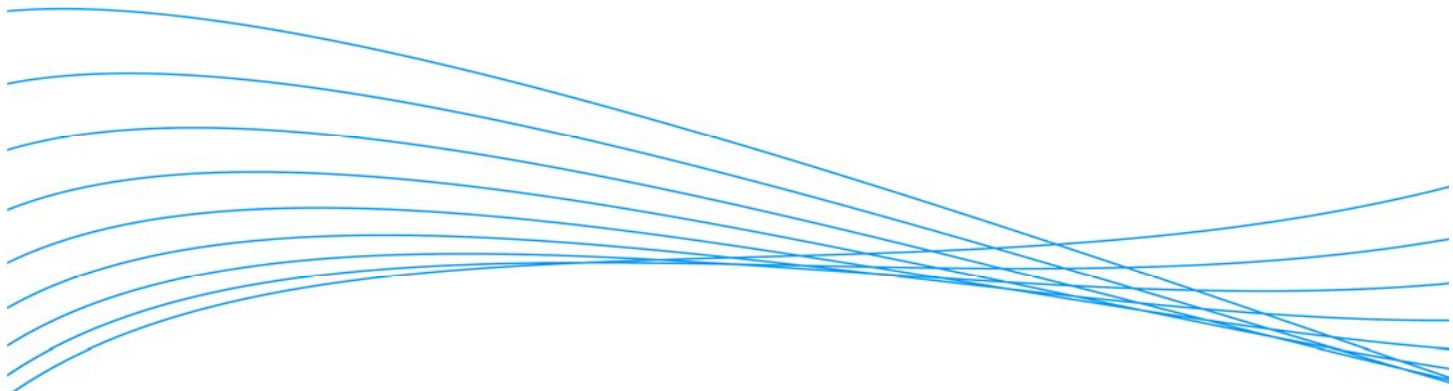


IPv6 – The Next Generation of Networking



Introduction	2
Benefits from IPv6.....	2
The IPv6 Protocol	3
IPv6 Technology Features and Benefits.....	4
Larger number of addresses	4
End-to-end connectivity	4
Efficient routing	4
Auto-configuration	4
Security.....	4
Mobility and multicast enhancements.....	4
The IPv6 Protocol Family	4
The Transition to IPv6.....	5
Dual Stacks.....	5
Tunneling.....	6
Comparison of the Transition Techniques.....	7
IPv6 Deployment Analysis	7
The Impact of IPv6 on Various Network Entities.....	7
How IPv6 affects Layer 2.....	7
How IPv6 affects Layer 3.....	7
What IPv6 means to the desktop/hosts	7
Deployment Issues.....	8
Protecting existing investment	8
Return on investment (ROI).....	8
Network planning.....	8
Instability in some IPv6 features	8
Service provider support	8
Deployment planning.....	8
Conclusion	10
Glossary	11

Introduction

Internet Protocol version 4 (IPv4) – is the fourth iteration of the Internet Protocol (IP) – is the basis of the TCP/IP communication protocols used to transport data, voice and video packets over the Internet. Internet Protocol version 6 (IPv6) is the next-generation network protocol, which has been standardized to replace the current IPv4. It holds great promise to become the backbone of the future of the Internet and offers a significant improvement over IPv4 in terms of scalability, security, mobility and convergence. The basic framework of the IPv6 protocol was standardized by the Internet Engineering Task Force (IETF) in the 1990s. However, there is still ongoing development of certain advanced aspects of the protocol.

This paper provides an introduction to IPv6 by discussing the potential business benefits that can result by deploying the technology. To understand how these benefits are derived, this white paper will explore some of the technical features and advantages of IPv6. The transition mechanisms developed to enable a seamless migration from IPv4 to IPv6 also will be examined. Finally, some deployment issues and strategies to prepare an adoption plan for deploying IPv6 in an enterprise will be analyzed.

Benefits from IPv6

The new features of IPv6 result in a number of business benefits:

- Lower network administration costs: The auto-configuration and hierarchical addressing features of IPv6 will make networks easy to manage.
- Optimized for next-generation networks: Getting rid of NAT re-enables the peer-to-peer model and helps with deploying new applications (e.g., communications and mobility solutions, such as VoIP.)
- Protection of company assets: Integrated IP security (IPsec) makes IPv6 inherently secure and provides for a unified security strategy for the entire network.
- Investment protection: The transition and translation suite of protocols helps with easy and planned migration from IPv4 and IPv6, while allowing for coexistence in the transition phase.

