IPv6 Design Guide for Alcatel-Lucent Enterprise Data Products

Release 1.0

AT THE SPEED OF IDEAS™

Alcatel·Lucent
Enterprise

Why Read This Document?

On the 3rd February 2011, the Internet Assigned Number Authority (IANA) assigned its last block of IPv4 addresses to the Regional Internet Registry (RIR). On the 15th April 2011 the Regional Internet Registry for the Asia/Pacific Region (APNIC) ran out of IPv4 addresses completely; **2011 became the year to re-focus on IPv6.**

The world explosion in internet users and more recently mobile devices has put immense pressure on the demand for IP addresses and specifically the need for IPv6 addresses.

Interestingly, it took 38 years for radio to reach 50 million people, whereas in just one recent year, the social network site Facebook signed up more than 200 million users and by the end of this year would have reached in total, almost one billion people.

In 2012, according to Europe's top engineers, there will be more mobile devices used throughout the world than people.

The importance of IPv6 migration continues to spread throughout Europe and legislation will follow if we are going to compete with Asia as they continue to grow their expertise and IPv6 infrastructure.

The effect in the Enterprise is forcing customers to demand not just IPv6 scalable networks, but the benefits and new services that it can provide.

As a minimum, all of us today should have an IPv6 migration strategy which includes planning, training, and the procurement of an IPv6 ready network infrastructure.

Which Sections Should You Read ?

Chapters 1, 3 and 4 have been written for **anyone** who wishes to learn about IPv6. These sections give a high level view of IPv6 today and what it will mean for the future.

The remaining chapters can be chosen based on your technical need.

Table of Contents

Introduction

Document history

Table 1-1 shows the revision history of this document.

Table 1-1 Document revision history

Date	Issue	Description	Author
11/12/11	001	Initial Draft Release	Central Pre-Sales Team
11/12/11	001	Final Draft Release	

Purpose of this Document

The purpose of this document is to prepare Alcatel-Lucent Business Partner's and their Customers for IPv6 and help understand the reasons why adoption is imminent and provides assistance when deploying IPv6 in the Enterprise and specifically with Alcatel-Lucent Data Products.

Intended audience

This document is intended for technical pre-sales specialists in the Alcatel-Lucent Business Partner community. It will assist them with IPv6 planning and implementation of Alcatel-Lucent Data Products.

1. IPv6 in the Enterprise

What is IPv6?

IPv6 is the newest version of Internet Protocol (IP).

The prime difference between IPv4 and IPv6 is the extended address space, namely from a 32 bit format, supporting around 4.3 billion addresses, to one of 128 bits, increasing the address space to over **340 billion billion billion billion** or 340 x 10^{36}, that's a lot of addresses.

What is IP?

IP is the acronym for **Internet Protocol**.

IP is a networking protocol that is responsible for providing addressing and communication over a layer 3 network.

Internet Protocol version 4 (IPv4) is the current and first networking protocol to be adopted by the Internet.

Although IP was conceived in the late 1960's and early 1970's, IPv4 was not widely used on the Internet until 1983, since then however it has played a major role in the Internet revolution until now and has set the standard for the future.

IPv4 was initially described in RFC791 over 30 years ago; it uses 32 bit addressing, split into 4 bytes that are normally shown in a decimal format, for example 192.168.10.1.

Thirty-two bit addressing (2^{32}) provides almost 4.3 billion 'theoretical addresses' (some are reserved) and has stood the test of time as it has supported the massive growth of the Internet.

However, in the early 1990's the IETF (Internet Engineering Task Force) decided to work on the successor to IPv4, namely IPv6 (IPv5 was previously assigned for something else, so could not be used).

So the question we could ask ourselves is, if IPv4 has been so successful supporting the Internet up to now, why is IPv6 so important ?

IPv6, why Now?

The question asked in the last section was if IPv6 was released more than 10 years ago, why is there a need to deploy it now ?

- Do we actually need more than 4 billion network addresses ?
- Do we really need to adopt IPv6 ?

Some might say… "Tant que ça marche, on ne touché à rein", or in English, ***"If it's not broke, don't fix it"***

Well, there are very good reasons why IPv6 planning and adoption is needed now.

This document will discuss the reasons why and help build a strategy for IPv6 migration, especially as you implement or upgrade Alcatel-Lucent Data Products in the Enterprise.

The remainder of this section discusses the market trends that are forcing the imminent adoption of IPv6 in the Internet and in the Enterprise worldwide.

What Market trends dictate IPv6 Adoption

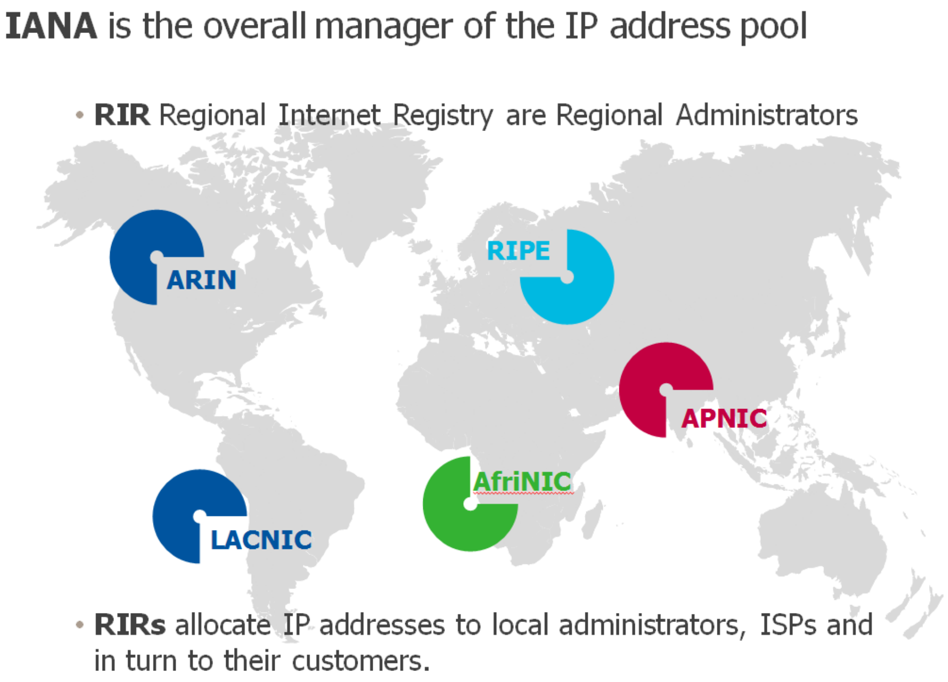
Why is 2011 the year to get excited about IPv6 ?

First and foremost, on the 3rd February 2011, IANA (the Internet Assigned Number Authority, who incidentally manage IPv4 address space), assigned its last block of IPv4 addresses.

Is there a need to panic, not just yet, as these addresses are managed in a hierarchical way.

To explain, the RIR (Regional Internet Registry), of which there are 5 globally, are the local administrators of the address space for their region.

These in turn are passed to the LIR (Local Internet Registry) or NIR (National Internet Registry) to redistribute to ISP's, Telco's etc.; in turn, these are allocated statically or dynamically to the end user or client, this is illustrated below.



IANA is the overall manager of the IP address pool

- **RIR** Regional Internet Registry are Regional Administrators
- **RIRs** allocate IP addresses to local administrators, ISPs and in turn to their customers.

So, if IPv4 has over 4 billion addresses, why are we running out ?

That's a good question, but bearing in mind that the world's population is nearing 7 billion, of which, almost 4 billion of those are living in Asia where the growth rate for Internet access is exponential, it gives you some idea of the pressure on the demand of IPv4 addresses.

In fact, on 15th April 2011 APNIC (Asia/Pacific Region) ran out of IPv4 addresses, it currently holds only a handful, which they are keeping in reserve.

For reference, see http://inetcore.com/project/ipv4ec/index_en.html

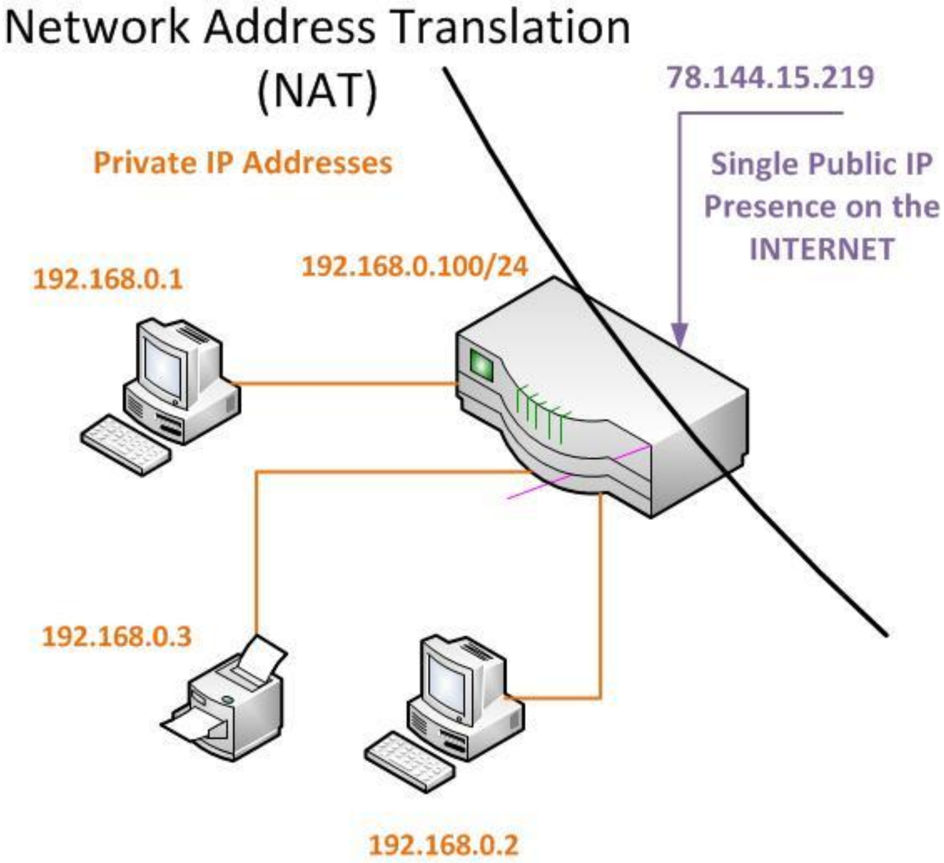
Take into account the explosion of mobile phones, smart devices and a whole host of different devices that consume IP addresses, it is no wonder that the implementation of IPv6 is as important as ever.

Think for a moment how many IP addresses you use, it is 10, 20, or even more private addresses ?

It is surprising how many that can be used, just image as the population increases and the increase in adoption of IP in everyday devices, the demand for IP addresses could soon exceed 100 billion.

Having mentioned private addresses, it is worth discussing Network Address Translation (NAT) for a moment.

NAT is one of the reasons why IPv4 has been so resilient during the Internet explosion. Why, because NAT gives the ability to use a single "public" IP address to hide a number of "private" IP addresses located in your network, illustrated in the diagram below.



While NAT has been the savior in reducing the number of public IP addresses that are currently needed, it does have a downside.

NAT translation unfortunately adds complexity, latency and breaks protocols that contain IP address within their payload (for example H.323), neither does it scale well as the Internet evolves peer to peer applications.

So it is not of a case of if IPv6 will be implemented, it's a case of when.

It is imperative that IPv6 adoption be accelerated if we are to maintain the growth of Internet services.

It is important for all to have a clear strategy in 2011.

As early as September 2003, the Department of Defense in the United States stipulated that they were to migrate to IPv6 within 5 years, in fact all equipment purchased from then must be IPv6 enabled.

With the Department of Defense having one of the largest IT budgets in the world, this gave vendors an incentive, if not a expedited commitment to IPv6.

World IPv6 Day on 8th June 2011 also highlighted the importance of IPv6, with the result that the French Government were no longer going to leave the ISP's to determine the timescales for IPv6 adoption, instead they were going to take an active role in this regard.

Monsieur Eric Besson from the Department of Industry promised to accelerate IPv6 migration in France and insisted that this is vital if the French were to preserve the competitiveness of their companies.

The importance of IPv6 migration continues to spread throughout Europe and legislation will follow if we are going to compete with Asia as they continue to grow their expertise and IPv6 infrastructure.

The effect in the Enterprise is forcing customers to demand not just IPv6 enabled networks, but are becoming more aware of specific protocol and service applications that are needed in the IPv6 world.

If you think this doesn't affect you, think again, you may find your local government will force ISP's into IPv6 adoption and in turn force you into the world of IPv6, sooner than you think.

IPv4 – IPv6 Intranet and Internet Interoperability

IPv4 and IPv6 are not compatible with each other; they can however coexist on the same network as long as they have their own IP enabled services.

For obvious reasons upgrading to IPv6 cannot be done overnight, it will take many years before the Internet will run on a fully native IPv6 platform.

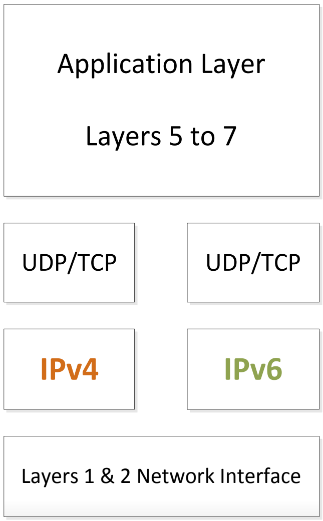
The fact that IPv4 and IPv6 can coexist on the same network will help with the migration, so what is needed is a means to stage the migration in a way of allowing IPv4 and IPv6 to work together.

There are a number of suggested ways that this can be done, consider the following, namely, Dual Stack, Tunneling and Translation.

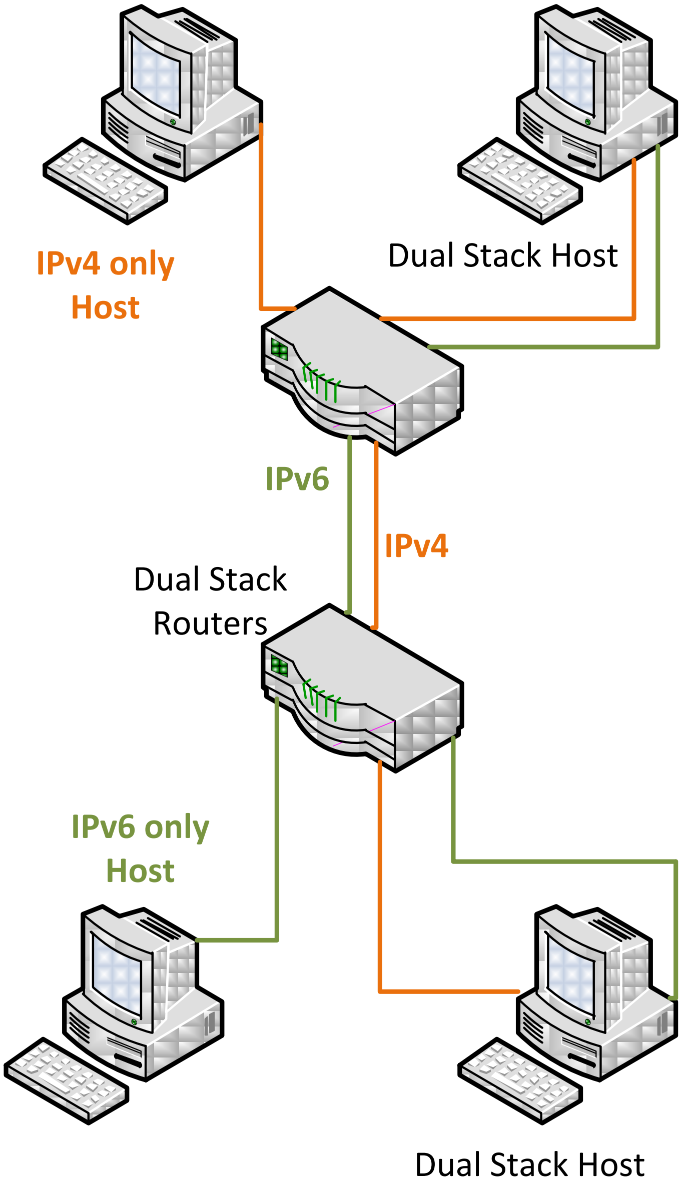
Dual Stack

This will allow devices to support both IPv4 / IPv6 and to coexist on the same network.

This will create an overhead in that the network will have multiple routing tables and possibly additional hardware and services, nevertheless, this will enable IPv4 and IPv6 stacks to work side by side in a node, as seen in the diagram below.



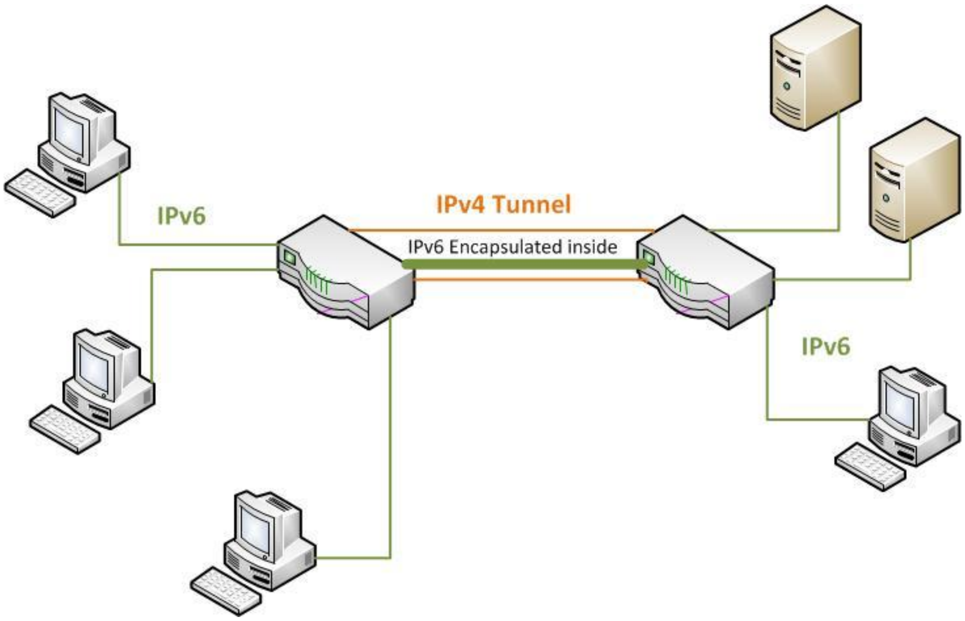
The topology view of a dual stack environment is depicted below.



Tunneling

Tunneling is simply a way of using IPv6 in an IPv4 environment.

IPv6 traffic is simply encapsulated in IPv4 frames, or in other words, a complete IPv4 header is added to the IPv6 packet and then transport across the Intranet or Internet using the current existing infrastructure and services as shown in the diagram below.



Tunneling provides a mechanism for transitioning an IPv4 network to IPv6 and/or maintaining interoperability between IPv4 and IPv6 networks.

There are two kinds of tunneling of IPv6 packets over IPv4 networks: configured and automatic.

For configured tunneling, the sending node is configured so that the route, as well as having a next hop, also has a tunnel end point address. This kind of tunnel is used for sites which architecture does not change often.

Automatic Tunnels can be created by using the 6to4 or ISATAP addresses, using IPv4 compatible addresses is no longer supported as these addresses have been depreciated.

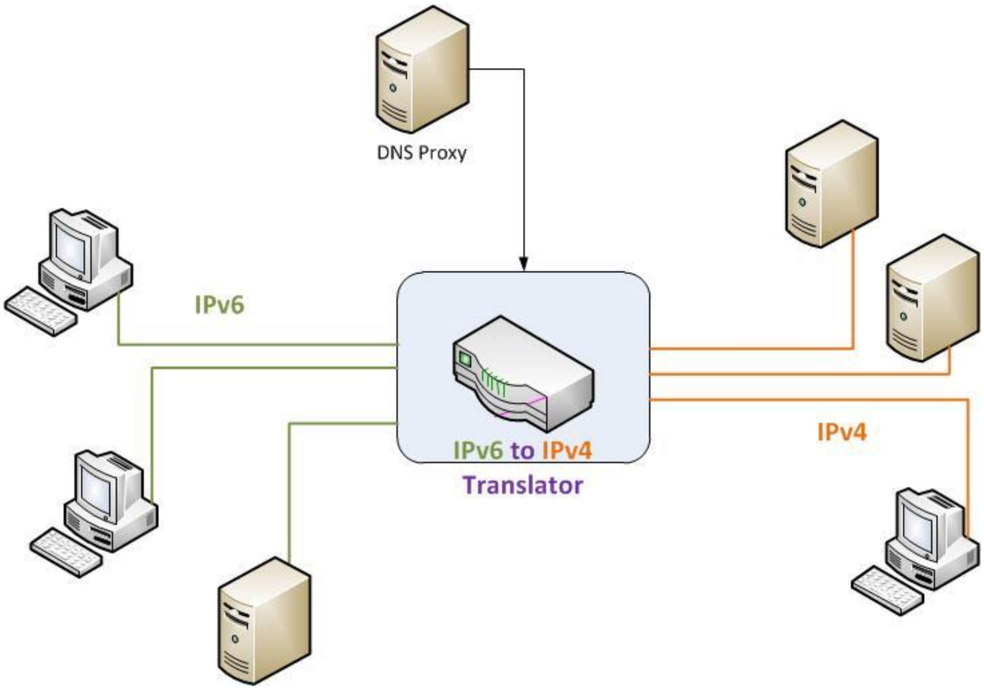
There is however a security issue with tunneling in that the protocols or indeed data encapsulated within the tunnel can be a security concern.

Careful consideration should be shown to ensure the appropriate mechanisms are in place to detect vulnerabilities deep inside the encapsulated data.

If Tunneling is chosen as the preferred mechanism for migrating to IPv6, we believe as IPv6 adoption develops and IPv4 addresses continue to deplete, it is more likely that IPv4 will interconnect its islands through an IPv6 backbone.

Translation - IPv4 / IPv6 Gateway

The Gateway approach offers a translation mechanism between IPv4 and IPv6. Some transition methods have been standardised, but others are still being developed as more vendors are building solutions for IPv6, the basic concept is illustrated below.



To give us some guidance on IPv6 migration it would make sense to consult the recommendations of the IETF (Internet Engineering Task Force).

The IETF was formed about 25 years ago with the remit to coordinate resources, create working groups and develop standards for the Internet.

The IETF have been working hard to address the impending migration of IPv6 and have a number of solutions to achieve this.

The next chapter discusses the scenarios offered by the IETF and discusses the recommended interoperability scenarios.

2 IETF Migration

Introduction

The IETF focuses on four primary scenarios for migration, there are others and these shouldn’t necessarily be viewed negatively, but their adoption is unlikely to be as popular in the Enterprise.

- Dual Stack
- Tunneling (Crossing IPv4 Islands)
- IPv6 (only) Core Network
- IPv6 (only) Deployment

See RFC 4213 (obsoletes RFC 2893) and RFC 6180, dated May 2011, for more information on basic transition mechanisms for IPv6.

Dual Stack

The Dual Stack approach (as discussed in the previous section), is simply a means to allow IPv4 and IPv6 to coexist on the same internetwork.

Both versions of IP will in run parallel, in effect each host can access both IPv4 and IPv6 services.

With this solution additional equipment and existing equipment upgrades will be needed.

There will also be additional overheads, namely dual routing tables, more CPU, more memory etc.; in reality, each router will be forwarding IPv4 and IPv6 traffic separately !

In addition, all hosts will also need to be configured to be able to participate in IPv6.

Stack duplication will also have an impact on network management and in some cases latency in the network.

Initially, the effort required to implement the additional IPv6 stack will be inversely proportional to the amount of IPv6 traffic that will actually be present on the network.

Having said that, the additional stack will set the framework for a progressive migration into a fully native IPv6 network; for more information, see RFC 4213 (which supersedes RFC 2893).

This is by far the preferred and the simplest method. It is also favored by the ISPs and Network Managers.

Tunneling (Crossing IPv4 Islands)

Where native end-to-end IPv6 connectivity is not possible, linking IPv6 through an IPv4 internetwork is achieved through tunneling; also referred to as encapsulation.

The downside as with any legacy tunneling protocol, is the additional load it puts on its networking equipment, CPU and encapsulation latency.

Tunneling can be achieved in several ways; a few are listed below, along with their respective RFC.

- **6to4** RFC 3056

  Essentially, 6to4 views IPv4 as a unicast point to point link layer interconnection between IPv6 enabled networks.

- **Manual Tunnels** (GRE, Protocol 41)

  As the name implies you can manually configure a tunnel with Generic Routing Encapsulation using Protocol Type 41 in the next header field as a means to traverse IPv6 over an IPv4 backbone.

- **Tunnel Brokering** RFC 5572 (3053)

  This method uses Tunnel Brokers, namely servers dedicated to automatically manage tunnel requests from clients.

- **Dual Stack Lite** (DS-Lite)

  This method encapsulates IPv4 over IPv6, a NAT function being used instead of a gateway.

- **Teredo** RFC 4380 (updated in RFC 6081)

  This protocol allows client devices to communicate through NAT, sending IPv6 traffic within UDP packets.

