



IPv6 Addressing Guide

● ● ● SBA FOR GOVERNMENT

The Purpose of this Document

This guide is a supplemental document to the *Cisco Smart Business Architecture (SBA) for Government Midsize Agencies—Borderless Networks Foundation Design Guide*. It describes the next generation of IP: IPv6 addressing. Reliable Network Services provided by the Cisco SBA, such as the Internet connection, WAN infrastructure, security, remote site and headquarters infrastructure, build on a solid and planned IP addressing design.

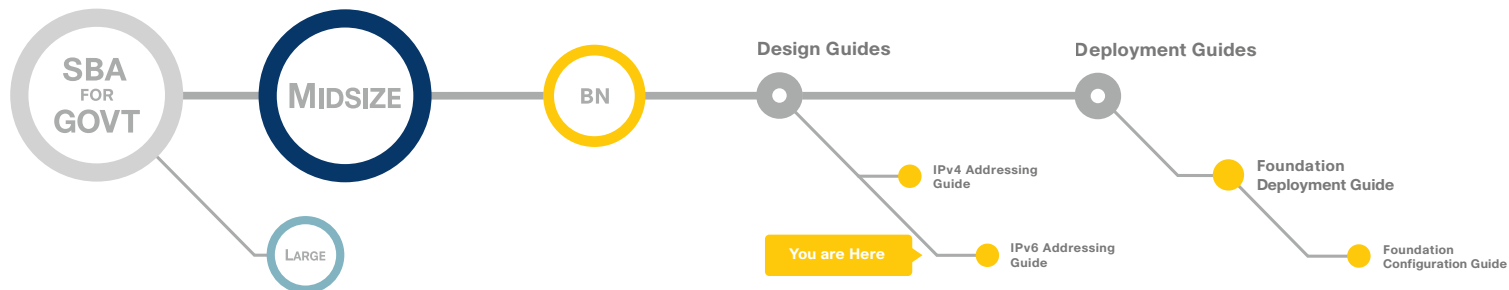
This guide addresses:

- How to successfully integrate IPv6 into a network that already has an existing IPv4 address space assigned
- How to handle multiple IP address ranges in the network
- When you should use a provider-independent IP space
- How to set up the IPv6 subnets

Who Should Read This Guide

This guide is intended for the reader with any or all of the following:

- An agency with 100-1000 connected employees
- An existing network and the need for guidance on how to add new services to the network.
- Concerns about IPv4 address space exhaustion and the need for guidance on how to transition to IPv6 addressing.



The reader may be looking for any or all of the following:

- An understanding of IPv6 addressing and subnetting
- General IPv6 addressing guidance to support their network redesign
- An understanding of how to communicate with an agency that has IPv6 deployed.
- An IPv6 address option for growth.

Related Documents

Before reading this guide

- **BN** Foundation Design Overview
- **BN** Foundation Deployment Guide
- **BN** Foundation Configuration Files Guide

Table of Contents

Introduction	1	IPv6 Address Plan Considerations	8
Guiding Principles	1	Prefix Sizing Considerations	8
IPv6 Addressing Technical Overview	2	IPv6 Address Space Assignments for Internet Connectivity	8
IPv6 Address Format.....	3	IPv6 Transition Technologies	9
Network Prefix	3		
IPv6 Address Types.....	3		
What's New in IPv6?	4		
Address Management and Assignment.....	4		
Static Configuration.....	4		
Stateless Address Auto Configuration	5		
Stateful DHCPv6.....	6		
Stateless DHCP.....	7		
		Appendix A: SBA for Midsize Agencies Document System	10

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental. Cisco Unified Communications SRND (Based on Cisco Unified Communications Manager 7.x)

© 2010 Cisco Systems, Inc. All rights reserved.

Introduction

The Cisco® SBA is a comprehensive design for networks with up to 1000 users. This out-of-the-box design is simple, fast, affordable, scalable, and flexible.

The Cisco SBA for Midsize Agencies incorporates LAN, WAN, wireless, security, WAN optimization, and unified communication technologies tested together as a solution. This solution-level approach simplifies the system integration normally associated with multiple technologies, allowing you to select the modules that solve your agency's problems rather than worrying about the technical details.