The IPv6 Protocol

The basic IPv6 protocol has a different packet header structure compared to IPv4. This is best illustrated by using a picture (see figures 1 and 2):

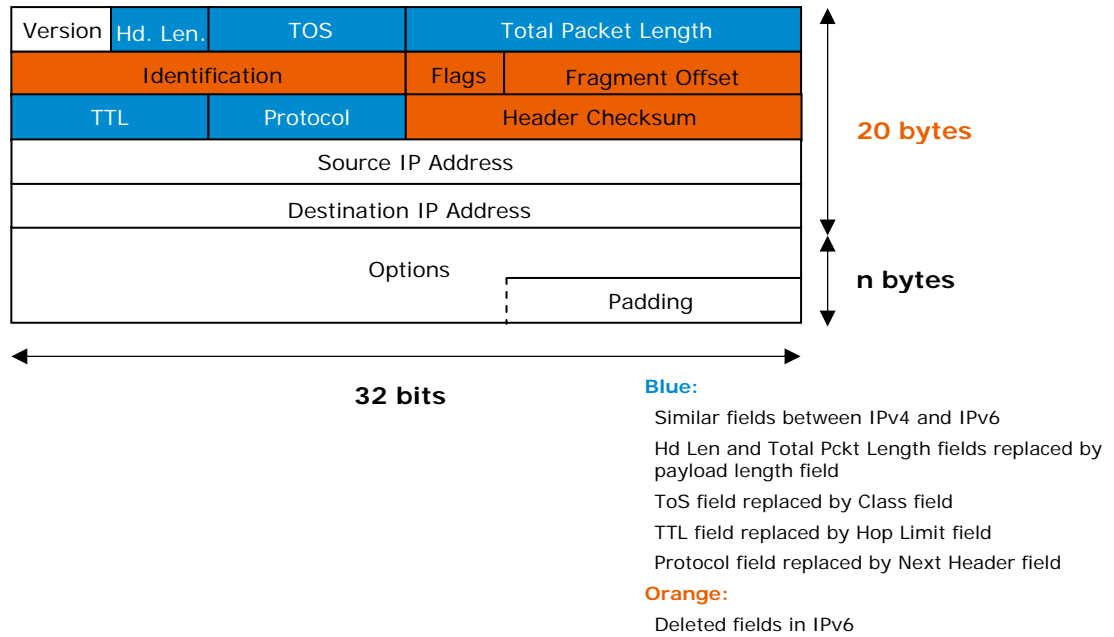


Figure 1 IPv4 header

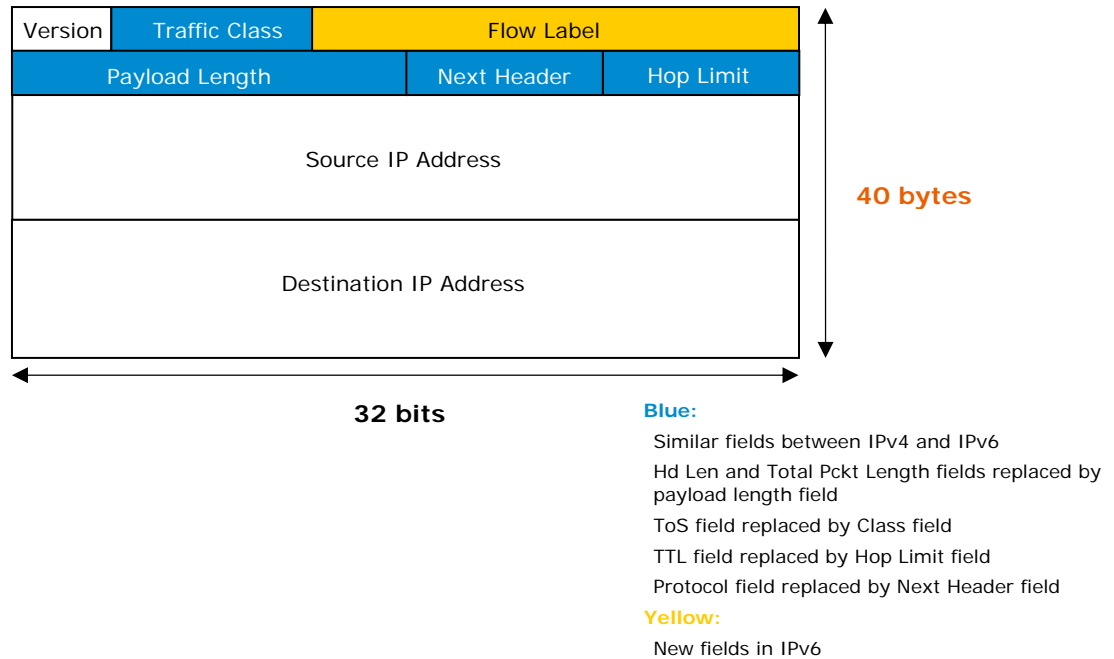


Figure 2 IPv6 header

As is shown in the illustration, the header is simplified. The options have been restructured to follow the header and are no longer part of it. This makes IPv6 header processing at intermediate nodes much easier. A new "flow label" field has been added to provide enhanced Quality of Service (QoS) in the future. The specific benefits resulting from the new header definition are listed in the next section.

IPv6 Technology Features and Benefits

Following are technical features that IPv6 adds beyond IPv4, as well as the benefits these features provide:

Larger number of addresses

IPv6 has 128-bit addresses, compared to 32 bits for IPv4 addresses. This results in a very large increase in the number of IP addresses available, and this creates a number of advantages. It eliminates scenarios where there is an IP address scarcity and NAT must be deployed to fix the issue. Getting rid of NAT results in a simplified network configuration, as well as reduced hardware and software complexity. The large number of IPv6 addresses also fits with the future vision of a networked home, where various appliances and gadgets will be networked and manageable over the Internet. In addition, the increasing deployment of wireless and mobile devices will not be cramped by IP address scarcity issues.

End-to-end connectivity

IPv4 needed NAT in certain situations in order to conserve scarce IP addresses. Unfortunately, NAT does not work well with peer-to-peer applications such as VoIP. IPv6 eliminates the need for NAT and thus, restores end-to-end connectivity. As a result, peer-to-peer applications work well with IPv6. Also, certain higher layer protocols like File Transfer Protocol (FTP) have a similar issue with NAT and need specialized software to work through it. Application protocols such as FTP can be enabled much more easily with IPv6.

Efficient routing

IPv6 has a more streamlined header compared to IPv4. Intermediate routing nodes do not recompute network-layer checksum, fragment/reassemble packets, or parse through headers. This reduces the processing overhead for routers, which reduces hardware complexity and enables faster packet processing. Also, hierarchical addressing in IPv6 allows for proper address space allocation, which results in smaller routing tables and more efficient routing in the overall network.