  A Microsoft lead protocol, Windows 7 clients use this protocol by default.

- **ISATAP** RFC 5214

  Intra-Site Automatic Tunnel Addressing Protocol allows IPv6 packets to talk to dual-stack interfaces over an Ipv4 network.

  It effectively defines a way of generating a link local IPv6 address from an IPv4 address and a method to perform Neighbor Discovery on top of IPv4.

IPv6 (only) Core Network

The best way to describe this method is to compare it with Tunneling.

In fact, it is the opposite, in that IPv6 is the prime protocol in the core and IPv4 is tunneled through the network, as IPv4 addresses deplete, this could become the most likely scenario.

IPv6 (only) Deployment

This is simply where all devices are IPv6 capable and native IPv6 is fully implemented in all parts of the network.

In reality this is not a migration strategy as such, but it is perfect for "Green-Site" Intranet applications.

In this scenario the network can fully benefit from all of the newer features added in IPv6, which will provide a faster, more secure and scalable solution as the Internet evolves in the 21st Century.

What about Today ?

In the real world, IPv6 adoption has been slow.

There has been a number of reasons for this, firstly, there is a huge amount of IPv4 addresses deployed around the world and migration overnight would simply be impossible, secondly, two IPv4 address conserving strategies were developed and released by the IETF in the early 1990's, namely, NAT (Network Address Translation) and CIDR (Classless Inter-Domain Routing); these were discussed earlier in this document.

The delay in adopting IPv6 has meant that a number of migration strategies that were originally suggested became less attractive and over time, discouraged or even depreciated.

In addition to supporting native IPv6, Alcatel-Lucent has chosen two of the surviving predominant migration strategies, namely,

- Dual Stack
- Tunneling

There are two types of tunnels supported with AoS,

- 6to4
- Configured.

Both types facilitate the interaction of IPv6 networks with IPv4 networks by providing a mechanism for carrying IPv6 traffic over an IPv4 network infrastructure. This is an important function since it is more than likely that both protocols will need to coexist within the same network for some time.

These two tunneling methods are discussed in detail below,

6to4 Tunnels

6to4 tunneling provides a mechanism for transporting IPv6 host traffic over an IPv4 network infrastructure to other IPv6 hosts and/or domains without having to configure explicit tunnel endpoints. Instead, an IPv6 6to4 tunnel interface is created at points in the network where IPv6 packets are encapsulated (IPv4 header added) prior to transmission over the IPv4 network or encapsulates (IPv4 header stripped) for transmission to an IPv6 destination.

An IPv6 6to4 tunnel interface is identified by its assigned address, which is derived by combining a 6to4 well-known prefix (2002) with a globally unique IPv4 address and embedded as the first 48 bits of an IPv6 address. For example, 2002:d467:8a89::137/64, where D467:8A89 is the hex equivalent of the IPv4 address 212.103.138.137.

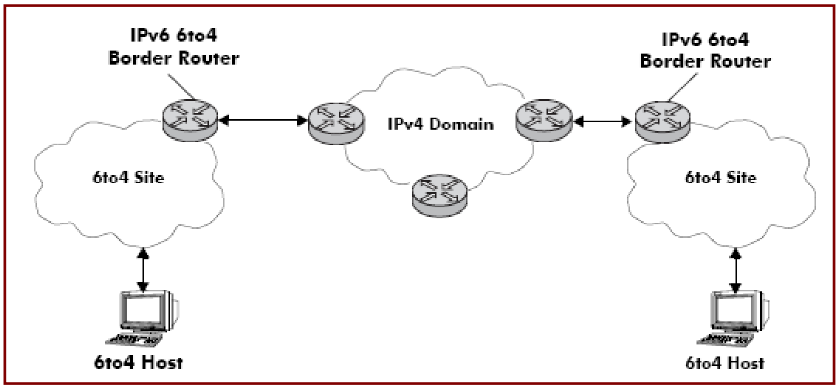
6to4 tunnel interfaces are configured on routers and identify a 6to4 site. Because 6to4 tunnels are point-to-multi-point in nature, any one 6to4 router can communicate with one or more other 6to4 routers across the IPv4 cloud.

Two common scenarios for using 6to4 tunnels are described below.

6to4 Site to 6to4 Site over IPv4 Domain

In this scenario, isolated IPv6 sites have connectivity over an IPv4 network through 6to4 border routers. An IPv6 6to4 tunnel interface is configured on each border router and assigned an IPv6 address with the 6to4 well known prefix, as described above. IPv6 hosts serviced by the 6to4 border router have at least one IPv6 router interface configured with a 6to4 address. Note that additional IPv6 interfaces or external IPv6 routing protocols are not required on the 6to4 border router.

The following diagram illustrates the basic traffic flow between IPv6 hosts communicating over an IPv4 domain:



In the above diagram:

1. The 6to4 hosts receive 6to4 prefix from Router Advertisement.

2. The 6to4 host sends IPv6 packets to 6to4 border router.

3. The 6to4 border router encapsulates IPv6 packets with IPv4 headers and sends to the destination 6to4 border router over the IPv4 domain.

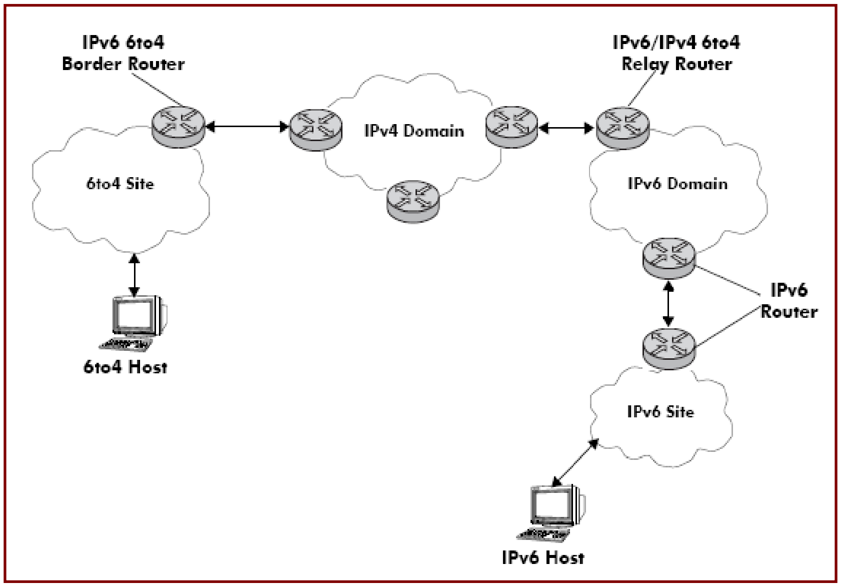
4. The destination 6to4 border router strips IPv4 header and forwards to 6to4 destination host.

6to4 Site to IPv6 Site over IPv4/IPv6 Domains

In this scenario, 6to4 sites have connectivity to native IPv6 domains through a relay router, which is connected to both the IPv4 and IPv6 domains. The 6to4 border routers are still used by 6to4 sites for encapsulating/decapsulating host traffic and providing connectivity across the IPv4 domain. In addition, each border router has a default IPv6 route pointing to the relay router.

In essence, a relay router is a 6to4 border router on which a 6to4 tunnel interface is configured. However, a native IPv6 router interface is also required on the relay router to transmit 6to4 traffic to/from IPv6 hosts connected to an IPv6 domain. Therefore, the relay router participates in both the IPv4 and IPv6 routing domains.

The following diagram illustrates the basic traffic flow between native IPv6 hosts and 6to4 sites:



In the diagram on the previous page :

1. The 6to4 relay router advertises a route to 2002::/16 on its IPv6 router interface.

2. The IPv6 host traffic received by the relay router that has a next hop address that matches 2002::/16 is routed to the 6to4 tunnel interface configured on the relay router.

3. The traffic routed to the 6to4 tunnel interface is then encapsulated into IPv4 headers and sent to the destination 6to4 router over the IPv4 domain.

4. The destination 6to4 router strips the IPv4 header and forwards it to the IPv6 destination host.

Configured Tunnels

A configured tunnel is where the endpoint addresses are manually configured to create a point-to-point tunnel. This type of tunnel is similar to the 6to4 tunnel on which IPv6 packets are encapsulated in IPv4 headers to facilitate communication over an IPv4 network. The difference between the two types of tunnels is that configured tunnel endpoints require manual configuration, whereas 6to4 tunneling relies on an embedded IPv4 destination address to identify tunnel endpoints.

Conclusion

In summary, IPv6 is something we should all be planning for, the IETF recommends all four scenarios mentioned above; dual stack and tunneling being the preferred choices.

As a minimum requirement enterprises need to educate, evaluate and plan for IPv6 migration.

Hopefully this document will go some way to assist you and more specifically help you design and configure Alcatel-Lucent data equipment in the world of IPv6.

3 Additional Enhancements to IPv6

Introduction

It’s not all about address space, IPv6 also supports other features that make it more efficient, more scalable, more secure and faster than IPv4.

IPv6 includes many features as standard that are optional in IPv4.

IPv6 applications and services will continue to evolve during the 21st century which gives another compelling reason why IPv6 should be adopted.

Additional Enhancements of IPv6

- Streamlined Header
- Auto-Configuration
- QoS (Quality of Service)
- Multicasting
- Security
- Mobility

Streamlined Header

The IPv6 header has been significantly improved, it has been streamlined which makes packet processing easier by the forwarding routers.

You may wonder how this is possible when the IPv6 packet is much larger. Well, bigger it may be, but with a simplified fixed 40 byte header, aligned with 64 bit processing and dedicated routing ASICs, means the forwarding process is more efficient; the result, less latency and faster networks.

Auto-Configuration

ICMPv6 (Internet Control Message Protocol, Version 6, as described in RFC 4443) allows the auto-configuration of IPv6 hosts; including routers !

This concept may be hard to grasp by networking technicians, sceptical of its reliability.

Nevertheless, it is fully backed by the IETF and will significantly change the way we will manage layer 3 networks in the future.

As an example, for hosts, when an IPv6 interface is created or a device is connected to the switch, an IPv6 link-local address is automatically assigned for the interface and/or device. This is required for “back office” IPv6 connectivity, for example Neighbor Discovery.

In addition to a link-local address, other Ipv6 addresses will be applied to the interface depending on its connectivity to the global Internet or local enterprise network.

QoS (Quality of Service)

When we think about the changes in the Internet over the years and the global applications that are now are in use, namely, VoIP (Voice over IP), video conferencing and converged applications, applying QoS to time critical traffic is as important as ever.

IPv4 has some mechanisms for traffic priority, namely, ToS, DiffServ (DSCP), but these are not as widely used as they could be and have not scaled well as network traffic evolved.

IPv6 QoS support is different, newer headers define and improves the way network traffic is handled.

These flow based improvements will benefit newer technologies; especially end-to-end multimedia applications and as internet services continue to evolve.

Multicasting

Multicasting is included in the standard implementation and expands the feature set of IPv4.

Multicasting applications are mandatory for IPv6 and will continue to be instrumental in the efficient use of network infrastructure.

Security

Whereas Internet Security was an afterthought of IPv4, it still remains an optional feature, with IPv6 however, IPSec (Internet Protocol Security) is supposed to be **mandatory**; or should be used.

Extension definitions provide support for authentication, data integrity, and confidentiality.

In a troubled and uncertain world, security plays an important role in the safety of people’s lives and their privacy; not to mention corporate intellectual rights.

Mobility

Mobility is increasingly becoming an important part of life in the enterprise.

IPv6 improves the way mobile devices connect to the network, more detail is provided in RFC 3775.

In short, the IPv6 mobility feature allows IPv6 devices to “roam” in an IPv6 world without any user interaction, changing their point of presence on the Internet, without even changing their IP address !

Anycast addresses

A new type of address. Packets sent to an Anycast address are delivered to one member of the Anycast group.

Neighbor Discovery protocol

A protocol defined for IPv6 that detects neighboring devices on the same link and the availability of those devices. Additional information that is useful for facilitating the interaction between devices on the same link is also detected (e.g., neighboring address prefixes, address resolution, duplicate address detection, link MTU, and hop limit values, etc.).

4 Being IPv6 Ready… what does it mean ?

For a technical person the term "Ready" always makes them feel a little suspicious; it's a bit like a marketing department trying to describe one of its 'run of the mill' products as if to imply that it has more functionality than it really has.

Do you remember the 1990's when the Internet and PC's were becoming affordable for the home user. Computer superstores were selling PC packages that were "Internet Ready", that is, if you purchased their package, went to another shop and bought a modem, subscribed to an internet service and then assuming you had the knowledge to put it all together and heaven forbid, actually make it work …a bit of an exaggeration, I know, but you get the point.

The term "IPv6 Ready" could be used in the same way today, some vendor's, no doubt will.

To avoid this, a number of providers and organisations are promoting certification as a means to give credibility to vendor IPv6 readiness.

The IPv6 Forum has released an **IPv6 Ready Logo** Program to prove interoperability, IETF conformance and to give confidence to the market that IPv6 is available and ready to go.

There are currently six approved testing labs across the globe to help encourage and promote this program; four are in the far-east and the remaining two are located in France and the USA.

- IRISA (France) : http://www.irisa.fr/tipi/

- UNH-IOL (United States) : http://www.iol.unh.edu/consortiums/ipv6/

The IPv6 Forum currently has two primary levels of accreditation, with a third planned for the future.

- IPv6 Readiness Phase 1; released September 2003

- IPv6 Readiness Phase 2; released February 2005

- *IPv6 Readiness Phase 3; TDB*

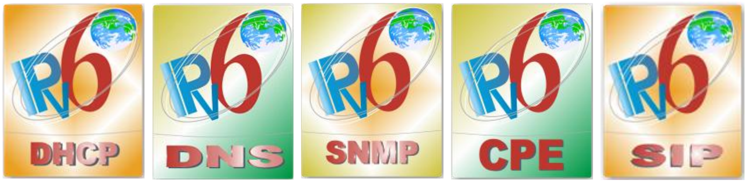
  Phase 3 will be similar to 2, the primary difference being IPSec support and testing will be mandatory; the program release date is still to be determined.

Other readiness logos can also be obtained, on the June 8th 2009 the IPv6 Ready Logo Committee announced validating wed-sites.

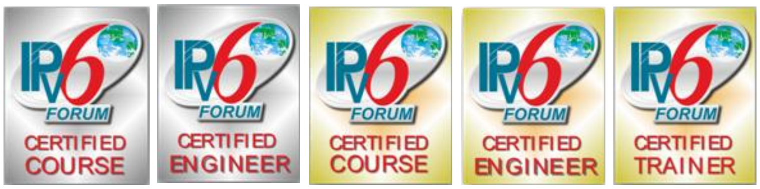
In June 2009 the validation program for ISP's was released.

And last year the IPSec logo was announced.

IPv6 Protocol specific compliances are also given logos.



To ensure IPv6 competency in education, a dedicated program has been released to define content and certify trainers. In turn, engineer's can achieve Silver and Gold accreditations.


IPv6 FORUM CERTIFIED COURSE
IPv6 FORUM CERTIFIED ENGINEER
IPv6 FORUM CERTIFIED COURSE
IPv6 FORUM CERTIFIED ENGINEER
IPv6 FORUM CERTIFIED TRAINER

IPv6 Readiness Phase 1 (Silver Logo)

Phase 1 commenced in September 2003 and focuses on core IPv6 protocols, the primary tests are taken from the following RFC's.

- **RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification**
- RFC 4291 - IPv6 Addressing Architecture
- RFC 4861 - Neighbor Discovery
- RFC 4862 - Stateless AutoConfiguration
- RFC 4443 - ICMPv6

There are approximately 170 tests carried out in Phase 1; these are also replicated in Phase 2.

This is the minimum requirement for IPv6 and is represented by the **Silver** IPv6 ready logo.

For vendors, IPv6 readiness phase 1 is not sufficient for the enterprise, as a minimum it is recommended that phase 2 be achieved.

For this reason the IPv6 forum has decided to retire phase 1.

The deadline for existing applications has been set for the end of September 2011, after that Phase 2 will be the only readiness program available, that is, until Phase 3 has been decided upon.

IPv6 Readiness Phase 2 (Gold Logo)

Phase 2 has been around since February 2005 and goes far beyond the fundamental tests carried out in Phase 1, as shown below,

- RFC 1981 - Path MTU Discovery for IPv6
- **RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification**
- RFC 4291 - IPv6 Addressing Architecture
- RFC 4443 - ICMPv6
- RFC 4861 - Neighbor Discovery
- RFC 4862 - Stateless AutoConfiguration

RFC 1981 Path MTU Discovery for IPv6 has been added to the above core tests of those carried out in Phase 1.

Almost 300 additional tests have been added to Phase 2 and extend conformance and interoperability testing beyond the core and into the remaining parts of the internetwork, as shown below,

- **Internet Protocol Security (IPSec)**
    - RFC 2404 The Use of HMAC-SHA-1-96 within ESP AH
    - RFC 2410 NULL Encryption Algorithm
    - RFC 2451 ESP CBC-Mode Cipher Algorithms
    - RFC 3602 AES-CBC Cipher Algorithm
    - RFC 3566 AES-XCBC-MAC-96 Algorithm
    - RFC 3686 AES Counter Mode with ESP
    - RFC 4301 Security Architecture for IP
    - RFC 4303 IP Encapsulating Security Payload (ESP)
    - RFC 4305 Cryptographic Algorithm for ESP and AH
    - RFC 4312 Camellia Cipher Algorithm

- **Internet Key Exchange Protocol v2 (IKEv2)**
  - RFC 4306 IKEv2 Protocol Specification
  - RFC 4307 Cryptographic Algorithms for IKEv2
  - RFC 4718 IKEv2 Clarifications and Guidelines

- **Mobile IP v2 (MIPv2)**
  - RFC 3775 Mobility Support in IPv6
  - RFC 3776 IPSec to Protect Mobile IP

- **Network Mobility (NEMO)**
  - RFC 3963 NEMO Protocol
  - RFC 3775 Mobility Support in IPv6

- **Dynamic Host Configuration Protocol (DHCPv6)**
  - RFC 3315 DHCPv6 Protocol
  - RFC 3646 DNS for DHCPv6
  - RFC 3736 Stateless DHCP for IPv6

- **Session Initiation Protocol (SIP)**
  - RFC 3261 SIP Protocol
  - RFC 3264 Offer Model for Session Description protocol
  - RFC 4566 Session Description protocol (SDP)
  - RFC 2617 HTTP Authentication
  - RFC 3665 Basic Call Flow Examples

- **Management (SNMP-MIBs)**
  - RFC 3416 SNMPv2
  - RFC 3418 MIB for SNMP
  - RFC 2578 SMIv2
  - RFC 2579 Textual Conventions for SMIv2
  - RFC 2580 Conformance Statements for SMIv2

It is worth mentioning at this point that IPv6 Phase 2 Readiness is not a “blanket” compliance or accreditation, each of the following components in the IPv6 world can be tested and obtain a readiness certification and associated logo.

- **IPv6 Core Protocols**
  - Host
  - Router
- **IPSec**
  - End-Node
  - Security Gateway
- **IKEv2**
  - End-Node
  - Security Gateway
- **MIPv6**
  - Correspondent Node
  - Home Agent
  - Mobile Node
- **NEMO**
  - Home Agent
  - Mobile Router
- **DHCPv6**
  - Client
  - Server
  - Relay Agent
- **SIP**
  - UA
  - Endpoint
  - B2BUA
  - Proxy
  - Registrar
- **Management (SNMP-MIBs)**
  - Agent
  - Manager
- **MLDv2**
  - Router
  - Listener

Care must be taken when choosing your IPv6 infrastructure, if IPv6 Readiness Phase 2 has been achieved by a networking vendor, it is important to confirm which specific features have been complied with.

Depending on whether you are a host or router, different tests and conformance certifications will assigned.

To help you, the program has defined an identification process by assigning the following parameters in the certification number.

This is done by using the following Phase-2 Logo format ID.

Phase (nn) – (*additional information*) – (ssssss)

Phase (nn)

This is a 2 digit field and denotes the IPv6 Readiness Phase achieved, in this case 02.

Additional Information

This is a variable length field that contains specific extended category tests achieved by the equipment, each character can be combined in this field.

C	IPv6 Core Protocol
S	IPsec
M	Mobile IP
N	Network Mobility
D	DHCPv6
P	SIP

Serial Number (ssssss)

This is a six digit field containing a world-wide unique serial number.

For example the OmniSwitch 6850 and Ruggedized OmniSwitch 6855 have been issued with the following serial number from the IPv6 Ready Logo Program, you can identify from this serial number that the 6850/6855 conforms to phase 2 core protocols.

02-C-000240.

Phase 2 is represented by the **Gold** IPv6 ready logo.

Whereas IPv6 Readiness Phase 2 is described as the optimum compliance, Alcatel-Lucent would suggest it is the minimum requirement for enterprise customers when choosing to invest in vendor equipment upgrades.

It is essential that any planned migration to IPv6 includes an infrastructure that is able to scale fully to native IPv6.

A list of vendor compliance can be viewed here…

https://www.ipv6ready.org/db/index.php/public

5 ALU IPv6 Data Readiness

AoS, the Alcatel-Lucent operating system is key to providing advanced switching and routing across its family of switches.

This Omni-product family meets the most stringent and mission critical networking requirements for the access layer, the distribution layer and in the core.

For this reason IPv6 support, is key to a scalable end-to-end networking solution for the enterprise.

Alcatel-Lucent takes seriously its commitment, conformance and interoperability with IPv6.

The following sections discuss each model in detail to assist with the design and implementation and deployment in the world of IPv6.

OmniSwitch Family

The Alcatel-Lucent OmniSwitch family consists of both chassis and virtual chassis based layer 2-4 fully featured advanced switching solutions.

The following AoS (Alcatel-Lucent Operating System) trains are discussed in the sections below,

- **AoS v6.6.2**
  - OmniSwitch 6250
  - OmniSwitch 6450

- **AoS v6.4.4**
  - OmniSwitch 6400
  - OmniSwitch 6850, 6855, 6850E
  - OmniSwitch 9000, 9000E

- **AoS v7.2.x - Next Generation Switches**
  - OmniSwitch 6900
  - OmniSwitch 10K

AoS v6.6.x

The Alcatel-Lucent OmniSwitch 6250 and 6450 are new value basic Layer 3 Fast Ethernet and Gigabit Stackable LAN family of switches for both the Enterprise and Ethernet access segments, with additional uplinks and software features such as Ethernet Services (VLAN stacking), VLAN translation, Ethernet OAM, Private VLANs, IPMC VLANs and more for a secure, guaranteed triple-play level of service expected by Service Provider customers.

The Alcatel-Lucent OmniSwitch 6250 and 6450 supports IPv6 with hardware-based forwarding for wire-speed classification and tunneling. It is flexible in that a choice of IPv4, IPv6, or IPv4/IPv6 can be deployed without compromising switch performance, supporting both RIPng and Static Routing.

Hardware-based classification using ACLs (access control lists) and QoS (quality of service) (QoS), as is forwarding and management for IPv6.

Transition from an existing IPv4 network can be achieved with tunneling.

Maximum IPv6 interfaces	16
Maximum IPv6 interfaces per VLAN	1
Maximum IPv6 global unicast addresses	16
Maximum IPv6 global unicast addresses per IPv6 interface	10
Maximum IPv6 static routes per switch	128
Maximum IPv6 host routes per switch	128
Maximum IPv6 neighbors (ND)	128
Maximum Number of RIPng Peers	10
Maximum Number of RIPng Interfaces	10
Maximum Number of RIPng Routes	128

RFCs for IPv6 supported on the OmniSwitch 6250 and 6450 are,

RFC 2292	Advanced Sockets API for IPv6
RFC 2373	IPv6 Addressing Architecture
RFC 2374	IPv6 Aggregatable Global Unicast Address Format
RFC 2452	IPv6 TCP/UDP MIBs
RFC 2454	IPv6 TCP/UDP MIBs
RFC 2460	IPv6 Specification
RFC 2462	IPv6 Stateless Address Autoconfiguration
RFC 2463	ICMPv6 & MIBs
RFC 2464	Transmission of IPv6 Packets over Ethernet
RFC 2466	ICMPv6 & MIBs
RFC 2553	Basic Socket Extensions for IPv6 (obsoleted by RFC 3493)
RFC 2893	Transmission Mechanisms for Hosts & Routers (obsoleted by RFC 4213; exc. Automatic Tunnels)
RFC 3056	IPv6 Tunneling
RFC 3493	Basic Socket Extensions for IPv6
RFC 3515	Session Initiation Protocol
RFC 3542	Advanced Sockets API for IPv6
RFC 3587	IPv6 Global Unicast Address Format

AoS v6.4.x

The OmniSwitch 6400, 6850, 6855, 6850E, 9000 & 9000E series is our line of advanced Layer 2/Layer 3 basic routing, GigE fixed configuration stackable and chassis based LAN switches.

The stackables are small in size but big in performance, it excels at the enterprise edge and in the SMB core with the industry's most advanced triple-play services, PoE, L2/L3 performance and extensive network security.

By providing price performance leadership, advanced QoS and layer-3 features, the OmniSwitch 6400 is fast enough to run wide open at the edge, and powerful enough to anchor your SMB core.

IPv6 support at Layer 3 includes RIPng and Static Routing.

