


IST-2001-32603	Deliverable D 2.4.2	
----------------	---------------------	--

Project Number:	<b>IST-2001-32603</b>
Project Title:	<b>6NET</b>
CEC Deliverable Number:	<b>32603/UOS/DS/2.4.2/A1</b>
Contractual Date of Delivery to the CEC:	30 <sup>th</sup> June 2003
Actual Date of Delivery to the CEC:	30 <sup>th</sup> September 2003
Title of Deliverable:	D2.4.2: Final report on IPv6-specific implications for Wireless LAN/MAN transition to IPv6
Work package contributing to Deliverable:	WP2
Type of Deliverable*:	R
Deliverable Security Class**:	PU
Editors:	Tim Chown (University of Southampton)
Contributors:	Work Package 2 participants

\* Type: P - Prototype, R - Report, D - Demonstrator, O - Other

\*\* Security Class: PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

**Abstract:**

In this report we complement the reporting in 6NET Deliverable D4.2.1 “IPv6 Access Issues for Wireless LANs” and the subsequent Deliverable D4.2.2 “A Framework for the Support of IPv6 Wireless LANs” by highlighting and commenting on issues that network managers used to thinking the “IPv4 way” should be aware of when considering IPv6 WLAN deployments. This is an update of the initial scoping report for those issues, D2.4.1.

**Keywords:**

IPv6 transition, IPv6 Wireless LAN

---

## Executive Summary

In this report we complement the reporting in 6NET Deliverable D4.2.1 “IPv6 Access Issues for Wireless LANs” and the subsequent Deliverable D4.2.2 “A Framework for the Support of IPv6 Wireless LANs” by highlighting and commenting on issues that network managers used to thinking the “IPv4 way” should be aware of when considering IPv6-only or dual-stack IPv4-IPv6 WLAN deployments.

These issues include:

- IPv6 address assignment and allocation management
- Traffic management
- Wireless LAN access point management and monitoring
- Layer 2 IPv6 Multicast support
- Access control and authentication methods
- IPv6 Mobility issues
- Security considerations
- New network devices and technologies

This report is an update of Deliverable D2.4.1.

## Table of Contents

<b>1.</b>	<b>INTRODUCTION.....</b>	<b>4</b>
<b>2.</b>	<b>ISSUES FOR INTRODUCTION OF IPV6 WLAN SERVICES.....</b>	<b>5</b>
2.1.	IPV6 ADDRESS ASSIGNMENT AND ALLOCATION MANAGEMENT.....	5
2.1.1.	<i>Private IP address space and NAT.....</i>	5
2.1.2.	<i>Increased subnet size.....</i>	5
2.1.3.	<i>Resizing subnets.....</i>	5
2.1.4.	<i>Use of DHCPv6.....</i>	6
2.1.5.	<i>Usage of stateful or stateless network autoconfiguration.....</i>	6
2.2.	TRAFFIC MANAGEMENT.....	6
2.3.	WIRELESS LAN ACCESS POINT MANAGEMENT AND MONITORING.....	7
2.4.	LAYER 2 MULTICAST SUPPORT.....	7
2.5.	ACCESS CONTROL AND AUTHENTICATION METHODS.....	7
2.5.1.	<i>Access control.....</i>	7
2.5.2.	<i>Support for roaming access.....</i>	8
2.6.	IPV6 MOBILITY ISSUES: INTRA-CAMPUS ROAMING.....	8
2.7.	SECURITY CONSIDERATIONS.....	9
2.7.1.	<i>Network port scanning.....</i>	9
2.7.2.	<i>IP-based identification and authentication.....</i>	9
2.7.3.	<i>Pre-generation of reverse DNS.....</i>	10
2.7.4.	<i>Rogue Router Advertisements.....</i>	10
2.7.5.	<i>Secure Neighbor Discovery.....</i>	10
2.7.6.	<i>Cryptographically Generated Addresses (CGA).....</i>	10
2.8.	NEW NETWORK TECHNOLOGIES.....	10
2.8.1.	<i>Requirements of new types of devices.....</i>	11
2.8.2.	<i>Personal Area Networks (PANs).....</i>	11
<b>3.</b>	<b>TECHNOLOGIES UNDER DEVELOPMENT.....</b>	<b>11</b>
<b>4.</b>	<b>CONCLUSIONS.....</b>	<b>12</b>
<b>5.</b>	<b>REFERENCES.....</b>	<b>13</b>

## 1. Introduction

The 6NET Project has already produced a detailed report on IPv6 Access Issues for Wireless LANs [d421], and the subsequent Deliverable D4.2.2 [d422] describing a Framework for the Support of IPv6 Wireless LANs. In those reports we detailed the Wireless LAN standards, deployment scenarios, access control methods, roaming methods available for IPv6 WLAN deployment (IPv6-only or dual-stack IPv4 and IPv6) and the relationship with Mobile IPv6.