In addition, IPv6 makes it easier for network administrators to assign and track addresses.

Auto-configuration

IPv6 provides auto-configuration of IP addresses on IPv6-enabled devices. This greatly improves scalability and manageability of networks. New devices can be connected directly to the network without manually configuring IP addresses or having a DHCP server. Also, administrators can migrate a large number of devices from one network to another with ease.

Security

IPsec is a part of IPv6 standards, thus providing a solid security framework for Internet communication. IPsec can be used to implement both encryption and authentication.

Mobility and multicast enhancements

IPv6 provides further enhancements for mobile IPv6, which helps with today's wireless networks. The addition of scope field for multicast has improved the framework for multicast traffic. Also, the IPv6 anycast address type can be used for efficient host location.

The IPv6 Protocol Family

IPv6 is not just a single, isolated protocol. It encompasses a family of protocols that will augment or replace the existing IPv4 family of protocols. The IPv6 protocol family includes the basic IPv6 protocol, with its new addressing architecture.

It also includes a vastly expanded ICMPv6 protocol, which provides auto-configuration and neighbor discovery (similar to the ARP functionality in IPv4); Path MTU discovery (important because only the originating node can fragment packets in IPv6); error and informational messaging (including pingv6); MLD (similar to IGMP for IPv4); and mobile IPv6 related functionality.

DHCPv6 is the new version of DHCP for IPv6. Note that since IPv6 supports auto-configuration of IP addresses, DHCPv6 is not always required. DHCPv6 has been completely redesigned and is only conceptually similar to DHCP. It also has additional functionality, such as server-originated reconfiguration and authentication.

The interior routing protocols for IPv6 include next generation RIP (RIPng) and OSPFv3. The RIPng protocol is very similar to RIPv2 and has been adapted to advertise IPv6 network prefixes. Thus, RIPng is a very simple routing protocol suitable for use in small to medium IPv6 networks with trade-offs similar to those with RIPv2.

