



# IPv6 Addressing over G5

---

## Deliverable 2.4.1.6

### Activity 2: Studies

### Sub-activity 2.4 > Specifications

Version: 2.00

Publication date: 12/05/2017



Co-financed by the Connecting Europe  
Facility of the European Union

## Information about the document

Document: IPv6 Addressing over G5

Date of publication: 12/05/2017

Responsible, Entity: Houda LABIOD, Telecom ParisTech

Status: Version 2.00 – Approved

Redactors: Djibrilla Amadou Kountché, Benjamin Cama, Jean-Marie Bonnin, Bernadette Villeforceix, Jean-Marc Odinot, Houda Labiod (Institut Mines Telecom, Orange), Guilhem Autret, Erwan Broquaire et Ludovic Simon

## Publication history

Date	Version	Contributor(s)	Updates & changes	Diffusion
10/08/2016	2.00	Ludovic SIMON	New del.	Release 2

### Reference to the version administration

Version number to be composed of 3 digits > vR.XY

- **R** corresponds to the release number : it is upgraded each time SC Studies validates the diffusion of a new release,
- **X** is the major version number: it is upgraded each time SC Studies validates the deliverable,
- **Y** is the minor version number: it is upgraded each time a contributor changes anything.

Once the deliverable is approved, its version number is upgraded from vR.XY to vR.(X+1)0

Once the deliverable is release, its version number is upgraded from vR.XY to v(R+1).00

As illustration :

- 0.03 > Work in progress version
- 0.10 > Del. Approved by SC Studies but not released
- 2.00 > Del. approved & released (in release 2)
- 2.05 > Del. Updated - in progress version

# Table of Contents

1.	Deliverable's purpose .....	7
2.	Introduction .....	7
3.	IPv6 Addressing.....	9
3.1	Address format .....	9
3.2	Global unicast address .....	10
3.3	Unique local address .....	10
3.4	Link Local Address .....	11
3.5	Multicast address.....	12
3.6	Conclusion.....	12
4.	Neighbor Discovery Protocol .....	13
5.	IPv6 Stateless Address Auto-configuration.....	14
5.1	Common autoconfiguration .....	14
5.2	ITSS-V Specific autoconfiguration .....	16
5.3	ITSS-R Specific autoconfiguration.....	18
6.	Implementation Considerations .....	19
6.1	General requirements.....	19
6.2	PRIVACY REQUIREMENTS.....	19
6.3	ITSS-V.....	20
6.4	ITSS-R.....	20
7.	Security and Privacy Considerations .....	21
7.1	Security .....	21
7.2	Privacy.....	21
8.	NDP Messages Format .....	22
8.1	Router solicitation message format .....	22
8.2	Router advertisement message format.....	23
8.3	Prefix Information .....	24
8.4	Fields.....	25
9.	ITSS-R Configuration.....	26
9.1	Configuration variables.....	26
9.2	Behavior .....	28
10.	ITSS-V Specification.....	29
10.1	Configuration Variables .....	29

---

10.2 Behavior .....	30
11. Conclusion.....	31
Bibliography .....	32

## List of Figures

Figure 1 Communication between ITSS-Vs and ITSS-Rs .....	7
Figure 2 A global unicast address.....	10
Figure 3 Unique local address .....	10
Figure 4 A link local address [4] .....	11
Figure 5 Transformation of a MAC address to an EUI-64.....	11
Figure 6 multicast addresses .....	12
Figure 7 Beginning of the auto-configuration.....	14
Figure 8 Duplication Detection of the link local address .....	15
Figure 9 Reception by the station of a RA.....	16
Figure 10 Duplication detection of the global address .....	17
Figure 11 Configuration of the interface with the address .....	17
Figure 12 RA message format .....	22
Figure 13 Format of the prefix option .....	24

# Glossary

Term/abbreviation	Definition
<b>IP</b>	Internet Protocol
<b>ITSS</b>	ITS-station
<b>ITSS-R</b>	ITS-station road side unit
<b>ITSS-UEVg</b>	ITS-station for road operators infrastructures
<b>ITSS-V</b>	ITS-station for vehicles
<b>NDP</b>	Neighbour Discover Protocol
<b>NS</b>	Neighbour Solicitation
<b>RA</b>	Router Advertisement
<b>SLAAC</b>	Stateless address auto-configuration
<b>UID</b>	Unique IDentifier

# 1. Deliverable's purpose

This deliverable specifies the IPv6 address auto-configuration process on G5 for ITS stations for the first phase (Phase 1) of the SCOOP@F project.

# 2. Introduction

This deliverable describes the address auto-configuration procedure of ITS Stations (Vehicles and Road Side Units) communicating over the ETSI G5 link as illustrated by the figure 1. ITSS-V can communicate directly with each other and with ITSS-Rs. In the following, we consider the IPv6 as network level protocol. In such a network, an ITSS-V can play two non-exclusive roles:

- *Router: It forwards IPv6 packets on behalf of the Application Units (APU) present inside the vehicle. It can also be used to auto-configure the APU, as it will be described later.*
- *Host: end point of the communication. Do not forward packets.*

However, in this deliverable, the ITSS-V is considered as a Host, since it will get automatically an address from ITSS-R and behaves as an endpoint for communication.

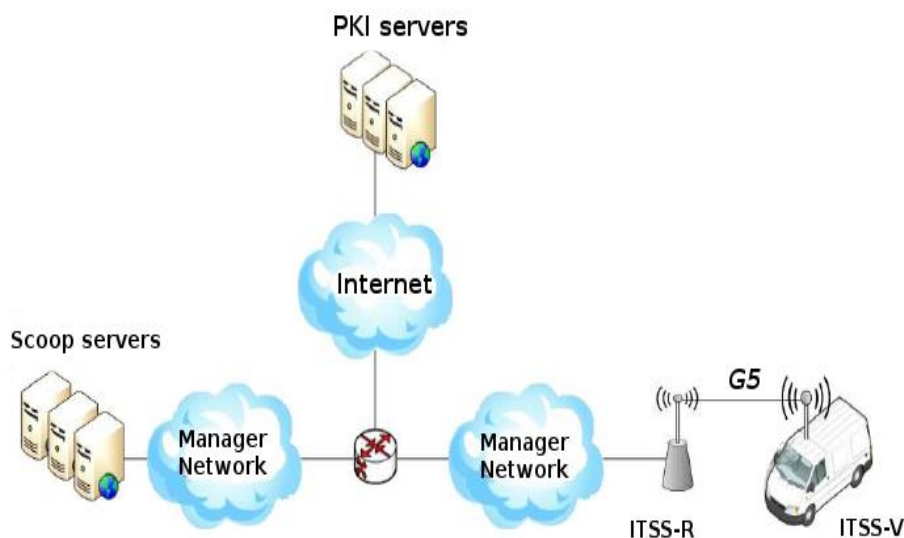


Figure 1 Communication between ITSS-Vs and ITSS-Rs

In order to communicate with other stations using IPv6 protocol, an ITSS-V needs an IPv6 address, which can be obtained manually or automatically via:

- *Statefull configuration via a DHCPv6 server,*
- *Stateless auto configuration.*

Auto-configuration of addresses with local scope (link-local addresses) [1] is done on every interface of ITS stations:

- *Generating a link-local address,*
- *Performing duplicate address detection.*

On Vehicle (ITSS-V), auto-configuration of addresses of global scope can be done on each interface by:

- *Determining the prefix(es) for the link,*
- *Generating one or more global addresses via stateless auto-configuration,*
- *Attempting duplicated address detection.*

In IP networks, a host generates link local addresses when a communication interface is enabled. They are only used for communicating with stations (hosts and routers) attached to the same local link.

Stateless Address Auto-configuration (SLAAC) allows nodes to auto-configure their interfaces using a local interface identifier and the prefixes advertised by the routers. Thus, this auto-configuration is made for each router (prefix advertised).

SLAAC is based on Neighbor Discovery Protocol (NDP) [2].

In ETSI G5, the interface identifier is a MAC address with the following requirements [3]:

- *Supports unicast, broadcast and multicast,*
- *Nodes shall implement a MAC address duplication mechanism,*
- *The use of MAC multicast addresses shall be prohibited in ITS-G5A (5 875 MHz to 5 905 MHz). Therefore, stateless auto-configuration shall only be used on other G5 channels.*

Address duplication procedure is used to ensure that all configured addresses (auto-configured or obtained via DHCPv6) are likely to be unique on a given link [2].

After describing the addressing in IPv6 in the next section, this deliverable presents respectively the NDP protocol and the SLAAC procedure in section 4 and 5. The requirements on implementing SLAAC and NDP in the Scoop@F project are given in section 6. The sections **7** to **10** give configuration parameters of the ITSS-R and ITSS-V. Finally, section **11** concludes this deliverable.



## 3. IPv6 Addressing

### 3.1 Address format

An IPv6 address is a 128 bits word (four times the length of an IPv4 address). This address has two roles:

- *Identification: it identifies a station in a communication,*
- *Localization: it serves for the delivery of the packet.*

These two functions are not yet separated, as the identification is still a research issue.

The quad-dotted IPv4 address representation is abandoned for 8 words of 16 bits representation. For example, the following IPv6 address:

```
00100000 00000001 00001101 10111000 00000000 00000000 00000000 00000000
00000000 00001000 00001000 00000000 00100000 00001100 01000001 01111010
```

is translated to a hexadecimal notation?

```
20 01 0d b8 00 00 00 00 00 08 08 00 20 0c 41 7a
```

Which is segmented into 8 words of 16 bits:

```
2001:0db8:0000:0000:0008:0800:200C:417A
```

The following rules defined how the address should be written:

- *The non-significant zero can be deleted*
- *A sequence of null fields can be replaced by "::". This sign should be applied on the longest sequences of zeros. In the case of equality, it is applied on the first one.*
- *The hexadecimal characters must be written in lower case*
- *When an upper layer port number is specified, the address must be put between brackets*

The preceding address became:

```
2001:db8::8:800:200c:417a
```

An IPv6 address can also be specified with the prefix as in IPv4 Classless Inter Domain Routing (CIDR) address:

```
2001:db8::8:800:200c:417a:/64
```

## 3.2 Global unicast address

A global address is a public IPv6 address. It is illustrated by the figure 2.

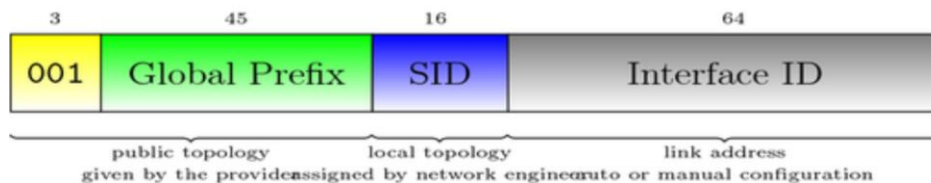


Figure 2 A global unicast address

For example, **2001:660:7301:1:250:baff:febe:712** is a global IPv6 address where :

- 2001: :/64 is the global unicast prefix,
- 660: is the prefix attributed by RIPE-NCC to Renater's Network,
- 7301: is attributed to Télécom Bretagne,
- 1: is the network number inside the Télécom Bretagne network,
- The remaining bits are the interface identifier.

## 3.3 Unique local address

These addresses are equivalent to IPv4 private addresses. They must not be routed out from the local site.

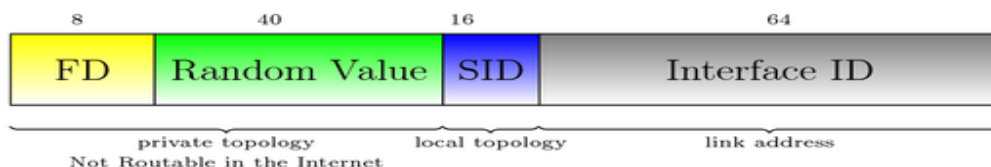


Figure 3 Unique local address

Where:

- Prefix (7 bits): FC00::/7 prefix for IPv6 unique local address (ULA)
- L (1 bit): 1: the prefix is locally set. 0 is reserved for future use.
- Global ID (40 bits): Identifier used to create a Globally Unique Prefix.
- Subnet ID (16 bits): subnet identifier inside the local site.
- Interface ID (64 bits): the interface identifier as described in next section 3.4.

## 3.4 Link Local Address

A link-local address is the concatenation of the prefix **FE80** : :/64 to the identifier of the interface to form an IPv6 address. It is used to communicate with the other station attached to the same physical link. The figure 4 shows this address.