We have designed the Cisco SBA to be easy to configure, deploy, and manage. This architecture:

- Provides a solid network foundation
- Makes deployment fast and easy
- Accelerates ability to easily deploy additional services
- Avoids the need for re-engineering of the core network

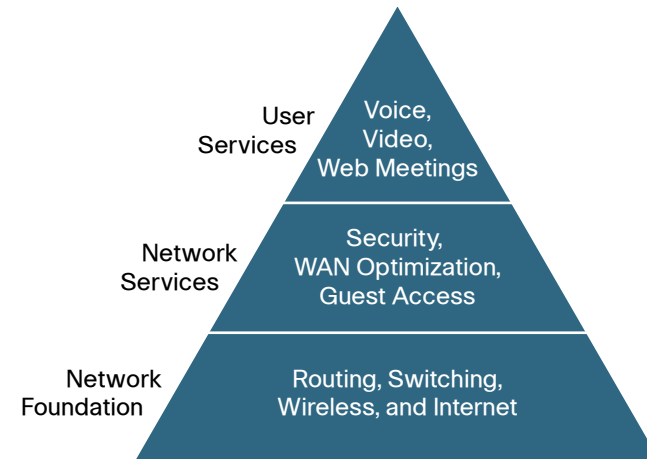
By deploying the Cisco SBA, your agency can gain:

- A standardized design, tested and supported by Cisco
- Optimized architecture for midsize agencies with up to 1000 users and up to 20 remote sites
- Flexible architecture to help ensure easy migration as the agency grows
- Seamless support for quick deployment of wired and wireless network access for data, voice, teleworker, and wireless guest
- Security and high availability for agency information resources, servers, and Internet-facing applications
- Improved WAN performance and cost reduction through the use of WAN optimization
- Simplified deployment and operation by IT workers with CCNA® certification or equivalent experience
- Cisco enterprise-class reliability in products designed for midsize agencies

Guiding Principles

We divided the deployment process into modules according to the following principles:

- **Ease of use:** A top requirement of Cisco SBA was to develop a design that could be deployed with the minimal amount of configuration and day-two management.
- **Cost-effective:** Another critical requirement as we selected products was to meet the budget guidelines for midsize agencies.
- **Flexibility and scalability:** As the agency grows, so too must its infrastructure. Products selected must have the ability to grow or be repurposed within the architecture.
- **Reuse:** We strived, when possible, to reuse the same products throughout the various modules to minimize the number of products required for spares.



The Cisco SBA can be broken down into the following three primary, modular yet interdependent components for the midsize agency.

- **Network Foundation:** A network that supports the architecture
- **Network Services:** Features that operate in the background to improve and enable the user experience without direct user awareness
- **User Services:** Applications with which a user interacts directly

IPv6 Addressing Technical Overview

Internet Protocol (IP) version 6 is a new IP protocol designed to replace IP version 4, which is deployed today and used throughout the world.

The current IP version, IPv4, has proven to be robust, easily implemented, interoperable, and has stood the test of scaling an internetwork to a global utility the size of the Internet today. However, the initial design of IPv4 did not anticipate the following conditions:

- The rapid growth of the Internet and the exhaustion of the IPv4 address space
- The need for simpler autoconfiguration and renumbering of network devices
- A requirement for security at the IP level
- A need for better support for real-time delivery of data—also called quality of service (QoS)

The lifetime of IPv4 has been extended with techniques such as private address space with Network Address Translation (NAT). Although these techniques seem to increase the address space and satisfy the traditional client-server setup, they fail to meet the requirements of IP address growth. The need to reach always-on environments (such as residential Internet through broadband, cable modem, or DSL) precludes IP-address conversion, pooling, and temporary allocation techniques. Also, the plug-and-play capabilities required by consumer Internet appliances further increase the address requirements.

The designers and users of the early Internet could not have anticipated the recent rapid growth of the Internet and the impending exhaustion of the IPv4 address space. The IPv6 address protocol meets the current requirements of the new applications and the never ending growth of the Internet.

The IPv6 address space makes more addresses available but it must be approached with careful planning. Successful deployment of IPv6 can be achieved with existing IPv4 infrastructures. With proper planning and design, the transition between IP version 4 and 6 is possible today as well.

The Cisco SBA is based on feedback from many customers and partners. Cisco has developed a solid network foundation with a flexible platform that

does not require reengineering to add overlay services and that emphasizes ease of use. Adding advanced services during or after the core network deployment is simplified. Time and expense is not wasted reengineering the network because the network is designed from the start to be flexible.

