Cisco Network Solutions for the Telco DCN: SONET/SDH OSI Environments

This document is directed to competitive local exchange carriers (CLECs), incumbent local exchange carriers (ILECs), and Post, Telephone and Telegraphs (PTTs), collectively referred to as *telcos* (short for telephone companies). This document describes Cisco network solutions for transporting data between Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH) and the Operations Support System (OSS) in a telco data communications network (DCN).

The DCN transports network management traffic between network elements and their respective OSS, making them a vital link between the service network and the network operations center (NOC). The solutions presented in this document will help telcos connect their SONET/SDH network elements to a router-based network using the Open System Interconnection (OSI) protocol, which simplifies the DCN and reduces equipment costs.

Version History

Version Number	Date	Notes
1	April 28, 2004	This document was created as a joint effort between Don Schriner in the Cisco CTO Consulting Engineering Group and Alliene Turner in Cisco IOS Documentation.
2	May 6, 2005	This document was updated.
3	November 5, 2012	This document was updated.

Contents

The document presents the recommended Cisco architecture for building the OSI network. Several methods for implementing and scaling an OSI network are included with detailed configuration examples. Specific Cisco IOS software features such as Intermediate System-to-Intermediate System (IS-IS) multiareas, VLAN support for International Standards Organization Connectionless Network Service (ISO CLNS), Target Identifier Address Resolution Protocol (TARP), and IS-IS attach bit control are described. These architectures and software features are described in the following main sections:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites

The features described in this document are supported on the Cisco Telco and Enterprise feature sets.

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator at http://www.cisco.com/go/fn.

To access Cisco Feature Navigator, you must have an account on Cisco.com. Qualified users can establish an account on Cisco.com by following the directions at http://www.cisco.com/register. If you have an account but have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you.

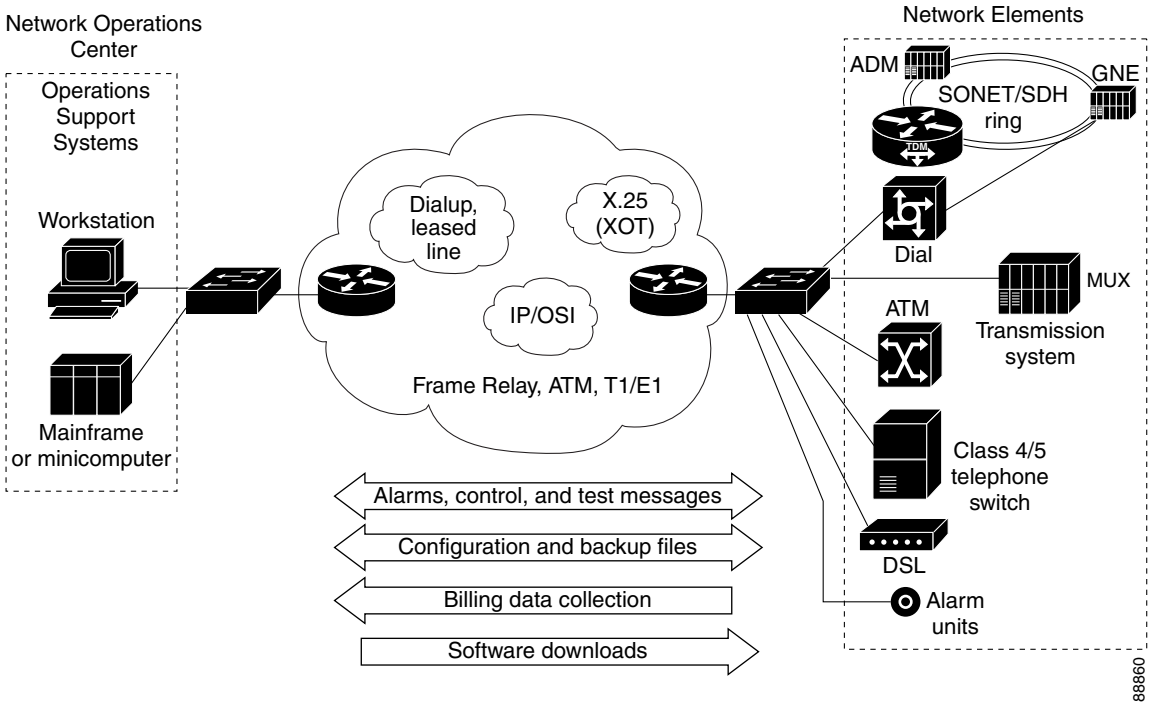
Scaling SONET/SDH in the Telco DCN: Overview

SONET/SDH has become the transport technology of choice for regional Bell operating companies (RBOCs), inter-exchange carriers (IXCs), Post, Telephone, and Telegraph (PTT) organizations, and other carriers to meet the demand for bandwidth and new services. The growth of SONET/SDH and the increasing demands for both existing time-division multiplexing (TDM) and new packet-based data services necessitate better and more scalable DCNs for network operations and management connectivity between network elements and their respective OSSs. As SONET/SDH rings grow in both size and number, the service provider needs to deploy higher bandwidth and more scalable DCN networks to manage SONET/SDH network elements.

