



Interconnecting IPv6 Domains Using Tunnels

Version History

Version Number	Date	Notes
1	30 July 2002	This document was created.
2	19 May 2003	Updated the related documents section.

This document describes how an enterprise customer can interconnect its existing IPv6 domains by tunneling across the existing IPv4 network infrastructure.

This document is one of a set of documents that support and complement the *IPv6 Deployment Strategies* document, which is available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/ipv6_sol/ipv6dswp.pdf

You should read this document in conjunction with *IPv6 Deployment Strategies* to better understand IPv6 deployment activities.

This document has the following sections:

- [Interconnecting IPv6 Domains Using Tunnels Overview, page 1](#)
- [Implementation, page 3](#)
- [Related Documents, page 16](#)

Interconnecting IPv6 Domains Using Tunnels Overview

A global enterprise wants to interconnect its three existing IPv6 domains. All three domains run native IPv6 and have connectivity to the IPv4 internet. The company wants to interconnect the domains to make available, to all users, various IPv6 services that are not provided within every domain. Such services could include IPv6 web servers, IPv6 Domain Name System (DNS) servers, FTP servers, or TFTP servers. In addition, there might be different host operating systems in use throughout the domains.

The configuration must scale to accommodate any future additional domains while conforming to the company IPv6 policy, with the ultimate goal of migrating the company completely to IPv6.

Because there is no native IPv6 connectivity between the three domains, the company must tunnel its IPv6 traffic over the existing IPv4 internet. The possible tunnel types are as follows:

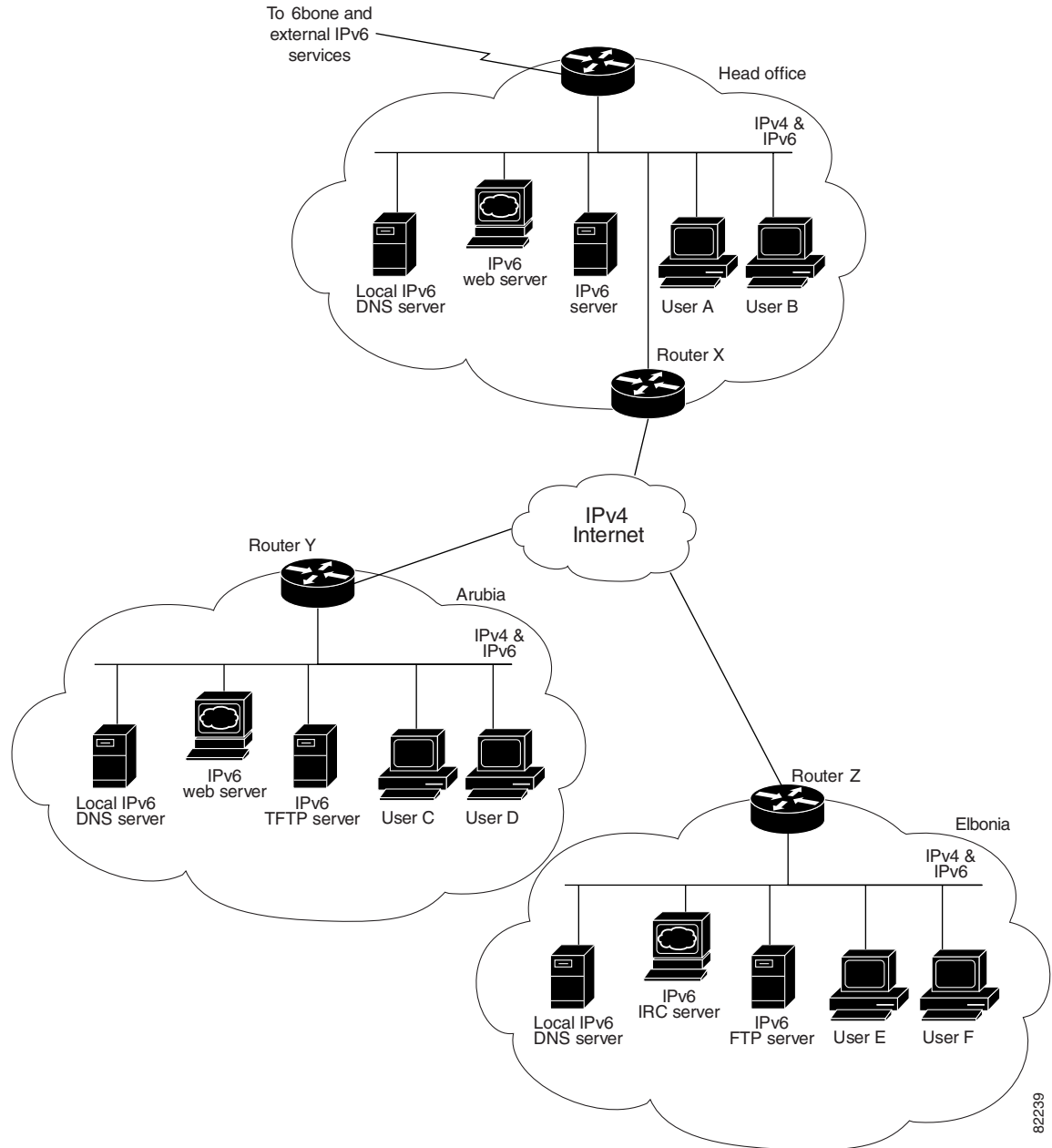
- IPv6 manually configured tunnels
- Automatic 6to4 tunnels