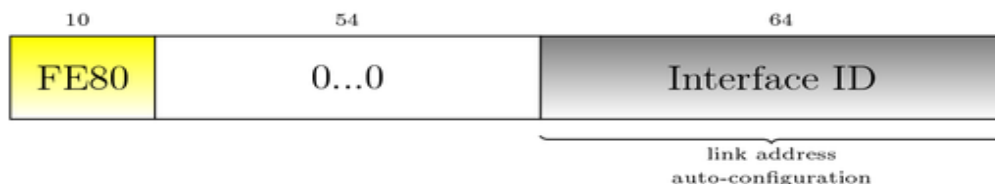


Figure 4 A link local address [4]

Depending on the type of interface identifier, rules exist to transform the link address to a 64 bits address [4]. For example, the figure 5 illustrates the transformation of a MAC address to an Extended Unique Identifier (EUI) of 64 bits.

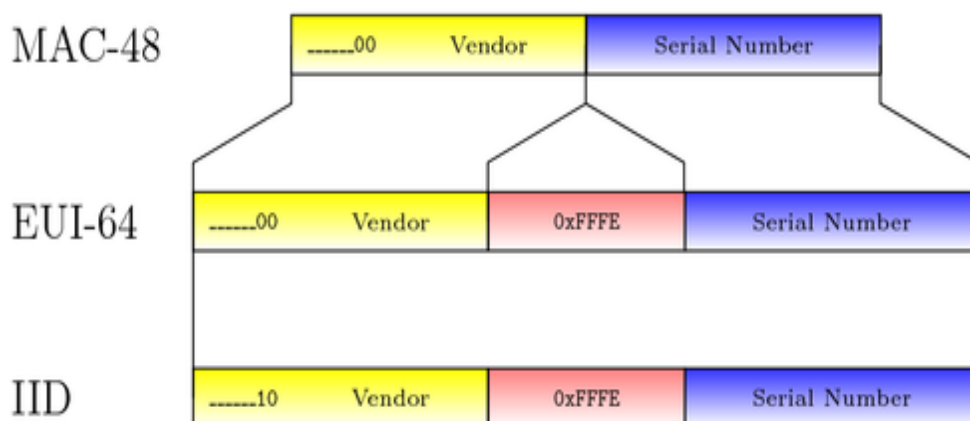


Figure 5 Transformation of a MAC address to an EUI-64

## 3.5 Multicast address

A multicast address identifies a group of machines. The packet sent to this address will be delivered to all the members of the group.



Figure 6 multicast addresses

Where:

- Prefix: *FF00::/8* is the value of IPv6 multicast address
- The bit *x* is not yet set
- *R* and *P* are described in (RFC3306, RFC3956)
- Scope: limit the scope of the multicast address
- Group ID determines the identifiers of the group.

## 3.6 Conclusion

To allow the use of IPv6 over G5 communication, ITSS-Vs are configured to discover the global prefix announced by the infrastructure (ITSS-Rs) and to identify the default router they need to configure their IPv6 communication interfaces.

Neighbor Discovery (NDP) is the protocol used by the ITSS-V to configure its local link address and the global unicast IPv6 address. ITSS-Vs have to build a global unicast IPv6 address to access to the Internet over the G5 link when the service is provided by the infrastructure (ITSS-R). This IPv6 Internet service is used to reach the log server and the PKI.

## 4. Neighbor Discovery Protocol

NDP brings solutions to many problems related to the communication of nodes on the local link. Examples of these problems related to node auto-configuration are given below [2]:

- *Router Discovery,*
- *Prefix Discovery,*
- *Address Auto-configuration is described in section 5,*
- *Duplicate Address Detection.*

Therefore, NDP defines different types of ICMP messages:

- *Router Solicitation/Router Advertisement,*
- *Neighbor Solicitation/Neighbor Advertisement,*
- *Redirect.*

A Router Solicitation message is sent by the host (ITSS-V) when an interface is enabled to request routers for a Router Advertisement instead of waiting for an unsolicited one.

A Router Advertisement message is periodically sent by routers (ITSS-R) to:

- *Advertise their presence,*
- *Indicate the parameters of the link and Internet,*
- *Give information to configure the address.*

A Neighbor Solicitation message is sent by a node (ITSS-V or ITSS-R) to:

- *Determine the link layer address of a neighbor,*
- *Verify that a neighbor is reachable,*
- *Detect duplicate addresses.*
- 

A Neighbor Advertisement message is sent as a response to Neighbor Solicitation message.

A Redirect message is sent by routers to indicate to hosts a better first hop for destination [2].

One of the NDP services assures address resolution as Address Resolution Protocol (ARP) in IPv4.

## 5. IPv6 Stateless Address Auto-configuration

Address auto-configuration is performed for each multicast-capable interface and is performed independently on each interface on multihomed hosts [1].

It has to be noted that this configuration is done for each prefix received from every newly seen router.



An ETSI G5 network uses IEEE 802.11 in the OCB mode (Outside the Context of a BSS). In such a mode, stations do not attach to an access point and the routers/access points do not retransmit the frame to other station in its range.

This deliverable made the hypothesis, that, even when hidden node exists, an address collision is less likely to happen when the MAC address is randomly generated on 48 bits or when the procedure specified in ETSI TS 102 636-6-1 (V1.2.1): GN6ASL, IPv6 over GeoNetworking (section 11) is used.

Therefore, if the IPv6 interface identifier is derived from the MAC address, collision should not occur.

### 5.1 Common autoconfiguration

This section presents approaches applied by the ITSS-V and the router.

The configuration procedure starts when the interface is enabled, for example at the system startup as illustrated by the figure 7.

Interface  
Lien-local:  
Global:  
Gateway:



Interface  
Lien-local: **fe80::IID1**  
Global: **GUA::IID1/64**

Figure 7 Beginning of the auto-configuration

First, the node generates a link-local address as described in section 3.4. This address is considered as a *tentative address* and is not assigned to the interface. Secondly, the node determines the uniqueness of the *tentative address* on the local link by sending a *Neighbor Solicitation message* (NS). This message contains the *tentative address* as target. This exchange is described on figure 8.