The total number of IPv6 routes supported in hardware (with no IPv4 routes) is 512.

The OmniSwitch 6850/E Stackable LAN Switch family offers versatile, fixed configuration Layer 3 Gigabit and 10 Gigabit Ethernet (10GigE) switches, which provide advanced services, high performance, and IEEE 802.3at compliant Power over Ethernet (PoE).

All models in the family are stackable and perform wire-rate, Gigabit switching and routing for both IPv4 and IPv6, delivering intelligent services to the edge of the network with optimal quality of service (QoS) and integrated security, as well as network admission control (NAC).

Also, the OmniSwitch 6850 protects your investment with native support of IPv4 and IPv6 switching.

The new OmniSwitch 9000/E family, comprised of the OS9700E and the OS9800E, are fully featured, high availability and high-performance 10Gigabit Ethernet (10GigE) chassis LAN switches designed for data centers, core and campus networks.

The OS9000E delivers wire-rate support of multiple-virtual routing and forwarding (VRF), the foundation for network virtualization in the data center. Network availability is enhanced through an in service software upgrade capability such that emergency patching is achieved without taking the network down.

The OmniSwitch 9000E family offers enterprises and service providers gigabit capacity, advanced Layer 3 switching, high availability through in-service software upgrades (ISSUs), layer-2 segregation using VLANs, stacked VLANs and Virtual Private LAN Service (VPLS), as well as Layer 3 segregation using multiple virtual routing and forwarding (VRF).

The OS9000E family provides full IPv6 support with hardware-based forwarding for wire-rate speeds, classification and tunneling to address various corporate and government requirements for IPv6. Unlike most switches that support IPv6, the performance of the OS9000s is unaffected by enabling IPv6 processing whether deploying IPv4, IPv6, or IPv4/IPv6. These switches address the U.S. Federal government Department of Defense (DoD) requirement that IPv6 be supported for migration by 2008 and addresses other countries' requirements including:

- Ability to connect to the IPv6 backbone
- Use of IPv6 across public organizations
- Ability to interconnect the IPv6 "island" through an existing IPv4 network through hardware-based tunneling
- Ability to control IPv6 flows with extensive QoS/ACL policies

The OS9000E family provides hardware-based classification (access control lists (ACLs) and quality of service (QoS), forwarding and management for IPv6. More importantly, it provides a way to transition from an existing IPv4 network with support of tunneling (configured and 6-in-4). The OS9000Es are able to work with the existing AOS switches, and support the full suite of unicast routing protocols, multicast registration and routing protocols, QoS/ACLs and tunneling.

RFCs for IPv6 supported on AoS v6.6.x are,

RFC 1886	DNS Extensions for IPv6
RFC 2292	Advanced Socket API
RFC 2373	IPv6 Addressing Architecture
RFC 2374	IPv6 Aggregatable Global Unicast Address Format
RFC 2452	IPv6 TCP MIBs
RFC 2454	IPv6 UDP MIBs
RFC 2460	Internet Protocol, Version 6 (IPv6) Specification
RFC 2461	Neighbor Discovery for IP Version 6 (IPv6)
RFC 2462	IPv6 Stateless Address Auto-configuration
RFC 2463	ICMPv6 for IPv6
RFC 2464	Transmission of IPv6 Packets Over Ethernet
RFC 2466	MIB for IPv6
RFC 2553	Basic Socket Extensions for IPv6
RFC 2893	Transition Mechanisms for IPv6 Hosts and Routers
RFC 3513	IPv6 Addressing Architecture
RFC 3056	Connection of IPv6 Domains via IPv4 Clouds
RFC 3493	Basic Socket Extensions for IPv6
RFC 3542	Advanced Sockets API for
RFC 3587	IPv6 Global Unicast Address
RFC 4213	Transition Mechanisms, exc. auto tunnels (obsoletes RFC 2893)

The following table shows IPv6 parameters supported on AoS v6.6.x

Maximum IPv6 router VLANs per switch	4094 (single MAC router mode)
Maximum IPv6 interfaces per tunnel	1
Maximum IPv6 static routes	1,000
Maximum RIPng routes	5K
Maximum RIPng interfaces	100
Maximum OSPFv3 routes	10K
Maximum OSPFv3 interfaces	10
Maximum OSPFv3 areas	5
Maximum OSPFv3 sessions	1
OSPF ECMP Gateways per destination	4
Maximum 6to4 tunnels per switch	1
Maximum configured tunnels per switch	255

AoS v7.2.x

The Alcatel-Lucent OmniSwitch 6900 Stackable LAN Switches are compact, high-density 10G and 40G platforms designed for the most demanding networks.

In addition to high performance and extremely low latency, the OmniSwitch 6900 platforms offer extensive QoS, Layer 2 and Layer 3 switching, as well as system and network level resiliency.

The Alcatel Lucent OmniSwitch 10K Modular LAN Chassis platform however, is a high-capacity, high-performance 10G Ethernet LAN switch.

The OmniSwitch 10K delivers uninterrupted network uptime with non-stop Layer 2 and Layer 3 forwarding, both IPv4 and IPv6 are supported along with the ability to tunnel IPv6 traffic over IPv4, the OmniSwitch 10K provides the following mechanisms to maintain compatibility between IPv4 and IPv6,

Both IPv4 and IPv6 are supported on AoS v7.X with the ability to tunnel IPv6 traffic over IPv4, the implementation of IPv6 on the OmniSwitch 6900 provides the following mechanisms to maintain compatibility between IPv4 and IPv6,

- Dual-stack support for both IPv4 and IPv6 on the same switch
- Configuration of IPv6 and IPv4 interfaces on the same VLAN.
- Tunneling of IPv6 traffic over an IPv4 network infrastructure

NOTE

The switch operates only in single MAC router mode. In this mode, each router VLAN is assigned the same MAC address, which is the base chassis MAC address for the switch.

When an IPv6 interface is created or a device is connected to the switch, an IPv6 link-local address is automatically assigned for the interface and/or device.

The standard IPv6 RFCs supported on AoS v7.2.x are as follows,

RFC 2893	Transition Mechanisms for IPv6 (Obsoleted by RFC4213)
RFC 2460	Internet Protocol, Version 6 (IPv6) Specification
RFC 2461	Neighbor Discovery for IP Version 6 (IPv6)
RFC 2462	IPv6 Stateless Address Auto-configuration
RFC 2463	ICMPv6 for the IPv6 Specification
RFC 2464	IPv6 Packets Over Ethernet Networks
RFC 2893	Transition Mechanisms for IPv6 Hosts and Routers
RFC 3513	IPv6 Addressing Architecture
RFC 3056	Connection of IPv6 Domains via IPv4 Clouds
RFC 4213	Transition Mechanisms (exc. Automatic tunneling)
RFC 2373	IPv6 Addressing Architecture
RFC 2374	IPv6 Aggregately Global Unicast Address Format
RFC 2553	Basic Socket Interface Extensions for IPv6

NOTE

IPv6 unicast cannot be enabled in non-default VRFs since it is dependent on IPv6 protocol which is available only in the default VRF.

IPv6 routed traffic is not supported in non-default VRFs.

However IPv6 traffic can be sent in a non-default environment and IPv6 QoS policies applied when the IPv6 traffic is sent in a bridged environment.

A summary of IPv6 features supported are listed below,

- RIPng (Routing Information Protocol next generation)
- OSPF v3
- Multicast Listener Discovery (MLD)
- VRRP v3
- MBGP Extension for IPv6
- IPv6 IPSEC encrypted control
- Multicast Route Boundaries

Each of the following features are discussed in detail below,

RIPng (Routing Information Protocol; next generation)

The Routing Information Protocol next generation (RIPng) is an interior gateway protocol (IGP) that uses a distance-vector algorithm to determine the best route to a destination, using the hop count as the metric. RIPng is a routing protocol that exchanges routing information used to compute routes and is intended for Internet Protocol version 6 (IPv6)-based networks.

Essentially, RIPng is an extension of RIPv2 to operate in the IPv6 world.

- RFC 2080 : RIPng for IPv6

Criteria	**Limit**
Maximum RIPng routes	5K
Maximum RIPng interfaces	100

OSPF v3

OSPFv3 is an extension of OSPF version 2 (OSPFv2) that provides support for networks using the IPv6 protocol. Like v2 OSPFv3 is a shortest path first (SPF), or link-state protocol and used to distribute routing information between routers in a single Autonomous System (AS) in an IPv6 network.

OSPFv3 will implement OSPFv3 graceful restart both as restarting system and as a helper; OSPF graceful restart assumes that a redundant CMM is available.

OSPFv3 requires the use of IPv6 protocol security it does not use MD5 encryption or authentication the way OSPFv2 does. An interface must exit to IPv6 to use the security features of IPv6 from the OSPFv3 module.

▪	RFC 2740	OSPF for IPv6 December 1999
▪	RFC 1826	IP Authentication Header
▪	RFC 1827	IP Encapsulating Security Payload
▪	RFC 2373	IPv6 Addressing Architecture
▪	RFC 2374	IPv6 Aggregatable Global Unicast Address Format
▪	RFC 2460	IPv6 base specification
▪	RFC 2553	Basic Socket Interface Extensions for IPv6

IETF Internet-Drafts Supported
draft-ietf-ospf-ospfv3-graceful-restart-xx.txt—OSPFv3 Graceful Restart
draft-ietf-ospf-ospfv3-mib-09.txt—Management Information Base for OSPFv3
draft-ietf-ospf-ospfv3-update-00.txt—OSPF for IPv6
draft-ietf-ospf-ospfv3-auth-05.txt—Authentication/ Confidentiality for OSPFv3
draft-ietf-ospf-ospfv3-mib-08.txt—MIB

NOTE

OSPFv3 requires the use of IPv6 protocol security and does not use MD5 encryption or authentication the way OSPFv2 does.

Multicast Listener Discovery (MLD)

MLD is used by IPv6 systems (hosts and routers) to report their IPv6 multicast group memberships to any neighboring multicast routers. MLD is derived from version 2 of IPv4's Internet Group Management Protocol, IGMPv2. MLD uses ICMPv6 message types, rather than IGMP message types.

MLD Version 1 (MLDv1) handles forwarding by IPv6 multicast destination addresses only. MLD Version 2 (MLDv2) handles forwarding by source IPv6 addresses and IPv6 multicast destination addresses.

MLDv2 uses source filtering and reports multicast memberships to neighboring routers by sending membership reports. MLDv2 also supports Source Specific Multicast (SSM) by allowing hosts to report interest in receiving packets only from specific source addresses or from all but specific source addresses.

- RFC 2710 Multicast Listener Discovery for IPv6
- RFC 3810 Multicast Listener Discovery v2 for IPv6
- RFC 3019 IPv6 MIB for Multicast Listener Discovery
- *IETF Internet-Drafts Supported - Draft-ietf-magma-snoop*

Criteria	**Limit**
IPv6 hardware-based Multicast Routing Supported	Yes
Max IPv6 Multicast routes supported	Limited by available memory
Max IPv6 Multicast Flows	1021
Max 64-byte IPv6 multicast packets forwarded per second	Wire-rate
Max 1518-byte IPv6 multicast packets forwarded per second	Wire-rate

VRRP v3

VRRPv3 is a standard router redundancy protocol for routers controlling IPv6 addresses that provides redundancy by eliminating the single point of failure inherent in a default route environment and is similar in operation to VRRP v2 for IPv4.

The VRRPv3 router, which controls the IPv6 address associated with a virtual router is called the master router, and is responsible for forwarding virtual router advertisements. If the master router becomes unavailable, the highest priority backup router will transition to the master state. Both versions of VRRP allow routers on a LAN to back up a static default route with a virtual router.

Both versions of VRRP support VRRP Tracking.

A virtual router's priority may be conditionally modified to prevent another router from taking over as master. Tracking policies are used to conditionally modify the priority setting whenever an IP interface, slot/port, and/or IP address associated with a virtual router goes down.

NOTE

Authentication is not supported and a total of 255 VRRPv3 instances can be configured if only IPv6 instances are configured.

MBGP Extension for IPv6

Multiprotocol Extensions to BGP-4 supports the exchange of IPv6 unicast addresses, as well as establishing BGP peering sessions with BGP speakers identified by their IPv6 address.

The OmniSwitch provides IPv6 support for BGP using Multiprotocol Extensions. The same procedures used for IPv4 prefixes can be applied for IPv6 prefixes as well and the exchange of IPv4 prefixes is not affected by this feature. However, there are some attributes that are specific to IPv4, such as AGGREGATOR, NEXT_HOP and NLRI. Multiprotocol Extensions for BGP also supports backward compatibility for the routers that do not support this feature. MP extensions for BGP are not VRF aware.

• RFC 4760	Multiprotocol Extensions for BGP-4
• RFC 2545	BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing

IPv6 IPSEC encrypted control

IPsec support is required to provide the IPv6 ESP (Encapsulated Security Payload) and AH (Authentication Header) functionality.

Security policies are defined to specify which traffic requires IPSec processing. A security policy requires that the source and destination of the traffic be specified.

The source and destination may either be specified as IPv6 addresses (along with an optional prefix length specification to cover a range of addresses) or as a host name. The policy may cover all traffic from the source to the destination, or be restricted further by specifying an upper-layer protocol, source, and/or destination ports. Each policy is unidirectional, applying either to inbound or outbound traffic. Therefore, to cover all traffic between a source and destination, two policies would need to be defined (one for inbound, one for outbound).

ESP & AH

Security Payload (ESP) and Authentication Header (AH) – Describes the cryptographic algorithms that are to be supported.

For ESP, support is provided for:

- NULL
- DES-CBC
- TripleDES-CBC
- AES-CBC (min with 128-bit keys)
- AES-CTR (min with 128-bit keys)

For AH, the supported algorithms are:

- HMAC-SHA1-96
- HMAC-MD5-96
- AES-XCBC-MAC-96

NOTE

In order to avoid export compliance reclassification for OmniSwitches as well as provision for possible future enhancements where any encryption related code is in a separate file, an additional software bundle is created which is not be part of the default software shipped for any of the products.

This "software" is handled the same way as the advanced routing software for today. There is an orderable marketing part in the price list.

The software bundle consists of one file, “xxxEncrypt.img” where xxx stands for "K2" "J" "F" "G" or whatever code letter is currently used to identify OmniSwitch families. This file is treated as any other *.img files meaning the expected location for it is /working and /certified directory.

When present, the IPSec feature can be enabled on the switch.

A summary of supported RFCs associated with IPSec,

- RFC 4301 Security Architecture for the Internet Protocol
- RFC 4302 IP Authentication Header
- RFC 4303 IP Encapsulating Security Payload
- RFC 4305 Crypto for ESP and Authentication Header (AH)

NOTE

This feature requires a special licence that must be ordered separately from AoS.

The licence is not per box; it is not bound to the device MAC Address.

Multicast Route Boundaries

AOS implementation includes support for IPv6 scoped multicast address as specified in RFC 4007.

For multicast addresses, there are fourteen possible scopes, ranging from interface-local to global (including link-local).

Administrative scoping, as specified in RFC 4007, permits a PIM domain to be divided into multiple admin-scope zones. Each admin-scope zone is a convex connected set of PIM routers and is associated with a set of group addresses. The boundary of the admin-scope zone is formed by Zone Border Routers (ZBRs). ZBRs are configured not to forward traffic for any of the configured scoped group addresses into or out of the scoped zone.

Zone Border Router

AIS implementation of PIM supports the administratively scoped range and enforces the following:

If an incoming multicast flow is received on a boundary interface for a multicast group that is operating in dense mode, PIM-DM needs to prune this boundary.

PIM-SM doesn’t accept joins for sparse-mode groups in the administratively scoped range.

PIM join/prune messages for administratively scoped ranges are not sent on the RPF interface when a boundary is defined.

Registers and Bootstrap router messages are also filtered on the boundary.

Bootstrap Router Mechanism

The PIM BSR mechanism provides support for BSR state per configured or learned scope zone. A separate BSR election will take place for every administratively scoped range, plus one for the global range. If administrative scoping is not configured, then only the global, non-scoped BSR will be running.

Configuration of multiple RPs is supported for scoped BSR.

- RFC 2365 Administratively Scoped IP Multicast
- RFC 2932 IPv4 Multicast Routing MIB
- RFC 4007 IPV6 Scoped Address Architecture
- RFC 5059 Bootstrap Router (BSR) Mechanism for PIM

Parameters relating to IPv6 are shown below,

Max Multicast Flows per switch, 1,021 (with hardware routing)

There is no hard limit on the number of static multicast groups that can be configured, but if user tries to send traffic to the entire group at the same time the forwarding is limited to 1,021 hardware flows; a flow is defined as a source-group pair.

In the case all hardware entries are exhausted, the IPMS will not perform software forwarding.

IP multicast tunneling is performed in software.

Valid Scoped Address Range: 239.0.0.0 to 239.255.255.255.

For IPv6, only one zone, the default zone, will be supported per scope zone.

- Support for 4093 multicast routes
- Support for 64 VRF instances.

RFC Summary for ALU Data Switches

AoS (Alcatel Lucent OS)		**v6.6.x**	**v6.4.x ***	**v7.x**
IPv6 Specification	**2460**	✓	✓	✓
IPv6 Addressing Architecture	~~2373~~	✓	✓	✓
	~~3513~~	✓	✓	✓
	4291	✓	✓	✓
Neighbor Discovery for IPv6	~~2461~~	✓	✓	✓
	4861	□	□	□
Stateless AutoConfiguration	~~2462~~	✓	✓	✓
	4862	□	□	□
ICMPv6	~~2463~~	✓	✓	✓
	4443	✓	✓	✓
Path MTU Discovery for IPv6	**1981**	✓	✓	✓
IPv6 Global Unicast Address Format	~~2374~~	✓	✓	✓
	3587	✓	✓	✓
Unique Local IPv6 Unicast Addresses	4193	□	✓	✓
Default Address Selection for IPv6	3484	□	✓	✓

		6.6.x	6.4.x	7.x
IPv6 Aggregatable Global Unicast Format	4007	□	✓	✓
Transmission of IPv6 over Ethernet	~~2464~~	✓	✓	✓
	6085	□	□	□
**DHCPv6	**3315**	✗	✗	✗
RIPng	2080	✓	✓	✓
OSPFv3	~~2740~~	□	✓	✓
	5340	□	□	□
BGP4	**4271**	□	✓	✓
Multiprotocol Extensions for BGP4	**4760**	□	✓	✓
BGP4 Extensions for IPv6	2545	□	✓	✓
IPv6 Transition Mechanisms (excluding AutoTunnels)	~~2893~~	✓	✓	✓
	4213	✓	✓	✓
6to4	3056	✓	✓	✓
Generic Packet Tunneling in IPv6	2473	✗	✗	✗

		6.6.x	6.4.x	7.x
IPv6 Router Alert Option	2711	□	✓	✓
VRRPv3	~~3768~~	□	✓	✓
	5798	□	□	□
Multicast Listener Discovery (MLD) for IPv6	2710	□	✓	✓
MLDv2 for IPv6 Update	3810	□	□	✓
Multicast Group Membership Discovery MIB	~~3019~~	□	✓	✓
	5519	□	□	□
IPv6 TCP MIBs	~~2452~~	✓	✓	✓
	4022	□	□	□
IPv6 UDP MIBs	~~2454~~	✓	✓	✓
	4113	□	□	□
MIB for IPv6	~~2466~~	✓	✓	✓
	4293	□	✓	✓
SMIv2	~~1902~~	□	□	□
	2578	✓	□	□
SMIv2 (Textual Conventions)	**2579**	✓	□	□

		6.6.x	6.4.x	7.x
Conformance Statements for SMIv2	**2580**	✓	□	□
	~~1886~~	✓	✓	✓
	~~3152~~	□	□	□
DNS Extensions for IPv6	**3596**	□	✓	✓
Admin Scoped IP MCMulticast	2365	□	✓	✓
	~~2292~~	✓	✓	✓
Advanced Socket API	**3542**	✓	✓	✓
	~~2553~~	✓	✓	✓
Basic Socket Extensions for IPv6	**3493**	✓	✓	✓
Security Architecture for IP	**4301**	□	✓	✓
IP Encapsulating Security Payload (ESP)	**4303**	□	□	✓
Cryptographic Algorithm for ESP and AH	**4305**	□	□	✓
	~~1826~~	□	□	✓
IP Authentication Header	**2402**	□	□	□
	~~1827~~	□	□	✓
IP Encapsulating Security Payload (ESP)	**2406**	□	□	□

		6.6.x	6.4.x	7.x
TC for Flow Label	3595	□	✓	✓
	~~2402~~	□	□	□
IP Authentication Header	**4302**	□	✓	✓
Bootstrap Router for PIM	5059	□	□	✓

NOTE

1. Exceptions being OmniSwitch 6400 which has limited L3 capabilities
2. Strikethrough RFC's are obsoleted
3. ** DHCPv6 (RFC 3315) is planned for AoS v6.4.5

6 Basic AoS IPv6 Configuration

The section discusses IPv6 basic configuration when using the Alcatel-Lucent Operating System, known as AoS, for advanced configuration please refer to the OmniSwitch AoS Release 6 / 7 Network Configuration Guide; non-technical readers may wish to skip this chapter.

AoS is common across all of the Alcatel-Lucent Data Switches and as such makes configuration and management easier when designing end-to-end networking solutions.

The only exception being with our value edge switches, the OmniSwitch 6250 and 6450, whereby Layer 3 functionality is limited in the hardware to RIPng and Static Routing. Nevertheless, the 6250 Ethernet and 6450 Gigabit switches support IPv6 with hardware-based forwarding for wire-speed classification and tunneling, ideal for SMB and edge solutions.

The Basics

In the following examples it is assumed that two VLANs have are already configured on the switch, namely, VLANs 10 & 20.

1. Configure an IPv6 interface for VLAN 10 by using the ipv6 interface command. For example:

```
-> ipv6 interface v6if-v10 vlan 10
```

NOTE

When the IPv6 interface is configured, the switch automatically generates a link-local address for the interface. This allows for communication with other interfaces and or devices on the same link for the purpose of address resolution and Neighbor Discovery, however, these interfaces ***do not provide routing between interfaces.***

2. Assign a unicast address to the v6if-v10 interface by using the IPv6 address command. For example:

-> ipv6 address 4100:1::/64 eui-64 v6if-v10

3. Configure an IPv6 interface for VLAN 20 by using the IPv6 interface command. For example:

-> ipv6 interface v6if-v300 vlan 20

4. Assign a unicast address to the v6if-v20 interface by using the ipv6 address command. For example:

-> ipv6 address 4100:2::/64 eui-64 v6if-v20

Note: if you would like to verify the IPv6 interface configuration, enter

-> show ipv6 interface

Example of "show ipv6 interface" display is shown below…

```
Name                   IPv6 Address/Prefix Length           Status  Device
----------------------+------------------------------------+------+--------
v6if-v10               fe80::2d0:95ff:fe12:fab5/64          Down    VLAN 10
                       4100:1::2d0:95ff:fe12:fab5/64
                       4100:1::/64

v6if-v20               fe80::2d0:95ff:fe12:fab6/64          Down    VLAN 20
                       4100:2::2d0:95ff:fe12:fab6/64
                       4100:2::/64

loopback               ::1/128                              Active  Loopback

                       fe80::1/64
```

NOTE

Link-Local addresses for the two new interfaces and the loopback interface were automatically created and included in the show ipv6 interface display output.

In addition, the subnet router anycast address that corresponds to the unicast address is also automatically generated for the interface.

5. Enable RIPng for the switch by using the ipv6 load rip command.

```
-> ipv6 load rip
```

6. Create a RIPng interface for each of the IPv6 VLAN interfaces by using the ipv6 rip interface command.

```
-> ipv6 rip interface v6if-v10
-> ipv6 rip interface v6if-v20
```

IPv6 routing is now configured for VLAN 10 and VLAN 20 interfaces, but it is ***not active*** until at least one port in each VLAN goes active.

Configuring an IPv6 Interface

The ipv6 interface command is used to create an IPv6 interface for a VLAN, when configuring an IPv6 interface, it is important to note that,

- A unique interface name is required for a VLAN interface.
- If creating a VLAN interface, the VLAN must already exist.
- The following configurable interface parameters are set to their default values unless otherwise specified when the ipv6 interface command is used.
- Each VLAN can have one IPv6 interface. Configuring both an IPv4 and IPv6 interface on the same VLAN is allowed. Note that the VLAN interfaces of both types are not active until at least one port associated with the VLAN goes active.
- A link-local address is automatically configured for an IPv6 interface when the interface is configured.
- Assigning more than one IPv6 address to a single IPv6 interface is allowed.

- Assigning the same link-local address to multiple interfaces is allowed. Each global unicast prefix, however, can only exist on one interface.

By way of example, if an interface for a VLAN 11 is configured with an address 4100:1000::1/64, an interface for VLAN 12 cannot have an address 4100:1000::2/64.

- Each IPv6 interface anycast address must also have a unique prefix.

Note: Multiple devices may share the same anycast address prefix to identify themselves as members of the anycast group.

Modifying an IPv6 Interface

The ipv6 interface command is also used to modify existing IPv6 interface parameter values. It is not necessary to first remove the interface and then create it again with the new values. The changes applied will overwrite existing parameter values.