- IPv6 over IPv4 generic routing encapsulation (GRE) tunnels

Initial Network Topology

Figure 1 shows the initial network topology for the enterprise. There are three IPv6 domains with connectivity to the IPv4 Internet.

Figure 1 Initial Network Topology



82239

Implementation

This section describes how you, as an enterprise customer, can use tunnels to interconnect the three IPv6 domains. It contains the following sections:

- [Prerequisites and Design Considerations](#)
- [Implementation Process Steps](#)
- [Configuration Files](#)

Prerequisites and Design Considerations

Before interconnecting the three IPv6 domains by deploying tunnels, you must consider the areas discussed in the following sections:

- [IPv6 Deployment Policy](#)
- [Which Border Routers to Use for Tunneling](#)
- [Routing Protocol](#)
- [Tunnel Type](#)
- [Addressing](#)
- [DNS](#)
- [Network Management](#)

IPv6 Deployment Policy

The company must have a global, uniform policy to define how IPv6 is to be deployed within each domain and between domains. An IPv6 deployment policy will help ensure an orderly transition to IPv6. Some of the areas to include in the IPv6 deployment policy are as follows:

- Host and router upgrades (hardware and software)
- Security and firewall considerations
- Which IPv6 routing protocols to deploy
- IPv6 prefix and address allocation

Which Border Routers to Use for Tunneling

In each domain, you must identify a router that is suitable to function as a border router for the tunnel. The border router candidates must have the following characteristics:

- Can be upgraded (if needed) to a Cisco IOS image that supports IPv6.
- Is capable of running dual stack.
- Has a reliable IPv4 connection to the remote router.

Router X, Router Y, and Router Z were identified as suitable border routers because they were already border routers connecting to the IPv4 Internet, and their software could be upgraded to run IPv6.

Routing Protocol

You must decide which routing protocols to use for IPv6. Consideration should be given to which IPv4 protocols are in use in each of the domains. Depending on previous IPv6 deployment methodology within the domains, the IPv6 routing protocols currently in use in the domains might need to be changed. We recommend that you use the same protocol for IPv6 that is being used for IPv4 because your existing IPv4 connectivity is optimized and assumed to be functioning reliably, and your network managers are already familiar with that protocol.

Tunnel Type

The possible tunnel types are as follows:

- IPv6 manually configured tunnels
- Automatic 6to4 tunnels
- IPv6 over IPv4 GRE tunnels.

The choice of IPv6 tunnel type does not affect the services being used within and between the IPv6 domains.

Manually Configured Tunnels

Manually configured IPv6 tunneling is a technique where an IPv6 address is manually configured on a tunnel interface and IPv4 addresses are manually configured at the tunnel source and the tunnel destination. Manually configured tunnels can be configured between border routers or between a border router and a host, and are generally used for permanent, dedicated connectivity. Because manually configured tunnels require configuration at both ends of the tunnel, they have a somewhat larger management overhead when multiple tunnels are implemented compared to the use of a 6to4 relay service. Because they are configured one-to-one between well-known endpoints, manually configured tunnels make traffic information available for each endpoint, and provide extra security against injected traffic.