To a large extent the text of those deliverables covers much of what could be written here. However, in this accompanying report we focus on the issues that network managers who are used to “thinking the IPv4 way” should be aware of when considering introducing IPv6 services over Wireless LANs.

These issues are categorised in the subsequent section into the following areas:

- IPv6 address assignment and allocation management – differences caused by the larger address space and in particular the larger default /64 IPv6 subnet size, and usage of stateful (DHCPv6) and stateless autoconfiguration
- Traffic management – IPv6 has no broadcast traffic but does make use of multicast, which can flood a WLAN is not controlled.
- Wireless LAN access point management and monitoring – WLAN access points need to be configurable and be monitored over IPv6, and include IPv6 MIBs.
- Layer 2 IPv6 Multicast support
- Access control and authentication methods
- IPv6 Mobility issues
- Security considerations
- New network devices and technologies

We then present a summary of ongoing developments in the most closely related supporting technologies. The project will continue to track these developments, mainly in the Work Package 4 activities.

## 2. Issues for Introduction of IPv6 WLAN Services

In this section we detail the new IPv6-specific issues for Wireless LAN management and operation. Specific detail of IPv6 WLAN technology is given in 6NET Deliverables D4.2.1 and D4.2.2.

### 2.1. IPv6 address assignment and allocation management

There are a number of issues in IP address assignment, allocation and management that differ between IPv4 and IPv6. These are not limited to the wireless medium.

#### 2.1.1. Private IP address space and NAT

The principal benefit of IPv6 is increased address space [rfc2460]. IPv6 offers a greatly increased address space compared to IPv4, i.e. 128 bits against 32 bits. It is thus not expected that IPv6 WLANs will use IPv6 NAT (as there is then no benefit to moving to IPv6).

IPv6 WLANs are expected to use provider-assigned globally routable addresses for ordinary usage when the WLAN is connected to the (IPv6) Internet.

For disconnected IPv6 WLANs some form of local addressing is required. At the time of writing the IETF is deprecating unicast site-local IPv6 scoped addresses. The most likely replacement will avoid the ambiguity problem in site-local addresses, and this is currently at the IETF Internet Draft stage [hinden03].

A disconnected site also can still use global provider-assigned addresses. Requirements for local-scope addressing for IPv6 are discussed in a recent IETF Internet Draft [lsareqts].

A dual-stack WLAN deployment may use private IPv4 addresses with NAT in parallel with globally routed IPv6 addresses.

#### 2.1.2. Increased subnet size

The standard IPv6 subnet (link) has a /64 length prefix (64 bits of network prefix, and thus 64 bits of host space in the subnet), which in theory can hold up to  $2^{64}$  hosts, although in practice one might not see more than a few hundred hosts in such a subnet. A typical IPv4 subnet plan might offer a /24 prefix to WLANs (a total of 256 addresses, 253 of which are typically available when the network, gateway and broadcast addresses are discounted).

IPv6 has no broadcast address. Instead functions such as Neighbor Discovery [rfc2461] (which replaces the arp function in IPv4) are performed through link-local multicast protocols.

#### 2.1.3. Resizing subnets

Because an IPv6 subnet has  $2^{64}$  bits of host space, the subnet can embrace any practical number of hosts. As a result, a network manager will not need to worry about efficient allocation of addresses into subnets as they would have to do for IPv4.

For example, in an IPv4 network a subnet with 45 hosts could be allocated a /26 prefix, allowing up to 61 hosts (64 less the network, gateway and broadcast addresses). If the network subsequently

grows (or shrinks) the IPv4 subnet would inevitably be changed in size, requiring subnet and gateway address planning and reconfiguration.

In IPv6, the /64 subnet presented to end host systems can allow the connection of any practical number of hosts, removing the need for alteration of subnet sizes and the associated administrative overhead. While IPv6 prefixes should still be used with some degree of conservatism, the freedom obtained through the (default) /64 subnet size is beneficial.

