Global Knowledge®

Expert Reference Series of White Papers

IP Version 6 Transition Mechanisms

1-800-COURSES

www.globalknowledge.com

IP Version 6 Transition Mechanisms

Joe Rinehart, MBA, CCIE #14256, CCNP/DP/VP

Introduction

Many events take place during the summer Olympic Games, which happened in London during the late summer of 2012. Even the most casual observer of the competition would notice the intense effort involved, particularly in the team-oriented events such as track and field. Critical to the success of the relay race is the passing of the baton, in which the racer for a specific leg of the race finishes their segment and transfers ownership of the race to the next participant of their team. While this may sound most familiar in the proverbial arena of sports, it applies equally to transitions regarding technology. The world of information technology is experiencing this exact type of shift as it moves from the familiar comfort of IP Version 4 into the “brave, new world” of IP Version 6.

Figure 1: Passing the Baton

www.microsoft.com

Effective transitions seldom take place overnight, and this includes network technologies as well. Nearly always, when installing new components into an infrastructure, there is a period of migration and/or coexistence, before committing fully to the new environment. IPv6 is no different, which has led to the development of various mechanisms designed to phase the protocol into existing networks. This paper will introduce and discuss the major options, and in some cases, the subcategories, of these transitional mechanisms.

Dual-Stack

One of the very first approaches used with regard to IPv6 is the dual-stack solution, which simply means that both IPv4 and IPv6 protocols exist simultaneously on devices on the network. In Figure 2 above, IP addressing for each protocol is configured on each LAN workstation (as labeled), as well as each device in the data path (routers and switches do not show the configured addresses). Each protocol exists separately from the other; no interaction between the two takes place in this model.

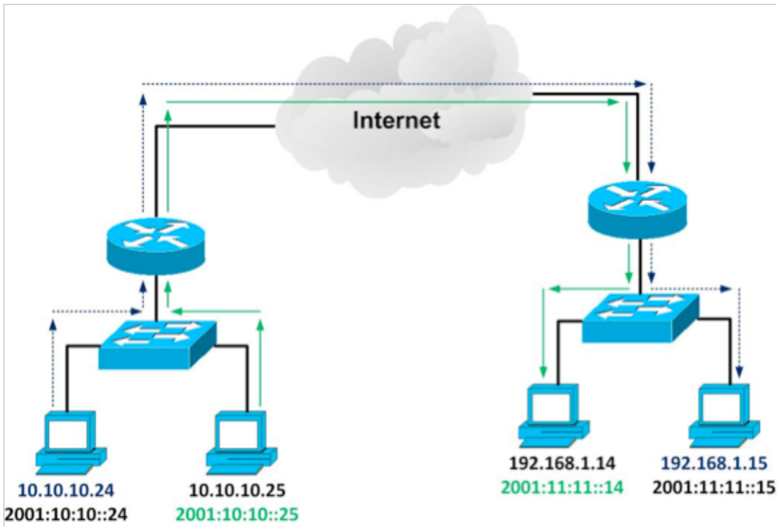
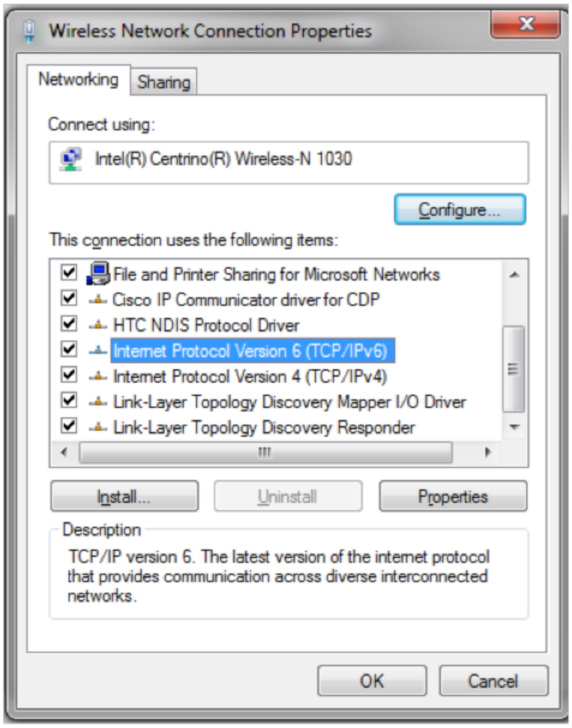


Figure 2: Dual Stack

Advantages of Dual-Stack



Connect using:

Intel(R) Centrino(R) Wireless-N 1030

This connection uses the following items:

☑ File and Printer Sharing for Microsoft Networks
☑ Cisco IP Communicator driver for CDP
☑ HTC NDIS Protocol Driver
☑ 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

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

Figure 3: IP Configuration in Windows 7

Deployment of a dual IPv4 and IPv6 solution has distinct advantages over other potential solutions. To begin with, use of the respective IP stacks means that no tunneling mechanisms in the internal network are required, nor are the headaches than can occur when using them. Second, using this solution allows for migrating devices on a more gradual basis, rather than all at once. Third, most network equipment manufacturers, including Cisco, recommend dual-stack as the most effective transition mechanism.