As mentioned previously, the Cisco SBA can be broken down into three primary modular layers: the Network Foundation, Network Services and User Services. For reliable delivery of agency applications and services, both internal and external to an agency's physical location, these three layers must work in a cohesive manner; otherwise, voice, video, and data can fail and even be compromised, placing the agency at risk. This guide focuses on all three layers of the architecture because IP addressing provides the foundation for voice, video, and security, in addition to core routing and switching.

The network, specifically IP addressing, provides the base for all network service, user services, and applications used every day. Without the foundation, it would not be possible to interact with network and user services, from using the phone to reading our email. The user and network services experience builds on the foundation.



Reader Tip

To learn more about Cisco SBA visit:

<http://www.cisco.com/go/sba>

<http://www.cisco.com/go/partner/smartarchitecture>

See <http://www.cisco.com/go/ipv6> for more details concerning transition technologies and design guidance.

The Internet Engineering Task Force (IETF) designed the IPv6 addressing scheme to provide interoperability with existing IPv4 network architecture and to allow the coexistence of IPv6 networks with existing IPv4 networks. IPv6 not only solves the IP address shortage problem in IPv4 but also enhances and improves some of the salient features of IPv4. IPv6:

- Enhances routing and addressing capabilities
- Simplifies the IP header
- Supports various types of IP addresses and larger address blocks for use with multicast routing
- Is described in RFC 4291

IPv6 Address Format

IPv6 uses 16-byte hexadecimal number fields separated by colons (:) to represent the 128-bit addressing format that makes the address representation less cumbersome and error-prone. Here is an example of a valid IPv6 address: 2001:db8:130F:0000:0000:09C0:876A:130B.

Additionally, to shorten the IPv6 address and make the address easier to represent, IPv6 uses the following conventions:

- Leading zeros in the address field are optional and can be compressed. For example: The following hexadecimal numbers can be represented as shown in a compressed format:
 - Example 1: 0000 = 0 (compressed form)
 - Example 2: 2001:db8:130F:0000:0000:09C0:876A:130B = 2001:db8:130F:0:0:9C0:876A:130B (compressed form)
- A pair of colons (::) represents successive fields of 0. However, the pair of colons is allowed just once in a valid IPv6 address.
 - Example 1: 2001:db8:130F:0:0:9C0:876A:130B = 2001:db8:130F::9C0:876A:130B (compressed form)
 - Example 2: FF01:0:0:0:0:0:1 = FF01::1 (compressed form)

An address parser can easily identify the number of missing zeros in an IPv6 address by separating the two parts of the address and filling in the 0s until the 128-bit address is complete. However, if two ::s are placed in the same address, then there is no way to identify the size of each block of zeros. The use of the :: makes many IPv6 addresses very small.

Network Prefix

In IPv6 there are references to prefixes which, in IPv4 terms, loosely equate to subnets. The IPv6 prefix is made up of the left-most bits and acts as the network identifier. The IPv6 prefix is represented using the IPv6-prefix or prefix-length format just like an IPv4 address is represented in the classless interdomain routing (CIDR) notation.

The /prefix-length variable is a decimal value that indicates the number of high-order contiguous bits of the address that form the prefix, which is the network portion of the address. For example: 2001:db8:8086:6502::/64 is an acceptable IPv6 prefix. If the address ends in a double colon, the trailing double colon can be omitted. So the same address can be written as 2001:db8:8086:6502/64. In either case, the prefix length is written as a decimal number 64 and represents the left-most bits of the IPv6 address. A similar address in IPv4 would be xxx.xxx.xxx.xxx/16.

IPv6 Address Types

There is a major difference in the IP address requirements between an IPv4 host and an IPv6 host. An IPv4 host typically uses one IP address; but an IPv6 host can have more than one IP address.

There are three major types of IPv6 addresses:

- Unicast: An address for a single interface. A packet that is sent to a unicast address is delivered to the interface identified by that address.
- Anycast: An address for a set of interfaces that typically belong to different nodes. A packet sent to an anycast address is delivered to the closest interface, as defined by the routing protocols in use, and identified by the anycast address.
- Multicast: An address for a set of interfaces (in a given scope) that typically belong to different nodes. A packet sent to a multicast address is delivered to all interfaces identified by the multicast address (in a given scope).

What's New in IPv6?