#### **2.1.4. Use of DHCPv6**

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) has now been defined and finalised as RFC3315 [rfc3315]. It is expected that DHCPv6 will be used in managed IPv6 networks just as DHCPv4 is used today (but with benefits such as the above resizing issue, as well as the ability to assign static addresses rather than dynamic ones to users wanting them).

Investigation needs to be done into whether DHCP and DHCPv6 servers are needed on a dual-stack network. It would be desirable to just run one such service.

Relay agents are defined in RFC3315 to allow DHCPv6 requests to be forwarded off link where no DHCPv6 server exists locally.

#### **2.1.5. Usage of stateful or stateless network autoconfiguration**

With IPv6, stateless autoconfiguration [rfc2462] may be the more common method of acquiring an IPv6 address, but stateful autoconfiguration using DHCPv6 as described above is available for managed networks. At present, there are few DHCPv6 implementations due to the fact that the protocol was only finalised in July 2003 within the IETF Dynamic Host Control WG [dhc].

One problem with stateless autoconfiguration is that there is no authentication for the host receiving the Router Advertisement carrying the network prefix and implied gateway address. However, we can expect authentication for “plug and play” networking to emerge in due course, but this may take 2-3 years to be developed and to mature to product. There is a new IETF WG for Securing Neighbor Discovery [send], but it is in its infancy at present.

A host entering a WLAN environment needs to know whether it can configure using DHCPv6 or through Router Advertisements. The Router Advertisement “managed bit” indicates whether the environment is managed or not. It may also be useful for RA’s to have an option to indicate whether privacy addresses (as per RFC3041) should be used, but no such definition exists at present.

There is no method at present to obtain an IPv6 DNS resolver address through stateless autoconfiguration; it has to be manually configured or obtained via DHCPv6, although a draft proposal exists for use of a well-known site-local address [dnsdisc]. This site-local proposal is unlikely to be widely adopted due to the IETF’s recent deprecation of unicast site-local scope addressing (see above).

A “DHCPv6 Light” would be useful for DHCPv6 to assign network information (e.g. NTP server, DNS resolvers) without having to store state (e.g. on IPv6 address leases to clients).

## **2.2. Traffic management**

When planning the routing and subnets of a WLAN network it is usually important to consider the “background” traffic. In IPv6 networks, multicast neighbour discovery and router advertisement traffic will be seen where in IPv4 broadcast traffic exists. In low bandwidth WLANs it is

important to keep the level of such background traffic down by not having excessively large subnets. Background multicast traffic can be “smartly” filtered by Layer 2 switches that understand the Multicast Listener Discovery (MLD) protocol (MLD version 1 for any source multicast and MLD version 2 for source specific multicast). However at the time of writing MLD “snooping” is not a common feature in switches, especially for MLDv2.

IPv6’s recommended /48 site prefix allocation allows deeper routing to be deployed than is the case for IPv4, if the hardware being used permits it, e.g. offering a /64 subnet to every office in a building or every room in a student dormitory. At present such usage is unlikely, as network managers will follow typical IPv4 practice is assigning subnets to collections of users or rooms, and cost-effective hardware to enable such routing is not yet available.

### **2.3. Wireless LAN Access Point Management and Monitoring**

Existing WLAN access points have management capability, but only over IPv4. Thus while such devices could be managed in a dual-stack deployment, if an IPv6-only network is to be run over WLAN, the devices would have to be pre-configured before deployment, or managed via serial or other interfaces. Note that many access points support the ability to get their own IP address via DHCP(v4), but of course do not yet have the ability to gain an IPv6 address (for monitoring or management purposes).

It is thus most likely that at present dual-stack WLANs would be used where network-based access point monitoring and management is required.

Note that the air interface of the WLAN access point can be IPv6-only, while the wired part, connecting the access point to a router, can be dual-stack.

In Deliverable D2.5.1 [d251] we reported on deployment of WLAN and WMAN networks in Tromsø, where IPv6-only networking is used.

The IETF is still finalising many of the IPv6-related MIBs at the time of writing.

### **2.4. Layer 2 Multicast support**

There have been some (rare) reports of devices that do not have proper support for multicast at layer 2. Such instances have been with PCMCIA-based 802.11b cards, and in each case a firmware upgrade on the card has resolved the issue. It is possible that old cards may be the cause of problems where IPv6 multicast traffic is not being forwarded on link. Such issues have not been reported with recent hardware.