For example, the following command changes the router advertisement (RA) reachable time and the RA retransmit timer values for interface v6if-v10:

```
-> ipv6 interface v6if-v10 ra-reachable-time 60000 ra-retrans-time 2000
```

IPv6 interface parameters

ra-send

ra-max-interval

ra-managed-config-flag

ra-other-config-flag

ra-reachable-time

ra-retrans-timer

ra-default-lifetime

ra-send-mtu

base-reachable-time

When an existing interface name is specified with the ipv6 interface command, the command modifies specified parameters for that interface.

If an unknown interface name is entered along with an existing VLAN parameter, a new interface is created with the name specified.

Removing an IPv6 Interface

To remove an IPv6 interface from the switch configuration, use the ***no form*** of the ipv6 interface command.

Note: it is only necessary to specify the name of the interface, as shown in the following example,

```
-> no ipv6 interface v6if-v200
```

NOTE

The subnet router "anycast" address is automatically deleted when the last unicast address of the same subnet is removed from the interface.

Configuring IPv6 Assigning IPv6 Addresses

As mentioned before, when an IPv6 interface is created for a VLAN, an IPv6 link-local address is automatically created for that interface. This is also true when a device, such as a workstation, is connected to the switch.

Link-local addresses, although private and non-routable, enable interfaces and workstations to communicate with other interfaces and workstations that are connected to the same link. This simplifies getting devices up and running on the local network. If this level of communication is sufficient, assigning additional addresses is not required.

If it is necessary to identify an interface or device to the entire network, or as a member of a particular group, or enable an interface to perform routing functions, then configuring additional addresses (e.g., global unicast or anycast) is required.

Use the ipv6 address command to manually assign addresses to an existing interface or device, for example, the following command assigns a global unicast address to the VLAN interface v6if-v10

-> ipv6 address 4100:1000::20/64 v6if-v10

In the above example, 4100:1000:: is specified as the subnet prefix and 20 is the interface identifier.

NOTE

That the IPv6 address is expressed using CIDR notation to specify the prefix length. In the above example, /64 indicates a subnet prefix length of 64 bits.

To use the MAC address of an interface or device as the interface ID, specify the eui-64 option with this command.

-> ipv6 address 4100:1000::/64 eui-64 v6if-v10

The above command example creates address…

4100:1000::2d0:95ff:fe12:fab2/64 for interface v6if-v10.

Note the following when configuring IPv6 addresses,

- It is possible to assign more than one address to a single interface.
- Any field of an address may contain all zeros or all ones, the exception to this is the interface identifier portion of the address, which cannot be all zeros. If the eui-64 option is specified with the ipv6 address command, this is not an issue.
- The EUI-64 interface identifier takes up the last 64 bits of the 128-bit IPv6 address. If the subnet prefix combined with the EUI-64 interface ID is longer than 128 bits, an error occurs and the address is not created.

- A subnet router anycast address is automatically created when a global unicast address is assigned to an interface. The anycast address is derived from the global address by adding an interface ID of all zeros to the prefix of the global address. For example, the global address 4100:1000::20/64 generates the anycast address 4100:1000::/64.
- Devices, such as a PC, are eligible for stateless autoconfiguration of unicast addresses in addition to the link-local address. If this type of configuration is in use on the network, manual configuration of addresses is not required.
- IPv6 VLAN interfaces are only eligible for stateless autoconfiguration of their link-local addresses.

Manual configuration of addresses is required for all additional addresses.

Creating an IPv6 Static Route

Static routes are user-defined and carry a higher priority than routes created by dynamic routing protocols.

That is, if two routes have the same metric value, the static route has the higher priority. Static routes allow you to define, or customise, an explicit path to an IPv6 network segment, which is then added to the IPv6 Forwarding table. Static routes can be created between VLANs to enable devices on these VLANs to communicate.

Use the ipv6 static-route command to create a static route, you **must** specify the destination IPv6 address of the route as well as the IPv6 address of the first hop (gateway) used to reach the destination. By way of example to create a static route to IPv6 address 212:95:5::/64 through gateway fe80::2d0:95ff:fe6a:f458 on interface v6if-137, you would enter,

```
-> ipv6 static-route 212:95:5::/64 gateway fe80::2d0:95ff:fe6a:f458 v6if-137
```

NOTE

In above example the IPv6 interface name for the gateway was included, this parameter is required only when a link local address is specified as the gateway.

When you create a static route, the default metric value of 1 is used. However, you can change the priority of the route by increasing its metric value. The lower the metric value, higher the priority. This metric is added to the metric cost of the route. The metric range is 1 to 15, for example,

```
-> ipv6 static-route 212:95:5::/64 gateway fe80::2d0:95ff:fe6a:f458 v6if-137 metric 3
```

Static routes do not age out of the IPv6 Forwarding table; you must delete them from the table, use the ***no ipv6 static-route*** command to do this, you must however specify the destination IPv6 address of the route as well as the IPv6 address of the first hop, for example, to delete a static route to IPv6 address 212:95:5::/64 through gateway fe80::2d0:95ff:fe6a:f458 on interface v6if-137, you would enter:

```
-> no ip static-route 212:95:5::/64 gateway fe80::2d0:95ff:fe6a:f458 v6if-137
```

The IPv6 Forwarding table includes routes learned through RIP as well as any static routes that are configured, use the show ***ipv6 routes*** command to display the IPv6 Forwarding table.

Verifying the IPv6 Configuration

show ipv6 rip

Displays the RIPng status and general configuration parameters.

show ipv6 redist

Displays the route map redistribution configuration.

show ipv6 interface

Displays the status and configuration of IPv6 interfaces.

show ipv6 tunnel

Displays IPv6 configured tunnel information.

show ipv6 routes

Displays the IPv6 Forwarding Table.

show ipv6 route-pref

Displays the configured route preference of a router.

show ipv6 router database

Displays a list of all routes that exist in the IPv6 router database.

show ipv6 prefixes

Displays IPv6 subnet prefixes used in router advertisements.

show ipv6 hosts

Displays the IPv6 Local Host Table.

show ipv6 neighbors

Displays the IPv6 Neighbor Table.

show ipv6 traffic

Displays statistics for IPv6 traffic.

show ipv6 icmp statistics

Displays ICMP6 statistics.

show ipv6 pmtu table

Displays the IPv6 Path MTU Table.

show ipv6 tcp ports

Displays TCP Over IPv6 Connection Table.

show ipv6 udp ports

UDP over IPv6 Listener Table.

7 Switch Management using IPv6

This section describes the ways in which IPv6 can be used as the transport mechanism for accessing the switch, for management purposes.

For non-technical readers, you may wish to skip this chapter.

FTP and SFTP over IPv6 will be discussed later in this section as a means to transfer files to and from the flash on the OmniSwitch along with basic troubleshooting commands that will help resolve connectivity issues within an IPv6 network.

There are four ways in which to configure the OmniSwitch.

- OmniVista
- Webview
- SNMP
- CLI

Currently, the preferred way to implement WebView is in an IPv4 environment.

Webview and full SNMP support for IPv6 will be developed for full native IPv6 networks in future releases.

NOTE

SNMP traps however, can be configured and forwarded to an IPv6 enabled Network Management Station, using IPv6 addresses.

This section will focus on ways in which CLI can be accessed over IPv6.

- Telnet
- Secure Shell (SSH)

NOTE

The assumption is being made that the necessary permissions and configuration have been performed to use the above features, for more information, please see the respective AoS Switch Management User Guide.

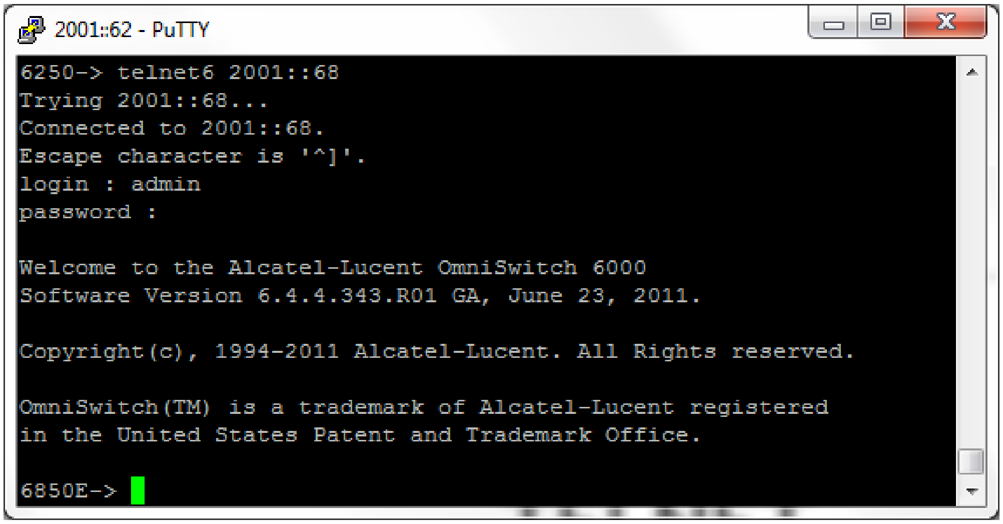
TELNET

A Telnet session is used to connect to a remote system or device.

Both "Telnet Server" and "Telnet Client" for IPv6 are supported using the CLI command "**telnet6**", as shown below.

NOTE

telnet6 has been removed for AoS v7, however, the alternative **telnet** command for AoS v7 works fine with IPv6 addresses.



```
6250-> telnet6 2001::68
Trying 2001::68...
Connected to 2001::68.
Escape character is '^]'.
login : admin
password :

Welcome to the Alcatel-Lucent OmniSwitch 6000
Software Version 6.4.4.343.R01 GA, June 23, 2011.

Copyright(c), 1994-2011 Alcatel-Lucent. All Rights reserved.

OmniSwitch(TM) is a trademark of Alcatel-Lucent registered
in the United States Patent and Trademark Office.

6850E->
```

SSH

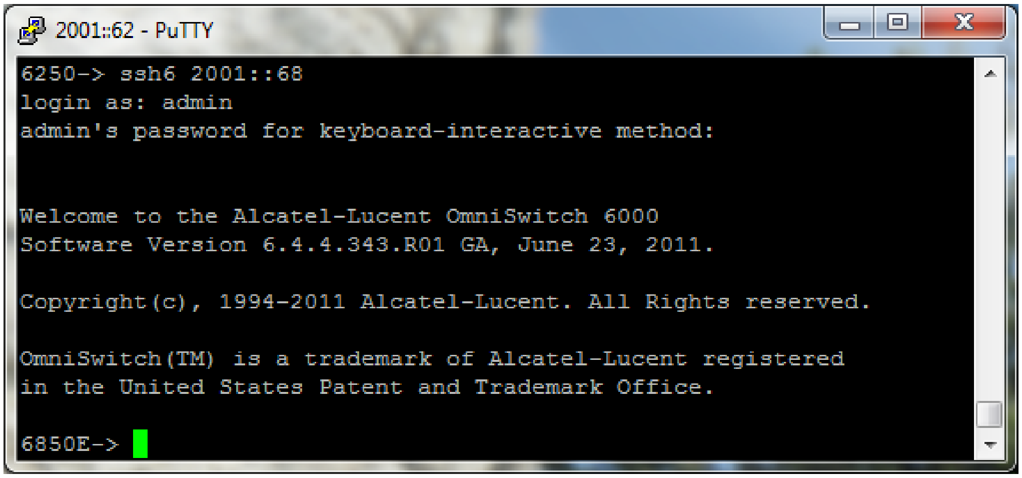
Invokes Secure Shell on the switch.

Secure Shell is used to make a secured connection to a remote system or device.

Both “SSH Server” and “SSH Client” for IPv6 are supported using the CLI command “**ssh6**”, as shown below.

NOTE

ssh6 has been removed for AoS v7, however, the alternative **ssh** command works fine with IPv6 addresses.



```
6250-> ssh6 2001::68
login as: admin
admin's password for keyboard-interactive method:


Welcome to the Alcatel-Lucent OmniSwitch 6000
Software Version 6.4.4.343.R01 GA, June 23, 2011.

Copyright(c), 1994-2011 Alcatel-Lucent. All Rights reserved.

OmniSwitch(TM) is a trademark of Alcatel-Lucent registered
in the United States Patent and Trademark Office.

6850E->
```

FTP and SFTP

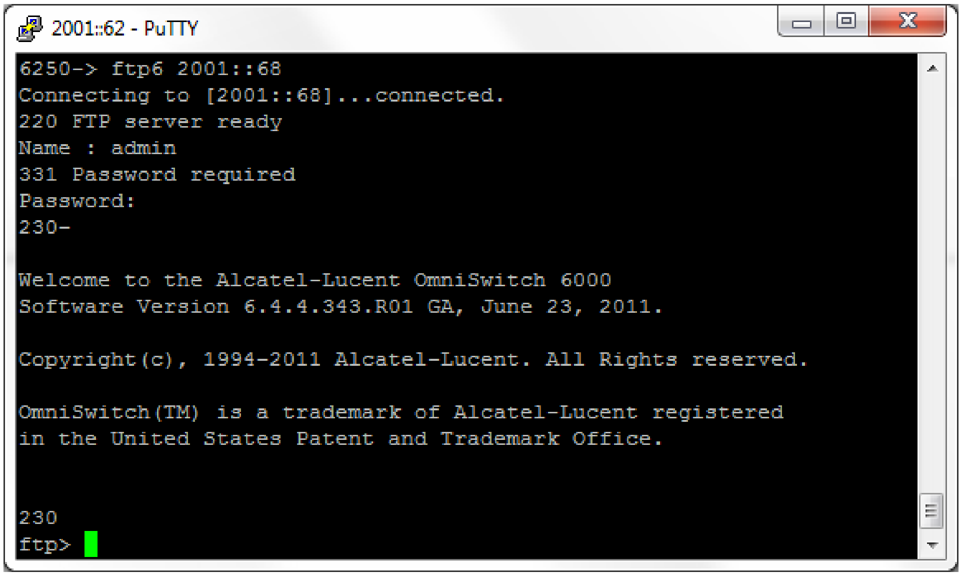
FTP and Secure FTP, “Client and Server” are supported in AoS, with the exception of AoS v7, where FTP client is not supported.

➔ **ftp6**

Starts an FTPv6 session.

NOTE

ftp6 has been removed for AoS v7.



```
6250-> ftp6 2001::68
Connecting to [2001::68]...connected.
220 FTP server ready
Name : admin
331 Password required
Password:
230-

Welcome to the Alcatel-Lucent OmniSwitch 6000
Software Version 6.4.4.343.R01 GA, June 23, 2011.

Copyright(c), 1994-2011 Alcatel-Lucent. All Rights reserved.

OmniSwitch(TM) is a trademark of Alcatel-Lucent registered
in the United States Patent and Trademark Office.


230
ftp>
```

➔ **sftp6**

Starts an SFTPv6 session, providing a secure file transfer method.

NOTE

ftp6 has been removed for AoS v7.

AoS Troubleshooting Commands for IPv6

Three primary AoS commands can be used for troubleshooting are, **ping6**, **traceroute6** and **show ipv6** …

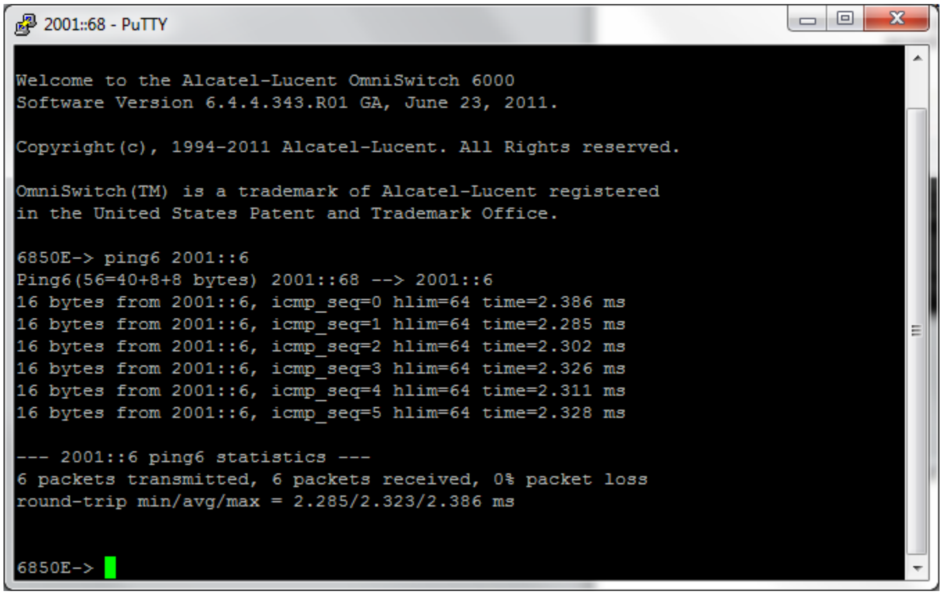
➔ ping6

Tests whether an IPv6 destination can be reached from the local switch.

This command sends an ICMPv6 echo request to a destination and then waits for a reply. To ping a destination, enter the ping6 command and enter either the destination's IPv6 address or hostname.

The switch will ping the destination using the default frame count, packet size, and interval (6 frames, 64 bytes, and 1 second respectively).

See the example below,

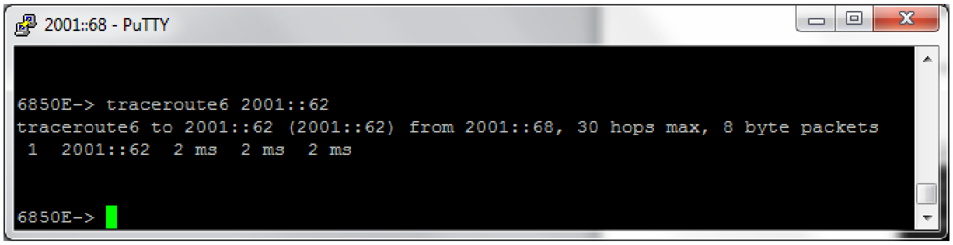


```
Welcome to the Alcatel-Lucent OmniSwitch 6000
Software Version 6.4.4.343.R01 GA, June 23, 2011.

Copyright(c), 1994-2011 Alcatel-Lucent. All Rights reserved.

OmniSwitch(TM) is a trademark of Alcatel-Lucent registered
in the United States Patent and Trademark Office.

6850E-> ping6 2001::6
Ping6(56=40+8+8 bytes) 2001::68 --> 2001::6
16 bytes from 2001::6, icmp_seq=0 hlim=64 time=2.386 ms
16 bytes from 2001::6, icmp_seq=1 hlim=64 time=2.285 ms
16 bytes from 2001::6, icmp_seq=2 hlim=64 time=2.302 ms
16 bytes from 2001::6, icmp_seq=3 hlim=64 time=2.326 ms
16 bytes from 2001::6, icmp_seq=4 hlim=64 time=2.311 ms
16 bytes from 2001::6, icmp_seq=5 hlim=64 time=2.328 ms

--- 2001::6 ping6 statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 2.285/2.323/2.386 ms


6850E->
```

➔ traceroute6

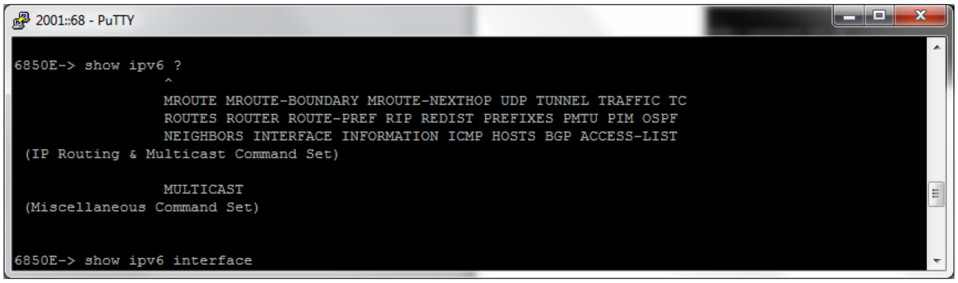
Finds the path taken by an IPv6 packet from the local switch to a specified destination.

This command displays the individual hops to the destination as well as some timing information.



```
6850E-> traceroute6 2001::62
traceroute6 to 2001::62 (2001::62) from 2001::68, 30 hops max, 8 byte packets
 1  2001::62  2 ms  2 ms  2 ms


6850E->
```

➔ show ipv6 …



```
6850E-> show ipv6 ?
                 ^
                 MROUTE MROUTE-BOUNDARY MROUTE-NEXTHOP UDP TUNNEL TRAFFIC TC
                 ROUTES ROUTER ROUTE-PREF RIP REDIST PREFIXES PMTU PIM OSPF
                 NEIGHBORS INTERFACE INFORMATION ICMP HOSTS BGP ACCESS-LIST
 (IP Routing & Multicast Command Set)

                 MULTICAST
 (Miscellaneous Command Set)


6850E-> show ipv6 interface
```

See section 6 of this document or the “OmniSwitch CLI Reference Guide” for a complete list of options for troubleshooting IPv6 configuration.

8 VitalSuite v11 in an IPv6 world

The initial support for IPv6 was added in VitalSuite Release 11.0. VitalSuite now offers support for auto discovery and data collection from IPv6 devices, as well as the flexibility to deploy VitalSuite software itself on dual-stack or IPv6 servers.

This provides network managers with important tools needed to introduce IPv6 into their networks.

IPv6 Autodiscovery and Data Collection

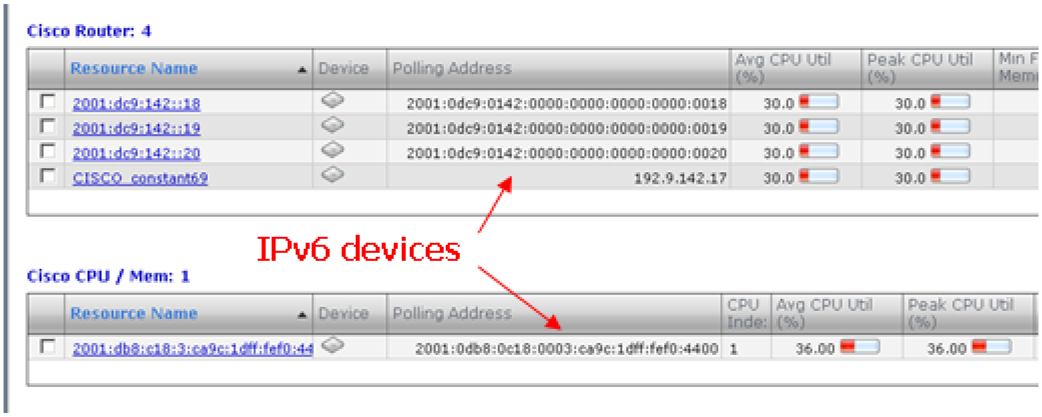
VitalNet can now autodiscover and collect performance data from a wide range of IPv6 devices.

Since it retains the ability to discover and collect from IPv4 devices, VitalSuite can monitor hybrid IPv4 / IPv6 networks when it is deployed on dual stack servers.

GUI

IPv6 addresses are displayed in the VitalSuite GUI as shown below,

Network->Operations Page:



Cisco Router: 4

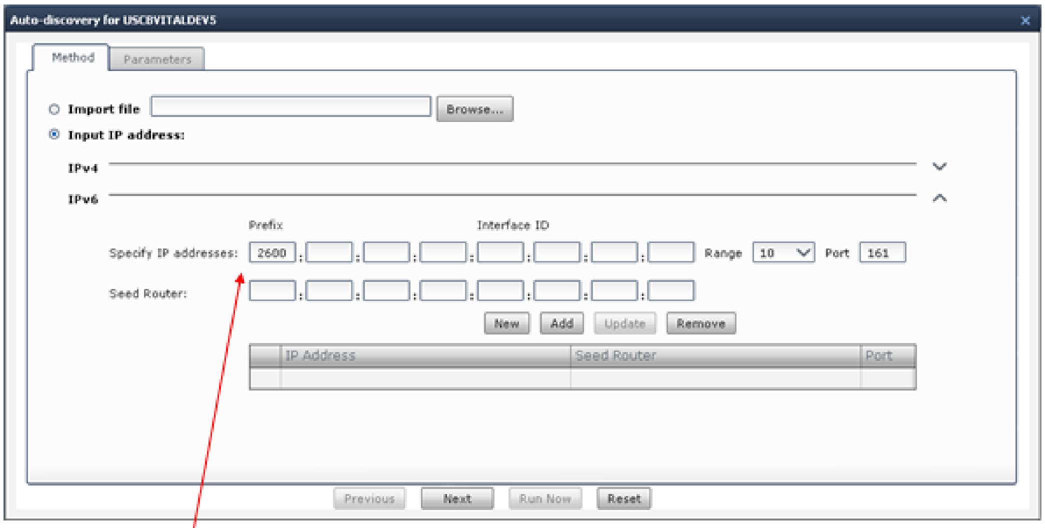
	Resource Name ▲	Device	Polling Address	Avg CPU Util (%)	Peak CPU Util (%)	Min F Mem
☐	2001:dc9:142::18	◇	2001:0dc9:0142:0000:0000:0000:0000:0018	30.0	30.0	
☐	2001:dc9:142::19	◇	2001:0dc9:0142:0000:0000:0000:0000:0019	30.0	30.0	
☐	2001:dc9:142::20	◇	2001:0dc9:0142:0000:0000:0000:0000:0020	30.0	30.0	
☐	CISCO_constant69	◇	192.9.142.17	30.0	30.0	

IPv6 devices

Cisco CPU / Mem: 1

	Resource Name ▲	Device	Polling Address	CPU Inde:	Avg CPU Util (%)	Peak CPU Util (%)
☐	2001:db8:c18:3:ca9c:1dff:fef0:44	◇	2001:0db8:0c18:0003:ca9c:1dff:fef0:4400	1	36.00	36.00

Admin->Network->Discovery Page:



Auto-discovery for USCBVITALDEVS

○ Import file [ ] Browse...