RBOCs, Inter-exchange carriers (IXCs), PTTs, and their vendors have worked with standards bodies to define more powerful management networks for SONET/SDH. These standards documents recommend that OSI-based protocols be used by the SONET/SDH network elements' ring network management.

While IP and OSI protocols are being widely adopted and deployed by RBOCs and PTTs within their DCNs, it is not realistic to replace their vast installed infrastructure of overlay networks that support legacy DCN protocols. To streamline operations and stay competitive, telcos must reduce the number of overlay DCNs they currently have deployed to support various legacy protocols. The new DCNs must support both legacy protocols, which will continue to be in use for the foreseeable future, and the new standards-based protocols. The challenge is to provide this support over a common infrastructure and create a seamless *network of networks* that can manage the network through a single DCN utility. Figure 1 shows a typical DCN network.

Figure 1 Typical DCN Network Elements



Multiple networks are included in the DCN network cloud. The networks serve to connect a mainframe or minicomputer and workstation configured as an OSS at a NOC to a large array of devices and systems referred to as network elements.

Network elements in a DCN include alarm units, telephone switches such as the Lucent 5ESS, SONET/SDH add-drop multiplexers (ADMs) and optical repeaters, voice switches, digital cross-connect systems, Frame Relay or ATM switches, routers, digital subscriber line access multiplexers (DSLAMs), remote access switches, digital loop transmission systems, and so on, that make up the provisioned services infrastructure used to deliver services to customers.

The OSS controls and stores the network management data collected about and from the various network elements.

DCNs are the networks deployed by a telco or service provider that contain all the cabling, network management (NM) stations, switches, network elements and other necessary equipment for delivering and managing services to the service providers' customers (see Figure 1). The DCN is an out-of-band network; that is, it does not transit the same bandwidth segment used by services such as voice and its associated in-band signaling. It does, however, share the same transport equipment and interfaces with switching equipment considered to be the infrastructure of the public switched telephone network (PSTN). This document focuses on a design architecture and Cisco IOS software features for scaling the OSI DCNs.

In addition to the need for scalability, there are other factors driving change in the traditional DCN that is providing operations support for today's TDM-based services.

These factors are:

- The use of IP and OSI-based intranets within the central office to facilitate communication between network elements and management stations (collectively, the OSS) is increasing.
- "Intelligent" (feature-rich) network elements are requiring more frequent software version updates than their less feature-rich predecessors.

- Software downloads to intelligent network elements across the management network—some many megabytes in size—are increasing bandwidth requirements.
- More and more network elements and OSSs are upgrading to support Ethernet interfaces.
- As competition offers more alternatives, upgraded DCNs are offering the ability to remotely turn up services faster as demanded by their customers.

OSI as a DCN Transport Mechanism

With the advent of SONET/SDH networks, service providers and their equipment vendors foresaw the need for new, more powerful service delivery support networks to manage today's optical networks. In 1988, the International Telecommunication Union (ITU) adopted the M.30 recommendation, which was revised in 1992 and again in 1996, and today is known as recommendation M.3010, *Principles for a Telecommunications Management Network*.

Recommendation M.3010 defines the architectural requirements for a Telecommunications Management Network (TMN) to support management network operators in planning, provisioning, installing, maintaining, operating, and administering telecommunications networks and services. Within that document, the ITU describes the DCN, which provides the communications backbone between network elements and OSSs in the PSTN.

Using the DCN concepts outlined in M.3010, in December 1995 Bellcore developed an industry standard for SONET—GR-253-CORE—that includes generic DCN requirements. GR253-CORE has become the standard for DCNs within the United States. These standards recommend that OSI-based protocols be used by the OSSs for SONET/SDH ring network management.

As a result of the GR253 and M.3010 standards, SONET/SDH vendors worldwide use the seven-layer OSI protocol stack for the management of their equipment. One application protocol that rides on Layer 7 of the OSI protocol stack, for example, is Transaction Language 1 (TL1). TL1 provides for the definition of messages and protocols between network elements and management stations, and facilitates the gathering of data from SONET equipment.