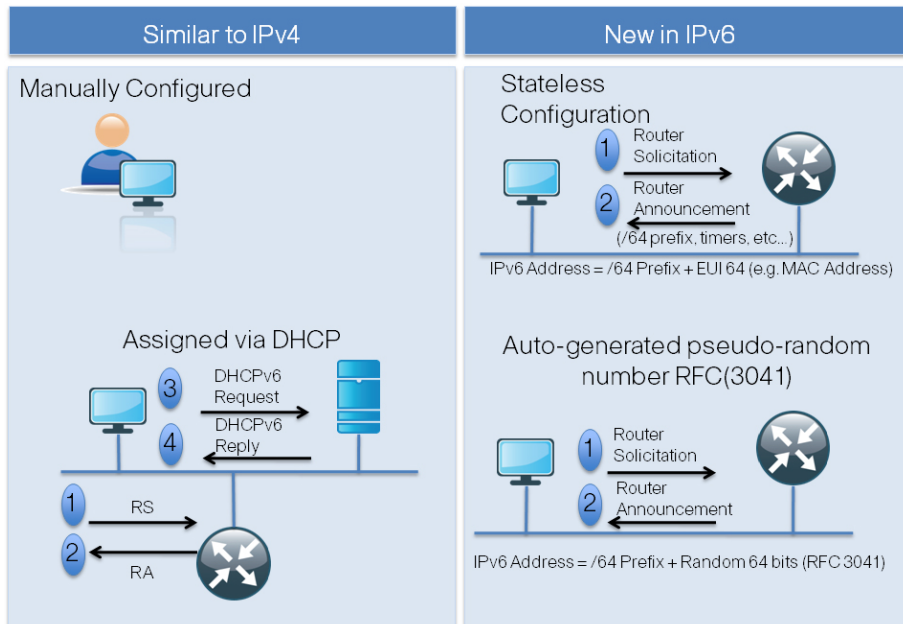
Figure 1 summarizes the parts of the configuration that are similar to IPv4, including:

- Static configuration
- DHCP

It also shows the parts that are new to IPv6, including:

- Stateless configuration
- Temporary addresses that are autogenerated

Figure 1. IPv6 Stateless Migration



Address Management and Assignment

There are four ways to configure a host address in IPv6:

- Static configuration: Similar to IPv4, the host address, mask, and gateway address are manually defined.
- Stateless Auto Address Configuration (SLAAC): In this case, the host autonomously configures its own address. Router solicitation messages are sent by booting nodes to request Router Advertisements (RAs) for configuring the interfaces (RFC2462).
- Stateful DHCPv6: The host uses DHCP to get its IPv6 address. This addressing management is similar to IPv4 behavior (RFC3315).
- Stateless DHCP: The host uses SLAAC and also DHCP to get additional parameters such as TFTP Server, WINS, etc.

The configuration choice relies on RA flags sent by the router on the LAN.

Static Configuration

As in IPv4, the host address can be statically defined. In this case, the IPv6 address, mask, and gateway address are all manually defined on the host.

Static address configuration is typically used for router interface configuration but is not likely to be used for hosts in IPv6.



Tech Tip

Using static configuration means that all autoconfiguration features provided by IPv6 are lost.

Stateless Address Auto Configuration

Nodes can use IPv6 stateless address auto configuration to generate addresses without the necessity of a DHCP server. IPv6 addresses are formed by combining network prefixes with an interface identifier. On interfaces with embedded Institute of Electrical and Electronics Engineers (IEEE) Identifiers, the interface identifier is typically derived from the IEEE identifier.

Tech Tip

There may be concerns regarding the use of a non-changing interface identifier such as the IEEE identifier because it is possible for that identifier to be used to correlate seemingly unrelated activity. Using DHCP to obtain the addresses is one way to address those concerns.