● Input IP address:

IPv4

IPv6

Prefix Interface ID

Specify IP addresses: 2600 : : : : : : : Range 10 Port 161

Seed Router: : : : : : : :

	IP Address	Seed Router	Port

Specify IPv6 Address and
Range

Other VitalSuite Components Supporting IPv6

The following VitalSuite components and features support IPv6:

- VitalNet – Data Collection, discovery, reporting, GUI
- VitalFlow – Flow Data Collection, reporting
- VitalART – ability to specify IPv6 device addresses in reports
- Northbound Traps – Northbound traps can be sent via IPv4 or IPv6 to a Northbound trap receiver

VitalSuite Platform Choices

VitalSuite 11.0 can be deployed on the following server platforms:

- IPv4
- IPv4 / IPv6 dual stack
- IPv6 (Windows Server 2008 minimum requirement).

Limitations that will be corrected in future releases:

The following limitations of VitalSuite 11.0 implementation of IPv6 should be noted:

- Collector types not listed in the annex G sections have not been converted to IPv6, and will only support IPv4 devices.
- VitalApps servers must run on IPv4 devices.
- Customers running both VitalApps and VitalNet in the same VitalSuite deployment should continue to deploy VitalSuite on IPv4 servers.
- VitalApps agents, including Desktop Agents, Mid-Tier Agents, Automon, VoIP Agent, and SIP Agent.
- All Agents must run on IPv4 devices.

9 Vital QIP - IPv6 Features

Vital QIP was an early adopter of IPv6 and the first to implement an IP Address Management (IPAM) solution.

Traditional methods of managing IPv4 addresses with spreadsheets, homegrown applications or simply by memory will not scale when you use IPv6; you simply cannot manage such a vast IPv6 address space in this way.

This makes the need for an IP Address Management solution as important as ever, for a smooth transition and should be included in your plans to adopt IPv6.

In summary, Vital QIP provides the following,

- Manage Stateful IPv6 addresses
- Combined IPv6 Address Allocation and IPv6 Address Management
- Enhance and streamline Nodes (DualStack)
- Provide simple, yet granular, IPv6 permissions
- Adaptable IPv6 solution
- Simple UI for daily operations
- Multi-threaded DHCPv6 Server
- DNS64 support

From the spring of 2012, the 2nd phase of our Vital QIP IPv6 Address Management Solution will be released.

A snapshot of the new features are shown below.

Manage Stateful IPv6 addresses

This will provide clients with either a dynamic or manual IPv6 addresses from the DHCPv6 Server. Support for IPv6 updates in QIP and dynamic DNS updates of IPv6 client addresses.

Combine IPv6 AA and IPv6 Address Management

This removes the need for multiple IPv6 hierarchies, creates intuitive flows and a visual representation.

Enhance and Streamline Nodes

This will create simple and logical grouping of IP addresses (per client/node). It will also allow for the dynamic creation of IPv6 addresses and Nodes based on DHCPv6 updates; creating a highly usable Node hierarchy or "Visual IP".

Provides simple, but granular IPv6 permissions

Extend permissions beyond "on or off".

Adaptable IPv6 solution

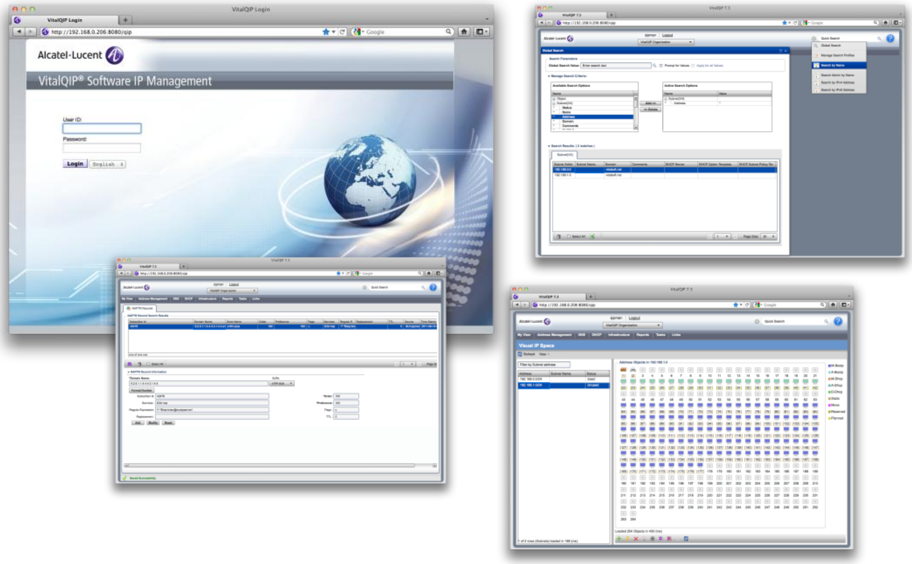
Hierarchy infrastructure supports multiple deployment strategies.

DHCPv6 Server

You can use an 'off the shelf' server to maintain performance; multi-threaded verses single threaded ISC reference implementation, Carrier grade multithreaded performance at enterprise level investment.

You also have the ability to generate configuration files and push to the server, similar to the current IPv4 support, namely, server, subnet, and range configuration with policies and options.

With Vital QIP a single hierarchical interface seamlessly combines the automation of VitalQIP's Address Allocation functionality with the IPv6 Address Management.


VitalQIP Login
http://192.168.0.206:8080/qip
Alcatel·Lucent
VitalQIP® Software IP Management
User ID
Password
Login
English

10 IPv6 and Microsoft Windows

As early as the late 1990's, Microsoft has been developing its IPv6 implementation.

There were problems to overcome, Microsoft needed to add a special domain for IP address resolution due to a conflict between the use of a "colon" for IPv6 address schemes and Microsoft drive letters.

This was resolved in the Microsoft's 'Universal Naming Convention' by replacing the colons in the IPv6 address with hyphens and then appending "ipv6-literal.net".

Although IPv6 was first released in Windows 95 and 98, Windows 2000 was one of the earlier platforms that helped developers work with Microsoft as a means to accelerate IPv6 adoption.

It wasn't until Server 2003 Service Pack 1, Windows XP/Vista and more notably with Server 2008 and Windows 7 that IPv6 became a reality.

NOTE

Windows XP and Windows Server 2003 **do not** support DHCPv6.

Windows Server 2008 and Windows 7 have IPv6 enabled by **default**.

Microsoft's email platform "Exchange Server 2007/2010" relies solely on IPv6 for its internal services.

Windows DOS Commands for IPv6

At the Windows Command Prompt, you will find some basic commands that will assist with you IPv6 connectivity and troubleshooting.

➔ **ping -6**

Using the existing ping command with the "-6" option allows you test the reachability of a host on the network.

➔ **tracert**

Trace Route, when using an IPv6 address, traces the network path to a specific destination.

➔ **telnet**

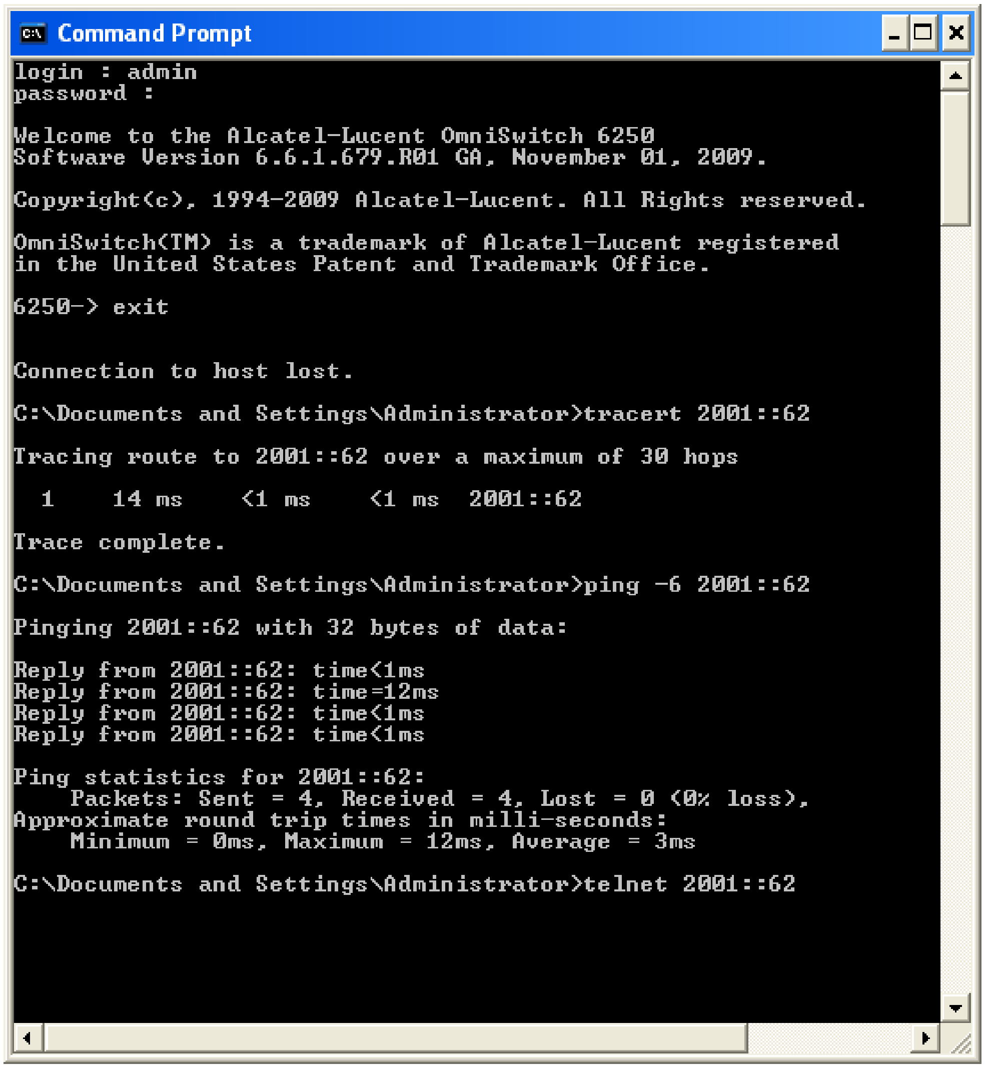
Telnet client using an IPv6 address allows you to connect to an IPv6 Telnet Server.

NOTE

Telnet is not loaded by default in Windows 7.

For in depth configuration and troubleshooting, "netsh" can still be used for advanced Microsoft Windows users.

The diagram below shows, **tracert**, **ping** and **telnet** being used at the Command Prompt.



```
login : admin
password :

Welcome to the Alcatel-Lucent OmniSwitch 6250
Software Version 6.6.1.679.R01 GA, November 01, 2009.

Copyright(c), 1994-2009 Alcatel-Lucent. All Rights reserved.

OmniSwitch(TM) is a trademark of Alcatel-Lucent registered
in the United States Patent and Trademark Office.

6250-> exit


Connection to host lost.

C:\Documents and Settings\Administrator>tracert 2001::62

Tracing route to 2001::62 over a maximum of 30 hops

  1    14 ms    <1 ms    <1 ms  2001::62

Trace complete.

C:\Documents and Settings\Administrator>ping -6 2001::62

Pinging 2001::62 with 32 bytes of data:

Reply from 2001::62: time<1ms
Reply from 2001::62: time=12ms
Reply from 2001::62: time<1ms
Reply from 2001::62: time<1ms

Ping statistics for 2001::62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 3ms

C:\Documents and Settings\Administrator>telnet 2001::62
```

➔ **ipconfig**

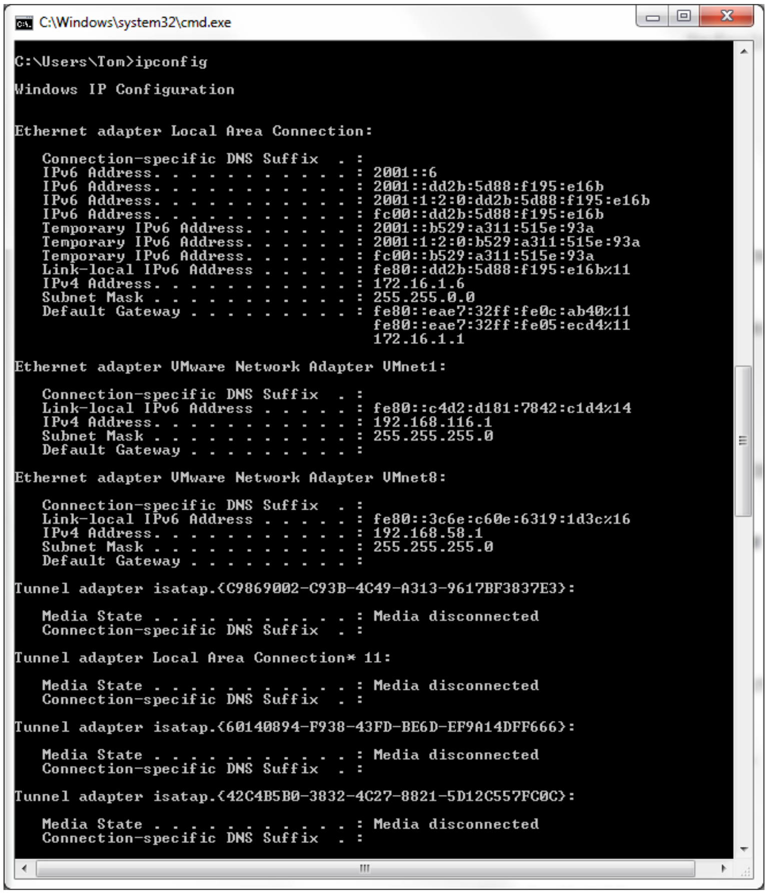
This command is the same as **winipcfg** used in earlier versions of Windows.

This command allows you to view the IP information for your computer, the **/all** option shows extended information for each IP interface.

The example shown below is for the basic **ipconfig** command.

NOTE

Notice the number of IPv6 addresses configured on a Windows 7 PC with a single physical LAN adapter installed.



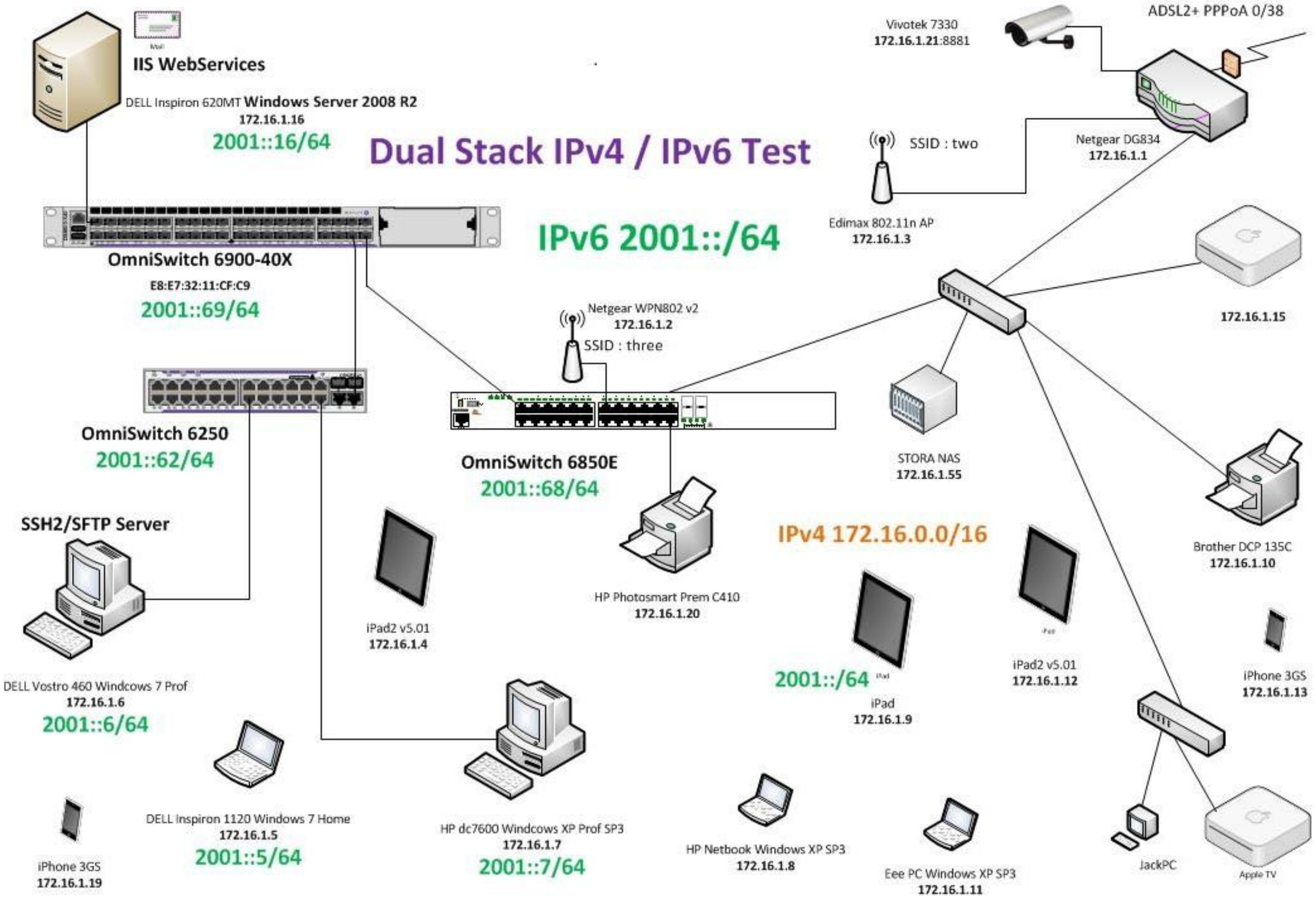
```
C:\Users\Tom>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001::6
   IPv6 Address. . . . . . . . . . . : 2001::dd2b:5d88:f195:e16b
   IPv6 Address. . . . . . . . . . . : 2001:1:2:0:dd2b:5d88:f195:e16b
   IPv6 Address. . . . . . . . . . . : fc00::dd2b:5d88:f195:e16b
   Temporary IPv6 Address. . . . . . : 2001::b529:a311:515e:93a
   Temporary IPv6 Address. . . . . . : 2001:1:2:0:b529:a311:515e:93a
   Temporary IPv6 Address. . . . . . : fc00::b529:a311:515e:93a
   Link-local IPv6 Address . . . . . : fe80::dd2b:5d88:f195:e16b%11
   IPv4 Address. . . . . . . . . . . : 172.16.1.6
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::eae7:32ff:fe0c:ab40%11
                                       fe80::eae7:32ff:fe05:ecd4%11
                                       172.16.1.1

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c4d2:d181:7842:c1d4%14
   IPv4 Address. . . . . . . . . . . : 192.168.116.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3c6e:c60e:6319:1d3c%16
   IPv4 Address. . . . . . . . . . . : 192.168.58.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{C9869002-C93B-4C49-A313-9617BF3837E3}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{60140894-F938-43FD-BE6D-EF9A14DFF666}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{42C4B5B0-3832-4C27-8821-5D12C557FC0C}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

11 IPv6 Dual Stack Scenario

The following page shows a diagram of a test scenario to demonstrate basic IPv6 services and traffic.

The pages in this section will discuss some configuration tips when using the hardware and software components in this lab.

- Building the Infrastructure
- Windows Server 2008 R2 Build 7601
- SMTP Mail Server for Microsoft Server 2008
- IIS WebServices
- Applications
- Printers
- File Sharing
- Microsoft Windows XP Client SP3
- Microsoft Windows 7 Client Service Pack 1
- Apple iPad and iPhone
- Android Devices
- Linux
- Tunnel Broker


IIS WebServices
Mail
DELL Inspiron 620MT Windows Server 2008 R2
172.16.1.16
2001::16/64
Dual Stack IPv4 / IPv6 Test
IPv6 2001::/64
OmniSwitch 6900-40X
E8:E7:32:11:CF:C9
2001::69/64
OmniSwitch 6250
2001::62/64
SSH2/SFTP Server
DELL Vostro 460 Windcows 7 Prof
172.16.1.6
2001::6/64
iPhone 3GS
172.16.1.19
DELL Inspiron 1120 Windows 7 Home
172.16.1.5
2001::5/64
iPad2 v5.01
172.16.1.4
HP dc7600 Windcows XP Prof SP3
172.16.1.7
2001::7/64
Netgear WPN802 v2
172.16.1.2
SSID : three
OmniSwitch 6850E
2001::68/64
HP Photosmart Prem C410
172.16.1.20
HP Netbook Windows XP SP3
172.16.1.8
IPv4 172.16.0.0/16
2001::/64
iPad
172.16.1.9
Eee PC Windows XP SP3
172.16.1.11
iPad2 v5.01
172.16.1.12
Vivotek 7330
172.16.1.21:8881
SSID : two
Edimax 802.11n AP
172.16.1.3
ADSL2+ PPPoA 0/38
Netgear DG834
172.16.1.1
172.16.1.15
STORA NAS
172.16.1.55
Brother DCP 135C
172.16.1.10
iPhone 3GS
172.16.1.13
JackPC
Apple TV

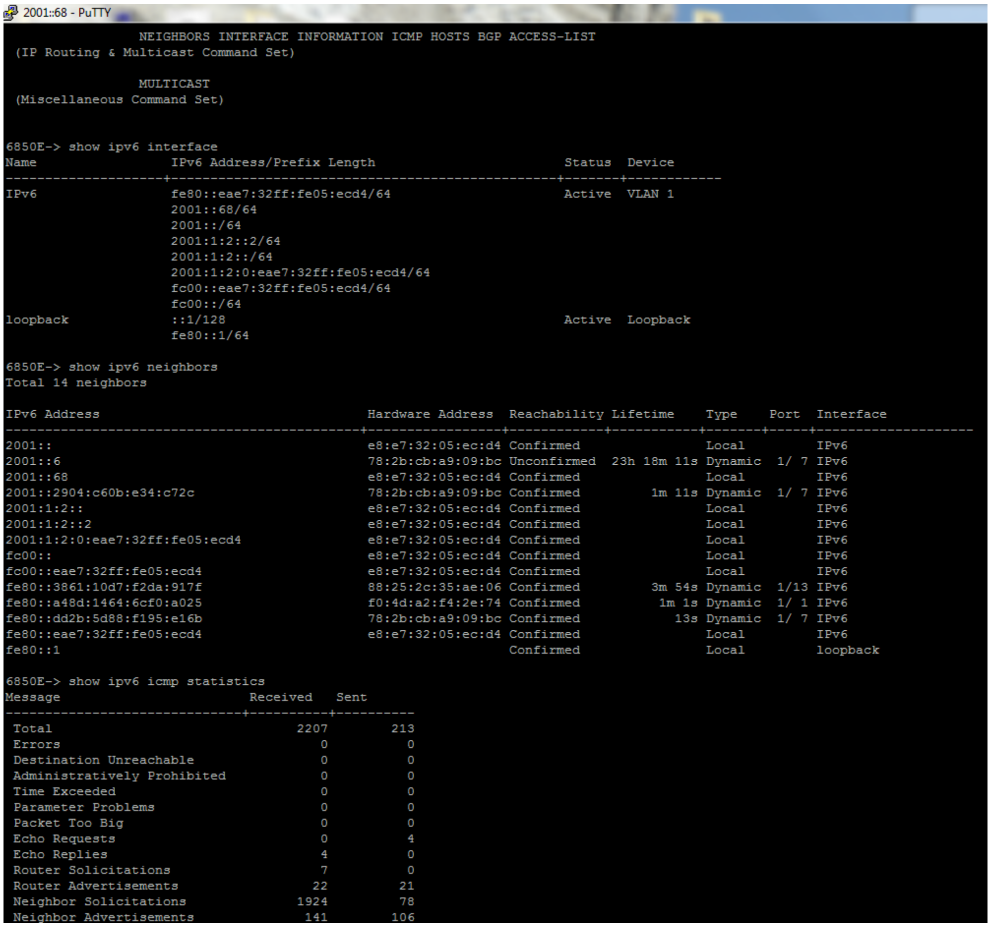
Building the Infrastructure

The OmniSwitch 6900, 6850E and 6250 switches were configured solely with the information contained in Section 6 “Basic AoS IPv6 Configuration” of this document.

For advanced IPv6 configuration, please refer to the “AoS Network Configuration Guide”

The screen capture below shows the results of entering the,

- show ipv6 interface
- show ipv6 neighbors
- show ipv6 icmp statistics



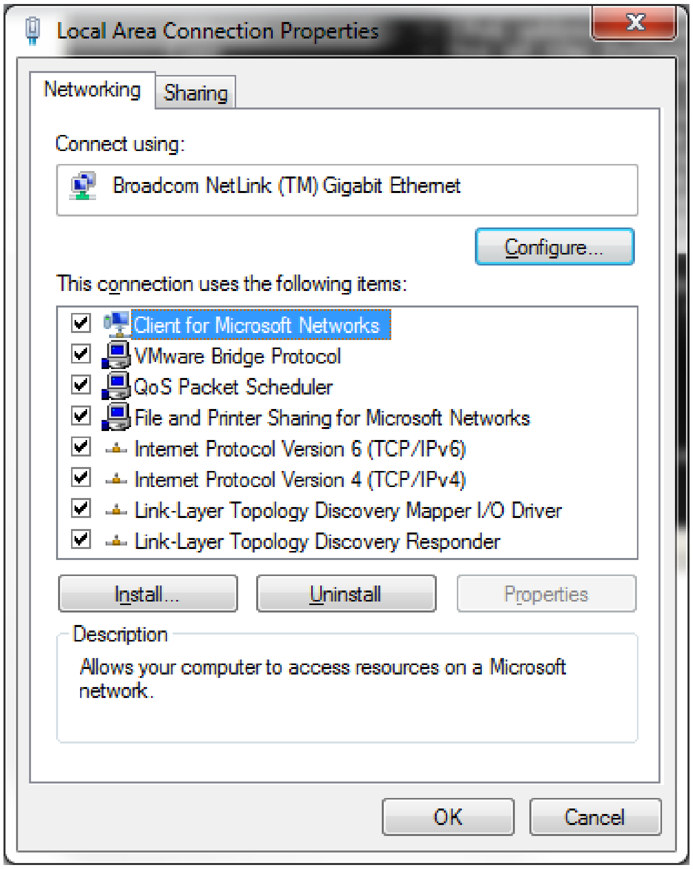
```
                 NEIGHBORS INTERFACE INFORMATION ICMP HOSTS BGP ACCESS-LIST
 (IP Routing & Multicast Command Set)