The OSPFv3 protocol is a link state routing protocol based on OSPFv2 with a number of modifications (e.g., support for IPv6 prefixes; OSPFv3 runs over a link rather than a subnet; each Link State Advertisement (LSA) has a flooding scope; removal of OSPF authentication by relying now on the inherent security provided by IPv6-IPsec). It follows the “ships-in-the-night” approach, i.e., a typical deployment will need both OSPFv2 and OSPFv3. OSPFv3 will exchange IPv6 routing information, while OSPFv2 will exchange IPv4 routing information.

Multicast Listener Discover (MLD) is used by a router to discover listeners for a specific multicast group. MLD is included with ICMPv6. This is similar to IGMP in IPv4. MLD snooping is similar to IGMP snooping, used to optimize layer 2 multicast forwarding.

The Transition to IPv6

The big question is not whether IPv6 will be widely deployed successfully in the Internet, but how and when. There are three transition mechanisms available to deploy IPv6 on IPv4 networks, and they may be used in any combination:

Dual Stacks

In this method, both IPv4 and IPv6 coexist on a device or node. Depending on which node it is talking to, the application will use IPv4 or IPv6, as appropriate. This also may be determined by the DNS response to a node-name. If DNS returns a v4 address, IPv4 will be used. If DNS returns a v6 address, IPv6 will be used. (see figure 3)

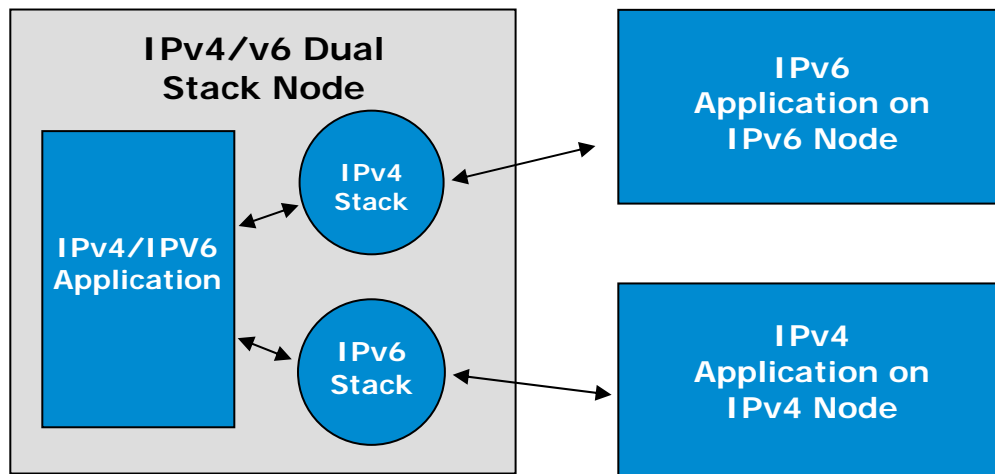


Figure 3 Dual Stack Method

Tunneling

The tunneling mechanism encapsulates IPv6 packets in IPv4 packets and can be used by two IPv6 nodes to communicate with each other over an IPv4 network. There are two ways to accomplish tunneling:

- "Automatic tunneling" uses IPv4-compatible IPv6 addresses to add a route to a special IPv6 prefix which points to a tunnel destination. Any packets destined for a v4-compatible address will be sent through the tunnel.
- In "configured tunneling," the address of the tunnel exit point is configured on the tunnel entry point and similar encapsulation is used. A combination of automatic and configured tunneling also can be used to route IPv6 packets across a v4 network. Teredo, ISATAP, 6to4 and 6over4 are other tunneling mechanisms.

Teredo encapsulates IPv6 packets over User Datagram Protocol (UDP), which allows them to pass through NAT nodes. ISATAP can be used by v6 hosts on a v4 network without any IPv6 routers using a specially constructed ISATAP address. 6to4 also uses a special prefix for tunneling. (see figure 4)