Automatic 6to4 Tunnels

6to4 tunneling is a technique where the tunnel endpoint is determined by the globally unique IPv4 address embedded in a 6to4 address. 6to4 tunnels are used for less-permanent, transient connectivity. A 6to4 IPv6 address is a combination of the unique routing prefix 2002::/16 and a globally unique 32-bit IPv4 address. (IPv4-compatible IPv6 addresses are a different format from 6to4 IPv6 addresses. IPv4-compatible IPv6 addresses are not used in 6to4 tunneling.) 6to4 tunnels are configured between border routers, or between a border router and a host. 6to4 tunnels require that a 6to4 relay site be configured to provide a point-to-multipoint 6to4 relay service. The 6to4 relay site will configure a dual-stack border router that will become the endpoint for the 6to4 tunnels. After the 6to4 relay site is set up for 6to4 tunneling, its management burden is minimal. At the other end of the tunnel, a simple router configuration enables access to the relay site through the 6to4 tunnel.

IPv6 over IPv4 GRE Tunnels

IPv6 over IPv4 GRE tunnels use the standard GRE tunneling technique that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme. As in IPv6 manually configured tunnels, GRE tunnels are links between two points, with a separate tunnel for each link. The tunnels are not tied to a specific passenger or transport protocol, but in this case carry IPv6 as the passenger protocol over GRE as the carrier protocol.

The primary use is for stable connections that require regular secure communication between two border routers or between a border router and an end system. The border routers and, in the case described, the end systems must be dual-stack implementations.

If the domain is using the Intermediate System-to-Intermediate System (IS-IS) protocol for internal routing, only GRE tunnels can be used. IS-IS runs over a Layer 2 data link, so tunneling techniques other than GRE cannot be used because IS-IS traffic cannot be distinguished from IPv6 traffic. GRE tunnels allow you to specify IS-IS as a passenger protocol, as you do for IPv6, and thus you can carry both IS-IS and IPv6 traffic at the same time over the same tunnel.

Addressing

You must determine whether internal (private) or globally routable addresses are required. Depending on whether domains are reachable by IPv4 global addresses (via internet), then you need global IPv6 addresses. If the domains are connected by private (corporate) network addresses, then globally routable addresses are not necessary. However, if private IPv4 addresses are being used and the goal is to connect the IPv6 domains to the 6bone or a production IPv6 internet, the IPv4 addressing scheme might need to be renumbered using IPv4 globally routable addresses.



Note

The manner in which IPv6 is deployed within each IPv6 domain must conform to the company IPv6 deployment policy. If the goal is to connect the domains to the 6bone or IPv6 internet, then you must obtain the appropriate IPv6 prefixes from the applicable registry. Arbitrary /48 prefixes could be used to address each IPv6 domain; however, the domains would need to be renumbered when they are opened up to the rest of the company or connected to other IPv6 domains (so that the domains conform to the company IPv6 policy and to international standards), so this approach is not recommended.

Refer to your Regional Internet Registry (RIR) IPv6 allocation policy to obtain IPv6 address space. At this time, the policy is to allocate /35 prefixes, but this policy might change.

DNS

For dual-stack hosts, your selected DNS must provide resolver libraries that can handle IPv6 AAAA resource record types and IPv4 A record types, and must be capable of handling the cases where a query locates both IPv4 and IPv6 resource records. In this case, the DNS resolver library might return the IPv6 address, the IPv4 address, or both addresses to the application. The application then uses the IPv6 protocol or the IPv4 protocol, or makes a choice between the two based on the type of IP traffic and particular requirements of the communication.

IPv6 for Cisco IOS software queries both DNS A and AAAA records over both an IPv4 and IPv6 transport.

Your DNS should be running, or have equivalent capabilities of, Berkeley Internet Name Domain (BIND) version 9. This version provides an implementation of the major components of the DNS (DNS server, DNS resolver library, and verification tools) for IPv6.

Network Management

The current dual-stack implementation in Cisco IOS software permits an interim network management solution, allowing applications such as TFTP, ping, Telnet, traceroute, and Secure Shell (SSH) to be run over either an IPv4 or IPv6 transport.

TFTP file downloading and uploading can be used to save the running configuration of the router to an IPv6 TFTP server. The **ping EXEC** command can accept a destination IPv6 address or IPv6 host name as an argument and send Internet Control Message Protocol version 6 (ICMPv6) echo request messages to the specified destination. The ICMPv6 echo reply messages are reported on the console. Extended ping functionality is also supported in IPv6. The Telnet client and server support IPv6 connections so that you can use Telnet to access the router or initiate Telnet connections from the router. The **traceroute EXEC** command accepts a destination IPv6 address or IPv6 host name as an argument and will generate IPv6 traffic to report each IPv6 hop used to reach the destination address. The Cisco IOS SSH client and server facilitate secure connections between two routers or between a host and a router.

