPv6.
- For 2G/3G access to UMTS networks from Release-9 there are three possible connection types: IPv4, IPv6 or IPv4v6 (dual-stack).
- For LTE (4G) access, which presents some technological advances in both the physical access to the base station and the core network, IP connectivity is offered in an equivalent way than for the previous case, but it is supported from Release-8 (2009).

As can be noted, last 3GPP releases are completely prepared for IPv6 support and even present transition features to make easier operators to move to IPv6 gradually. One of these facilities is the dual-stack support for allowing terminals to connect with both IPv4 and IPv6-based telephone operators. This will allow application providers to start porting implementations to IPv6, while users will be able to use legacy software during several years.

## 5.4 Convergence with non-ITS sectors

### 5.4.1 Internet of Things

The evolution of the Internet towards the Future Internet, with the Internet of Things (IoT) as one of the main drivers, is defining an extension from the initial Industrial Internet, where several sensors, actuators and devices (now called things), are connected to the Internet through gateways and Supervisory Control And Data Acquisition platforms (SCADAs). This Intranet of Things is being extended to smart things with a higher scalability, pervasiveness, and integration into the core of the Future Internet.

This Extranet of Things, is starting to be located on the Internet, addressable through Internet addressing (i.e. IPv6), and consequently accessible through Internet protocols such as

Web Services. The ongoing and future work is the creation of an extended IoT, which requires from the beginning a design of the solutions and products considering the requirements for the integration of the Internet technologies, in order to reach a homogenous integration of the Future Internet, services, people, and the things reaching the Future Internet of Things, Services and People.

This drive to integrate everything into the Internet core is motivated by the market wish to have all processes remotely accessible, together with an understanding that re-engineering an infrastructure to allow this for each application would be prohibitively costly and time-consuming. Moreover, the current evolution from uniform mass markets, to personalized ones, where the customization and user-specified adaptation is a requirement, makes a uniform infrastructure, the Internet, imperative. This allows many components to be re-used, and services to be shared, with correspondingly huge economies of scale and shortened completion times. Clients are always looking for new areas where this infrastructure can be employed. One example is logistics, where there is need to trace small deliveries for customized products from e-business. Other areas are health (where personalized healthcare is allowing the adaptation of the therapy to the context and status of the patient, building automation (where user feedback allows energy-usage optimization from more user involvement, better usage information provision and more ubiquitous control), and smart cities (where citizens want to locate a free parking place for his car) and, generally speaking Intelligent Transportation Systems, where vehicle and roadside sensors could be remotely accessed and, what is more important, IPv6-addressed.

IoT fills the gap between the needs from the evolution of the market, information, users, and things, through moving all of them to a common framework: the Internet. This will be different from the current approach, where applications are based on isolated solutions. Users now require more flexibility and freedom. Offering a common framework allows choice among the available manufacturers, suppliers, service providers, delivery options, and payment services. While this will obviate the need for stand-alone or proprietary solutions, it requires a high level of integration. In fact, it requires a Future Internet of Things, Services and People.

As can be noted, one further step is reached for the integration of IPv6 in the IoT, which is part of the coexistence strategy to manage the heterogeneity of the involved technologies and architectures, in order to meet the interoperability across business, service providers, and users.

# APPENDIX A

---

## List of acronyms

---

**2G** 2nd Generation mobile telecommunications  
**3G** 3rd Generation mobile telecommunications  
**A-GPS** Assisted GPS  
**AnaVANET** ANALyzer for Vehicular Adhoc NETworks  
**AP** Access Point  
**AR** access router  
**ASN.1** Abstract Syntax Notation One  
**AU** Application Unit  
**BA** Binding Acknowledgement  
**BC** Binding Cache  
**BE** Binding Error  
**BID** Binding Identification number  
**BOP** Basic Open Platform  
**BU** Binding Update  
**BUL** Binding Update List  
**BR** border router  
**BT** Bluetechnix Mechatronische Systeme GmbH  
**C2C-CC** Car-to-Car Communication Consortium  
**C2CNet** Car-to-Car Network  
**CALM** Communications Access for Land Mobiles  
**CAM** Co-operative Awareness Messages  
**CCU** Communication and Control Unit  
**CDMA** Code Division Multiple Access  
**CE** Correspondent Entity  
**CEN** European Committee for Standardization  
**CI** Communication Interface  
**C-ITS** Cooperative Intelligent Transportation Systems  
**C-ITSS** central ITS station  
**CIMAE** Communication Interface Management Adaptation Entity  
**CN** Correspondent Node  
**CoA** Care-of Address  
**CoDrive** Co-Pilote pour une Route Intelligente et des Véhicules Communicants  
**Coopers** Co-operative Systems for Intelligent Road Safety  
**CoT** Care-of Test  
**CoTI** Care-of Test Init  
**CR** central router  
**CVIS** Cooperative Vehicle-Infrastructure Systems  
**DAD** Duplicated Address Detection  
**DENM** Decentralized Environmental Notification Messages  
**DHAAD** Dynamic Home Agent Address Discovery  
**DHCP** Dynamic Host Configuration Protocol  
**DMIPS** Dhrystone MIPS, Million instructions per second  
**DNS** Domain Name System  
**DoT** U.S. Department of Transportation  
**DriveC2X** Connecting vehicles for safe, comfortable and green driving on European roads  
**DSRC** Dedicated Short Range Communications