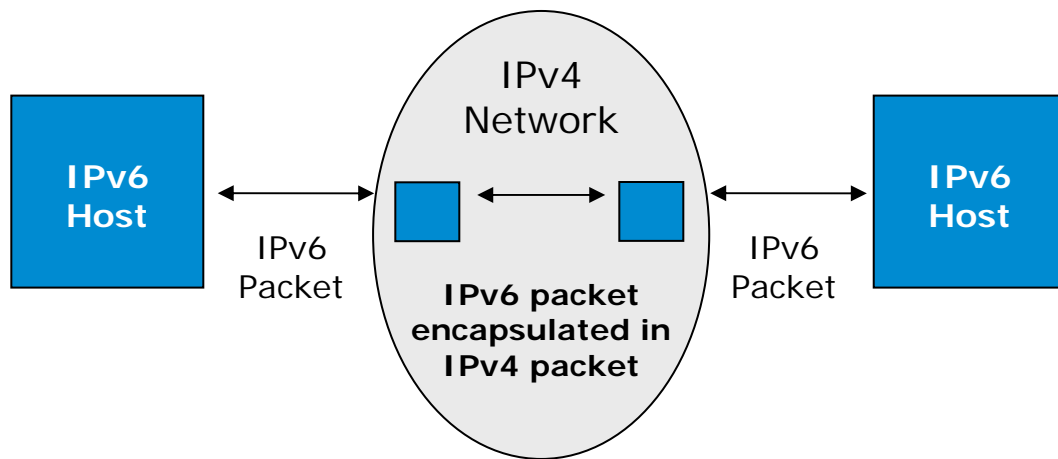


Figure 4 IPv6 tunneling

Comparison of the Transition Techniques

The dual stack method is easy to use and flexible. However, it needs two IP stacks, must maintain two processing tables, and requires more memory. Also, applications must be able to determine whether the peer is using IPv4 or IPv6. Tunneling allows gradual deployment of IPv6 even without IPv6 support from an ISP, since communication can occur by using IPv6 over a v4 network. Disadvantages are typical of other tunneling mechanisms; tunnel entry and exit points need to perform extra work and can be single points of failure.

IPv6 Deployment Analysis

The Impact of IPv6 on Various Network Entities

How IPv6 affects Layer 2

The Layer 2 switches' process packets are based on MAC addresses, which are independent of IPv6. Hence, implementing IPv6 over Layer 2 networks should not need significant changes to the Layer 2 switches. However, IPv6 support for protocol Virtual Local Area Networks (VLANs) may need hardware support. Functionality, such as ACL (Access Control Lists) and MLD snooping (equivalent to IPv4 IGMP snooping), will need to take into account changes for IPv6.

How IPv6 affects Layer 3

In addition to the basic IPv6 modules, for Layer 3 support the routing and forwarding mechanism must be aware of IPv6. Hence, protocols such as RIPng and OSPFv3 will have to be deployed, and the hardware will need to be IPv6-capable in order to conduct line rate processing of IPv6 packets. Thus, a significant change to hardware and software functionality will be required in routers to support IPv6.

What IPv6 means to the desktop/hosts

To deploy IPv6 on hosts, the desktop operating system has to support IPv6. Also, the enterprise and consumer applications must be ported to IPv6 so there is an application base for IPv6. New IPv6 applications that support end-to-end and peer-to-peer communications models on the Internet will have to be developed.

For hosts to communicate using IPv6, the necessary infrastructure must be in place to support IPv6. A transition plan has to be formulated for the network. The strategy will determine whether the transition requires specific software support from the host, or will be seamless. Again, depending on the network topology plan, DHCP or DNS support may be needed.

Deployment Issues

IPv6 technology promises to bring a number of benefits to network communications. However, given the complexity of the entire IPv6 protocol family, and the need for a robust infrastructure supporting the protocols, it would be wise for an enterprise to give thoughtful consideration to issues concerning IPv6 deployment.

Protecting existing investment

Vendors need to protect existing investments in switches, routers and hosts. Thus, they need a strategy which will maximize the returns on current investments

Return on investment (ROI)

IPv6 will need software and hardware upgrades on hosts, switches and routers. It may need deployment of new applications. Also, IPv6 transition must be planned carefully; typically, a pilot network is created to evaluate the strategy. All of this requires time and adds to expenses. Hence, a clear business case should be made to trigger migration of enterprise networks to IPv6.

Network planning

IPv6 can be deployed in two ways: having completely independent IPv6 and IPv4 networks, or overlaying IPv4 and IPv6 networks. This strategy can affect the IPv6 features required on hosts, switches and routers.

Instability in some IPv6 features

Certain standards like mobile IPv6, standards that define flow label are not stable yet, and this is necessary for successful deployment, particularly to avoid interoperability issues.