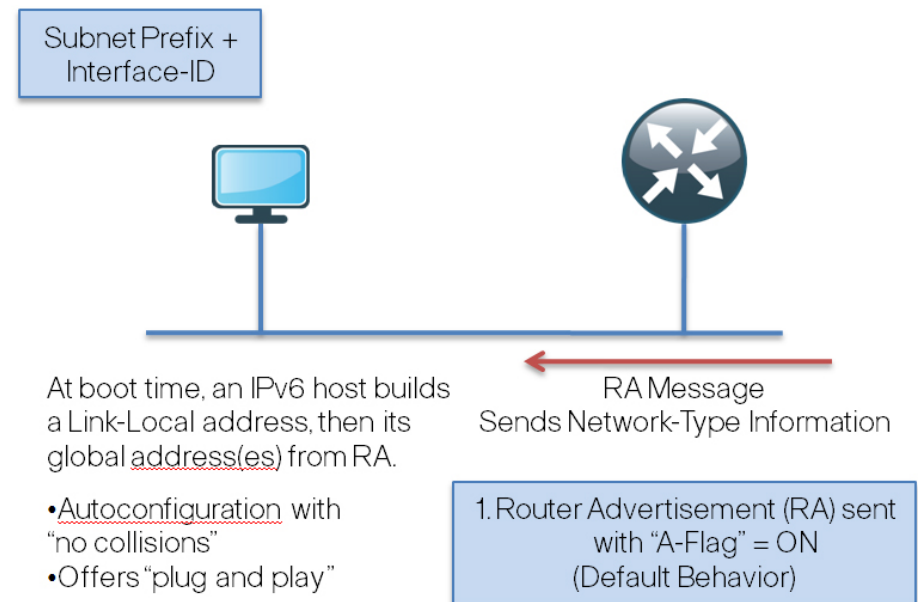
Easier Deployment

The address autoconfiguration feature is built into the IPv6 protocol to facilitate Intranet-wide address management that enables a large number of IP hosts to easily discover the network and get new and globally unique IPv6 addresses associated with their location. The autoconfiguration feature enables plug-and-play Internet deployment of new consumer devices, such as cell phones, wireless devices, home appliances, and so on. As a result, network devices can connect to the network without manual configuration and without any servers, such as DHCP servers.

Principles

A router on the local link sends network-type information through RA messages, such as the prefix of the local link and the default route in its router advertisements. The router provides this information to all the nodes on the local link as shown in Figure 2.

Figure 2. IPv6 Router Advertisements



A host can then build its address by appending a host identifier to the /64 prefix received from the router. As a result, an Ethernet host can autoconfigure itself by appending its 48-bit link layer address (MAC address) in an extended universal identifier EUI-64-bit format to the 64 bits of the local link prefix advertised by the router.

Windows Vista and Windows 7 do not use the EUI-64 technique by default when forming their interface identifier. Randomized addresses are generated for non-temporary autoconfigured addresses including public addresses, and link-local addresses are used instead of EUI-64 addresses as shown in Figure 3.

Tech Tip

With Windows Vista and Windows 7, the randomized addressing should be turned off. This is the default with Service Pack 1.

Figure 3. Windows IPv6 Addresses

```
C:\> netsh int ipv6 sh addr

<snip>

Interface 11: Local Area Connection

Addr Type  DAD State  Valid Life Pref. Life Address
-----
Temporary Preferred    4m26s    4m26s 2001:db8:1:cafe:a588:46c6:6024:33a5
Public     Preferred    4m26s    4m26s 2001:db8:1:cafe:b407:e685:fb14:c12d
Other      Preferred    infinite infinite fe80::b407:e685:fb14:c12d%11

C:\>
```

Easier Renumbering

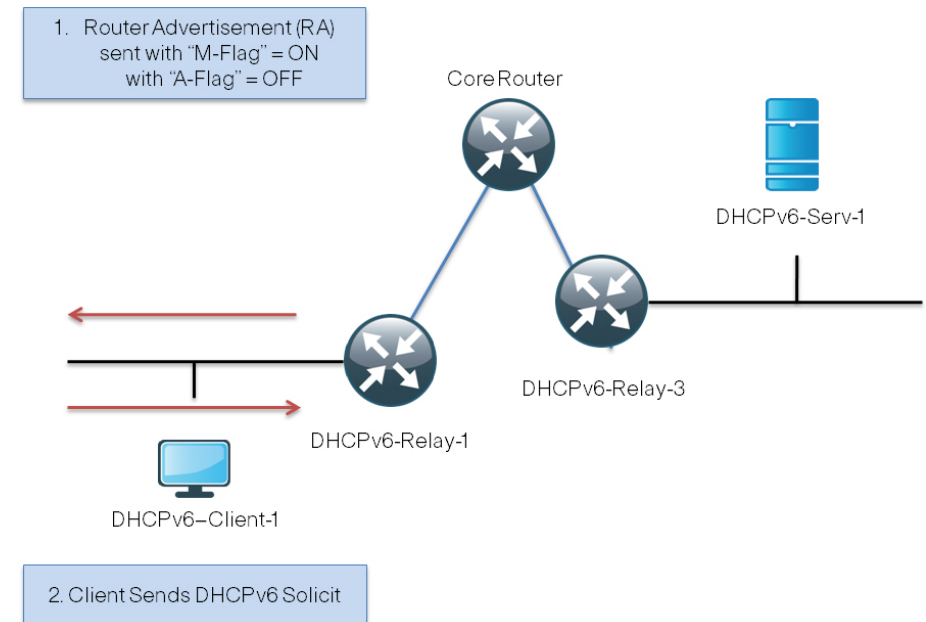
In IPv6 networks, the autoconfiguration feature makes renumbering an existing network simple and relatively easy compared to IPv4. The router sends the new prefix from the new upstream provider in its router announcements. The hosts in the network automatically pick the new prefix from the router advertisements and then use it to create their new addresses. As a result, the transition from provider A to B becomes manageable for network operators.