IPv6 network management is covered by a series of Internet-Drafts for IP version-independent MIBs. Cisco plans to support these MIBs. Simple Network Management Protocol (SNMP) over IPv6 is scheduled for the next phase of IPv6 for Cisco IOS software. Cisco will add further applications as required. Network management software, such as HP OpenView or IBM Tivoli NetView, does not support an IPv6 transport either.

Full management of IPv6 networks depends on the IPv6 support within your particular network management system.

Implementation Process Steps

To interconnect the three IPv6 domains with manually configured tunnels, perform the following steps:

1. Obtain an IPv6 prefix allocation for your company from the applicable RIR. For the purposes of this document we assume that you obtained the IPv6 prefix of 2001:xxxx::/35.



Note The 2001:xxxx::/35 and 2001:xxxx::/40 prefixes used in the example configurations in this document are not globally routable and are provided for illustrative purposes only.

2. Allocate IPv6 address prefixes from the RIR allocation to the three domains. The address prefixes were allocated as follows:

Domain	Prefix Allocation
Head Office	2001:xxxx:0100::/40
Arubia	2001:xxxx:0200::/40
Elbonia	2001:xxxx:0300::/40

3. Allocate IPv6 addresses to the nodes in each domain. For example, the Head Office DNS server was allocated the address of 2001:xxxx:0100::2.

4. Configure the router interfaces.

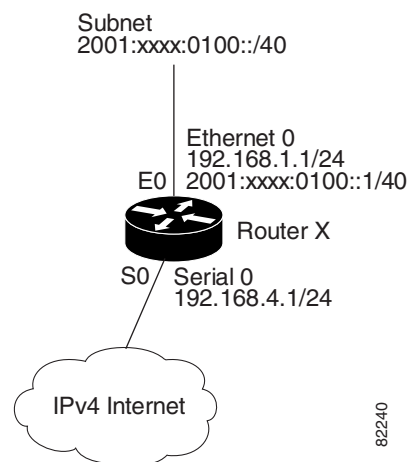
To configure the interfaces for router X, refer to [Figure 2](#) and enter the following commands:

```
ipv6 unicast-routing

interface ethernet 0
  description Connection to Head Office LAN
  ip address 192.168.1.1 255.255.255.0
  ipv6 address 2001:xxxx:0100::1/40

interface serial 0
  description Connection to IPv4 Internet
  ip address 192.168.4.1 255.255.255.0
```

Figure 2 Configured Interfaces on Router X



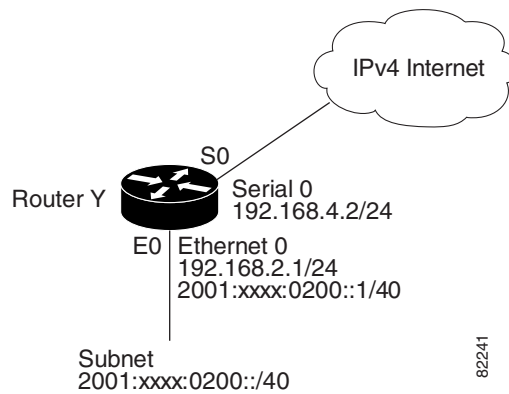
To configure the interfaces for router Y, refer to [Figure 3](#) and enter the following commands:

```
ipv6 unicast-routing

interface ethernet 0
description Connection to Arubia LAN
ip address 192.168.2.1 255.255.255.0
ipv6 address 2001:xxxx:0200::1/40

interface serial 0
description Connection to IPv4 Internet
ip address 192.168.4.2 255.255.255.0
```

Figure 3 Configured Interfaces on Router Y



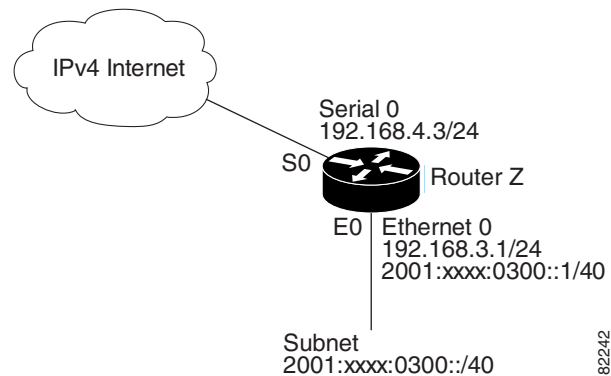
To configure the interfaces for router Z, refer to [Figure 4](#) and enter the following commands:

```
ipv6 unicast-routing

interface ethernet 0
description Connection to Elbonia LAN
ip address 192.168.3.1 255.255.255.0
ipv6 address 2001:xxxx:0300::1/40

interface serial 0
description Connection to IPv4 Internet
ip address 192.168.4.3 255.255.255.0
```

Figure 4 Configured Interfaces on Router Z



5. Choose a suitable tunnel type. Manually configured tunnels were chosen because they provide stable, secure, point-to-point communication between the routers.
6. Configure manually configured tunnels between each domain border router.