Disadvantages of Dual-Stack

Deployment a side-by-side solution with dual protocols instantly creates a greater amount of complexity for the individuals and teams supporting the network. This automatically adds additional work to the operational environment, both in terms of personnel and equipment. Machines using the dual-stacks will experience greater loads because of the additional processing involved.

Network Address Translation (NAT)Protocol

When the address depletion with IPv4 became self-evident, the introduction of RFC 1918 Private Addressing, along with NAT helped to solve the immediate problem. One of the many advantages of IPv6 is that with a vast address space at its disposal, NAT would no longer be necessary for daily operations. That being said, NAT is a solution for transition from IPv4 to IPv6, as illustrated in the diagram above. The same dynamics of traditional NAT exist for NAT-PT, except in this case translation is taking place between each respective protocol.

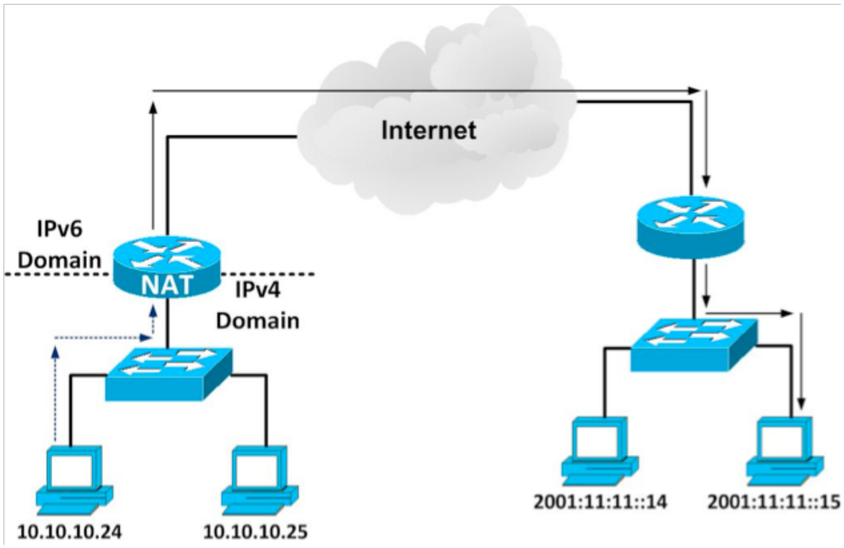


Figure 4: NAT-Protocol Translation

Advantages of NAT-PT

As was the case with traditional NAT, deployment of the address translation process can be isolated to the router or firewall performing this function, avoiding the need to involve every device on the network. Another advantage is that IPv6-only hosts have the capability to interact with IPv4-only hosts and vice-versa.

Disadvantages of NAT-PT

The original conception of the Internet Protocol envisioned end-to-end communication between hosts, with no intervening devices involved, a concept clearly broken through the use of NAT, regardless of the specific version involved. Another disadvantage of this transition mechanism is that it introduces a single point of failure (the NAT device), which goes against best design principles. Another problem with NAT-PT is that it provides basic connectivity and neglects the more advanced features of IPv6. While this transition mechanism was among the first to be proposed and/or used, it is generally discouraged for use. It should be noted that another version of NAT, referred to as NAT64, is available, but has some of the same disadvantages previously discussed.