                 MULTICAST
 (Miscellaneous Command Set)


6850E-> show ipv6 interface
Name                 IPv6 Address/Prefix Length                         Status  Device
--------------------+-------------------------------------------------+-------+------------
IPv6                 fe80::eae7:32ff:fe05:ecd4/64                       Active  VLAN 1
                     2001::68/64
                     2001::/64
                     2001:1:2::2/64
                     2001:1:2::/64
                     2001:1:2:0:eae7:32ff:fe05:ecd4/64
                     fc00::eae7:32ff:fe05:ecd4/64
                     fc00::/64
loopback             ::1/128                                            Active  Loopback
                     fe80::1/64

6850E-> show ipv6 neighbors
Total 14 neighbors

IPv6 Address                                  Hardware Address  Reachability Lifetime    Type    Port  Interface
---------------------------------------------+-----------------+------------+-----------+-------+-----+--------------------
2001::                                        e8:e7:32:05:ec:d4 Confirmed                Local         IPv6
2001::6                                       78:2b:cb:a9:09:bc Unconfirmed  23h 18m 11s Dynamic  1/ 7 IPv6
2001::68                                      e8:e7:32:05:ec:d4 Confirmed                Local         IPv6
2001::2904:c60b:e34:c72c                      78:2b:cb:a9:09:bc Confirmed         1m 11s Dynamic  1/ 7 IPv6
2001:1:2::                                    e8:e7:32:05:ec:d4 Confirmed                Local         IPv6
2001:1:2::2                                   e8:e7:32:05:ec:d4 Confirmed                Local         IPv6
2001:1:2:0:eae7:32ff:fe05:ecd4                e8:e7:32:05:ec:d4 Confirmed                Local         IPv6
fc00::                                        e8:e7:32:05:ec:d4 Confirmed                Local         IPv6
fc00::eae7:32ff:fe05:ecd4                     e8:e7:32:05:ec:d4 Confirmed                Local         IPv6
fe80::3861:10d7:f2da:917f                     88:25:2c:35:ae:06 Confirmed         3m 54s Dynamic  1/13 IPv6
fe80::a48d:1464:6cf0:a025                     f0:4d:a2:f4:2e:74 Confirmed          1m 1s Dynamic  1/ 1 IPv6
fe80::dd2b:5d88:f195:e16b                     78:2b:cb:a9:09:bc Confirmed            13s Dynamic  1/ 7 IPv6
fe80::eae7:32ff:fe05:ecd4                     e8:e7:32:05:ec:d4 Confirmed                Local         IPv6
fe80::1                                                         Confirmed                Local         loopback

6850E-> show ipv6 icmp statistics
Message                        Received   Sent
------------------------------+----------+----------
 Total                               2207        213
 Errors                                 0          0
 Destination Unreachable                0          0
 Administratively Prohibited            0          0
 Time Exceeded                          0          0
 Parameter Problems                     0          0
 Packet Too Big                         0          0
 Echo Requests                          0          4
 Echo Replies                           4          0
 Router Solicitations                   7          0
 Router Advertisements                 22         21
 Neighbor Solicitations              1924         78
 Neighbor Advertisements              141        106
```

Windows Server 2008R2 Build 7601

Building a Windows Server 2008 R2 is no different with IPv6, in fact, it is enabled by **default**.

Some of the improvement for IPv6 support are, automatic default installation, dual IP architecture, full IPSec support, DHCPv6, a GUI interface for configuration and the random use of interface IDs for mobile security.

If you wish to configure a specific IPv6 address, use the “Local Area Connection Properties” which can be found in “Control Panel”, and “Properties” under “Change Adapter Settings”, see figure below.



Connect using:

Broadcom NetLink (TM) Gigabit Ethernet

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ VMware Bridge Protocol
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Allows your computer to access resources on a Microsoft network.

Select “Internet Protocol Version 6 (TCP/IPv6)” and click “Properties”, a new window appears allowing you to configure the IPv6 address, default gateway… as shown below.

SMTP Mail Server - hMail Server

Interestingly, a 3rd party SMTP server was required for this scenario because the SMTP embedded in Windows 2008 R2 server doesn't support IPv6.

Development for IPv6 was focused in Microsoft's Exchange Server. Interestingly, it is used in its core which means you cannot disable IPv6, otherwise the Exchange Server will not work.

hMailServer is a free mail server used by internet providers, government, schools, companies and individuals all around the world.

It supports the standard SMTP, POP3, IMAP for both IPv4 and IPv6, it also includes spam/virus interconnectivity.

The software can be downloaded at www.hmailserver.com/

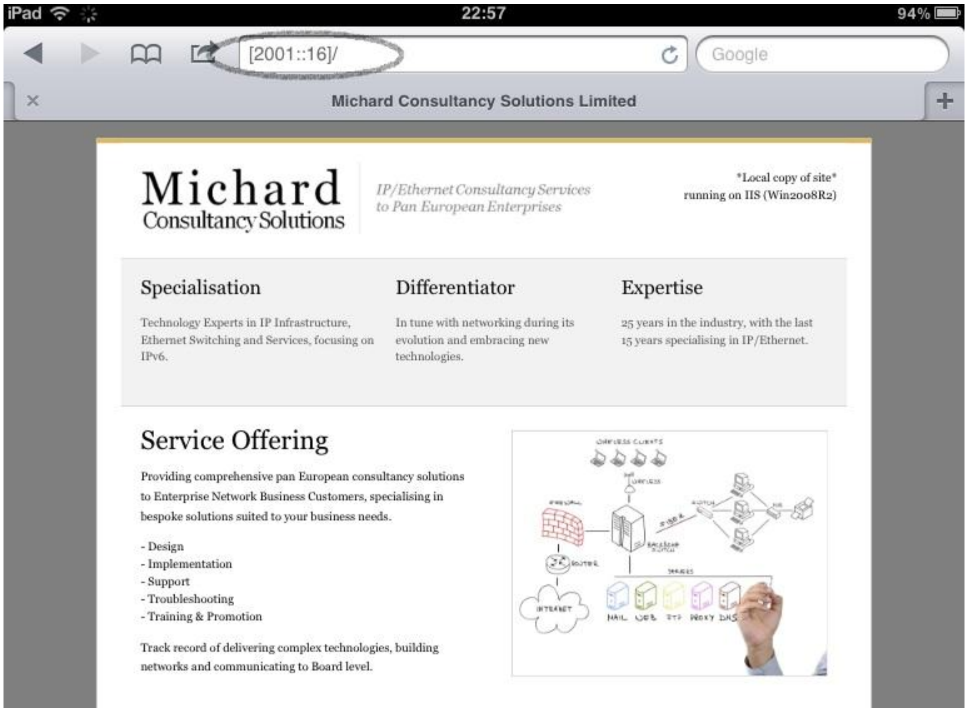
IIS WebServer

Configuring the IIS server is relatively straightforward; no additional configuration is needed for IPv6.

The sample content stored on the webserver (c:\inetpub\wwwroot) in this working scenario could be viewed with the following clients,

- Windows XP SP3 client using Explorer v7
- Windows 7 SP1 with Explorer v9
- Apple iPad
- Apple iPad2
- Apple iPhone 3GS

A screen shot of this working on an Apple iPad, is shown over the page,



Michard Consultancy Solutions

IP/Ethernet Consultancy Services to Pan European Enterprises

Local copy of site running on IIS (Win2008R2)

Specialisation

Technology Experts in IP Infrastructure, Ethernet Switching and Services, focusing on IPv6.

Differentiator

In tune with networking during its evolution and embracing new technologies.

Expertise

25 years in the industry, with the last 15 years specialising in IP/Ethernet.

Service Offering

Providing comprehensive pan European consultancy solutions to Enterprise Network Business Customers, specialising in bespoke solutions suited to your business needs.

- Design
- Implementation
- Support
- Troubleshooting
- Training & Promotion

Track record of delivering complex technologies, building networks and communicating to Board level.

NOTE

In the absence of DNS, an IPv6 address can be entered at the URL line as show above, unlike IPv4 however, IPv6 addresses for web browsers must be encapsulated in “open and close square brackets”; see RFC 2732 for reference.

Applications

This is a difficult area as there are so many variables when it comes to choosing the right application for your business and making sure they are compatible with your current software platforms, along with their ability to support IPv6.

As seen in this section, there will always be exceptions, especially as software vendor's "phase in" IPv6 support.

For example, in this scenario, it was discovered that the SMTP server included in Server 2008 R2 does not support IPv6, instead Microsoft decided to focus on Exchange Server for future IPv6 development instead.

Some applications include IP addresses within their IP payload; this can have serious implications in an IPv6 environment.

It is important that any future applications procured are IPv6 compliant.

Take time to research and validate your purchases to ensure it will scale to IPv6.

The following URL is a good place to start,

http://en.wikipedia.org/wiki/Comparison_of_IPv6_application_support

Printers

With the exception of corporate printers (notably HP), small business and home printer applications, predominantly use IPv4.

Printer vendors have been slow to adopt IPv6 support for small office home office (SOHO) and small to medium sized businesses (SMB); this will change as the focus on IPv6 accelerates.

This is not an issue today because IPv6 dual stack client configurations will handle IPv6 and IPv4 for printing solutions.

File Sharing

Is supported with IPv6, but as discussed earlier in this document, there were problems to overcome.

To resolve the issue, namely, a conflict between the use of a “colon” for IPv6 address schemes and drive letters, Microsoft needed to add a special domain for IP address resolution.

ipv6-literal.net

This was resolved in the Microsoft’s ‘Universal Naming Convention’ by replacing the colons in the IPv6 address with hyphens and then appending “ipv6-literal.net”, an example is shown below,

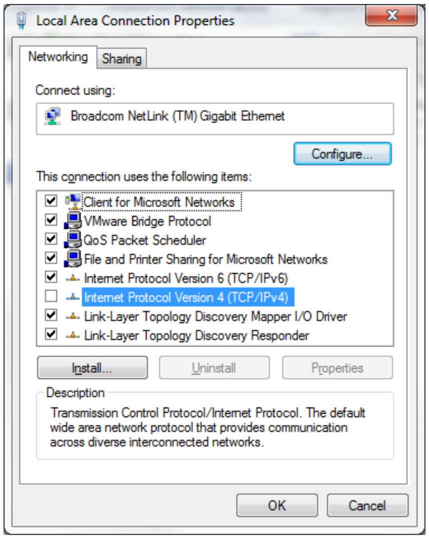
\\2001-0000-0000-0000-0000-0000-0000-0016.ipv6-literal.net.

Demonstrating “File Sharing” with IPv6 on Windows 7

Following the steps below you will see how you can successfully navigate the directory structure on the wireless Dell Windows 7 laptop (2001::5) from a native IPv6 Dell Windows 7 desktop PC (2001::6).

The graphics shown demonstrate this working scenario.

1. IPv4 was disabled on the Dell Vostro desktop (172.16.1.6)



Local Area Connection Properties

Networking | Sharing

Connect using:

Broadcom NetLink (TM) Gigabit Ethernet

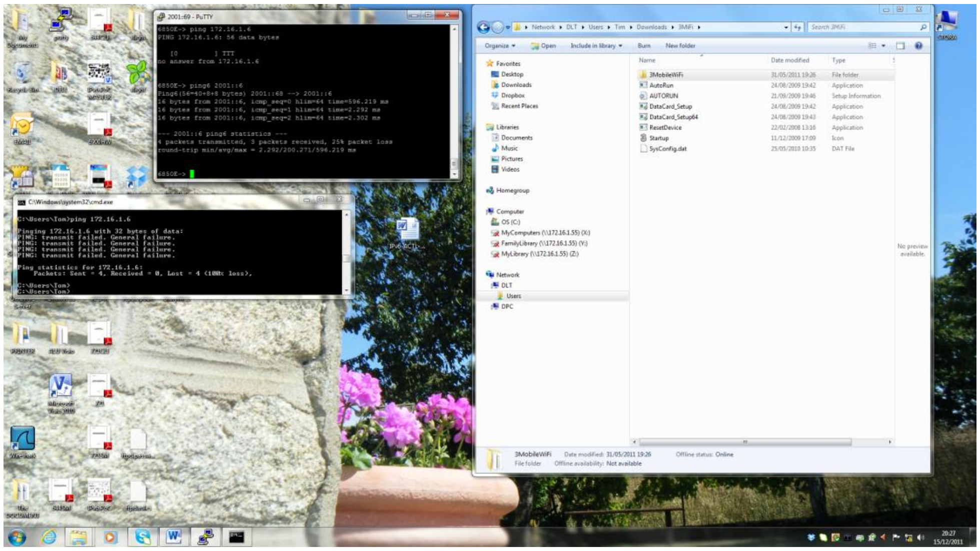
This connection uses the following items:

☑ Client for Microsoft Networks
☑ VMware Bridge Protocol
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☐ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

2. A Ping was sent 172.16.1.6 to confirm IPv4 had been disabled.
3. A Ping was sent to 2001::6 to confirm IPv6 was still active.
4. Exploring the network discovered the wireless Dell Laptop and once the user credentials were entered, the directory structure could be navigated, as seen in the screen capture below.



2001::69 - PuTTY

```
6850E-> ping 172.16.1.6
PING 172.16.1.6: 56 data bytes

   [0         ] TTT
no answer from 172.16.1.6


6850E-> ping6 2001::6
Ping6(56=40+8+8 bytes) 2001::68 --> 2001::6
16 bytes from 2001::6, icmp_seq=0 hlim=64 time=596.219 ms
16 bytes from 2001::6, icmp_seq=1 hlim=64 time=2.292 ms
16 bytes from 2001::6, icmp_seq=2 hlim=64 time=2.302 ms

--- 2001::6 ping6 statistics ---
4 packets transmitted, 3 packets received, 25% packet loss
round-trip min/avg/max = 2.292/200.271/596.219 ms


6850E->
```

C:\Windows\system32\cmd.exe

```
C:\Users\Tom>ping 172.16.1.6

Pinging 172.16.1.6 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 172.16.1.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Tom>
C:\Users\Tom>
```

Network ▸ DLT ▸ Users ▸ Tim ▸ Downloads ▸ 3MiFi ▸

Name	Date modified	Type
3MobileWiFi	31/05/2011 19:26	File folder
AutoRun	24/08/2009 19:42	Application
AUTORUN	21/09/2009 19:46	Setup Information
DataCard_Setup	24/08/2009 19:42	Application
DataCard_Setup64	24/08/2009 19:43	Application
ResetDevice	22/02/2008 13:16	Application
Startup	11/12/2009 17:09	Icon
SysConfig.dat	25/05/2010 10:35	DAT File

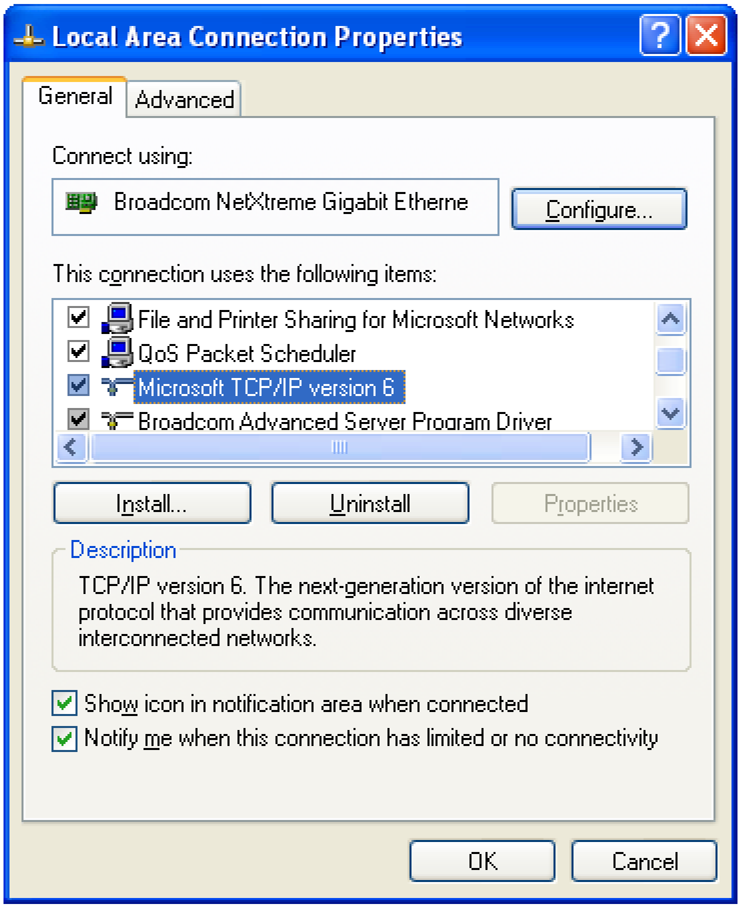
3MobileWiFi Date modified: 31/05/2011 19:26 Offline status: Online
File folder Offline availability: Not available

Microsoft Windows XP Client SP3

IPv6 for Windows XP is not enabled by default, neither is DHCPv6 supported.

To enable IPv6, use “Local Area Connection Properties” to add “Protocol” IPv6, as shown below.

You will notice that you cannot add any specific properties to this entry, normally in an IPv4 environment the tab will allow you to configure parameters such as IP address, Default Gateway and DNS.



Connect using:

Broadcom NetXtreme Gigabit Etherne

This connection uses the following items:

- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Microsoft TCP/IP version 6
- ☑ Broadcom Advanced Server Program Driver

Description

TCP/IP version 6. The next-generation version of the internet protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

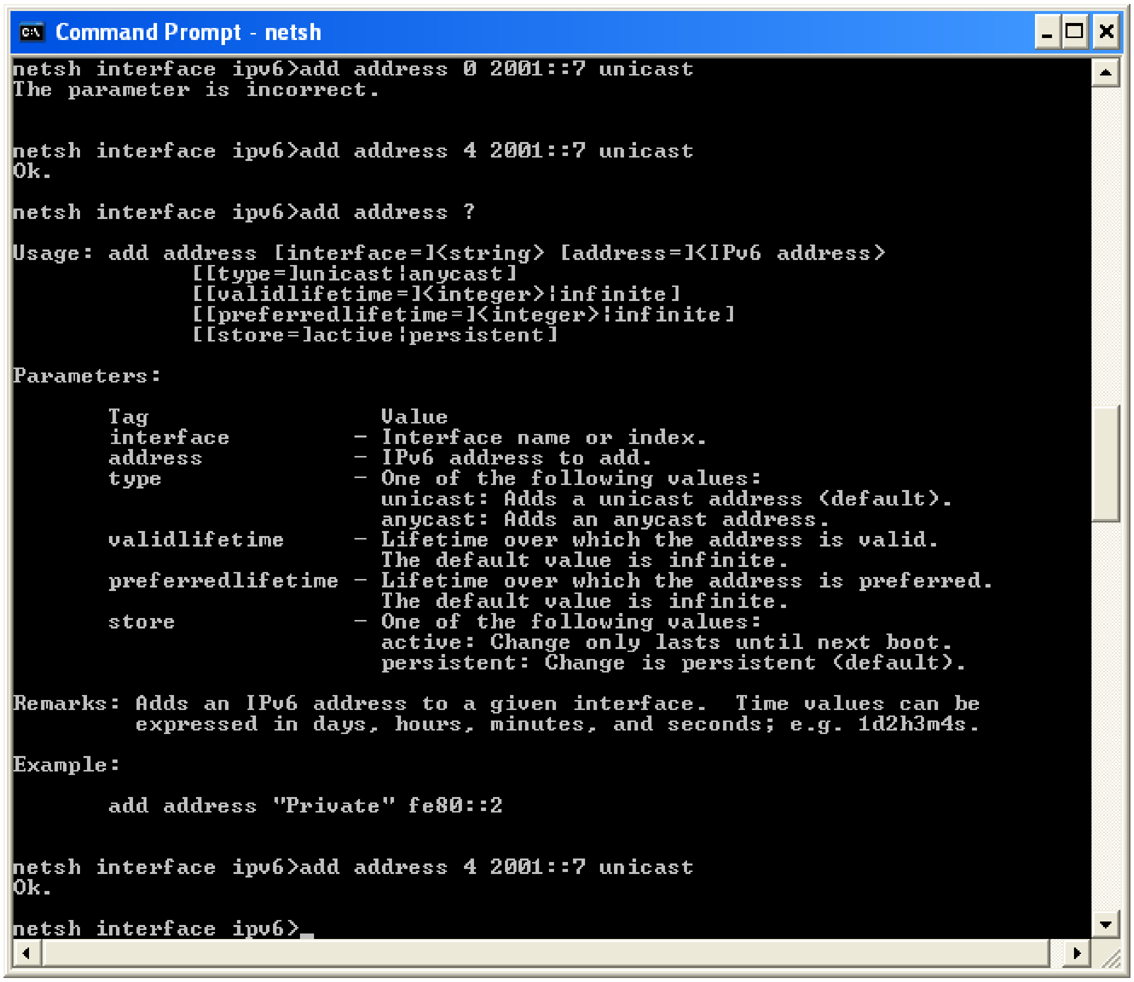
☑ Notify me when this connection has limited or no connectivity

To configure additional IPv6 parameters this must be done using “netsh” in the DOS command window.

To do, launch “Command Prompt” from the start menu or run “cmd”.

Once the DOS window appears, enter the "netsh" command and configure IPv6 parameters at "interface ¦ ipv6", as shown below.

To add an IPv6 address, use the "add address" command.



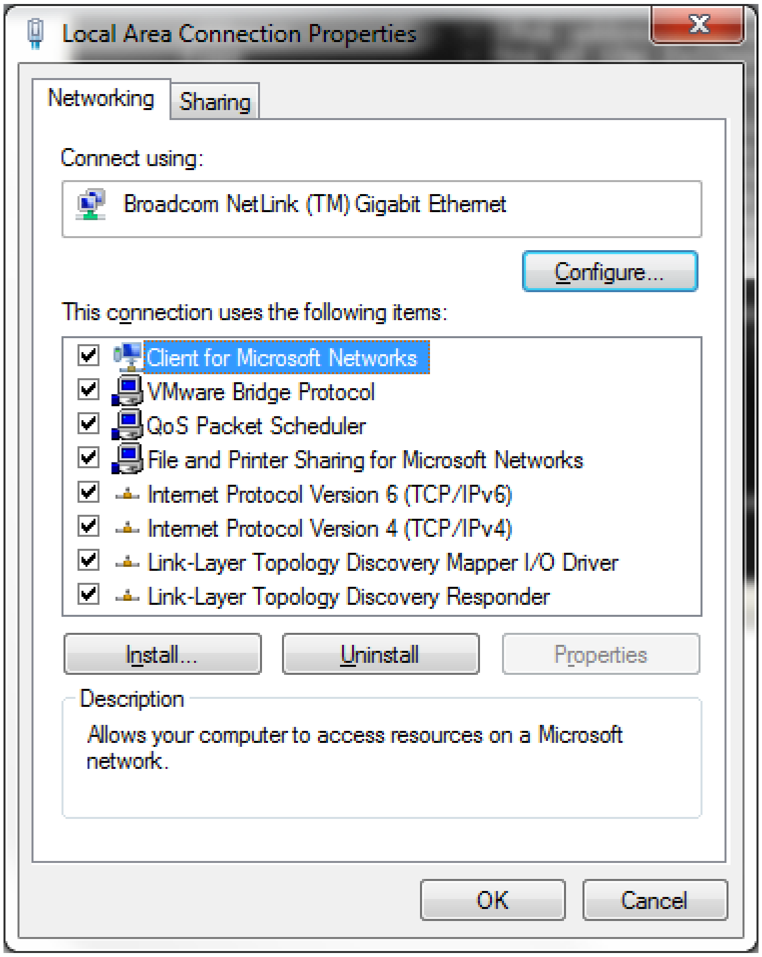
```
netsh interface ipv6>add address 0 2001::7 unicast
The parameter is incorrect.


netsh interface ipv6>add address 4 2001::7 unicast
Ok.

netsh interface ipv6>add address ?