**EC** European Commission  
**ETSI** European Telecommunications Standards Institute  
**FlowID** Flow Identifier  
**FM** Frequency Modulation  
**FMIPv6** Fast Handovers for Mobile IPv6  
**FOT** Field Operational Test  
**FOTsis** Field Operational Test on Safe, Intelligent and Sustainable Road Operation  
**FP6** Sixth Framework Programme  
**FP7** Seventh Framework Programme  
**GLONASS** Global Navigation Satellite System  
**GeoNet** IPv6 GeoNetworking  
**GPRS** General Packet Radio Service  
**GPS** Global Positioning System  
**GPSR** Greedy Perimeter Stateless Routing  
**GSM** Global System for Mobile communications  
**HA** home agent  
**HIP** Host Identity Protocol  
**HMIPv6** Hierarchical Mobile IPv6  
**HNA** Host and Network Association  
**HoA** Home Address  
**HoT** Home Test  
**HoTI** Home Test Init  
**HSPA** High Speed Packet Access  
**I2V** Infrastructure-to-Vehicle  
**ICMPv6** Internet Control Message Protocol version 6  
**ICT** Information Communication Technologies  
**IEEE** Institute of Electrical and Electronics Engineers  
**IETF** Internet Engineering Task Force  
**IME** Interface Management Entity  
**INP** Internal Network Prefix  
**INPA** Internal Network Prefix Advertisement  
**Inria** Institut National de Recherche en Informatique et en Automatique  
**INPD** IPv6 Internal Network Prefix Discovery  
**IINP** ITS Station Internal Network Prefix  
**IP** Internet Protocol  
**IPFR** IP Filter Rule  
**IPsec** Internet Protocol security  
**IPTE** Schalk & Shalk OG  
**IPv6** Internet Protocol version 6  
**ISO** International Organization for Standardization  
**ITS** Intelligent Transportation Systems  
**ITSSP** ITS Station Protocol  
**ITSSPD** ITS Station Protocol Daemon  
**ITS-S** ITS station  
**ITSSv6 web page** <http://www.itssv6.eu>  
**IT** Institut Mines Telecom  
**ITU** International Telecommunication Union  
**L2** Layer 2  
**L2TP** Layer-2 Tunneling Protocol  
**L3** Layer 3  
**LAN** Local Area Network  
**LDM** Local Dynamic Map  
**LLC** Logical Link Control  
**LTE** Long Term Evolution  
**LS** Location Service  
**LT** Location Table  
**LW** lesswire  
**MAC** Medium Access Control  
**MADM** Multiple Attribute Decision Making  
**MAN** Metropolitan Area Network  
**MANET** Mobile Ad-hoc Network  
**MAP** Mobility Anchor Point  
**MCoA** Multiple Care-of Addresses Registration  
**MIB** Management Information Base  
**MIPS** Million instructions per second  
**MLME** Medium Access Control (MAC) Layer Management Entity  
**MN** Mobile Node  
**MNN** mobile network node  
**MNP** Mobile Network Prefix  
**MNPP** Mobile Network Prefix Provisioning