Issues with MLD(v2) snooping are described above.

### **2.5. Access Control and Authentication methods**

#### **2.5.1. Access control**

Authentication methods are discussed in some detail in Deliverable D4.2.1 [d421].

In the short term, access control for IPv4 WLANs is still in its relative infancy, thus expectations for IPv6 must be realistic.

Proposed methods, e.g. combinations of 802.1x [8021x] and RADIUS, may also be used in wired networks for access control. Extensions of RADIUS for IPv6 [rfc3162] have been defined, but implementations are likely to be in the early stages at the time of writing.

Alternative access control mechanisms include web-redirect based authentication, where the user is redirected to an authentication page when they attempt a web access, and are not allowed off the local network until they authenticate successfully, and VPN access, whereby users are only allowed off the local WLAN if connecting to a trusted VPN server.

The web-redirect method for IPv6 requires the smart gateway to redirect IPv6 web requests to the authentication web server, which itself must support IPv6. However, in a dual stack network the challenge could be handled over IPv4, but this would require that a) the user did not first try to go to an IPv4 web site and b) that the authentication server can control IPv6 access across the smart gateway.

IPv6 VPNs have been implemented, e.g. the FreeS/WAN implementation for Linux, so these could be used for the restricted VPN access control mechanism.

It is not clear that any IPv6-only access control methods are widely available at present. The 6NET project will track the available tools and trial them as appropriate, in Work Package 2 or Work Package 4.

In the longer term, the IETF Protocol for Carrying Authentication for Network Access WG [pana] is studying methods that may be applicable in this area. The WG is also in its early phases though.

### **2.5.2. Support for roaming access**

There is a growing requirement for users to be able to roam between Wireless LAN providers, e.g. a researcher moving from one university to another.

The TERENA Mobility WG [tmob] is seeking to evaluate and promote interoperable methods for WLAN authentication such that users can roam within and between NREN networks in Europe.

Roaming capability comes from the ability to cross-authenticate between providers. The Mobility WG is investigating methods such as deployment of a pan-NREN RADIUS referral hierarchy that could support 802.1x or web-redirect based authentication requests from roaming users to their home institution authentication servers. This activity is being tracked within 6NET.

## **2.6. IPv6 Mobility issues: intra-campus roaming**

In the scope of WLAN provision in university campus environments, a deployment should be made available that:

- a) Allows the use of WLAN PDA and laptop devices, which are becoming more common for staff and student use
- b) Scales to the campus (which may include geographically disparate sites, and thus not one single “hotspot” coverage area)
- c) Allows seamless roaming while on the campus (TCP sessions should keep alive as the device moves between different IP subnets)
- d) Enables roaming to other networks, in particular other universities
- e) Allows roaming devices to communicate locally while in common remote networks (rather than communication via remote Mobile IP home agents)



An IPv4 WLAN deployment could be made using a single subnet for the Wireless LAN. However, this does not scale well to a campus-sized network with potentially many thousands of hosts, not least because of the bandwidth available on such a shared wireless segment is relatively low, but also because of the bandwidth required for multicast router advertisements (and neighbour discovery) and for IPv6 Multicast applications that might “flood” the subnet (in the absence of MLD snooping).

To enable routed solutions with mobility, and to support the requirements (c,d,e) above, Mobile IPv6 is the only long-term viable solution.

It is thus prudent that campuses interested in IPv6 run experiments at an early stage with IPv6 Mobility. Note that this requires existing applications to be available over IPv6 also, unless interworking methods such as DSTM or NAT-PT are used (these are discussed in the 6NET IPv6 transition cookbooks being produced in Work Package 2 [d232]).

The Mobile IPv6 standard in the IETF is now finalised [mipv6] and is being published to RFC status at the time of writing.

## 2.7. Security Considerations

There are some particular IPv6-related security considerations. These may apply to wired and wireless devices.

### 2.7.1. Network port scanning

Due to the vastly increased address space in an IPv6 subnet – 64 bits of host space instead of typically 8 bits in an IPv4 subnet – remote port scanning will take significantly longer to complete. Even if the target network uses stateless autoconfiguration and some parts of the host address can thus be guessed (the ‘fffe’ stuffing and well-known vendor Ethernet prefixes) then the scanning effort is still significantly greater (and at its greatest if the local network uses “random” host addresses rather than sequential numbering from <prefix::1>).