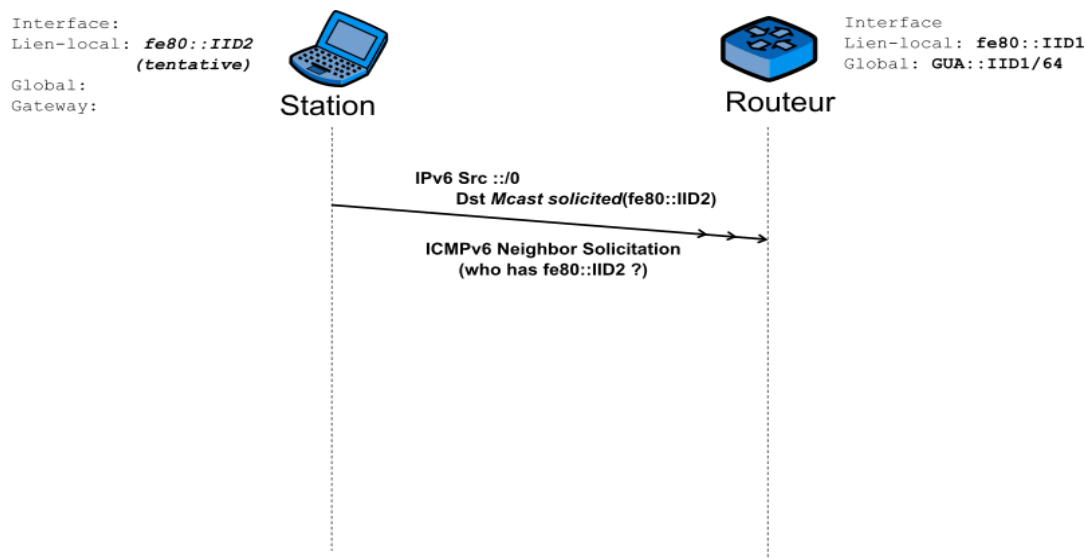


Figure 8 Duplication Detection of the link local address

Upon receiving this message, a receiver node might reply by a:

- *Neighbor Advertisement message (NA) indicating it is using the address;*
- *Another Neighbor Solicitation message indicating it is attempting to auto-configure itself with this address.*

Two different parameters need to be defined for NS emission [2]:

- *The number of times the Neighbor Solicitation is (re) transmitted*
- *The delay time between consecutive solicitations*

When the tentative address is not unique, the auto-configuration process stops. Therefore, two cases can be distinguished:

- *Recover the auto-configuration by specifying an alternate interface identifier considered as unique on the local link;*
- *Or manually configure the address.*

When the tentative address is unique, the node assigns it to the interface. The generation of the link-local address and its uniqueness verification can be done in parallel with waiting for a Router Advertisement.

Because, a router may delay responding to a Router Solicitation for a few seconds, the total time needed to complete auto-configuration can be significantly longer if the two steps are done serially [2].

## 5.2 ITSS-V Specific autoconfiguration

After completing the preceding phase, the ITSS-V determines whether routers are present or not.

When routers are present, they send periodically *Router Advertisement message* (RA) that specify the type of auto-configuration the ITSS-V can apply as illustrated by figure 9.

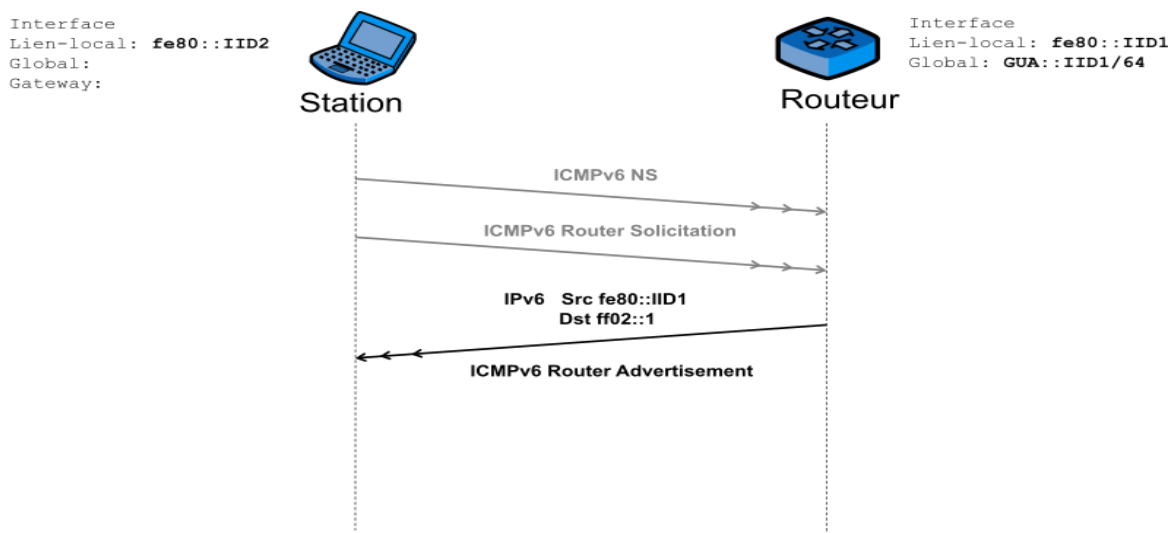


Figure 9 Reception by the station of a RA

Each ITSS-R shall send a Router Advertisement each 2 second.

### Remark:

As proposed in the IETF working document [11] and accordingly to RFC 6275, each ITSS-R should send a Router Advertisement 10 times per second. But such a frequency leads to a high overhead on the G5 wireless access. Anyway, the period of the advertisement might be longer than the time the ITSS-V is ready to wait to configure a new default access router while on the move.

In this case, an ITSS-V can send one or more *Router Solicitations* (RS) to the all-routers multicast group (**FF02::2**) [2]. Any evidence that a new router is available could be used to trigger such a *router solicitations*, for example the reception of a CAM-I message.

The Router Advertisements messages contain zero or more *Prefix Information* options that contain information used by stateless auto-configuration to generate global addresses.



The *autonomous address-configuration flag* option field of *Prefix Information* option indicates whether or not the option applies to stateless auto-configuration. When this flag is activated, other field options can be taken into consideration to indicate:

- A subnet prefix
- Lifetime values

Both values indicate how long the created address remains preferred and valid. An ITSS-V continually receives new advertisements from routers. It then processes new information and updates information received in previous advertisements.