Stateful DHCPv6

Many enterprises currently use DHCP to distribute addresses to their hosts. IPv6 can be deployed with the same DHCP mechanism.

The process for acquiring configuration data for a client in IPv6 is similar to that in IPv4. However, DHCPv6 uses multicast for many of its messages. Initially, the client must first detect the presence of routers on the link using neighbor discovery messages. If a router is found, then the client examines the router advertisements to determine if DHCP should be used. If the router advertisements enable use of DHCP on that link (disabling the Autoconfiguration flag and enabling the Managed flag in RA messages allows a host to use DHCPv6 to obtain an IPv6 address), then the client starts a DHCP solicitation phase to find a DHCP server as shown in Figure 4.

Figure 4. DHCP Solicit Managed Flag On, A Flag Off



Using DHCPv6 provides the following benefits:

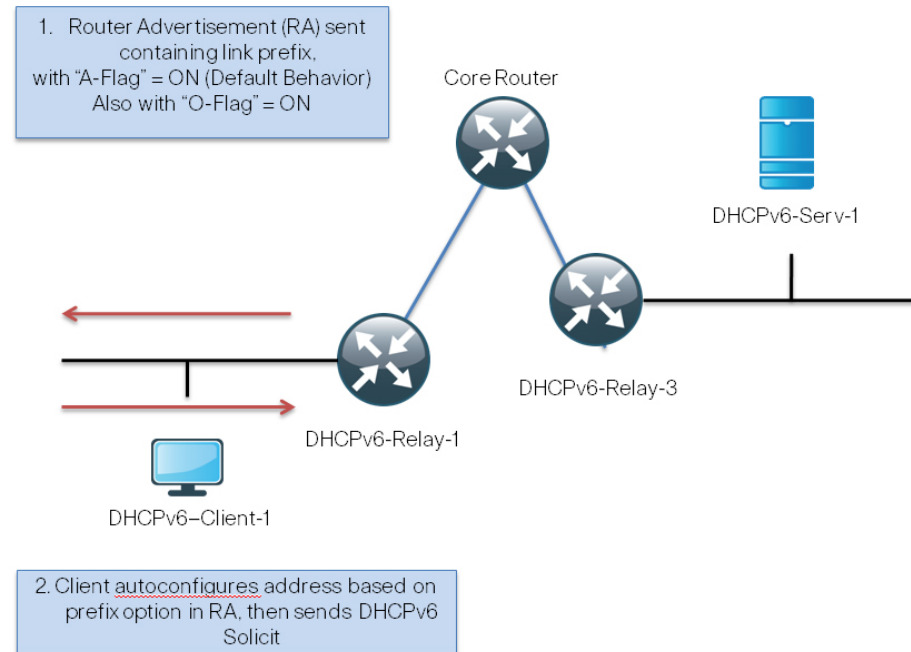
- It provides more control than serverless/stateless autoconfiguration.
- It can be used concurrently with stateless autoconfiguration .
- It can be used for renumbering.
- It can be used for automatic domain name registration of hosts using dynamic DNS.
- It can be used to delegate the IPv6 prefix to leaf customer-premise equipment (CPE) routers.

Stateless DHCP

Stateless DHCPv6 normally combines stateless autoconfiguration for address assignment with DHCPv6 exchange for all other configuration settings. In this case, DHCPv6 is only used for the host to acquire additional parameters, such as a TFTP Server, a DNS server, and so on.

A host builds its address by appending a host identifier to the /64 prefix received from the router and then issues a DHCP solicit message to the DHCP server as shown in Figure 5.