Service provider support

For enterprises which require IPv6 communication over the Internet, it is necessary to look into what IPv6 services and applications are offered by the service providers.

Deployment planning

The initial network deployment in enterprises typically would be conducted as pilot projects in test environments as a way to gain comfort in the understanding and operation of IPv6. In addition to host and routing IPv6 products, it will be necessary to analyze the required management, applications, middleware and security infrastructure required in the final network. (see figure 5)

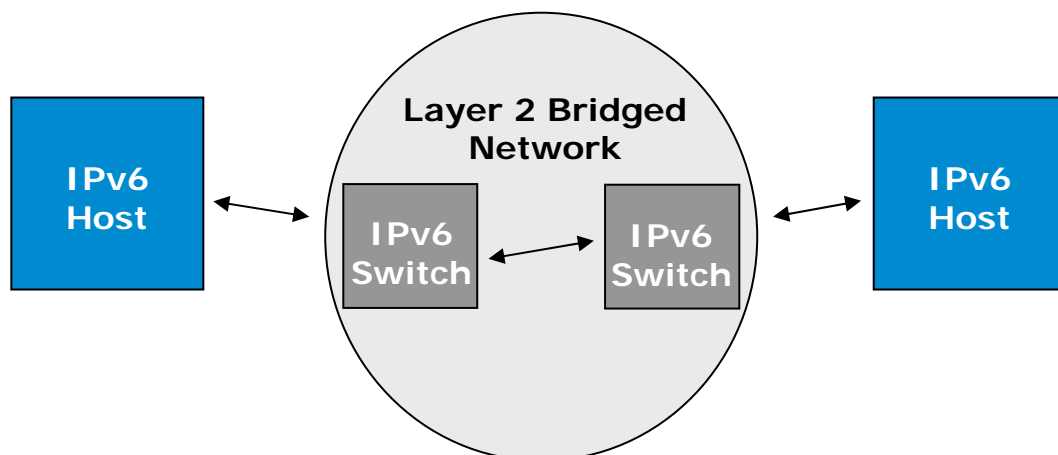


Figure 5 IPv6 layer 2 bridged network

A typical deployment strategy may involve introducing IPv6 functionality in stages. Initially, IPv6 host functionality may be deployed on end-nodes to gain familiarity with IPv6 issues. The host functionality would provide basic IPv6 connectivity. In the next stage, Layer 2 IPv6 switching could be deployed to allow end-nodes to communicate over the same network and to evaluate how end-to-end IPv6 applications interact. IPv6 host functionalities (include dual IPv4/IPv6 stack, DNSv6, Telnet6, etc) can also be deployed on layer 2 switches at this stage. In the final stage, IPv6 routing can be deployed to have full IPv6 network facility. Then, transition technologies can be deployed to have interoperability between IPv4 and IPv6, depending on the transition strategy. Network Working Group, Request for comments (RFC 4057) discusses in further detail enterprise network planning and scenarios for IPv6. (see figure 6)