The address duplication detection phase must be applied independently whether it was obtained manually, via stateless address auto-configuration or via DHCPv6 as illustrated by figure 11.

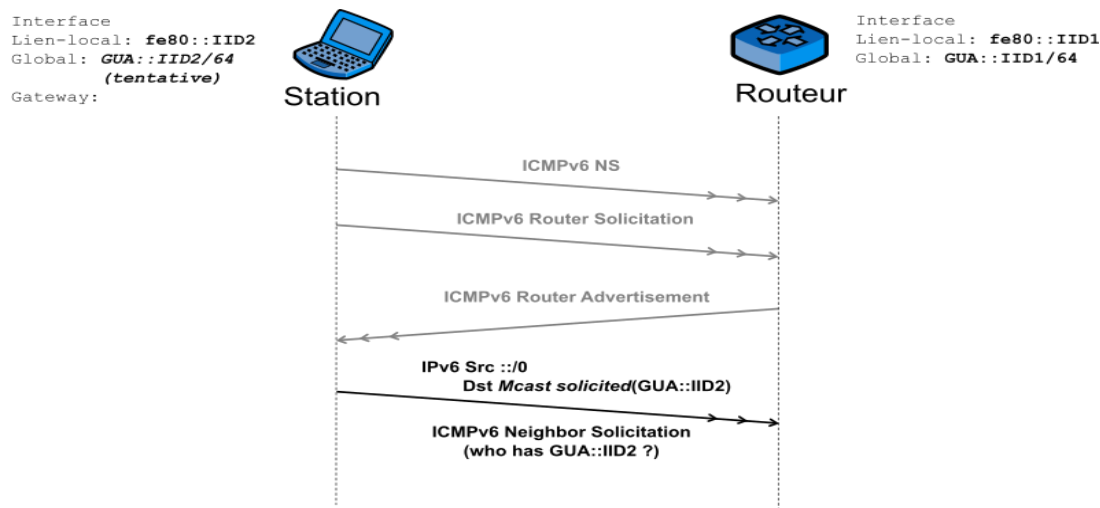


Figure 10 Duplication detection of the global address

Finally, the interface is configured with the global address as illustrated by figure 11.

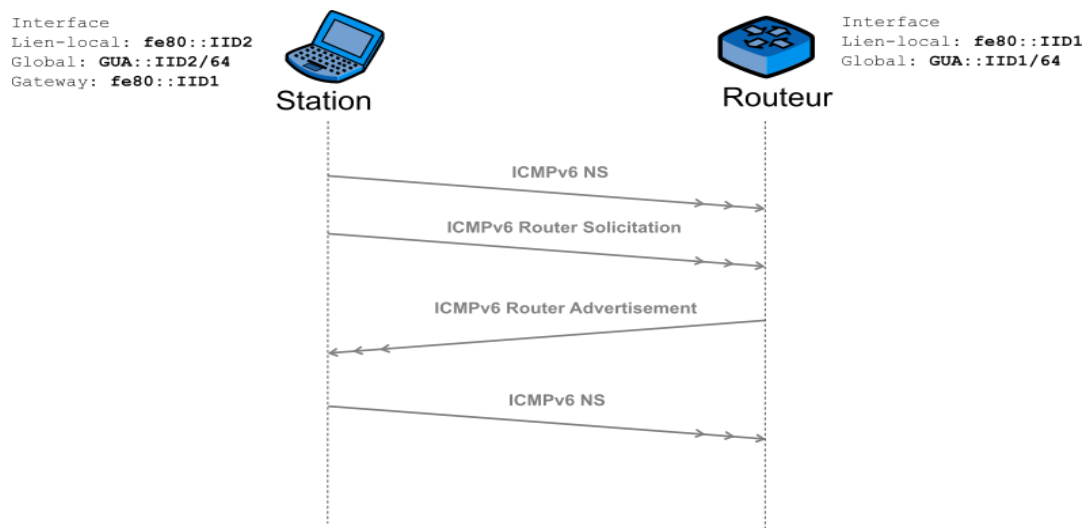


Figure 11 Configuration of the interface with the address

## 5.3 ITSS-R Specific autoconfiguration

The routers are implemented inside the ITSS-R. A Router can:

- *Generate a link-local address using the procedure outlined below.*
- *Perform Duplicate Address Detection on all addresses prior to assigning them to one of its interfaces*

## 6. Implementation Considerations

In this section, the requirements for the implementation of NDP/SLAAC for SCOOP@F project are detailed.



Usually, when the SLAAC procedure is not able to assign the address; it stops and waits for manual configuration.

We propose to implement an automatic recovery procedure, where the ITSS-V will regenerate randomly a local address and restarts the SLAAC procedure until it is correctly configured.

### 6.1 General requirements

- *All the ITS Stations must implement and support the requirements set by the "IPv6 Node Requirements" [5], which includes NDP and SLAAC.*
- *All the ITS Stations must comply with the RFC 4861. Specific updates for SCOOP@F for these stations are given in the appendices of this deliverable.*
- *Source address selection must be done appropriately [6].*

#### 6.1.1 Optional requirements:

- *NDP messages must not be fragmented while they are being sent. Also upon reception nodes must not accept fragmented NDP messages [7].*
- *Implement a better resilience to Neighbor Solicitation message loss [8]*

### 6.2 PRIVACY REQUIREMENTS

For privacy concerns, any permanent identifier of the station must not be revealed. Therefore, the link-local address can be randomly generated or determined from the pseudonym through cryptographic methods (as described in Deliverable 2.4.4-8).

- *The ITSS-V must not use its Original unique identifier (OUI) for the SLAAC purpose. Use mechanisms defined in the next item,*
- *Use one of the following mechanisms to avoid having a permanent identifier for layer 3 addresses [9]:*
  - *Randomly-generated interface identifiers,*
  - *Cryptographically Generated interface identifiers,*
  - *Both of the preceding identifiers need to change over the time.*

Therefore, for IPv6 over G5, all IPv6 related identifier (IID) shall be changed upon pseudonym change. This is similar to the procedure specified in ETSI TS 102 636-6-1 (V1.2.1): GN6ASL, IPv6 over GeoNetworking (section 11).

