Project Number:	**IST-2001-32603**
Project Title:	**6NET**
CEC Deliverable Number:	**32603/UOS/DS/2.4.1/A1**
Contractual Date of Delivery to the CEC:	30th September 2002
Actual Date of Delivery to the CEC:	6th December 2002
Title of Deliverable:	D2.4.1: Initial report on technology 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 existing 6NET Deliverable D4.2.1 on Access Issues for IPv6 WLANs by highlighting and commenting on issues for IPv6 WLAN deployment that network managers more used to thinking the "IPv4 way" should be aware of. This is an initial scoping report for the issues, which will be expanded during the project. A more detailed version of this report will be delivered in M18 of the project (by July 2003).

Keywords:

IPv6 transition, IPv6 Wireless LAN

Executive Summary

This report complements Deliverable D4.2.1 [d421]by highlighting and commenting on the issues that a network manager experienced in operating an IPv4 WLAN service should be aware of when migrating to an IPv6 service, or a dual-stack IPv4-IPv6 service.

These issues include:

- New types of wireless devices (compact PDAs, sensor equipment, etc)
- Wireless LAN management capability
- Layer 2 multicast support
- Authentication assumptions (e.g. IPv6 privacy address implications)
- IPv6 protocol requirements (e.g. RADIUS with IPv6)
- Layered networks (e.g. personal area networks)

As the 6NET project progresses, and more partner sites deploy and run IPv6 WLANs, these issues will be explored and expanded, leading to a second version of this report, Deliverable D2.4.2, by July 2003.

Table of Contents

1. Introduction

The 6NET Project has already produced a detailed report on IPv6 Access Issues for Wireless LANs [d421]. In that report, we detailed the WLAN standards, deployment scenarios, access control methods, roaming methods and the relationship with Mobile IPv6. To a large extent, the text of that deliverable covers much of what could be written here. However, in this brief report we highlight the issues that network managers used to thinking the "IPv4 way" should be aware of when considering introducing IPv6 services over WLANs.

2. Issues for Introduction of IPv6 WLAN Services

In this section we describe issues that have arisen to date when considering introduction of IPv6 WLAN services, for network operators more familiar with IPv4 services.

2.1. IPv6 subnet allocations and requirements of new types of devices

IPv6 offers a greatly increased address sapce over IPv4. A /64 subnet could in theory hold 2^64 hosts, although in practice one might not see more than a few hundred in many situations. A typical IPv4 subnetting plan might offer /24 prefixes to WLANs (256 addresses). When subnetting it is still important to consider the "background" traffic – in IPv6 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. IPv6's recommended /48 site prefix allocation allows deep subnetting to be deployed if necessary.

New types of 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].

2.2. Wireless LAN Access Point Management

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 report on deployment of WLAN and WMAN networks in Tromsø, where IPv6-only networking is used.

2.3. 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. If IPv6 multicast traffic is not being forwarded on link, it is possible that old cards may be the cause.

Such issues have not been reported with recent hardware.

It is also worth noting that, as with IPv4 multicast, WLANs may be subject to being "swamped" by IP Multicast, where layer 2 switches are not IPv4 or IPv6 Multicast group-aware. There have been proposals for MLD and MLDv2 snooping to address this, but many consider this to be a layer violation. In low bandwidth WLANs, the presence of (relatively) high-traffic IPv6 Multicast (e.g. vic and rat) could cause problems.

2.4. Authentication methods

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. 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. 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 early stages.

It is not clear that there is any available IPv6-only access control method available at present.

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. IP-based identification

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 [defaddr] are used) or from hosts that run RFC3041 IPv6 Privacy Extensions [rfc3041] (where a host may have a public statelessly autoconfigured address as well as a "random" address 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 addressing is often used in combination with IP addresses; the MAC addresses themselves would not change for such layer 2 based authentication.

2.6. Stateful vs stateless autoconfiguration

With IPv6, stateless autoconfiguration may be the more common method of acquiring an IPv6 address, but stateful autoconfiguration using DHCPv6 [dhcpv6] is also possible. At present, there are few DHCPv6 implementations due to the ongoing nature of the development of DHCPv6 in the IETF Dynamic Host Control WG [dhc].

There is a new IETF WG for Securing Neighbor Discovery [send], but it is in its infancy at present. However, we can expect authentication for "plug and play" networking to emerge in due course, but this may take 2-3 years.

A host entering a WLAN environment needs to know whether it can configure using DHCPv6 or through Router Advertisements. It may be desirable to have some kind of "managed bit" to indicate whether the environment is managed or not, though this should not preclude use or acquistion of other types of addresses. It may also be useful for RA's to have an option to indicate that privacy addresses should not be used.

There is also no method at present to obtain a DNS server address with stateless autoconfiguration; it has to be manually configured or obtained via DHCP(v6), although a draft proposal exists for use of a well-known site-local address [dnsdisc].

2.7. 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.

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

2.8. IPv6 Mobility issues: campus roaming

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

a) Allow the use of WLAN PDA and laptop devices, which are becoming more common for staff and student use

b) scale to the campus (which may include geographically disparate sites)

c) allow seamless roaming while on the campus (TCP sessions should keep alive)

d) enable roaming to other networks, in particular other universities

e) allow roaming devices to communicate locally while in common remote networks

An IPv4 WLAN deployment could be made using a single subnet for the WLAN. 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 segment, and bandwidth required for multicast router advertisements (and neighbour discovery) and that might be "lost" to IPv6 Multicast applications such as vic and rat that may "flood" the subnet.

To enable routed solutions with mobility, and to support 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 due in January 2003 and updated annually in the project lifetime).

3. Conclusions

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

It does not discuss what other mechanisms are required to make 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 scoping report [d231].

There is work to be done in the IETF standards processes before full IPv6 mobility can be supported in WLAN environments, but work is also required, as it is for IPv6 in general, from application developers and application service providers.

The TERENA Mobility WG will also be tracking IPv6 usage and requirements in this area.

The 6NET project will release a more detailed version of this document by July 2003 as Deliverable D2.4.2.

4. References

[d231] "IPv4 to IPv6 transition scoping report for end sites and universities", 6NET Project Deliverable D2.3.1, T. Chown editor, July 2002, http://www.6net.org/publications/deliverables/D2.3.1.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

[8021x] "802.1x – Port Based Network Access Control", http://www.ieee802.org/1/pages/802.1x.html

[defaddr] "Default Addres Selection for IPv6", R. Draves, IETF Internet Draft, August 2002, draft-ietf-ipv6-default-addr-select-09.txt

[dhc] IETF Dynamic Host Configuration WG, http://www.ietf.org/html.charters/dhc-charter.html

[dhcpv6] "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", R. Droms et al, IETF Internet Draft, November 2002, draft-ietf-dhc-dhcpv6-28.txt

[dnsdisc] "Well known site local unicast addresses to communicate with recursive DNS servers", IETF Internet Draft, A. Durand et al, October 2002, draft-ietf-ipv6-dns-discovery-07.txt

[inode] Internet Node (i-Node), http://www.i-node.co.jp/e/

[ipv6pc] IPv6 Promotion Council of Japan, http://www.v6pc.jp/en/

[pana] IETF Protocol for Carrying Authentication for Network Access WG, http://www.ietf.org/html.charters/pana-charter.html

[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

[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, November 2002, draft-ietf-dhc-dhcpv6-opt-prefix-delegation-01.txt