**MobiSeND** Mobile Secure Neighbor Discovery

**MR** mobile router

**MTU** Maximum Transmission Unit

**NA** Neighbor Advertisement

**NAT** Network Address Translation

**NDP** Neighbor Discovery Protocol

**NEMO** Network Mobility

**NemoBS** Network Mobility Basic Support

**NEPL** Network Mobility (**NEMO**) Platform for Linux

**NMEA** National Marine Electronics Association

**NS** Neighbor Solicitation

**NTP** Network Time Protocol

**OASIS** Operation of Safe, Intelligent and Sustainable Highways

**OBU** On-Board Unit

**OLSR** Optimized Link State Routing

**OSI** Open Systems Interconnection

**OSPF** Open Shortest Path First

**PAN** Personal Area Network

**PathID** Path Identifier

**PDR** Packet Delivery Ratio

**PFBU** Peer Flow Binding Update

**PHY** Physical

**P-ITSS** personal ITS station

**PM** Person-Month

**PLME** PHY Layer Management Entity

**PMIPv6** Proxy Mobile IPv6

**PPP** Point-to-Point Protocol

**PR** personal router

**PRESERVE** Preparing Secure Vehicle-to-X Communication Systems

**QoS** Quality of Service

**R2C** Roadside ITS station to Central ITS station

**RA** Router Advertisement

**RADVD** Router Advertisement Daemon

**RDS** Radio Data System

**RFC** Request for Comments

**RIPng** Routing Information Protocol

**R-ITSS** roadside ITS station

**RO** Route Optimization

**RPDB** Routing Policy Database

**RS** Router Solicitation

**RSSI** Received Signal Strength Indication

**RSU** Road Side Unit

**RR** roadside router

**RTT** Round-Trip Time

**SafeSpot** Cooperative vehicles and road infrastructure for road safety

**SAP** Service Access Point

**SAT** ITS station access technologies layer

**SAW** Simple Additive Weighing

**SCORE@F** Système COopératif Routier Expérimental Français

**SCTP** Stream Control Transmission Protocol

**SeVeCom** Secure Vehicular Communication

**SF** ITS station facilities layer

**SHIM6** Level 3 Multihoming Shim Protocol for IPv6

**SHIM6** Site Multihoming by IPv6 Intermediation

**SLAAC** Stateless Address Auto-Configuration

**SME** ITS station management entity

**SMIPv2** Structure of Management Information Version 2

**SNMP** Simple Network Management Protocol

**SNT** ITS station networking & transport layer

**SPI** Security Parameter Index

**SSE** ITS station security entity

**STP** Specific Target Platform

**SZTAKI** Magyar tudományos akademia szamitastechnikai es automatizalasi kutato intezet

**SZT** SZTAKI

**TC204 WG16** Technical Committee 204 Working Group 16

**TCP** Transmission Control Protocol

**UDP** User Datagram Protocol

**UMU** Universidad de Murcia

**UMTS** Universal Mobile Telecommunications System

**UTC** Coordinated Universal Time  
**V2C** Vehicle ITS station to Central ITS station  
**V2I** Vehicle-to-Infrastructure  
**V2L** Vehicle ITS station to legacy system  
**V2P** Vehicle ITS station to Personal ITS station  
**V2R** Vehicle ITS station to Roadside ITS station  
**V2V** Vehicle ITS station to Vehicle ITS station  
**VANET** Vehicular Ad-hoc Network  
**V-ITSS** vehicle ITS station  
**VR** vehicle router  
**VCI** Virtual Communication Interface  
**WAVE** Wireless Access in Vehicular Environments  
**WG** Working Group  
**WGS-84** World Geodetic System 84  
**WIMAX** Worldwide Interoperability for Microwave Access  
**WLAN** Wireless Local Area Network  
**WSMP** Wireless Access in Vehicular Environments (**WAVE**) Short Message Protocol  
**XML** Extensible Markup Language