Local subnet hosts and routers can still be discovered by a local device by probing the well-known multicast address, e.g. ff02::1 for all hosts.

### 2.7.2. IP-based identification and authentication

In the IPv4 world, IP-based authentication or access control is commonly used, as a compromise between having no control and deploying a full certificate-based authentication scheme. Also, statically or dynamically assigned IPv4 addresses may be used for accounting and billing purposes.

With IPv6 it is expected that devices will have multiple IPv6 addresses. These may come from multiple service providers (as is the case with “classic” IPv6 multihoming proposals where Default Address Selection methods [rfc3484] are used) or from hosts that run RFC3041 IPv6 Privacy Extensions [rfc3041] (where a host may have a public statelessly autoconfigured address for new inbound connections as well as a “random” address for initiation of outbound connections which changes periodically). Windows XP implements RFC3041 in such a way that new privacy addresses may typically be regenerated daily, with a lifetime of one week. In such cases a host is no longer identifiable by a single IP address, and it may change (source) address with time.

In the case of WLANs, MAC addresses are often used in combination with IP addresses for access control (or DHCP addresses are only assigned to known MAC address devices); the MAC

addresses themselves would not change for such layer 2 based authentication, but layer 2 addresses can be spoofed quite easily in most operating systems.

### 2.7.3. Pre-generation of reverse DNS

Many sites will only allow certain services to operate, e.g. handling of email received via SMTP, when an IP address successfully looks up in the reverse DNS hierarchy. There is thus a requirement, if such “authentication” is carried forward to IPv6, to determine a method to populate, or simulate the population of, the reverse DNS for an IPv6 subnet, in particular where stateless autoconfiguration is used and the possible number of reverse entries is huge. An IETF Draft discusses the problem [dnsissues] but there is as yet no widely adopted solution for the issue.

### 2.7.4. Rogue Router Advertisements

Any IPv6-enabled host may be configured as a router and transmit Router Advertisements on a local link. It is thus possible that – accidentally or by design – a host may appear as a “rogue” router on link.

An example sometimes seen in a WLAN at a conference venue is a Windows laptop generating a 6to4 address (see [d232]) based on the IPv4 autoconfiguration prefix and advertising itself as an available router (6to4 gateway).

There is an obvious security risk for any host able to masquerade as a genuine site router.

An IETF Internet Draft exists [defrouter] that allows a Router Advertisement to carry a priority value, which would help ensure that accidentally misconfigured hosts did not cause a problem, but this does not help the malicious case.

### 2.7.5. Secure Neighbor Discovery

Secure Neighbor Discovery – being defined in the IETF SEND WG [send]) may help address the above concern in time. It also should ensure that only the intended set of hosts may attach to a network, rather than any device being able to statelessly autoconfigure. The SEND standards are currently still in development.

### 2.7.6. Cryptographically Generated Addresses (CGA)

Through its increased address size, IPv6 has the capability to carry cryptographically generated addresses (CGAs). These are being worked on within the IETF SEND WG [cga].

Such addresses are formed by using a hash of a public key within the address, in effect the host “signs” the address, which allows the recipient to have confidence in the identity of the sender of the packet.

CGAs are not possible with IPv4, due to the much smaller address size.

At the time of writing there are very few public implementations of CGAs, but there is quite strong interest in the possibilities they create. It is reasonable to expect their use to grow to some extent in the coming years. However their value in IPv6 deployments – including WLANs - has yet to be assessed from a practical experience viewpoint.

## 2.8. New network technologies

### 2.8.1. Requirements of new types of devices

New types of IPv6-enabled devices may include the expected PDAs and laptops, but also embedded systems (where device to device communication is more the norm than “person” to device). Examples of large sensor networks running IPv6 have been demonstrated in Japan [inode][ipv6pc].

By having a large (minimum) default subnet size – a /64 – IPv6 allows subnets to embrace large numbers of such embedded or wireless devices without the need for the network subnet to be grown (and reconfigured) by the network administrator or manager.

### 2.8.2. Personal Area Networks (PANs)

As Personal Area Networks (PANs) evolve, it is likely that WLAN environments will need not only to offer connectivity to hosts, but also to (mobile) networks. Thus an IPv6 prefix may be required for the PAN gateway device. Thus the IPv6 prefix delegation methods being designed and implemented for ISP DSL networks [v6pd] may also in time become applicable to WLANs. The requirements are currently far from clear however.