Figure 5. DHCP Solicit A Flag On



Notes

IPv6 Address Plan Considerations

IPv6 provides a significantly larger address space than IPv4, which enables lots of flexibility in how you can define logical and practical addressing plans. You can assign subnet prefixes based on various logical schemes that involve factors detailed in the IP Addressing Guide and on additional factors that pertain to IPv6 such as:

- Using existing IP addressing schemes
 - Translating the existing subnet numbers into IPv6 subnet IDs
 - Translating the VLAN IDs into IPv6 subnet IDs
- Redesigning your IP addressing scheme
 - Allocating IPv6 addresses according to your needs

When redesigning IP addressing schemes, you can allocate according to your need. Such logical addressing plans have the potential to simplify network operations and service offerings as well as network management and troubleshooting.

The addressing plan must take the following into consideration:

- Prefix aggregation: The large IPv6 addresses can lead to large routing tables unless network designers actively pursue aggregation.
- Network growth: It is important to design the address infrastructure to take network growth into account
- Use of Unique Local Addresses (RFC4193): As in IPv4, there is private address space within IPv6. The main difference is that in IPv4 every organization has the same private address space to choose from. In IPv6 the address space is just for the one network and is globally unique. This private address space can be used to address devices and services that do not need to connect to the Internet.

Prefix Sizing Considerations

The IPv6 specification prescribes a /64 prefix length for the normal IPv6 unicast addresses. Because there is a very large address space available for IPv6, you may want to use a different prefix length than /64.

A prefix length other than a /64 in IPv6 will break the operation of the following technologies:

- Neighbor Discovery (ND)
- Secure Neighbor Discovery (SEND) [RFC3971]
- Privacy extensions [RFC4941]
- Parts of Mobile IPv6 [RFC4866]
- Protocol Independent Multicast - Sparse Mode (PIM-SM) with Embedded-RP [RFC3956]
- Site Multihoming by IPv6 Intermediation (SHIM6) [SHIM6]

The /64 Prefix

The 64-bit prefix should be used for the traditional LAN/WAN interfaces of network devices.

The /126 Prefix

The 126-bit prefix is typically used for point-to-point links similar to the IPv4 address-conservative /30 allocation for point-to-point links. However, the address space in IPv6 is significantly larger than the IPv4 address space. The general recommendation is to use /64 on point-to-point links.

The /127 Prefix

Using the /127 prefix, the equivalent of the IPv4 /31 on point-to-point links (RFC 3021), is considered harmful according to RFC3627. This allocation is just like the /126 allocation for a point-to-point link, but is driven by address conservation. For operational simplicity, consider using the /64 prefix for point-to-point links.

The /128 Prefix

The 128-bit prefix may be used in those situations where one address is required. An example of this type of address is the loopback address of a network device.

IPv6 Address Space Assignments for Internet Connectivity

IPv6 is not very different from IPv4. For an agency to connect to the Internet using IPv6 addresses, it must acquire a block of IPv6 addresses from the routable Internet space. IPv6 address blocks are distributed just as IPv4 blocks are with one exception: IPv6 blocks are either local to a region or global.

Provider-assigned (PA) address space is not portable between service providers and stays in the service provider's region. Service providers may include provider- assigned address space as part of the service. Unless the service itself is multihomed, PA address space is sufficient. If an agency is multihomed, it should procure provider-independent (PI) address space from its Regional Internet Registry. Different registries have different policies and cost structures relating to PI address space.

IPv6 Transition Technologies

The success of IPv6 originally was thought to depend on the new applications that run over it. However, it is becoming very clear that the exhaustion of IPv4 will ultimately end up being the driver for IPv6 adoption. A key part of any good IPv6 design is its ability to integrate into and coexist with existing IPv4 networks. IPv4 and IPv6 hosts need to coexist for a substantial length of time during the steady migration from IPv4 to IPv6, and the development of transition strategies, tools, and mechanisms has been part of the basic IPv6 design from the start.

There are three IPv6 transition technologies: dual-stack, tunneling, and translation.

Dual Stack

Dualstack is the basic strategy to use for large agencies that are adopting IPv6. It involves configuring devices to be able to run IPv4 and IPv6 simultaneously. IPv4 communication uses the IPv4 protocol stack, and IPv6 communication uses the IPv6 protocol stack.

Applications choose between using IPv4 or IPv6 based on the response to DNS requests. The application selects the correct address based on the type of IP traffic. Because dual stack allows hosts to simultaneously reach existing IPv4 content and IPv6 content as it becomes available, dual stack offers a very flexible adoption strategy. However, because IPv4 addresses are still required, dual stack is not a long-term solution to address exhaustion.