## 6.3 ITSS-V

- Use the address of the ITSS-R send in the RA to configure its IPv6 layer (default router, prefix, addresses). It should never configure the default router address statically.
- Use optimistic Duplicate Address Detection (DAD)<sup>1</sup> to speed up the address auto-configuration procedure and layer-3 handovers [10]
- We do not currently use DHCPv6, but a vehicle should be able to handle this protocol in the future. The infrastructure can decide to use this protocol to configure complementary information (ex. Domain Name Server or DNS) when such information is not statically present on the station. However, when this information is statically configured in UEV or UBR, it shall be updated if addresses of the configured DNS servers change.
- The ITSS-V shall implement a DNS client to cope with dynamic changes in the network architecture and addressing. However, this is not mandatory in the phase 1 of the Scoop@F project, when such a client is not available, it is necessary to have a procedure to configure the IP addresses of servers used by the UEV (eg. Log or PKI).

## 6.4 ITSS-R

- Optimization of router advertisement [2],
- Implement Border router requirements [13],
- Use advertisement interval option and Neighbor Unreachability option to indicate to ITSS-V that the ITSS-R is still reachable,
- Increase the RA frequency (each 2 second) to ensure faster detection of ITSS-R station in range.
- Do not set the "Managed address configuration" flag, as we are not currently using DHCPv6,
- Determine a way to select the "best" ITSS-R, which will avoid the ITSS-R to do handover. This can be a CAM message, the RSSI of RA, etc. [11].
- An ITSS-V can « see » at the same time many ITSS-Rs and will configure an IPv6 address for each of the prefix received. Therefore, the ITSS-V has to choose the default address to use as source address and also which router is the default router. Use the router having the longest AdvReachableTime.
- Vehicles should not use addresses from a prefix announced by a no-more reachable router. This can be achieved on the ITSS-R by short-lived prefixes, or by exchanging reachability information with the lower-layer protocol
- IT shall be considered to use wireless bridges to extend the scope of the ITSS-Rs

### Remark:

Each ITSS-R will announce a specific prefix of 64 bits of length.

<sup>1</sup> Optimistic DAD has been introduced to:

- Minimize address configuration delays in the successful case,
- Reduce disruption as far as possible in the failure case
- Remain interoperable with unmodified hosts and routers

Therefore, a station will start by using the address (Optimistic address) as source address before the completion of the DAD process.

## 7. Security and Privacy Considerations

### 7.1 Security

It is well known that NDP is subject to the following security threats:

- *Denial-of-Service (DoS),*
- *Address spoofing,*
- *Router spoofing.*

The implementation of secure neighbor discovery could be considered if necessary [14]:

- *Secure Neighbor Discovery (SEND) mechanisms.*

### 7.2 Privacy

ITSS is potentially subject to the following privacy attacks:

- *Correlation of activities over time,*
- *Location tracking,*
- *Others device specific.*

Implements if necessary:

- *Considerations indicated in [9, 12].*



For privacy issues, we propose that by default, ITSS-Vs randomly generate their interface identifiers on 48 bits and change the application level pseudonyms.

## 8. NDP Messages Format

NDP messages are ICMP messages encapsulated in IP.

### 8.1 Router solicitation message format

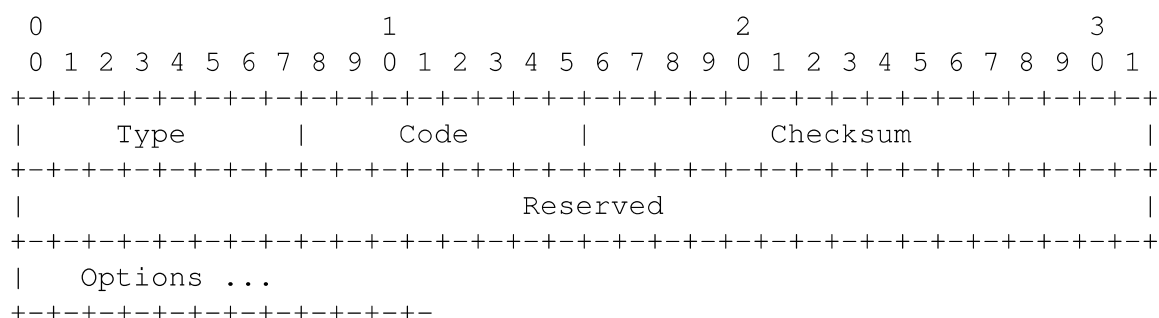


Figure 12 RA message format

#### 8.1.1 IP Header

**Source Address** MUST be the link local address assigned to the interface from which this message is sent.

**Destination Address** All-routers multicast address (**FF02:: 2**).

**Hop Limit** 255

#### 8.1.2 ICMP Header

**Type:** 133

**Code:** 0

**Checksum:** ICMP Checksum.

**Reserved:** Unused field. MUST be initialized to zero.

#### 8.1.3 Options

**Source link-layer address:** The link layer address of the sender, if known. MUST not be included if the Source Address is the unspecified address ( **: :128**). Otherwise, it SHOULD be included on link layers that have addresses.

## 8.2 Router advertisement message format

### 8.2.1 IP Header

**Source Address** MUST be the link local address assigned to the interface from which this message is sent.

**Destination** Can be:

- Can be the: Source address of an invoking RS.
- All-nodes multicast address (FF02 ::1)

Hop Limit 255

### 8.2.2 ICMP Field

Type	134
Code	0
Checksum	ICMP Checksum
Cur. Hop Limit	8-bit unsigned. Default values that nodes should place in the Hop Count Field of the IP header of outgoing IP packets. 0 means unspecified by this router.
M	<i>Managed address configuration flag.</i> Is set to 0 to indicate that in Scoop@F, DHCPv6 is not used
O	<i>Other configuration flag</i> indicates that other configuration information are used via DHCPv6. Is set to 0 as M
Reserved	MUST be initialized to zero by the sender. MUST be ignored by the receiver.
Router LifeTime	The lifetime associated with the default router in units of seconds.
Reachable Time	The time, in milliseconds, that a node assumes a neighbor is reachable after having received a reachability confirmation. Use by Neighbor Unreachability detection algorithm (NUD). 0 means unspecified by this router
Retrans Timer	The time, in milliseconds, between retransmitted NS messages. Used by address resolution and the NUD algorithm. 0 means unspecified by this router.