Tunneling

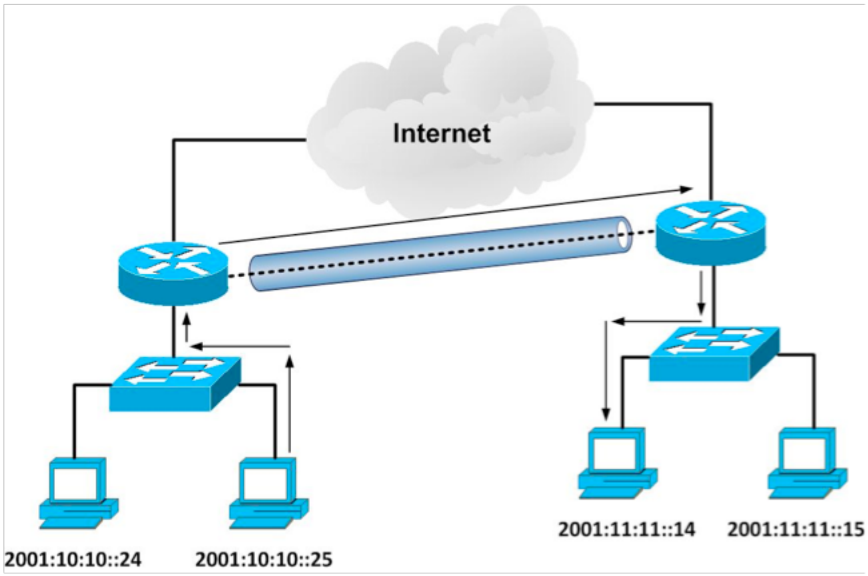


Figure 5: IPv6 over IPv4 Tunneling

While it may sound impossible by today's standards, the Internet Protocol (IPv4 specifically) had numerous competitors and was not considered the dominant, let alone only, means for transporting data. Over time, these protocols, such as Novell Netware's IPX and Apple's Appletalk, began to fade, but needed support over IP networks. One of the many useful features of tunneling is to carry non-IP traffic across an IP network, and this is still the case when dealing with IPv6 traffic. This transition mechanism makes use of a configured tunnel to transport IPv6 over a native IPv4 network, which may consist of two sites (as pictured above) or more. Unlike the previous transition mechanisms, tunneling is not monolithic; while the basic principles may be similar, the operations are different. The following chart gives a breakdown of the current, major tunneling types in use, particularly in a Cisco environment:

Tunneling Mechanism	Tunnel Type	Encapsulation	Description	Limitations
Manually Configured Tunnel (MCT)	Manual	**ipv6ip**	• Dual Stack on Tunnel Interface • Must specify source & destination • Point-to-Point Topology	Dynamic routing unsupported, not scalable
IPv6-over-IPv4 GRE Tunnel	Manual	**ipvip gre**	• Dual Stack on Tunnel Interface • Must specify source & destination • Point-to-Point Topology • Routing Protocol Support	Not Scalable
6to4 Tunnel	Automatic	**ipv6ip 6to4**	• Dual Stack on Tunnel Interface • Must specify source • Point-to-multipoint Topology • IPv4 Destination Embedded in IPv6 Address (2002::/16 prefix)	IPv4 public addressing needed, dynamic routing unsupported, no multicast
Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Tunnel	Automatic	**ipv6ip isatap**	• Must specify source • Within Site Only • IPv4 Destination Embedded in last 32 bits of IPv6 Address	No site-to-site support, dynamic routing unsupported, no multicast

Table 1: IPv6 Tunneling Types

General Advantages of Tunneling

When IPv6 routing domains are isolated and need to communicate, tunneling mechanisms can allow connectivity across an existing IPv4 network (including the Internet) without widespread configuration issues. In many cases, this is a router-to-router (or gateway) type of deployment, though some mechanisms exist for host-to-host (such as Microsoft's Teredo tunneling), or host-to-router. Some tunneling mechanisms require explicit source and destination designations, while others are automated, using embedded addressing to locate the peer device. In most cases, tunneling allows for isolated and/or simplified IPv6 deployment, coining the phrase "dual stack where you can; tunnel where you must."

General Disadvantages of Tunneling

Tunnel-based transition mechanisms can create scaling issues, particularly if the tunnel type is point-to-point. Dealing with a handful of sites may seem simple enough, but creating a meshed network requires numerous tunnels, increasing both complexity and overhead. Furthermore, with a few exceptions, most tunnels require IPv6 static routing, negating the automated features of dynamic protocols in a network. Finally, as with any tunneling protocol, the internal contents of the tunnel are shielded from the transit network, negating the ability to use certain traffic control features.

Conclusion

As with the adoption of any new technology, the move from IP version 4 to IP Version 6 will take a number of years to complete. During that transition phase, various mechanisms will be necessary to continue support of the older protocol as the newer gains widespread momentum. In addition, there has been some evolution even within the availability of these mechanisms, some of which have already passed from general use into deprecated status. Network engineering professionals already proficient in the use of IPv6, as well as the available coexistence mechanisms, will undoubtedly stay in high demand throughout this process.

Learn More

To learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge, Global Knowledge suggests the following courses:

ROUTE - Implementing Cisco IP Routing v1.0

IPv6 Fundamentals

Introduction to IPv6: Protocols, Services, and Migration

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

Joe Rinehart, MBA, CCIE #14256, CCNP/DP/VP is a professional trainer specializing in technology, business, and social media. He is also a successful speaker and published author, as well as a columnist for the Federal Way Mirror. He is active in the social media space, managing one of the largest groups on LinkedIn, as well as serving on the national steering committee of the Cisco Collaboration Users Group. Joe also serves as president of the Seattle Cisco Users Group, serving technology professionals throughout the Puget Sound region.

Joe Rinehart
MBA, CCIE #14256, CCNP/DP/VP
President and Chief Edutainment Officer
Gracestone Professionals, LLC
jrinehart@gracestonecompany.com
Twitter: jjrinehart