Dual stack also avoids the need to translate between protocol stacks. Translation is a valid adoption mechanism, but it introduces operational complexity and lower performance. Because a host automatically selects the right transport to use to reach a destination based on DNS information, there should not be a need to translate between an IPv6 host and an IPv4 server.

Tunneling

Tunnels encapsulate IPv6 traffic within IPv4 packets, and are primarily used for communication between IPv6 (or dual-stack) sites or for connection to remote IPv6 networks or hosts over an IPv4 backbone. There are many different tunneling techniques, including 6to4, ISATAP, Teredo, 6PE, 6VPE, and mGRE v6 over v4. Tunnels may be manually configured or automatically configured. Most modern operating systems include support for tunneling in addition to dual stack.

Translation

Address Family Translation (AFT) is the process of translating addresses from one addressfamily to another. During the adoption phase, AFT is primarily used to translate between IPv6 hosts and IPv4 content. AFT may be stateless, where reserved portions of the IPv6 address space are automatically mapped to IPv4, or it may be stateful, with addresses from a configured range used to map packets between address families.

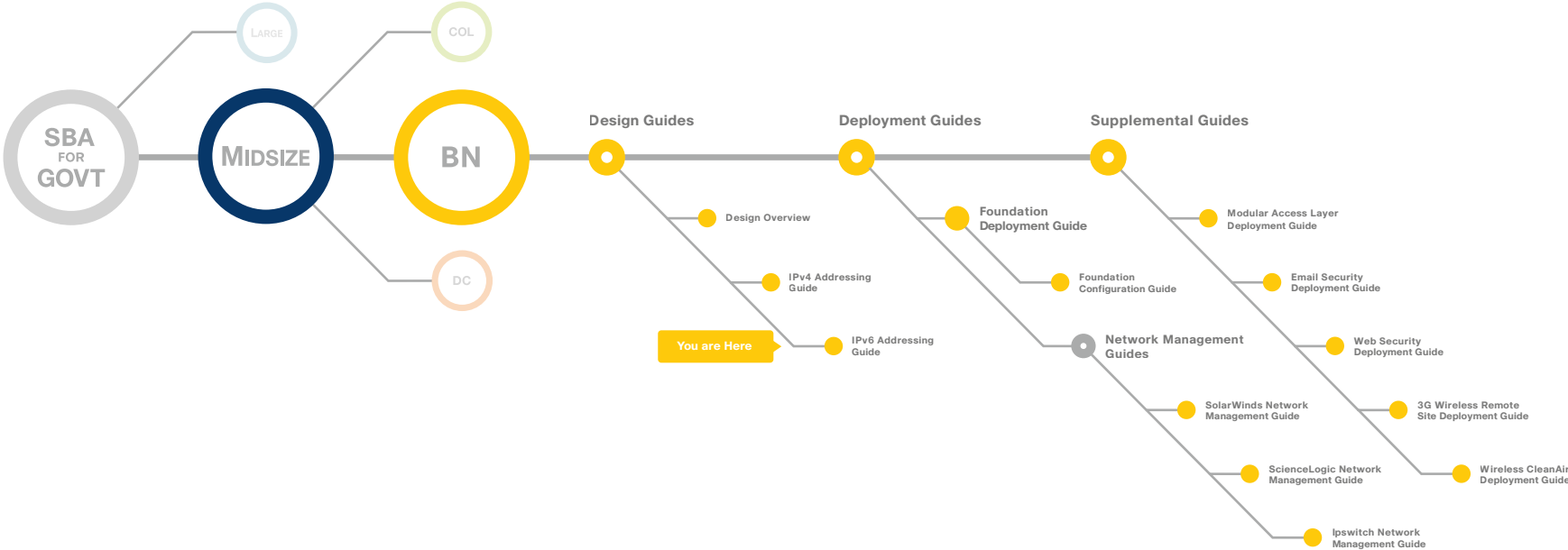
Nearly all enterprise deployments of IPv6 use dualstack internally. Dual stack offers a nondisruptive way to learn about and gain operational experience with a new addressfamily, which is an important part of successfully managing the transition.

Pilots and trials depend on specific requirements. An example strategy is shown below in Figure 6.

Figure 6. Sample Transition Strategies

IP Networks	Transition Strategy
Data Center	AFT for public web presence
Campus	Dual stack
WAN	Site-to-site IPv6 over IPv4 tunnels
Remote access	Host-initiated tunnels

Appendix A: SBA for Midsize Agencies Document System





SMART BUSINESS ARCHITECTURE



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

C07-641125-00 12/10