## 8.2.3 Options

Source link-layer address	The link-layer address of the interface from which the RA is sent. Only used on link layers that have addresses. A router MAY omit this option in order to enable inbound load sharing across multiple link-layer addresses.
MTU	Set for links having variable values.
Prefix information	Set the options for the SLAAC.

## 8.3 Prefix Information

The Prefix Information option provides hosts with on-link prefixes and prefixes for Address Auto-configuration. The Prefix Information option appears in Router Advertisement packets and MUST be silently ignored for other messages.

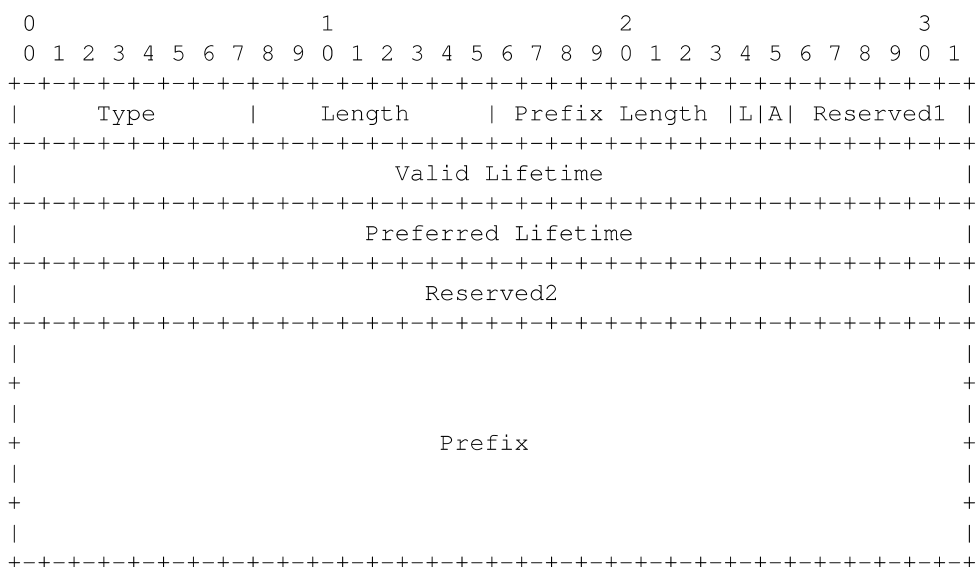


Figure 13 Format of the prefix option



## 8.4 Fields

Type	3
Length	4
Prefix Length	8-bit unsigned. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128. The prefix Length field provides necessary information for on-link determination (when combined with L flag in the prefix information option). It also assists with address auto-configuration as specified as in [1] for which there may be more restrictions on the prefix Length.
L	1-bit on-link flag. When set, indicates that this prefix can be used for on-link determination. When not set the advertisement makes no statement about on-link or off-link properties of the prefix. In other words, if the L flag is not set a host MUST NOT conclude that an address derived from the prefix is off-link. That is, it MUST NOT update a previous indication that the address is on-link
A = 1	1-bit autonomous address-configuration flag. When set indicates that this prefix can be used for SLAAC [1].
Reserved1	6-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.
Valid Lifetime	32-bit unsigned integer. The Length of time in second (relative to the time the packet is sent) that the prefix is valid for the purpose of on-link determination. A value of all one bits (0xffffffff) represents infinity. The Valid Lifetime is also used by SLAAC.
Preferred Lifetime	32-bit unsigned integer. The length of time in seconds (relative to the time the packet is sent) that addresses generated from the prefix via SLAAC remain preferred. A value of all one bits (0xffffffff) represents infinity. The Valid Lifetime is also used by SLAAC. Note that the value of this field MUST NOT exceed the Valid Lifetime field to avoid preferring addresses that are no longer valid.
Reserved2	This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.
Prefix	An IP address or a prefix of an IP address. The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length are reserved and MUST be initialized to zero by the sender and ignored by the receiver. A router SHOULD NOT send a prefix option for the link-local prefix and a host SHOULD ignore such a prefix option.

## 9. ITSS-R Configuration

### 9.1 Configuration variables

The specifications in this section describe the default implementation of the NDP protocol.

Thus, it does not target specific IPv6 implementations such as MIPv6 needs. Therefore, for such cases, it is recommended to handle them in a different deliverable which will update the recommendations made here. For example, the RFC 6275 gives updated values for certain of the variables presented in this section.

IsRouter	<p>A Indicates whether routing (packet forwarding) is enabled on this interface.</p> <p><i>Default: TRUE</i></p>
AdvSendAdvertisements	<p>Indicates whether or not the router sends periodic Router Advertisements and responds to Router Solicitations.</p> <p><i>Default: TRUE</i></p>
MaxRtrAdvInterval	<p>Maximum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds. MUST be in [4, 1800] seconds.</p> <p><i>Default: 2 seconds</i></p>
MinRtrAdvInterval	<p>Minimum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds. MUST be in [3, 0.75 × MaxRtrAdvInterval]</p> <p><i>Default : {</i> <math>0.33 * \text{MaxRtrAdvInterval}</math> <i>If MaxRtrAdvInterval ≥ 9 seconds</i></p> <p><i>MaxRtrAdvInterval otherwise</i></p>
AdvManagedFlag	<p>Value of "Managed address configuration" flag field in the Router Advertisement.</p> <p><i>Default: FALSE</i></p>
AdvOtherConfigFlag	<p>Value of "Other configuration" flag field in the Router Advertisement.</p> <p><i>Default: FALSE</i></p>

AdvLinkMTU	<p>Value of MTU options sent by the router.</p> <p>Default: 0</p>
AdvReachableTime	<p>Value of the Reachable Time field in the Router Advertisement messages sent by the router. MUST be no greater than 3,600,000 milliseconds (1 hour).</p> <p>Default: 0</p>
AdvRetransTimer	<p>Value of the Retrans Timer field in the Router Advertisement messages sent by the router. Default: 0</p>
AdvCurHopLimit	<p>Value of the Cur Hop Limit field in the Router Advertisement messages sent by the router. The value should be set to the current diameter of the Internet.</p> <p>Default: 64</p>
AdvDefaultLifetime	<p>Value of the Router Lifetime field of Router Advertisements sent from the interface, in seconds. MUST be either zero or between MaxRtrAdvInterval and 9000 seconds. A value of zero indicates that the router is not to be used as a default router.</p> <p>Default: <math>3 * \text{MaxRtrAdvInterval}</math></p>
AdvPrefixList	<p>List of prefixes to be placed in Prefix Information options in Router Advertisement messages sent from the interface.</p> <p>Default: all the on-link prefixes</p> <p>The link-local prefix SHOULD NOT be included in the list of advertised prefixes.</p>