To configure a tunnel between Router X and Router Y, refer to [Figure 5](#) and enter the following commands:

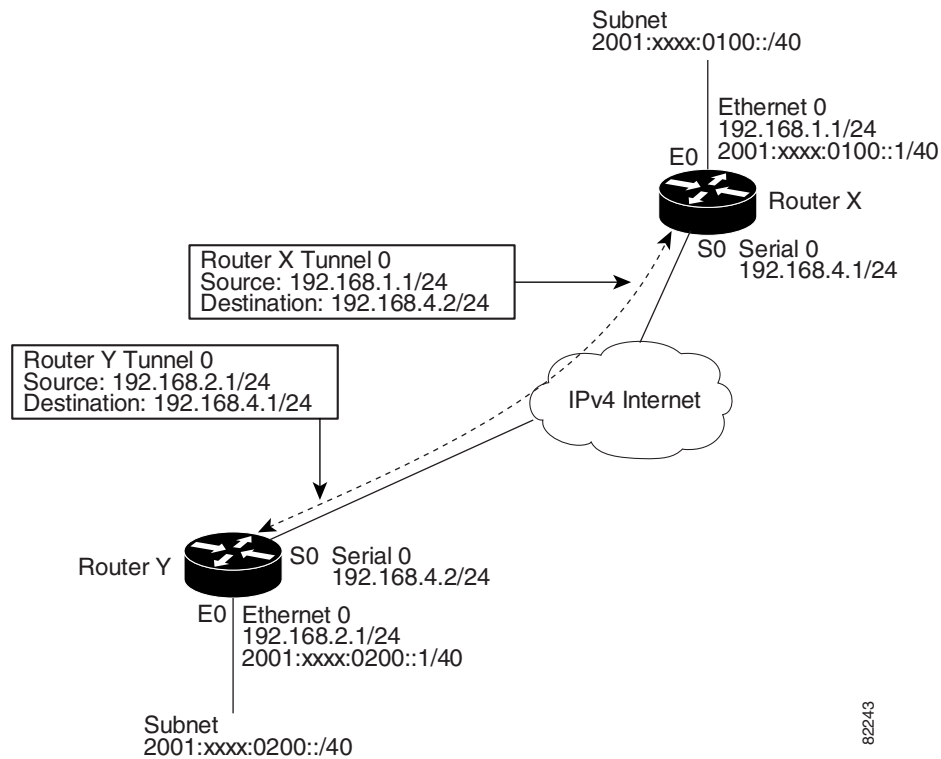
For router X:

```
interface tunnel 0
description Tunnel to Arubia (Router Y)
ipv6 unnumbered ethernet 0
tunnel source ethernet 0
tunnel destination 192.168.4.2
tunnel mode ipv6ip
```

For router Y:

```
interface tunnel 0
description Tunnel to Head Office (Router X)
ipv6 unnumbered ethernet 0
tunnel source ethernet 0
tunnel destination 192.168.4.1
tunnel mode ipv6ip
```

Figure 5 Manually Configured Tunnel Between Router X and Router Y



82243

To configure a tunnel between Router X and Router Z, refer to [Figure 6](#) and enter the following commands:

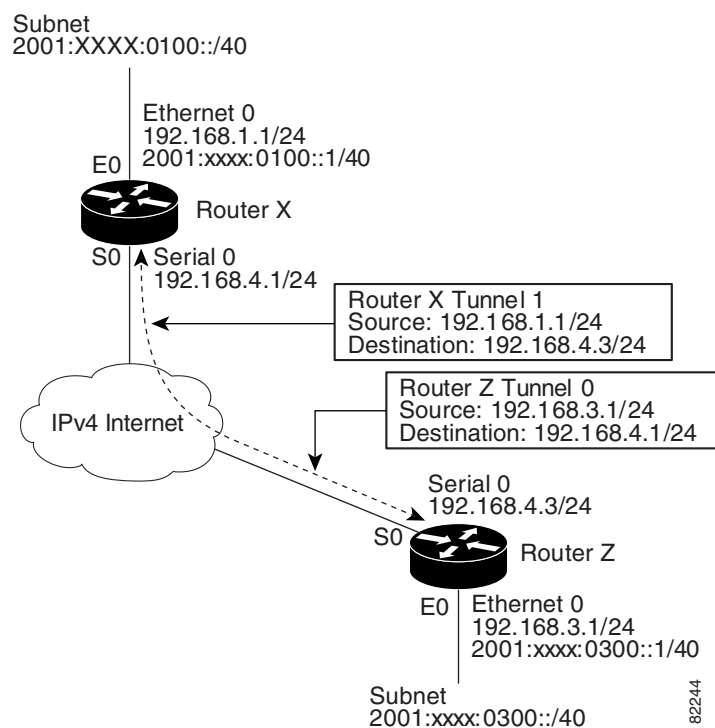
For router X:

```
interface tunnel 1
  description Tunnel to Elbonia (Router Z)
  ipv6 unnumbered ethernet 0
  tunnel source ethernet 0
  tunnel destination 192.168.4.3
  tunnel mode ipv6ip
```

For router Z:

```
interface tunnel 0
  description Tunnel to Head Office (Router X)
  ipv6 unnumbered ethernet 0
  tunnel source ethernet 0
  tunnel destination 192.168.4.1
  tunnel mode ipv6ip
```

Figure 6 Manually configured Tunnel Between Router X and Router Z



To configure a tunnel between Router Y and Router Z, refer to [Figure 7](#) and enter the following commands:

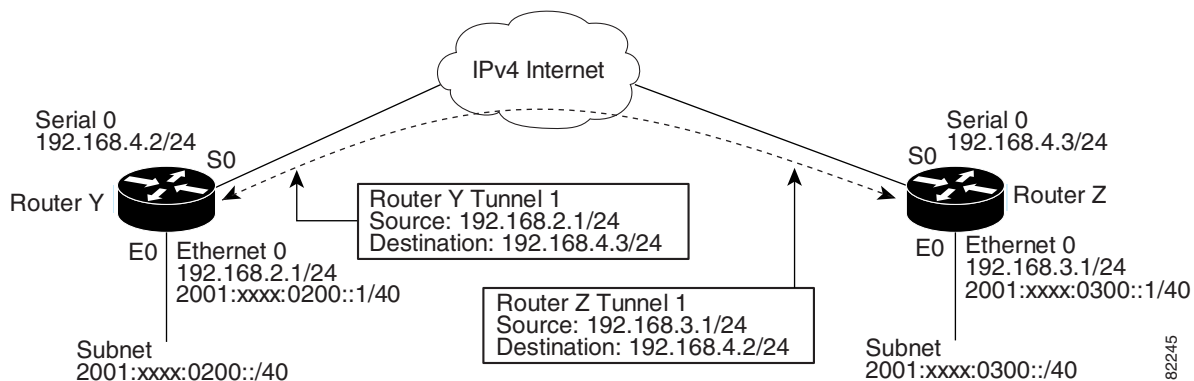
For router Y:

```
interface tunnel 1
  description Tunnel to Elbonia (Router Z)
  ipv6 unnumbered ethernet 0
  tunnel source ethernet 0
  tunnel destination 192.168.4.3
  tunnel mode ipv6ip
```

For router Z:

```
interface tunnel 1
  description Tunnel to Arubia (Router Y)
  ipv6 unnumbered ethernet 0
  tunnel source ethernet 0
  tunnel destination 192.168.4.2
  tunnel mode ipv6ip
```

Figure 7 Manually Configured Tunnel Between Router Y and Router Z



7. Choose a suitable routing protocol. Next Generation Routing Information Protocol (RIPng) is an appropriate interior routing protocol for use with manually configured tunnels.
8. Configure the routing protocols by entering the following commands:

For router X:

```
ipv6 router rip head

interface tunnel 0
  ipv6 rip head enable

interface tunnel 1
  ipv6 rip head enable
```

For router Y:

```
ipv6 router rip arubia

interface tunnel 0
  ipv6 rip arubia enable

interface tunnel 1
  ipv6 rip arubia enable
```

For router Z:

```
ipv6 router rip elbonia

interface tunnel 0
  ipv6 rip elbonia enable

interface tunnel 1
  ipv6 rip elbonia enable
```



Note

This is a very basic configuration. Refer to the *IPv6 for Cisco IOS Software, File 2 of 3: Configuring* publication listed in the [Related Documents](#) section for more-detailed configuration information.