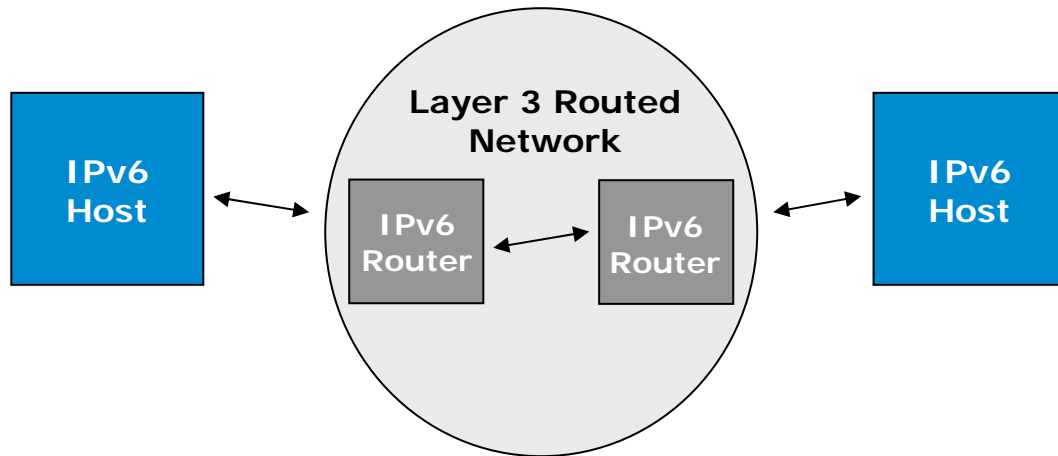


Figure 6 IPv6 layer 3 routed network

While analyzing a large-scale network, it will be useful to understand what kind of networking (Layer 2 vs. Layer 3) is deployed at various parts (core, distribution, edge). This will help to understand which IPv6 features are needed at what place in the network. In one scenario, only the core may be doing Layer 3 routing, while the distribution and edge may be Layer 2. In this case, the distribution and edge products probably will need IPv6 host and Layer 2-related IPv6 features (e.g., MLD), while the core may need IPv6 host, routing and IPv6 translation and transition features. In a second scenario, Layer 3 may be deployed in the core, distribution and edge. In this case, the distribution and edge products may need IPv6 host and routing, and the core may require IPv6 routing and IPv6 translation and transition. (see figure 7)

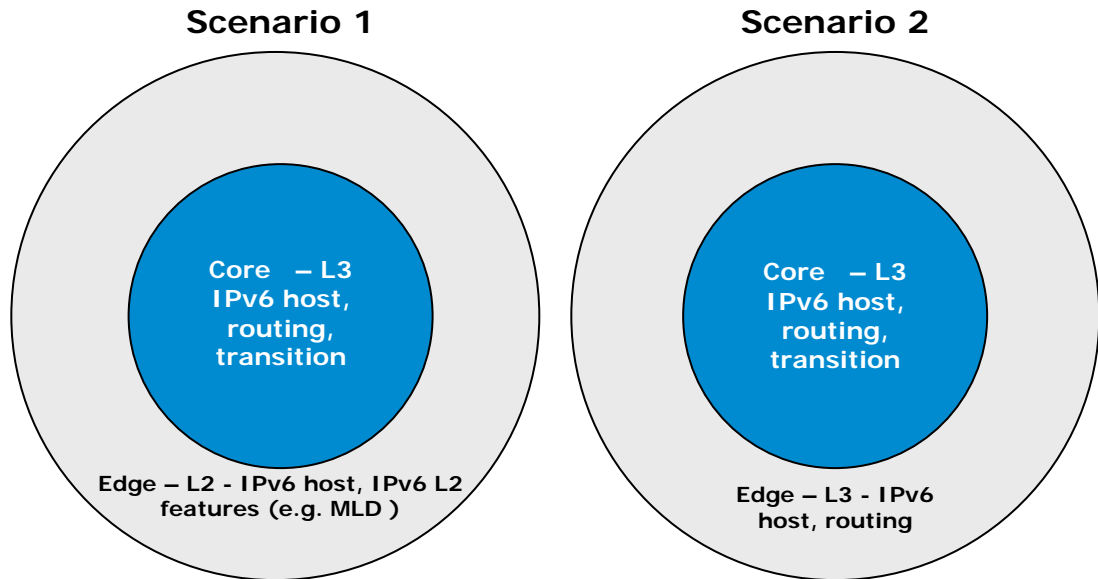


Figure 7 IPv6 needs at network core/edge

Conclusion

IPv6 will be the critical backbone of next-generation networking technology. It holds tremendous promise; however, enterprises and businesses need to have a carefully planned evaluation and transition strategy for IPv6. Looking forward to the future, enterprises must plan their investment in networking equipment with great care to be certain the IPv6 is deployed in a sequential and organized manner, while also making sure the investments are justified. The potential business benefits resulting from IPv6 include lower network administration costs, protection of company assets via a unified security model, investment protection by phased transition, and deployment of new applications.

Glossary

IETF – Internet Engineering Task Force

IPv4 – Internet Protocol version 4

IPv6 – Internet Protocol version 6

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

NAT – Network Address Translation

ICMP – Internet Control Message Protocol

IGMP – Internet Group Management Protocol

MTU – Maximum Transmission Unit

NDP – Neighbor Discovery Protocol

MLD – Multicast Listener Discovery

ISATAP – Intra-site Automatic Tunnel Addressing Protocol

NAT-PT – Network Address Translation – Protocol Translation

SIIT – Stateless IP-ICMP Translation

VoIP – Voice over IP

OSPFv3 – Open Shortest Path First Version 3

RIPng – Routing Information Protocol – Next Generation

To find out more about
ProCurve Networking
products and solutions,
visit our web site at

www.procurve.com



© 2007 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA0-4810ENW Rev. 1, 12/2007