## 9.1.1 Prefix information configuration variables

AdvValidLifetime	<p>Value of the Valid Lifetime in the Prefix Information option, in seconds. A value of all 0xffffffff represents infinity. Implementations MAY allow AdvValidLifetime to be specified in two ways: - a time that decrements in real time, that is, one that will result in a Lifetime of zero at the specified time in the future, or</p> <p>- A fixed time that stays the same in consecutive advertisements.</p> <p>Default: depends of the reachability of the ITSS-R</p>
AdvOnLinkFlag	Value of the on-link flag («L-bit ») field in the prefix information option
SLAAC additional information associated with each of the prefixes	
AdvPreferredLifetime	<p>Value of the Preferred Lifetime in the Prefix Information option, in seconds. A value of all 0xffffffff represents infinity. See [1] for details on how this value is used. The ways to specify the value is the same as the one given for AdvValidLifetime.</p> <p>Default: TODO Link to ITSS-R reachability</p> <p>This value MUST NOT be larger than AdvValidLifetime.</p>
AdvAutonomousFlag	<p>Value of the Autonomous Flag field in the Prefix Information option.</p> <p>Default: TRUE</p>

## 9.2 Behavior

In this deliverable, the behavior corresponds to how the station handles the following items as defined in [2].

Redefine, if necessary, the behavior of ITSS-R

- *Sending Unsolicited Router Advertisements*
- *Ceasing To Be an Advertising Interface*
- *Processing Router Solicitations*
- *Router Advertisement Consistency*
- *Link-local Address Change*

## 10. ITSS-V Specification

### 10.1 Configuration Variables

Defines here configuration variables for the ITSS-VR. None are defined for host.

#### 10.1.1 Host Variables

This section describes configuration variables values for each interface.

LinkMTU	The MTU of the link.  Default: ETSI G5 MTU value.
CurHopLimit	The default hop limit to be used when sending IP packets.  Default: 64
BaseReachableTime	A base value used for computing the random ReachableTime value. Default: REACHABLE_TIME milliseconds.
ReachableTime	The time a neighbor is considered reachable after receiving a reachability confirmation.  This value should be a uniformly distributed random value between MIN_RANDOM_FACTOR and MAX_RANDOM_FACTOR times BaseReachableTime milliseconds. A new random value should be calculated when BaseReachableTime changes (due to Router Advertisements) or at least every few hours even if no Router Advertisements are received.
RetransTimer	The time between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. Default: RETRANS_TIMER milliseconds

## 10.2 Behavior

In this deliverable, the behavior corresponds to how the station handles the following items as defined in [2].

Redefine, if necessary, the behavior of ITSS-V

- *Interface Initialization*
- *Processing Received Router Advertisements*
- *Timing out Prefixes and Default Routers*
- *Default Router Selection*
- *Sending Router Solicitations*

## 11. Conclusion

This deliverable describes the mechanisms used to configure ITSS-V and ITSS-R addresses. By using these mechanisms, a vehicle can be able to automatically acquire IPv6 addresses and communicate on the ETSI G5 local link or connect to Internet when available. Stateless Address Auto-Configuration (SLAAC) is the main mechanism described. It allows the ITSS-V to create a unique link local address and global address based on the advertised prefix from the ITSS-R.

## Bibliography

- [1] Narten, T., S. Thomson and T. Jinmei. "IPv6 Stateless Address Autoconfiguration." RFC 4862 (Draft Standard). Internet Engineering Task Force, sep 2007.
- [2] Narten, T., et al. "Neighbor Discovery for IP version 6 (IPv6)." RFC 4861 (Draft Standard). Internet Engineering Task Force, sep 2007.
- [3] ETSI. "202 663 V1. 1.0 (2010-01) Intelligent Transport Systems (ITS)." European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 (n.d.).
- [4] Cizault, Gisèle. IPv6: Théorie et pratique. O'Reilly France, 2005.
- [5] Jankiewicz, E., J. Loughney and T. Narten. "IPv6 Node Requirements." RFC 6434 (Informational). Internet Engineering Task Force, dec 2011.
- [6] Thaler, D., et al. "Default Address Selection for Internet Protocol Version 6 (IPv6)." RFC 6724 (Proposed Standard). Internet Engineering Task Force, sep 2012.
- [7] Gont, F. "Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery." RFC 6980 (Proposed Standard). Internet Engineering Task Force, aug 2013.
- [8] Krishnan, S., D. Anipko and D. Thaler. "Packet-Loss Resiliency for Router Solicitations." RFC 7559 (Proposed Standard). Internet Engineering Task Force, may 2015.
- [9] Narten, T., R. Draves and S. Krishnan. "Privacy Extensions for Stateless Address Autoconfiguration in IPv6." RFC 4941 (Draft Standard). Internet Engineering Task Force, sep 2007.
- [10] Moore N., "Optimistic Duplicate Address Detection (DAD) for IPv6." RFC 4429 (Proposed Standard). Internet Engineering Task Force, apr 2006.
- [11] Benamar, Nabil, Tim Leinmueller and Alexandre Petrescu. "Transmission of IPv6 Packets over IEEE 802.11 Networks Outside the Context of a Basic Service Set." Internet-Draft. Ed. Internet Engineering Task Force. Internet Engineering Task Force, 2016.
- [12] Cooper, A., F. Gont and D. Thaler. "Security and Privacy Considerations for IPv6 Address Generation Mechanisms." RFC 7721 (Informational). Ed. Internet Engineering Task Force. mar 2016.
- [13] Singh, H., et al. "Basic Requirements for IPv6 Customer Edge Routers." RFC 7084 (Informational). Internet Engineering Task Force, nov 2013.
- [14] Arkko, J., et al. "SEcure Neighbor Discovery (SEND)." RFC 3971 (Proposed Standard). Internet Engineering Task Force, mar 2005