9. Configure the name servers by entering the following commands:

For router X:

```
ip name-server 2001:xxxx:0100::2 !Head Office DNS server
ip name-server 2001:xxxx:0200::2 !Arubia DNS server
ip name-server 2001:xxxx:0300::2 !Elbonia DNS server
```

For router Y:

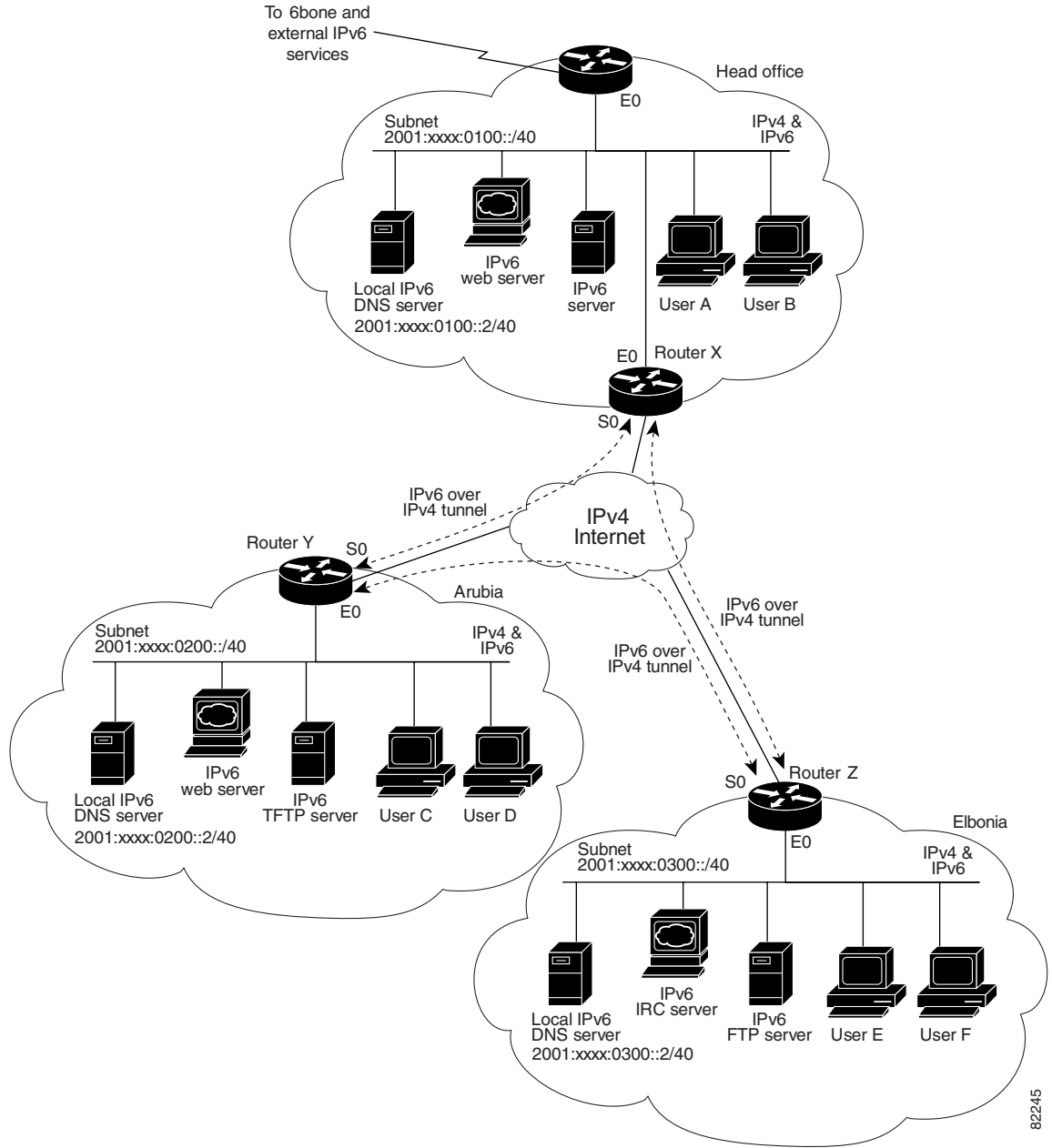
```
ip name-server 2001:xxxx:0200::2 !Arubia DNS server
ip name-server 2001:xxxx:0100::2 !Head Office DNS server
ip name-server 2001:xxxx:0300::2 !Elbonia DNS server
```

For router Z:

```
ip name-server 2001:xxxx:0300::2 !Elbonia DNS server
ip name-server 2001:xxxx:0100::2 !Head Office DNS server
ip name-server 2001:xxxx:0200::2 !Arubia DNS server
```

Figure 8 shows the postimplementation network topology for the enterprise. The three IPv6 domains are interconnected with manually configured tunnels.