Usage: add address [interface=]<string> [address=]<IPv6 address>
             [[type=]unicast|anycast]
             [[validlifetime=]<integer>|infinite]
             [[preferredlifetime=]<integer>|infinite]
             [[store=]active|persistent]

Parameters:

       Tag                  Value
       interface          - Interface name or index.
       address            - IPv6 address to add.
       type               - One of the following values:
                            unicast: Adds a unicast address (default).
                            anycast: Adds an anycast address.
       validlifetime      - Lifetime over which the address is valid.
                            The default value is infinite.
       preferredlifetime - Lifetime over which the address is preferred.
                            The default value is infinite.
       store              - One of the following values:
                            active: Change only lasts until next boot.
                            persistent: Change is persistent (default).

Remarks: Adds an IPv6 address to a given interface.  Time values can be
         expressed in days, hours, minutes, and seconds; e.g. 1d2h3m4s.

Example:

       add address "Private" fe80::2


netsh interface ipv6>add address 4 2001::7 unicast
Ok.

netsh interface ipv6>_
```

Using "netsh" is a little clumsy. Newer versions of Windows however, greatly simplify this configuration; you will notice this when using Windows 7.

Microsoft Windows 7 Client Service Pack 1

Windows 7 significantly improves the way IPv6 is configured, in fact, it is enabled by **default** and it could be said that this is by far the best IPv6 implementation in a Windows platform so far.

Adding IPv6 is configured the same way as Windows XP in the “Local Area Connection Properties”, see figure below.



Connect using:

Broadcom NetLink (TM) Gigabit Ethernet

This connection uses the following items:

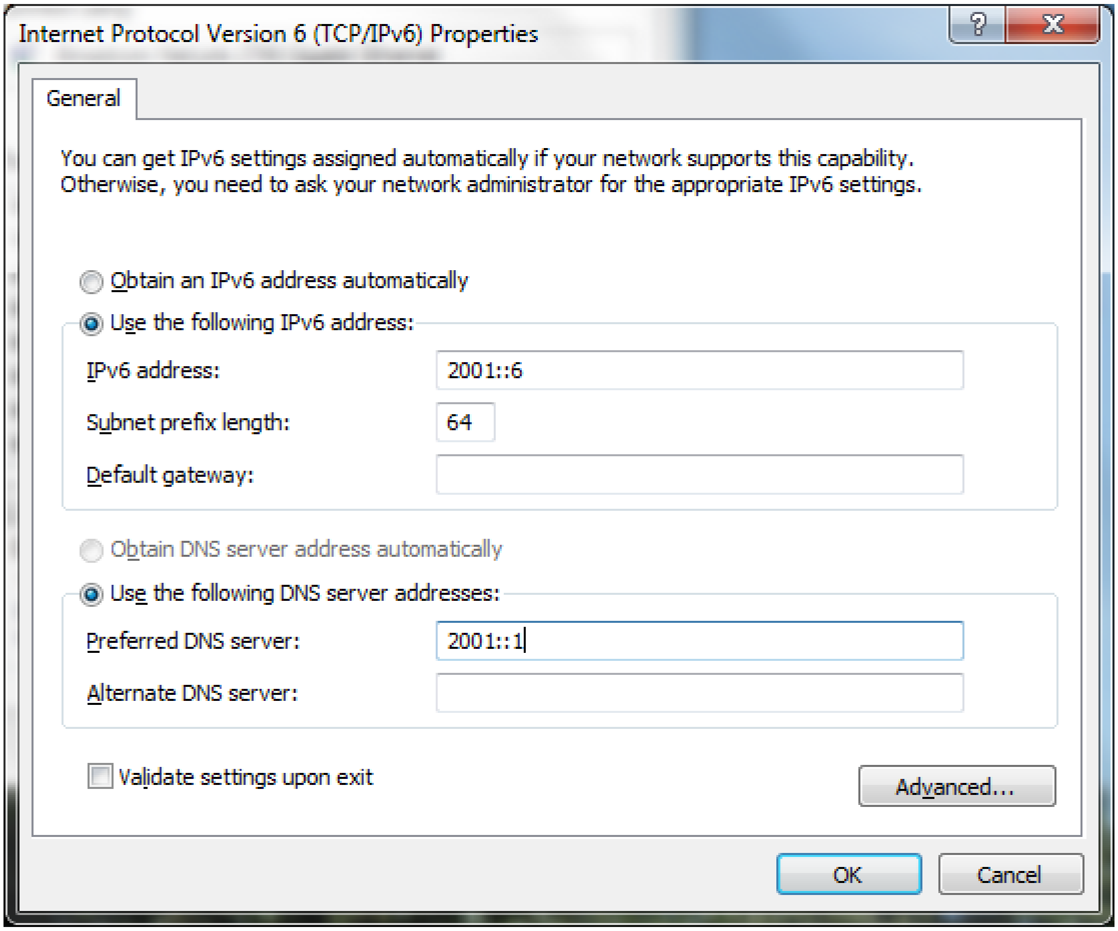
- ☑ Client for Microsoft Networks
- ☑ VMware Bridge Protocol
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Allows your computer to access resources on a Microsoft network.

Now select “Internet Protocol Version 6 (TCP/IPv6)” and click “Properties”, a new window appears allowing you to configure the IPv6 address, default gateway etc, this is shown on the below.

This is a major improvement over Windows XP, in that, “netsh” is no longer needed to configure IPv6 specific properties.



Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

○ Obtain an IPv6 address automatically

● Use the following IPv6 address:

IPv6 address: 2001::6

Subnet prefix length: 64

Default gateway:

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 2001::1

Alternate DNS server:

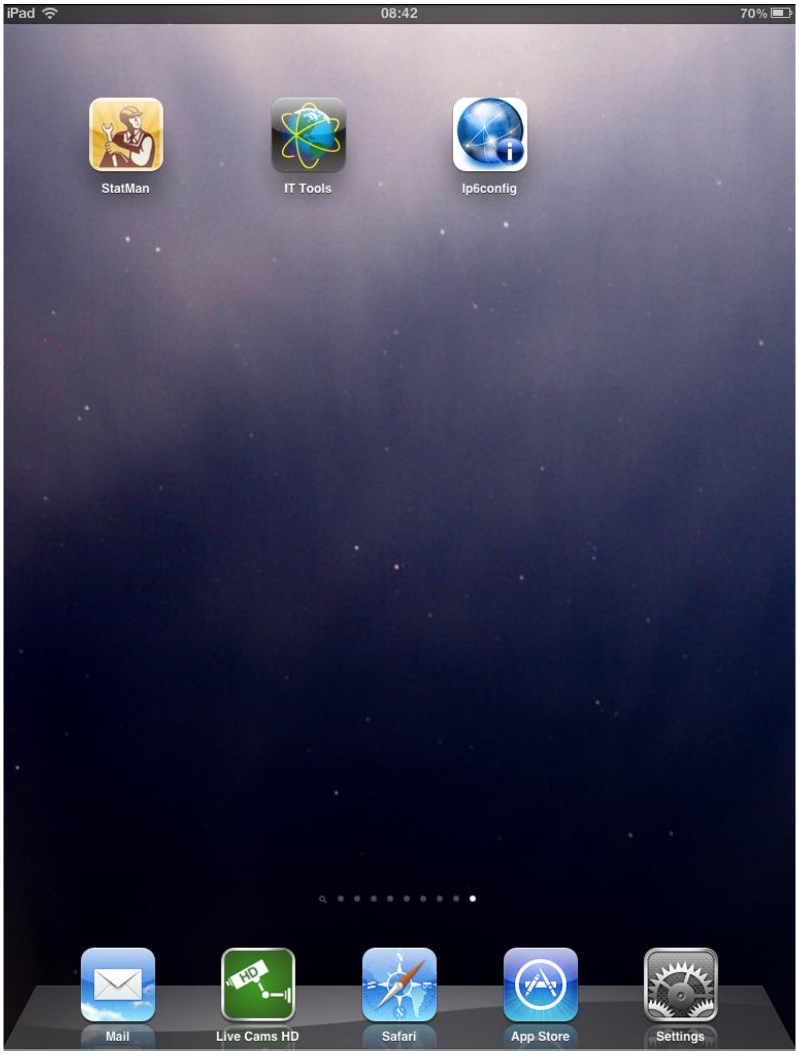
□ Validate settings upon exit

Apple iPad and iPhone

Apple has enabled IPv6 by default for the iTouch, iPhone's and the iPad.

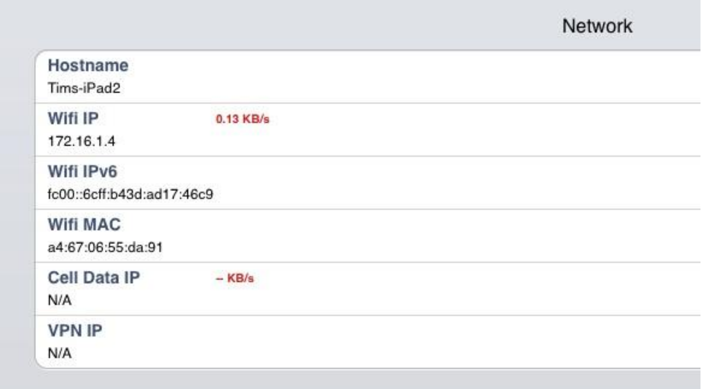
Unfortunately, IPv6 properties cannot be viewed in iOS (v5.0.1).

Unlike IPv4, the address, subnet mask, default router etc, can be viewed in "settings", for IPv6, the only way to view these is by purchasing an "App" from Apple's "App Store"; you can see below three Apps that will show you IPv6 properties.



For the majority of iPhone and iPad users they are unaware that IPv6 is enabled and will participate in an IPv6 world.

Below is a snapshot of the IPv6 address for the iPad.



Hostname
Tims-iPad2

Wifi IP 0.13 KB/s
172.16.1.4

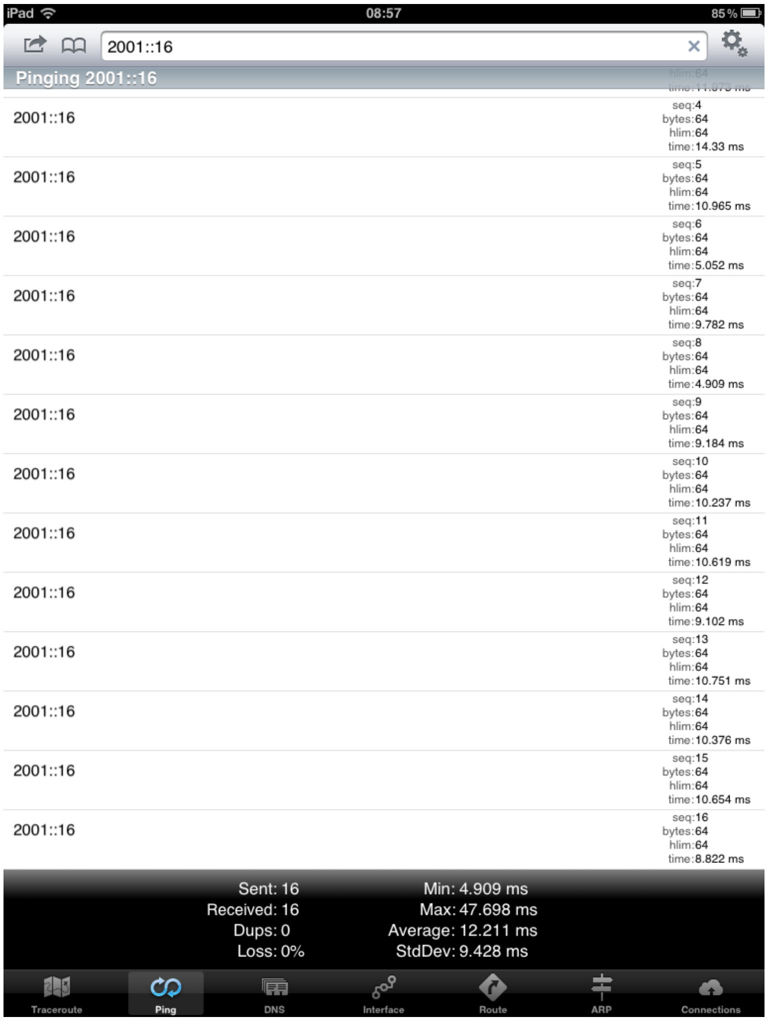
Wifi IPv6
fc00::6cff:b43d:ad17:46c9

Wifi MAC
a4:67:06:55:da:91

Cell Data IP -- KB/s
N/A

VPN IP
N/A

An example using iPad IPv6 Tools to ping the Windows Server 2008 R2.



```
2001::16

Pinging 2001::16                                   hlim:64
                                                   time:11.873 ms
2001::16                                           seq:4
                                                 bytes:64
                                                  hlim:64
                                                  time:14.33 ms
2001::16                                           seq:5
                                                 bytes:64
                                                  hlim:64
                                                  time:10.965 ms
2001::16                                           seq:6
                                                 bytes:64
                                                  hlim:64
                                                  time:5.052 ms
2001::16                                           seq:7
                                                 bytes:64
                                                  hlim:64
                                                  time:9.782 ms
2001::16                                           seq:8
                                                 bytes:64
                                                  hlim:64
                                                  time:4.909 ms
2001::16                                           seq:9
                                                 bytes:64
                                                  hlim:64
                                                  time:9.184 ms
2001::16                                           seq:10
                                                 bytes:64
                                                  hlim:64
                                                  time:10.237 ms
2001::16                                           seq:11
                                                 bytes:64
                                                  hlim:64
                                                  time:10.619 ms
2001::16                                           seq:12
                                                 bytes:64
                                                  hlim:64
                                                  time:9.102 ms
2001::16                                           seq:13
                                                 bytes:64
                                                  hlim:64
                                                  time:10.751 ms
2001::16                                           seq:14
                                                 bytes:64
                                                  hlim:64
                                                  time:10.376 ms
2001::16                                           seq:15
                                                 bytes:64
                                                  hlim:64
                                                  time:10.654 ms
2001::16                                           seq:16
                                                 bytes:64
                                                  hlim:64
                                                  time:8.822 ms