---

## Bibliography

---

- [CVIS-D3.4] CVIS. D.CVIS.3.4, Final Architecture and System Specifications. Public deliverable, June 2010. pages 15, 33
- [Draft3GPPv6] J. Korhonen, J. Soininen, B. Patil, G. Bajko, and K. Iisakkila. IPv6 in 3GPP Evolved Packet System. IETF Draft, September 2011. pages 42
- [EC-COM-313] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - ADVANCING THE INTERNET - Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe, May 2008. COM(2008) 313 final. pages 15
- [EC-COM-5893] Updated Work Programme 2009 and Work Programme 2010 - Cooperation - Theme 3 - ICT - Information and Communications Technologies, July 2009. COM(2009) 5893. pages 15
- [EC-COM-886] Action plan for the deployment of Intelligent Transport Systems in Europe, December 2008. COM(2008) 886 final. pages 13
- [EC-ICT-Standardization] 2010-2013 ICT Standardisation Work Programme, March 2010. pages 15
- [EC-IPv6-web] IPv6: Enabling the Information Society), 2008, last visited 2010. [http://ec.europa.eu/information\\_society/policy/ipv6/index\\_en.htm](http://ec.europa.eu/information_society/policy/ipv6/index_en.htm). pages 15
- [EC-M/453] STANDARDISATION MANDATE ADDRESSED TO CEN, CENELEC AND ETSI IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGIES TO SUPPORT THE INTEROPERABILITY OF CO-OPERATIVE SYSTEMS FOR INTELLIGENT TRANSPORT IN THE EUROPEAN COMMUNITY, October 2009. pages 10, 13, 15
- [ETSI-EN-302-665] Intelligent Transport Systems (ITS); Communications Architecture, September 2010. ETSI EN 302 665 V1.1.1 (2010-09). pages 12, 17, 22, 33
- [ETSI-TR-102-863] Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM); Rationale for and guidance on standardization, June 2011. ETSI TR 102 863 V1.1.1 (2011-06). pages 24
- [ETSI-TS-102-636-4-1] Intelligent Transport Systems (ITS); Vehicular Communications; Part 4: Geographical Addressing and Forwarding for Point-to-Point and Point-to-Multipoint Communications; Sub-part 1: Media-Independent Functionality, June 2011. ETSI TS 102 636-4-1 V1.1.1 (2011-06). pages 21
- [ETSI-TS-102-636-4-2] Intelligent Transportation Systems (ITS); Vehicular Communications; Part 4: Geographical Addressing and Forwarding for Point-to-Point and Point-to-Multipoint Communications; Sub-part 2: Media-Dependent Functionalities for ITS-G5A media, May 2010. ETSI, work in progress, ETSI-TS-102-636-4-2. pages 21, 42

- [ETSI-TS-102-636-6-1] Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols, March 2011. ETSI TS 102 636-6-1 V1.1.1 (2011-03). pages 13, 16, 21, 40
- [ETSI-TS-102-637-2] Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, March 2011. ETSI TS 102 637-2 V1.2.1 (2011-03). pages 13, 24
- [ETSI-TS-102-637-3] Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification (DENM) Basic Service, September 2010. ETSI TS 102 637-3 V1.1.1 (2010-09). pages 13, 24
- [ETSI-TS-102-723-1] ETSI. Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 1: Architecture and addressing schemes, October 2011. pages 22
- [ETSI-TS-102-723-3] ETSI. Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 3: Interface between management entity and access layer, October 2012. pages 22
- [ETSI-TS-102-723-4] ETSI. Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 4: Interface between management entity and network and transport layers, October 2011. pages 22
- [ETSI-TS-102-731] ETSI. Intelligent Transport Systems (ITS); Security; Security Services and Architecture, October 2010. pages 23
- [Ernst2009] Thierry Ernst, Vilmos Nebhaj, and Runar Sorasen. CVIS: CALM Proof of Concept Preliminary Results. In *9th International Conference on ITS Telecommunications (ITST)*, Lille, France, October 2009. pages 15
- [GeoNet-D1.2] GeoNet. D1.2 Final GeoNet Architecture Design. Public deliverable, June 2010. pages 16, 33
- [GeoNet-D2.2] GeoNet. D2.2 Final GeoNet Specification. Public deliverable, June 2010. pages 16
- [GeoNet-D7.1] GeoNet. D7.1 GeoNet Experimentation Results. Public deliverable, June 2010. pages 15, 16
- [ISO-16788] ISO. Intelligent transport systems – Communications access for land mobiles (CALM) – IPv6 Networking Security, April 2012. ISO/NP 16788:2012(E). pages 13, 34
- [ISO-16789] ISO. Intelligent transport systems – Communications Access for Land Mobiles (CALM) – IPv6 Networking Optimization, April 2012. ISO/NP 16789:2012(E). pages 13, 34
- [ISO-17425] ISO. Intelligent transport systems – Cooperative Systems – Data exchange specification for in-vehicle presentation of external road and traffic related data (In Vehicle signage), April 2012. ISO/NP 17425:2012(E). pages 14
- [ISO-17426] ISO. Intelligent transport systems – Cooperative Systems – Contextual speed, April 2012. ISO/NP 17426:2012(E). pages 14
- [ISO-17429] ISO. Intelligent transport systems – Cooperative Systems – Profiles for processing and transfer of information between ITS stations for applications related to transport infrastructure management, control and guidance, April 2012. ISO/NP 17429:2012(E). pages 14
- [ISO-17465] ISO. Intelligent transport systems – Cooperative Systems – Terms, Definitions and Guidelines for Standards Documents – Part 1, April 2012. ISO/NP 17465:2012(E). pages 10
- [ISO-21210] ISO. Intelligent transport systems – Communications Access for Land Mobiles (CALM) – IPv6 Networking, January 2011. ISO 21210:2011(E). pages 12, 13, 15, 21, 34
- [ISO-21212] ISO. Intelligent transport systems – Communications Access for Land Mobiles (CALM) – CALM using 2G Cellular Systems, April 2008. ISO/IS 21212:2008. pages 23
- [ISO-21213] ISO. Intelligent transport systems – Communications Access for Land Mobiles (CALM) – CALM using 3G Cellular Systems, April 2008. ISO/IS 21212:2008. pages 23
- [ISO-21214] ISO. Intelligent transport systems – Communications Access for Land Mobiles (CALM) – CALM Infra Red, April 2008. ISO/IS 21214:2008. pages 23