Figure 8 Enterprise Network Topology with Interconnected IPv6 Domains



82245

Configuration Files

This section contains the partial configuration files for the border routers in each domain. Only the commands related to the subject of this document are listed.

Head Office Router X

```

ipv6 unicast-routing
!
interface ethernet 0
  description Connection to Head Office LAN
  ip address 192.168.1.1 255.255.255.0
  ipv6 address 2001:xxxx:0100::1/40
!
interface serial 0
  description Connection to IPv4 Internet
  ip address 192.168.4.1 255.255.255.0
!
interface tunnel 0
  description Tunnel to Arubia (Router Y)
  ipv6 unnumbered ethernet 0
  ipv6 rip head enable
  tunnel source ethernet 0
  tunnel destination 192.168.4.2
  tunnel mode ipv6ip
!
interface tunnel 1
  description Tunnel to Elbonia (Router Z)
  ipv6 unnumbered ethernet 0
  ipv6 rip head enable
  tunnel source ethernet 0
  tunnel destination 192.168.4.3
  tunnel mode ipv6ip
!
ipv6 router rip head
!
ip name-server 2001:xxxx:0100::2
ip name-server 2001:xxxx:0200::2
ip name-server 2001:xxxx:0300::2

```

Arubia Router Y

```

ipv6 unicast-routing
!
interface ethernet 0
  description Connection to Arubia LAN
  ip address 192.168.2.1 255.255.255.0
  ipv6 address 2001:xxxx:0200::1/40
!
interface serial 0
  description Connection to IPv4 Internet
  ip address 192.168.4.2 255.255.255.0
!
interface tunnel 0
  description Tunnel to Head Office (Router X)
  ipv6 unnumbered ethernet 0
  ipv6 rip arubia enable
  tunnel source ethernet 0
  tunnel destination 192.168.4.1
  tunnel mode ipv6ip
!
!

```

```

interface tunnel 1
  description Tunnel to Elbonia (Router Z)
  ipv6 unnumbered ethernet 0
  ipv6 rip arubia enable
  tunnel source ethernet 0
  tunnel destination 192.168.4.3
  tunnel mode ipv6ip
!
ipv6 router rip arubia
!
ip name-server 2001:xxxx:0200::2
ip name-server 2001:xxxx:0100::2
ip name-server 2001:xxxx:0300::2

```

Elbonia Router Z

```

ipv6 unicast-routing
!
interface ethernet 0
  description Connection to Elbonia LAN
  ip address 192.168.3.1 255.255.255.0
  ipv6 address 2001:xxxx:0300::1/40
!
interface serial 0
  description Connection to IPv4 Internet
  ip address 192.168.4.3 255.255.255.0
!
interface tunnel 0
  description Tunnel to Head Office (Router X)
  ipv6 unnumbered ethernet 0
  ipv6 rip elbonia enable
  tunnel source ethernet 0
  tunnel destination 192.168.4.1
  tunnel mode ipv6ip
!
interface tunnel 1
  description Tunnel to Arubia (Router Y)
  ipv6 unnumbered ethernet 0
  ipv6 rip elbonia enable
  tunnel source ethernet 0
  tunnel destination 192.168.4.2
  tunnel mode ipv6ip
!
ipv6 router rip elbonia
!
ip name-server 2001:xxxx:0300::2
ip name-server 2001:xxxx:0100::2
ip name-server 2001:xxxx:0200::2

```

Related Documents

Refer to the following documents for additional information about IPv6 for Cisco IOS software:

- *IPv6 Deployment Strategies*
- *IPv6: Connecting to the 6bone Using Manually Configured Tunnels*
- *IPv6: Connecting to the 6bone Using 6to4 Tunnels*
- *IPv6: Providing IPv6 Services over an IPv4 Backbone Using Tunnels*
- *Start Here: Cisco IOS Software Release Specifics for IPv6 Features*

- *Implementing IPv6 for Cisco IOS Software*
- *IPv6 for Cisco IOS Software Command Reference*

Refer to the following website on Cisco.com for more information on the Cisco implementation of IPv6:

<http://www.cisco.com/ipv6>