         Sent: 16             Min: 4.909 ms
     Received: 16            Max: 47.698 ms
         Dups: 0         Average: 12.211 ms
         Loss: 0%         StdDev: 9.428 ms
```

Android Devices

Android devices were not used in this test scenario; however, IPv6 is supported.

IPv6 support appears to be limited to the WiFi interface and there is some confusion whether or not IPv6 is supported for 3G. Implementing 3G IPv6 support is not issue, mobile data for IPv6 could be.

3G IPv6 services differ from continent to continent, even within Europe each country offers different levels of support, so 3G IPv6 is needed before any serious testing of Android devices can be done.

Linux

Linux models have supported IPv6 ready kernels for many years and have been ahead of the game in implementing IPv6.

The downside of being early adopters of IPv6 technology results in different versions reflecting the IPv6 evolution. It is important to check the software versions to make sure they have the latest RFC's that include newer or modified specifications.

Tunnel Broker (SixXS)

In countries where IPv6 support is not readily available, access to the world of IPv6 can be done through Tunnel Brokers.

As the name suggests, IPv6 connectivity is provided through Tunnels. Be aware that there could be some issues if used in conjunction with Network Address Translation (NAT), see your local provider for more information.

SixXS is a free IPv6 tunnel broker service that has been available to users for more than 10 years.

SixXS supports the acceleration of IPv6 adoption and provides free access to IPv6 networks around the global. It is a useful tool for those preparing to migrate to IPv6.

URL reference, www.sixxs.net

Other Tunnel Broker services are available worldwide, if you live in North America, you may wish to use Hurricane Electric Internet Services.

URL reference, see www.tunnelbroker.net

12 Firewalls

The use of Firewalls is essential for network security.

When implementing IPv6, it is important to choose the right product to protect your network.

Some have chosen to delay this migration due to a lack of IPv6 Firewall support on the market. At first this may appear true, but closer examination shows that a third of vendors on the market today have IPv6 support.

If you are delaying IPv6 adoption and concluded that you do not need to worry about an IPv6 enabled Firewall, think again.

Why, because a number of devices that you are likely to install on your network already have IPv6 enabled by **default**.

Are you using any of the following platforms ?

- Windows 7
- Linux
- MacOS X
- iPhones / iPad
- Android Devices
- Corporate HP Printers

If so, then you will have IPv6 in your network now !

How can you tell if you have IPv6 running on your network ?

Try searching for the following types of traffic,

- Ethertype 0x86dd (as opposed to 0x0800 for IPv4)
- IPv4 UDP Port 3544 (the Teredo Listener)
- IPv4 Protocol Header Type 41 (IPv6 encapsulated)
- IPv4 address 192.99.88.1 (6to4 anycast relay)
- ICMPv6 type 134; Neighbour Advertisement

If you find any of the above packets, then you have IPv6.

There are two problems associated with unwittingly having IPv6 in your network, the first, you have traffic consuming bandwidth that is not needed, the second, and the most important, is one of security.

IPv6 has been designed such that, in the absence of DHCP, Stateless Auto configuration (SLAAC) will configure the node automatically enabling it for the IPv6 world.

The result, you have an unsecure network.

13 Conclusion

2011 is the year when everyone is talking about IPv6.

On the 3rd February 2011, IANA assigned its last block of IPv4 addresses and on the 15th April 2011 APNIC (Asia/Pacific Region) ran out of IPv4 addresses.

Interestingly, it took 38 years for radio to reach 50 million people, whereas in just one recent year, the social network site Facebook signed up more than 200 million users and by the end of this year would have reached in total, almost one billion people.

In 2012, according to Europe's top engineers, there will be more mobile devices used throughout the world than people.

The world explosion in internet users and more recently mobile devices and androids has put immense pressure on the demand for IP addresses and specifically the need for IPv6 addresses.

The importance of IPv6 migration continues to spread throughout Europe and legislation will follow if we are going to compete with Asia as they continue to grow their expertise and IPv6 infrastructure.

As an example, Microsoft not only enables IPv6 on its software platforms by default, but it also builds software application that depends on IPv6; Microsoft's email platform, "Exchange Server 2007/2010" relies solely on IPv6 as its core protocol; so you cannot disable it.

The effect in the Enterprise is forcing customers to demand not just IPv6 scalable networks, but the benefits and new services that it can provide.

If you think this doesn't affect you, think again, you may find your local government will force ISP's into IPv6 adoption and in turn force you into the world of IPv6, sooner than you think.

As a minimum, all of us today should have an IPv6 migration strategy which includes planning, training, and the procurement of an IPv6 ready network infrastructure.

A Fundamental RFCs

RFC 2460	-	IPv6 Fundamental Specification (obsoletes RFC 1883, see RFC 5095)
RFC 3315	-	DHCP v6 for IPv6 (**Note** : DHCP Relay will be supported in AoS v6.4.5 R02 Q42012)
RFC 3879	-	Deprecating Site Local Addresses
RFC 4291	-	IPv6 Addressing (obsoletes RFC 3513)
RFC 4443	-	ICMPv6 for IPv6 (obsoletes RFC 2463, see RFC 2780)
RFC 4861	-	Neighbor Discovery (obsoletes RFC 2461)
RFC 4862	-	Stateless Auto Configuration (obsoletes RFC 2462)
RFC 3484	-	Default Address Selection for IPv6

B IPv6 Addressing

One of the main differences between IPv6 and IPv4 is that the address size has increased from 32 bits to 128 bits, increasing the size of the address space to the point where running out of IPv6 addresses is no longer a concern.

The following types of IPv6 addresses are supported:

- Unicast

  Standard unicast addresses, similar to IPv4.

- Multicast

  Addresses that represent a group of devices. Traffic sent to a multicast address is delivered to all members of the multicast group.

- Anycast

  Traffic that is sent to this type of address is delivered to one member of the Anycast group. The device that receives the traffic is usually the one that is easiest to reach as determined by the active routing protocol.

IPv6 does not support the use of broadcast addresses !

This functionality is replaced using improved multicast addressing capabilities.

IPv6 addresses are expressed using colon hexadecimal notation and consist of eight 16-bit words, as shown in the following example:

1234:000F:531F:4567:0000:0000:BCD2:F34A

Note that any field may contain all zeros or all ones. In addition, it is possible to shorten IPv6 addresses by suppressing leading zeros. For example: 1234:F:531F:4567:0:0:BCD2:F34A.

Another method for shortening IPv6 addresses is known as zero compression. When an address contains contiguous words that consist of all zeros, a double colon (::) is used to identify these words.

For example, using zero compression the address

0:0:0:0:1234:531F:BCD2:F34A

is expressed as follows:

::1234:531F:BCD2:F34A

Because the last four words of the above address are uncompressed values, the double colon indicates that the first four words of the address all contain zeros.

Using the double colon is only allowed once within a single address.

So if the address was 1234:531F:0:0:BCD2:F34A:0:0, a double colon could not replace both sets of zeros. For example, the first two versions of this address shown below are valid; the last version is not valid:

1 1234:531F::BCD2:F34A:0:0

2 1234:531F:0:0:BCD2:F34A::

3 1234:531F::BCD2:F34A:: ***(not valid)***

With IPv6 addresses that have long strings of zeros, the benefit of zero compression is more dramatic.

For example, address FF00:0:0:0:0:0:4501:32 becomes FF00::4501:32.

Note that hexadecimal notation used for IPv6 addresses resembles that, which is used for MAC addresses.

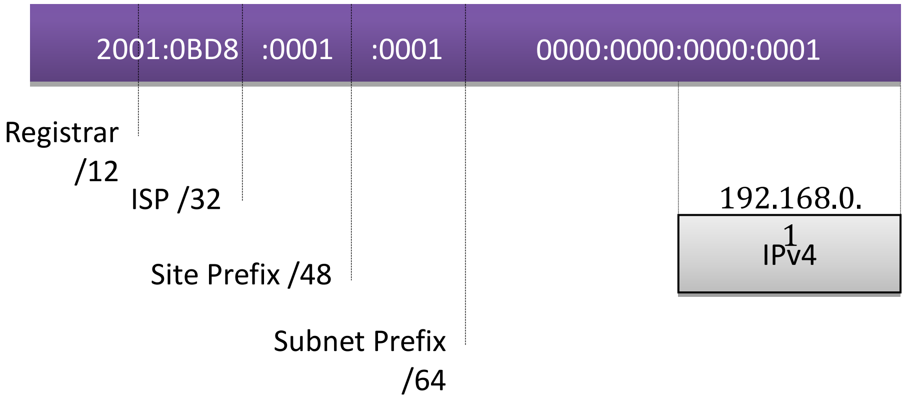
However, it is important to remember that IPv6 addresses still identify a device at the Layer 3 level and MAC addresses identify a device at the Layer 2 level.

Another supported IPv6 address notation includes embedding an IPv4 address as the four lower-order bits of the IPv6 address. This is especially useful when dealing with a mixed IPv4/IPv6 network.

For example: 0:0:0:0:0:0:212.100.13.6

The Classless Inter-Domain Routing (CIDR) notation is used to express IPv6 address prefixes. This notation consists of the 128-bit IPv6 address followed by a slash (/) and a number representing the prefix length (IPv6-address/prefix-length). For example, the following IPv6 address has a prefix length of 64 bits: FE80::2D0:95FF:FE12:FAB2/64

Another example of an IPv6 address is shown below.



From a global perspective, ISP's will generally be given /32 from their Regional Internet Registry, which equates to almost 80 billion, billion, billion addresses.

Organisations are likely to be given /48 by their ISP Registry and in turn an individual will be given /64, which is around 18 billion billion to manage.

This is understood easier by looking at the graphical view on the previous page.

For a comprehensive list of common IPv6 addresses, please see an extract from RFC 5156 on the following pages.

Network Working Group
Request for Comments: 5156
Category: Informational

M. Blanchet
Viagenie

April 2008

Special-Use IPv6 Addresses

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

This document is a compilation of special IPv6 addresses defined in other RFCs. It can be used as a checklist of invalid routing prefixes for developing filtering policies for routes and IP packets. It does not discuss addresses that are assigned to operators and users through the Regional Internet Registries.

Table of Contents

1. Introduction

This document is a compilation of special IPv6 addresses defined in other RFCs. It can be used as a checklist of invalid routing prefixes for developing filtering policies for routes and IP packets. It does not discuss addresses that are assigned to operators and users through the Regional Internet Registries.

The document is structured by address types. The document format is similar to [RFC3330].

Some tips about filtering are given, but are not mandatory to implement.

The addresses listed in this document must not be hard-coded into implementations.

2. Address Blocks

2.1. Node-Scoped Unicast

::1/128 is the loopback address [RFC4291].

::/128 is the unspecified address [RFC4291].

These two addresses should not appear on the public Internet.

2.2. IPv4-Mapped Addresses

::FFFF:0:0/96 are the IPv4-mapped addresses [RFC4291]. Addresses within this block should not appear on the public Internet.

2.3. IPv4-Compatible Addresses

::<ipv4-address>/96 are the IPv4-compatible addresses [RFC4291]. These addresses are deprecated and should not appear on the public Internet.

2.4. Link-Scoped Unicast

fe80::/10 are the link-local unicast [RFC4291] addresses. Addresses within this block should not appear on the public Internet.

2.5. Unique-Local

fc00::/7 are the unique-local addresses [RFC4193]. Addresses within this block should not appear by default on the public Internet. Procedures for advertising these addresses are further described in [RFC4193].

2.6. Documentation Prefix

The 2001:db8::/32 are the documentation addresses [RFC3849]. They are used for documentation purposes such as user manuals, RFCs, etc. Addresses within this block should not appear on the public Internet.

2.7. 6to4

2002::/16 are the 6to4 addresses [RFC3056]. The 6to4 addresses may be advertised when the site is running a 6to4 relay or offering a 6to4 transit service. Running such a service [RFC3964] entails filtering rules specific to 6to4 [RFC3964]. IPv4 addresses disallowed in 6to4 prefixes are listed in section 5.3.1 of [RFC3964].

2.8. Teredo

2001::/32 are the Teredo addresses [RFC4380]. The Teredo addresses may be advertised when the site is running a Teredo relay or offering a Teredo transit service.

2.9. 6bone

5f00::/8 were the addresses of the first instance of the 6bone experimental network [RFC1897].

3ffe::/16 were the addresses of the second instance of the 6bone experimental network [RFC2471].

Both 5f00::/8 and 3ffe::/16 were returned to IANA [RFC3701]. These addresses are subject to future allocation, similar to current unallocated address space. Addresses within these blocks should not appear on the public Internet until they are reallocated.

2.10. ORCHID

2001:10::/28 are Overlay Routable Cryptographic Hash IDentifiers (ORCHID) addresses [RFC4843]. These addresses are used as identifiers and are not routable at the IP layer. Addresses within this block should not appear on the public Internet.

2.11. Default Route

::/0 is the default unicast route address.

2.12. IANA Special-Purpose IPv6 Address Registry

An IANA registry (iana-ipv6-special-registry) exists [RFC4773] for Special-Purpose IPv6 address block assignments for experiments and other purposes. Addresses within this registry should be reviewed for Internet routing considerations.

2.13. Multicast

ff00::/8 are multicast addresses [RFC4291]. They contain a 4-bit scope in the address field where only some values are of global scope [RFC4291]. Only addresses with global scope in this block may appear on the public Internet.

Multicast routes must not appear in unicast routing tables.

3. Security Considerations

Filtering the invalid routing prefixes listed in this document should improve the security of networks.

4. IANA Considerations

To ensure consistency and to provide cross-referencing for the benefit of the community, IANA has inserted the following paragraph in the header of the iana-ipv6-special-registry.

C Useful URL References

www.useipv6.com
www.test-ipv6.com
www.ipv6.org
www.ipv6.org.uk
www.6uk.org.uk
www.uk.ipv6tf.org
www.ipv6forum.com
www.ipv6ready.org
ipv6eyechart.ripe.net
www.ipv6.com
www.ipv6.net
www.6deploy.org
test-ipv6.com
ipv6.he.net
www.ipv6actnow.com
www.ipv6.ac.uk
tools.ietf.org/html/rfc*[rfcnumber]*
worldipv6day.org
blog.go6.net
freeworld.thc.org/thc-ipv6
www.secdev.org/projects/scapy

For the procurement of IPv6 equipment see,

http://www.ripe.net/ripe/docs/ripe-501

D IPv6 Ready Logo RFCs

1996, August	**RFC 1981**	**Path MTU Discovery for IP version 6**
1998, December	**RFC 2460**	**IPv6 Spec (obsoletes RFC 1883, see RFC 5095)**
2006, February	**RFC 4291**	**IPv6 Addressing (obsoletes RFC 3513)**
2006, March	**RFC 4443**	**ICMPv6 (obsoletes RFC 2463, see RFC 2780)**
2007, September	**RFC 4861**	**Neighbor Discovery (obsoletes RFC 2461)**
2007, September	**RFC 4862**	**IPv6 Stateless AutoConfig (obsoletes RFC 2462)**

****The above RFC's are required for IPv6 Ready Logo Phase II; Core Protocols***

2003, July	RFC 3315	DHCP v6
1998, November	RFC 2404	HMAC-SHA-1-96 within ESP AH
1998, November	RFC 2410	NULL Encryption Algorithm
1998, November	RFC 2451	ESP CBC-Mode Cipher Algorithms
1999, April	RFC 2578	SMIv2 (obsoletes RFC 1902)
1999, April	RFC 2579	Textual Conventions SMI (obsoletes RFC 1903)
1999, April	RFC 2580	SMI Conformance (obsoletes RFC 1904)
1999, June	RFC 2617	HTTP Authentication (SIP) (obsoletes RFC 2069)
2002, June	RFC 3261	Session Initiation Protocol (obsoletes RFC 2543)

2002, June	RFC 3264	Offer Model for SDP (obsoletes RFC 2543)
2002, December	RFC 3416	SNMPv2 (obsoletes RFC 1905)
2002, December	RFC 3418	MIB for SNMP (obsoletes RFC 1907)
2003, September	RFC 3566	AES-XCBC-MAC-96 IPSec Algorithm
2003, September	RFC 3602	AES-CBC Cipher Algorithm for IPSec
2003, December	RFC 3646	DNS for DHCPv6
2003, December	RFC 3665	Basic Call Flow Examples for SIP
2004, January	RFC 3686	AES Counter Mode with ESP for IPSec
2004, April	RFC 3736	Stateless DHCP for IPv6
2004, June	RFC 3775	Mobility Support in IPv6
2004, June	RFC 3776	IPSec to Protect Mobile IPv6
2004, September	RFC 3879	Deprecating Site Local Addresses**
2005, January	RFC 3963	NEMO Protocol
2005, December	RFC 4301	IP Security Architecture (obsoletes RFC 2401)
2005, December	RFC 4303	IP ESP (obsoletes RFC 2406)
2005, December	RFC 4305	Crypto for ESP/AH (obsoletes RFCs 2404 & 2406)
2005, December	RFC 4306	IKEv2 (obsoletes RFCs 2407, 2408 & 2409)
2005, December	RFC 4307	Cryptographic Algorithms for IKEv2
2005, December	RFC 4312	Camellia Cipher Algorithm for IPSec
2006, July	RFC 4566	SDP (obsoletes RFCs 2327 & 3266)
2006, October	RFC 4718	IKEv2 Clarifications and Guidelines

E IPv6 RFC Reference

1969, April	RFC 1	Host Software
1981, September	RFC 791	Internet Protocol
1981, September	RFC 792	DARPA IP Protocol Specification
1993, November	RFC 1546	Host Anycasting Service
1993, December	RFC 1550	Next Generation Internet Protocol, or IPng White Paper
1995, January	RFC 1752	Next Generation Internet Protocol, or IPng (pre-IPv6)
1995, June	RFC 1809	Using the Flow Label Field in IPv6
1995, August	RFC 1826	IP Authentication Header
1995, August	RFC 1827	IP Encapsulating Security Payload (ESP)
1995, December	RFC 1881	IP Address Allocation Management
1995, December	RFC 1883	IPv6 Specification (obsoleted by RFC 2460)
1995, December	RFC 1884	IPv6 Addressing (obsoleted by RFC 2373)
1995, December	RFC 1886	DNS Extensions for IPv6
1996, February	RFC 1918	Address Allocation for Private Internets
1996, August	RFC 1981	Path MTU Discovery for IP version 6
1997, January	RFC 2080	RIPng for IPv6
1998, February	RFC 2292	Advanced Socket API (see RFC 3542)

1998, July	RFC 2363	PPP Over FUNI
1998, July	RFC 2365	Administratively Scoped IP Multicast
1998, November	RFC 2373	IPv6 Addressing (see RFC 1884 & 3513)
1998, November	RFC 2374	IPv6 Aggregatable Global Unicast Address Format
1998, July	RFC 2375	IPv6 Multicast Address Assignments
1998, November	RFC 2404	HMAC-SHA-1-96 within ESP AH
1998, November	RFC 2410	NULL Encryption Algorithm
1998, November	RFC 2451	ESP CBC-Mode Cipher Algorithms
1998, December	RFC 2452	IPv6 TCP MIBs (see RFC 4022)
1998, December	RFC 2454	IPv6 UDP MIBs (see RFC 4113)
1998, December	RFC 2460	IPv6 Spec (obsoletes RFC 1883, see RFC 5095) **
1998, December	RFC 2461	Neighbor Discovery for IPv6
1998, December	RFC 2462	IPv6 Stateless AutoConfiguration (obsoletes RFC 1971)
1998, December	RFC 2463	ICMPv6 (obsoletes RFC 1885, see RFC 4443)
1998, December	RFC 2464	Transmission of IPv6 over Ethernet (obsoletes RFC 1972)
1998, December	RFC 2466	MIB for IPv6 (see RFC 4293)
1998, December	RFC 2471	IPv6 Testing Address Allocation (obsoletes RFC 1897)
1998, December	RFC 2473	Generic Packet Tunneling in IPv6
1998, December	RFC 2474	Definition of DS Field in the IPv4 and IPv6 Headers
1998, December	RFC 2475	Architecture for Differentiated Services
1999, March	RFC 2526	Reserved IPv6 Subnet Anycast Addresses
1999, March	RFC 2545	BGP4 Extensions for IPv6

1999, March	RFC 2553	Basic Socket Extensions for IPv6 (obsoletes RFC 2133, see RFC 3493)
1999, April	RFC 2578	SMIv2 (obsoletes RFC 1902)
1999, April	RFC 2579	Textual Conventions SMI (obsoletes RFC 1903)
1999, April	RFC 2580	SMI Conformance (obsoletes RFC 1904)
1999, June	RFC 2617	HTTP Authentication (SIP) (obsoletes RFC 2069)
1999, August	RFC 2663	IP Network Address Translator (NAT)
1999, August	RFC 2671	Extension Mechanisms for DNS (EDNS0)
1999, August	RFC 2675	IPv6 Jumbograms (obsoletes RFC 2147)
1999, August	RFC 2676	QoS Routing Mechanisms and OSPF Extensions
1999, October	RFC 2710	Multicast Listener Discovery (MLD) for IPv6
1999, October	RFC 2711	IPv6 Router Alert Option
1999, December	RFC 2740	OSPFv3 for IPv6
2000, January	RFC 2743	Generic Security Service (GSS-API) (obsoletes RFC 2078)
2000, February	RFC 2766	NAT - Protocol Translation
2000, March	RFC 2780	IANA Guidelines for values IP and Related Headers
2000, June	RFC 2858	Multiprotocol Extensions for BGP4 (obsoletes RFC 2283)
2000, August	RFC 2893	Transition Mechanisms (obsoletes RFC 1933, see RFC 4213)
2000, August	RFC 2894	Router Renumbering for IPv6
2000, October	RFC 2932	IPv4 Multicast Routing MIB
2000, October	RFC 2983	Differentiated Services and Tunnels
2000, November	RFC 2993	Architectural Implications of NAT
2001, January	RFC 3019	IPv6 MIB for MLDP

2001, January	RFC 3041	Private Ext for Stateless Address Autoconfiguration
2001, January	RFC 3056	DHCP Relay Agent Information Option
2001, January	RFC 3053	IPv6 Tunnel Broker
2001, February	RFC 3056	Connection of IPv6 Domains via IPv4
2001, June	RFC 3068	Anycast Prefix for 6to4 Relay Routers
2001, April	RFC 3086	Definition of DS Behaviors and Rules
2001, June	RFC 3122	Neighbor Discovery Extensions for Inverse Discovery
2001, June	RFC 3140	Per Hop Behavior Identification Codes
2001, September	RFC 3177	IAB/IESG Recommendations on IPv6 Address Allocations
2002, April	RFC 3260	New Terminology and Clarifications for Diffserv
2002, June	RFC 3261	Session Initiation Protocol (obsoletes RFC 2543)
2002, June	RFC 3264	Offer Model for SDP (obsoletes RFC 2543)
2002, August	RFC 3306	Unicast Prefix based IPv6 Multicast Addresses
2002, August	RFC 3307	Allocation Guidelines for IPv6 Multicast Addresses
2002, September	RFC 3314	Recommendations for IPv6 in 3G Projects
2003, July	RFC 3315	DHCP v6 **
2003, July	RFC 3319	DHCPv6 Options SIP Servers
2002, October	RFC 3384	LDAP v3 Replication Requirements
2002, December	RFC 3416	SNMPv2 (obsoletes RFC 1905)
2002, December	RFC 3418	MIB for SNMP (obsoletes RFC 1907)
2003, February	RFC 3484	Default Address Selection for IPv6
2003, February	RFC 3493	Basic Socket Extensions for IPv6 (obsoletes RFC 2553)

2003, April	RFC 3513	IPv6 Addressing Architecture (obsoletes RFC 2373)
2003, April	RFC 3515	Session Initiation Protocol refer Method
2003, May	RFC 3542	Advanced Sockets API for IPv6 (obsoletes RFC 2292)
2003, September	RFC 3566	AES-XCBC-MAC-96 IPSec Algorithm
2003, August	RFC 3574	Transition Scenarios for 3GPP Networks
2003, August	RFC 3587	IPv6 Global Unicast Address Format (obsoletes RFC 2374)
2003, September	RFC 3590	Source Address Selection for the MLD
2003, September	RFC 3595	Textual Conventions for IPv6 Flow Label
2003, October	RFC 3596	DNS Extensions for IPv6 (obsoletes RFC 3152 & 1886)
2003, September	RFC 3602	AES-CBC Cipher Algorithm for IPSec
2003, December	RFC 3633	IPv6 Prefix Options for DHCP version 6
2003, December	RFC 3646	DNS for DHCPv6
2003, December	RFC 3665	Basic Call Flow Examples for SIP
2004, January	RFC 3686	AES Counter Mode with ESP for IPSec
2004, February	RFC 3696	Techniques for Checking and Transformation of Names
2004, April	RFC 3736	Stateless DHCP for IPv6
2004, May	RFC 3756	IPv6 Neighbor Discovery Trust Models and Threats
2004, June	RFC 3775	Mobility Support in IPv6
2004, June	RFC 3776	IPSec to Protect Mobile IPv6
2004, June	RFC 3810	MLDv2 for IPv6 (updates RFC 2710)
2005, January	RFC 3948	UDP Encapsulation of IPsec ESP Packets
2004, July	RFC 3849	IPv6 Address Prefix Reserved for Documentation

2004, September	RFC 3879	Depreciating site Local Addresses **
2004, November	RFC 3956	Embedding Rendezvous Point Address in IPv6 MC
2005, January	RFC 3963	NEMO Protocol
2005, March	RFC 3971	SEcure Neighbor Discovery (SEND)
2005, March	RFC 4007	IPv6 Scoped Address Architecture
2005, March	RFC 4022	MIB Base for TCP (obsoletes RFC 2452 & 2012)
2005, March	RFC 4029	Scenarios and Analysis for IPv6 in ISP's
2005, March	RFC 4038	Application Aspects of IPv6 Transition
2005, April	RFC 4048	RFC 1888 is Obsolete
2005, June	RFC 4057	IPv6 Enterprise Network Scenarios
2005, June	RFC 4087	IP Tunnel MIB (obsoletes RFC 2667)
2005, June	RFC 4113	MIB for UDP (obsoletes RFC 2454 & 2013)
2005, September	RFC 4192	Renumbering IPv6 without a Flag Day (updates RFC 2072)
2005, October	RFC 4193	Unique Local IPv6 Unicast addresses
2006, January	RFC 4271	BGP4 (obsoletes 1771)
2005, October	RFC 4213	Transition Mechanisms (obsoletes RFC 2893)
2005, October	RFC 4215	Analysis on IPv6 Transition in 3G Projects
2005, December	RFC 4241	A Model of IPv6/IPv4 Dual Stack Internet Access Service
2006, February	RFC 4291	IPv6 Addressing (obsoletes RFC 3513) **
2006, April	RFC 4293	MIB for IP (obsoletes RFC 2011, 2465 & 2466)
2005, December	RFC 4301	IP Security Architecture (obsoletes RFC 2401)
2005, December	RFC 4302	IP Authentication Header (obsoletes RFC 2402)

2005, December	RFC 4303	IP ESP (obsoletes RFC 2406)
2005, December	RFC 4305	Crypto for ESP/AH (obsoletes RFCs 2404 & 2406)
2005, December	RFC 4306	IKEv2 (obsoletes RFCs 2407, 2408 & 2409)
2005, December	RFC 4307	Cryptographic Algorithms for IKEv2
2005, December	RFC 4312	Camellia Cipher Algorithm for IPSec
2006, February	RFC 4361	DHCPv6 (updates RFC 2131, 2132 & 3315)
2006, February	RFC 4380	Teredo, Tunneling IPv6 over UDP through NAT
2006, March	RFC 4443	ICMPv6 (obsoletes RFC 2463, see RFC 2780) **
2006, April	RFC 4489	Link-Scoped IPv6 Multicast Addresses (obsoletes 3306)
2006, July	RFC 4566	SDP (obsoletes RFCs 2327 & 3266)
2006, August	RFC 4649	DHCPv6 Relay Agent Remote-ID Option
2006, October	RFC 4718	IKEv2 Clarifications and Guidelines
2007, January	RFC 4760	Multiprotocol Extensions for BGP4 (obsoletes RFC 2858)
2007, February	RFC 4798	Connecting IPv6 Islands over IPv4 MPLS
2007, April	RFC 4852	IPv6 Enterprise Network Analysis Layer 3
2007, September	RFC 4861	Neighbor Discovery (obsoletes RFC 2461) **
2007, September	RFC 4862	IPv6 Stateless AutoConfig (obsoletes RFC 2462) **
2007, April	RFC 4884	Extended ICMP (updates RFC 792, 4443)
2007, May	RFC 4890	Filtering ICMPv6 Messages in Firewalls
2007, September	RFC 4941	Privacy Ext for Stateless Autoconfig (obsoletes RFC 3041)
2007, July	RFC 4966	Reasons to Move the NAT-PT
2008, January	RFC 5059	BSR for PIM (obsoletes RFC 2362, updates RFC 4601)

2007, December	RFC 5095	Deprecation of Type 0 Routing Headers in IPv6
2008, April	RFC 5156	Special-Use IPv6 Addresses
2008, March	RFC 5157	IPv6 Implications for Network Scanning
2008, March	RFC 5175	IPv6 Router Advertisement Flags Option (obsoletes RFC 5075)
2008, May	RFC 5181	IPv6 Deployment Scenarios in 802.16
2008, July	RFC 5211	Internet Transition Plan
2008, March	RFC 5214	ISATAP (obsoletes 4214)
2008, July	RFC 5218	What Makes For a Successful Protocol ?
2010, July	RFC 5245	ICE for NAT Offer/Answer Protocols (obsoletes RFC 4091 & 4092)
2009, March	RFC 5454	Dual-Stack Mobile IPv4
2009, June	RFC 5555	Mobile IPv6 Support for Dual Stack Hosts and Routers
2009, June	RFC 5565	Softwire Mesh Framework
2010, February	RFC 5572	IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP)
2010, March	RFC 5747	4over6 using IP Encapsulation and MP-BGP Extensions
2010, March	RFC 5798	VRRPv3 for IPv4 and IPv6 (obsoletes RFC 3768)
2010, May	RFC 5844	IPv4 Support for Proxy Mobile IPv6
2010, August	RFC 5969	IPv6 Rapid Deployment on IPv4
2010, October	RFC 6036	IPv6 Emerging Service Provider Scenarios
2010, October	RFC 6052	IPv6 Addressing of IPv4/IPv6 Translators
2011, January	RFC 6081	Teredo Extensions (updates RFC 4380)
2011, February	RFC 6104	Rogue IPv6 Router Advertisement Problem Statement
2011, February	RFC 6105	IPv6 Router Advertisement Guard

2011, February	RFC 6106	Advertisement Options for DNS Config (obsoletes RFC 6106)
2011, May	RFC 6127	IPv4 Run-Out and IPv4-IPv6 Co-Existence
2011, April	RFC 6144	Framework for IPv4/IPv6 Translation
2011, April	RFC 6145	IP/ICMP Translation Algorithm
2011, April	RFC 6146	Stateful NAT64 Clients to IPv4 Servers
2011, April	RFC 6147	DNS64: DNS extensions for NAT
2011, April	RFC 6169	Concerns with IP Tunneling
2011, May	RFC 6180	IPv6 Transition Guidelines
2011, May	RFC 6221	Lightweight DHCPv6 Relay Agent (updates RFC 3315)
2011, June	RFC 6302	Logging Recommendations for Internet Facing Servers
2011, August	RFC 6333	Dual Stack Lite Broadband Deployments
2011, August	RFC 6334	DHCPv6 Option for Dual-Stack Lite
2011, August	RFC 6342	Mobile Network Consideration (obsoletes RFC 6312)
2011, October	RFC 6384	FTP Application for IPv6 to IPv4 Translation
2011, November	RFC 6436	Rationale for update to IPv6 Flow Label
2011, November	RFC 6437	IPv6 Flow Label Specification (obsoletes 3697, updates 2205 & 2460)
2011, November	RFC 6438	Using IPv6 Flow Label for ECMR and LA in Tunnels

F IPv6 Tools for PreSales

VMWare Server	www.vmware.com/products
Ubuntu Appliances	www.ubuntu.com/download/server/download
	http://www.secdev.org/projects/scapy
	http://freeworld.thc.org/thc-ipv6
	http://metanav.uninea.no
	http://www.digriz.org.uk/slaacer
	http://resources.infosecinstitute.com/slaac-attack
	http://ramond.sourceforge.net
	http://www.sixxs.net
	http://www.tunnelbroker.net
	http://www.ripe.net/ripe/docs/ripe-501
	http://isoc.org/wp/worldipv6day/
	http://www.ipv6tools.org/

G IPv6 VitalSuite Collectors

VitalNet collector types that support IPv6 are shown in the following list:

a. 3comCollector
b. atmCollector
c. bayCollector
d. ciscCollector
e. ciscoproccollector
f. ciscprotcollector
g. cpqCollector
h. frCollector
i. hubCollector
j. ifCollector
k. lucentCollector
l. netscoutCollector
m. ntCollector
n. rmonCollector
o. strmCollector
p. serverCollector
q. uCollector
r. ldCollector
s. aCollector

1. Cisco Call Manager and CUCM (5 resource types)
2. Avaya VMM (4 resource types)

bCollector

1. Lucent Brick
2. Lucent Brick Interface
3. VoIP Agent Stats
4. HSS Call Server Interface
5. HSS App Server Interface
6. HSS Database
7. HSS Server
8. HSS File System
9. Windows Server Metrics
10. Windows Process Metrics
11. SQL Server Metrics
12. Exchange Server Metrics
13. IIS Server Metrics
14. OmniPCX Enterprise
15. OmniPCX Ent Coupler
16. OmniPCX Ent IP-Phone
17. SIP VoIP
18. ALU SROS Router
19. ALU SROS CPU
20. ALU SROS Memory
21. ALU SROS Interface
22. ALU SROS MPLS Interface
23. ALU SROS MPLS LSP
24. ALU SROS SAP Queue In
25. ALU SROS SAP Queue Out
26. ALU SROS SDP In
27. ALU SROS SDP Out
28. ALU SROS SDP Binding
29. SDC ADSL Line
30. SDC Bridge Port
31. SDC DS1/E1
32. SDC DS3/E3
33. SDC Ethernet
34. SDC SDH
35. SDC SHDSL Span
36. SDC XDSL Line
37. ALU SROS Network In
38. ALU SROS Network Out
39. ALU SROS Link Aggr Group

pingCollector Local-to-Remote

saaCollector Cisco IP SLA

The following IP SLA collector types are supported:

a. tcp-connect
b. udp-echo
c. icmp-echo
d. udp-jitter

The above list maps to the following IPSLA operation types:

a. SAA / IP SLA TCP (dsid 62)
b. SAA / IP SLA UDP (dsid 61)
c. SAA / IP SLA Ping (dsid 60)
d. SAA / IP SLA Jitter (dsid 64)
e. SAA / IP SLA VoIP Jitter (dsid 69)

NOTE: Cisco router where the IPSLA operations run must also:

1. Have IPv6 enabled
2. Support this MIB: CISCO-RTTMON-IP-EXT-MIB

navisCollector

1. Via IPv6 FTP server ok
2. Via IPv6 Sybase server – not supported in VN 11.0

H IPv6 Migration Checklist

- Choose Software Applications that are independent of IPv4/IPv6
- Procure IPv6 Ready Logo or Compliant Network Components
- Train IT Staff
- Investigate Security Requirements
- Review Network Management Tools
- Upgrade DNS infrastructure to include the new AAAA records
- Analyse, propose and test transition mechanisms
- Set up a test scenario
- Review the need to obtain IPv6 address prefixes
- Talk to your carrier provider about IPv6 services
- Migrate your Network Infrastructure to IPv6