Network mobility is being studied by the IETF Network Mobility WG [nemo].

This issue is also related to the different types of WLAN networks available, e.g. 802.11b, or Bluetooth.

## 3. Technologies under Development

There are a number of technologies under development at the time of writing that will be important for the full deployment of IPv6 WLANs.

IPv6 WLANs can be operated now; the technologies listed here will enhance their functionality and ability to be managed or monitored.

The technologies can loosely be split into near-term and longer-term requirements. The near-term requirements, for which we can expect to see solutions within the next 12 months, include:

- DHCPv6 implementations – DHCPv6 was standardised in July 2003; implementations are now emerging for managed IPv6 network deployment.
- Availability of a unicast IPv6 site-local addressing scheme for disconnected or intermittently connected IPv6 WLANs.
- Consolidation or interaction of DHCPv6 and DHCP(v4) services for dual-stack networks.
- DNS resolver discovery in statelessly autoconfiguring networks (via DHCPv6).
- Multicast Listener Discovery (MLD) protocol snooping – required by Layer 2 switches to reduce multicast flooding in a switched network. Currently not commonly available.

The longer-term technologies, with robust commercial solutions still over 12 months away, include:

- Mobile IPv6 implementations – these are required to deploy IPv6 across a large “hotspot” such as a university campus, such that users can be mobile across multiple IPv6 subnets

while maintaining application connections (e.g. for voice or audio/video streaming applications).

- Management of WLAN access points over IPv6 – generally not needed until WLANs run IPv6-only, as access points can be managed over IPv4 in a dual-stack wireless network.
- IPv6 MIBs for WLAN access points.
- IPv6-enabled methods for access control, e.g. web-redirect based authentication for IPv6 devices.

The latter three points depend a lot on whether a demand is perceived for IPv6-only WLAN deployments, as management and access control can occur over IPv4 in dual-stack networks.

The following technologies – in terms of widespread deployment - may be further on the horizon:

- Roaming support, including operation with access control methods including 802.1x, web-redirect and restricted VPN destinations.
- Secure access at the link layer, from the IETF SEND WG and probably via use of CGAs
- Mobile network technology, currently under study in the IETF Nemo (Network Mobility) WG.

These areas are generally being studied/trialled within the 6NET project, and will be reported as appropriate in future project deliverables.

## 4. Conclusions

This report briefly highlights the implications of IPv6 deployment in WLANs for those network operators used to IPv4-only deployment.

Many of the technologies described here also apply to wired deployments.

The report does not discuss what other mechanisms are required to make an IPv6-only WLAN viable as a service per se; that would involve the transition methods discussed in other Deliverables from this Work Package, e.g. dual-stack Web proxies, NAT-PT, DSTM (which has appeal in a network with IPv6-only infrastructure but dual-stack hosts), etc, in particular in the Site Transition cookbook report [d232]. Most deployments now are currently dual-stack.

Technologies exist now for IPv6 WLAN deployment, in a simple form. However full access control, mobility and roaming support, and secure operation are still at least a year away at the time of writing.

The 6NET project will work on developing and trialling the emerging components required for IPv6 WLANs.