- [ISO-21215] ISO. Intelligent transport systems – Communications Access for Land Mobiles (CALM) – CALM M5 , April 2010. ISO/IS 21215:2010. pages 23
- [ISO-21217] ISO. Intelligent transport systems – Communications Access for Land Mobiles (CALM) – Architecture, April 2010. ISO 21217:2010(E). pages 11, 17, 33
- [ISO-21218] ISO. Intelligent transport systems – Communications access for land mobiles (CALM) – Medium service access points, August 2008. ISO/DIS 21218:2008(E). pages 13
- [ISO-24102] ISO. Intelligent transport systems – Communications Access for Land Mobiles (CALM) – Management, September 2010. ISO/FDIS 24102:2010(E). pages 13, 22, 34
- [ISO-24102-1] ISO. Intelligent transport systems – Communications Access for Land Mobiles (CALM) – Part 1: ITS station management, May 2011. ISO/CD 24102-1:2011(E). pages 22, 26
- [ISO-29281-2] ISO. Intelligent transport systems – Communication Access for Land Mobiles (CALM) – Part 2: Fast networking & transport layer protocol (FNTP), June 2011. ISO/CD 29281-2:2011(E). pages 21
- [Lee2011b] Jong-Hyouk Lee, Thierry Ernst, and Jean-Marie Bonnin. Cross-layered architecture for securing IPv6 ITS communication: Example of pseudonym change. In *Cross Layer Design (IWCLD), 2011 Third International Workshop on*, pages 1–6, 2011. pages 23
- [Lee2012a] Jong-Hyouk Lee, Jiefeng (Terence) Chen, and Thierry Ernst. Securing mobile network prefix provisioning for NEMO based vehicular networks. *Mathematical and Computer Modelling*, 55(1-2):170–187, January 2012. pages 23
- [Moe2010] Marie Moe, Vilmos Nebehaj, and Thierry Ernst. CVIS Performance Test Results: Handovers in an 802.11p Network. In *ITST 2010 : 10th International Conference on Intelligent Transport System Telecommunications*, Kyoto, Japan, 2010. pages 15
- [RFC2460] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460 (Draft Standard), December 1998. Updated by RFCs 5095, 5722, 5871. pages 14, 34
- [rfc1918] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear. Address allocation for private internets. RFC 1918 (Best Current Practice), February 1996. pages 14
- [rfc2461] T. Narten, E. Nordmark, and W. Simpson. Neighbor discovery for ip version 6 (ipv6). RFC 2461 (Proposed Standard), 1998. pages 14
- [rfc3775] D. Johnson, C. Perkins, and J. Arkko. Mobility Support in IPv6. RFC 3775 (Proposed Standard), June 2004. Obsoleted by RFC 6275. pages 34, 35
- [rfc3963] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert. Network Mobility (NEMO) Basic Support Protocol. RFC 3963 (Proposed Standard), January 2005. pages 35
- [rfc4877] V. Devarapalli and F. Dupont. Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture. RFC 4877 (Standards Track), 2007. pages 35
- [rfc791] Internet Engineering Task Force. *RFC 791 Internet Protocol - DARPA Internet Programm, Protocol Specification*, September 1981. pages 14
- [url-CVIS] CVIS Project: Cooperative Vehicle-Infrastructure Systems. Web page, Last Visited August 2006. [http://www.ertico.com/en/activities/efficiency\\_\\_environment/cvis.htm](http://www.ertico.com/en/activities/efficiency__environment/cvis.htm). pages 15
- [url-GeoNet] GeoNet Project: IPv6 GeoNetworking. Web page, Last Visited May 2012. <http://www.geonet-project.eu/>. pages 16