## 5. References

- [cga] “Cryptographically Generated Addresses”, T. Aura, IETF Internet Draft (work in progress), August 2003, <http://www.ietf.org/internet-drafts/draft-ietf-send-cga-01.txt>
- [d222] “Initial IPv4 to IPv6 transition cookbook for Organisational/ISP (NREN) and backbone networks”, 6NET Project Deliverable D2.2.2, T. Chown editor, March 2003, <http://www.6net.org/publications/deliverables/D2.2.2.pdf>
- [d232] “Initial IPv4 to IPv6 transition cookbook for end sites and universities”, 6NET Project Deliverable D2.3.2, T. Chown editor, February 2003, <http://www.6net.org/publications/deliverables/D2.3.2.pdf>
- [d251] “Initial scoping report on IPv6-only end systems and components missing for IPv6-only site operation”, 6NET Project Deliverable D2.5.1, T. Chown editor, December 2002, <http://www.6net.org/publications/deliverables/D2.5.1.pdf>
- [d421] “IPv6 Wireless LAN Access Issues”, 6NET Project Deliverable D4.2.1, M. Dunmore editor, July 2002, <http://www.6net.org/publications/deliverables/D4.2.1.pdf>
- [d422] “Framework for the Support of IPv6 Wireless LANs”, 6NET Project Deliverable D4.2.2, M. Dunmore editor, July 2003, <http://www.6net.org/publications/deliverables/D4.2.2.pdf>
- [8021x] 802.1x – Port Based Network Access Control, <http://www.ieee802.org/1/pages/802.1x.html>
- [defrouter] “Default Router Preferences, More Specific Routes and Load Sharing”, R. Draves, R. Hinden, IETF Internet Draft (work in progress), June 2002, <http://www.ietf.org/internet-drafts/draft-ietf-ipv6-router-selection-02.txt>
- [dhc] IETF Dynamic Host Configuration WG, <http://www.ietf.org/html.charters/dhc-charter.html>
- [dnssdisc] “Well known site local unicast addresses to communicate with recursive DNS servers”, A. Durand et al., IETF Internet Draft (expired), October 2002, [draft-ietf-ipv6-dns-discovery-07.txt](http://www.ietf.org/internet-drafts/draft-ietf-ipv6-dns-discovery-07.txt)
- [dnssissues] “IPv6 DNS transition issues”, A. Durand, J. Ihen, IETF Internet Draft (work in progress), February 2003, <http://www.ietf.org/internet-drafts/draft-ietf-dnsop-ipv6-dns-issues-02.txt>
- [hinden03] “Unique Local Unicast IPv6 Addresses”, R. Hinden, B. Haberman, IETF Internet Draft (work in progress), June 2003, <http://www.ietf.org/internet-drafts/draft-hinden-ipv6-global-local-addr-02.txt>
- [inode] Internet Node (i-Node), <http://www.i-node.co.jp/e/>
- [ipv6pc] IPv6 Promotion Council of Japan, <http://www.v6pc.jp/en/>
- [lsareqts] “Requirements for Limited-scope Unicast Addressing in IPv6”, F. Templin, IETF Internet Draft (work in progress), June 2003, <http://www.ietf.org/internet-drafts/draft-templin-lsareqts-00.txt>

- 
- [mipv6] “Mobility Support in IPv6”, D. Johnson, C. Perkins, J. Arkko, IETF Internet Draft (awaiting RFC publication), June 2003, <http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-24.txt>
- [nemo] IETF Network Mobility WG, <http://www.ietf.org/html.charters/nemo-charter.html>
- [pana] IETF Protocol for Carrying Authentication for Network Access WG, <http://www.ietf.org/html.charters/pana-charter.html>
- [rfc2460] “Internet Protocol Version 6 (IPv6) Specification”, S. Deering, R. Hinden, IETF RFC2461, December 1998, <http://www.ietf.org/rfc/rfc2460.txt>
- [rfc2461] “Neighbor Discovery for IPv6”, T. Narten, E. Nordmark, W. Simpson, IETF RFC2461, December 1998, <http://www.ietf.org/rfc/rfc2461.txt>
- [rfc2462] “IPv6 Stateless Autoconfiguration”, S. Thomson, T. Narten, IETF RFC2462, December 1998, <http://www.ietf.org/rfc/rfc2462.txt>
- [rfc3041] “Privacy Extensions for Stateless Address Autoconfiguration in IPv6”, T. Narten and R. Draves, IETF RFC3041, January 2001, <http://www.ietf.org/rfc/rfc3041.txt>
- [rfc3162] “RADIUS and IPv6”, B. Aboba et al, IETF RFC3162, August 2001, <http://www.ietf.org/rfc/rfc3162.txt>
- [rfc3315] “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, R. Droms et al, IETF RFC3315, July 2003, <http://www.ietf.org/rfc/rfc3315.txt>
- [rfc3484] “Default Address Selection for IPv6”, R. Draves, IETF RFC3484, February 2003, <http://www.ietf.org/rfc/rfc3484.txt>
- [send] IETF Securing Neighbor Discovery WG, <http://www.ietf.org/html.charters/send-charter.html>
- [tmob] TERENA Mobility WG, <http://www.terena.nl/tech/mobility/>
- [v6pd] “IPv6 Prefix Options for DHCPv6”, O. Troan and R. Droms, IETF Internet Draft (work in progress), June 2003, <http://www.ietf.org/internet-drafts/draft-ietf-dhc-dhcpv6-opt-prefix-delegation-04.txt>