As SONET/SDH rings grow in both size and number, telcos must deploy higher bandwidth and more scalable DCN networks to manage SONET/SDH network elements. This growth necessitates a migration of DCNs from X.25 networks running from 9.6 kbps to 56 kbps to intranets running at 1.544 Mbps or higher. Both synchronous and asynchronous interfaces are migrating to Ethernet interfaces running at 10 Mbps on network elements and OSSs.

OSI protocol stacks used in SONET/SDH network elements for management require that the DCN be able to use OSI to route to and from the network element and its associated OSS, in addition to the higher bandwidth requirements. A typical RBOC, for example, may have already deployed several thousand SONET rings and is rapidly adding new rings by the hundreds or thousands annually. This large number of SONET network elements demands a DCN that can scale.

IP Standards Development for the DCC and the DCN

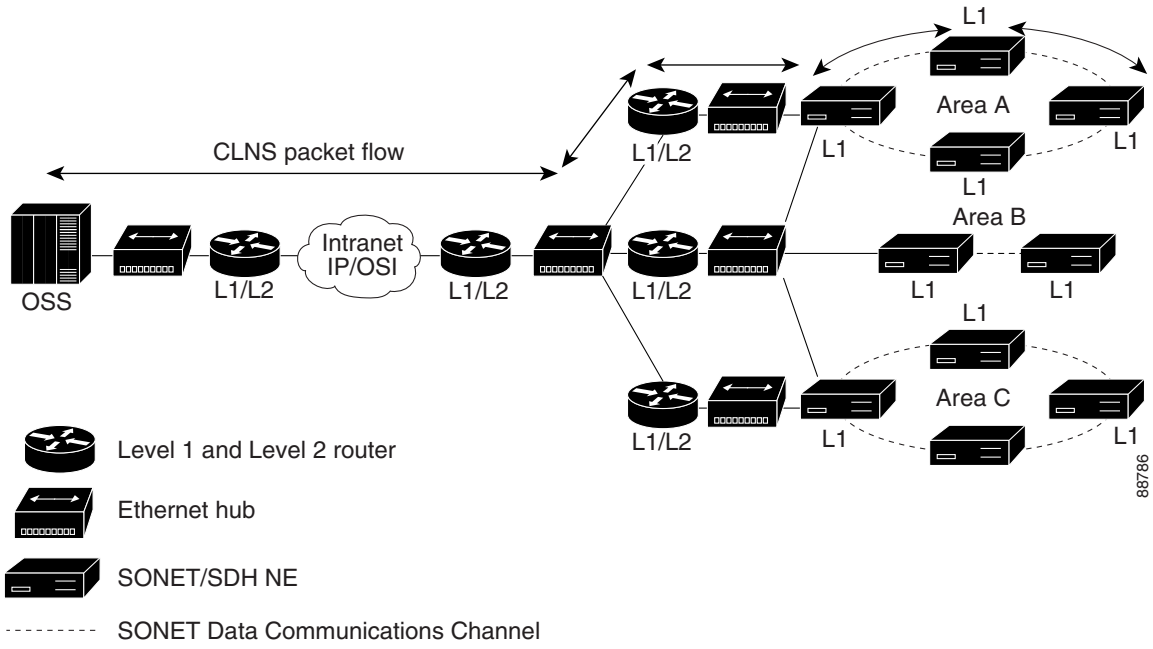
The ITU-T has developed a new standard outlining architecture requirements for IP-only domains, OSI-only domains, and IP and OSI domains titled *Architecture and Specification of the Data Communication Network*, document number G.7712/Y.1703. Basically, the standard adds IP to the DCN and the data communications channel (DCC) architectures. The premise of the standard is that SONET/SDH network elements will still act as routers to forward management traffic across the DCC. In OSI environments, IS-IS is the routing protocol of choice. In mixed environments, Integrated IS-IS is the routing protocol of choice. In IP-only environments, the routing protocol can be either Open Shortest

Path First (OSPF) or Integrated IS-IS. The ITU-T document also describes manual tunneling mechanisms for bridging IP-only or for CLNS-only involvements; however, this document focuses on only OSI solutions for SONET/SDH.

DCN Design Considerations for OSI

The current Bellcore and ITU standards recommend the use of the OSI protocol stack for the management of SONET/SDH network elements. Figure 2 shows the packet flow from the OSS to a SONET network element. The packet leaves the OSS and is routed across the DCN by routers to the gateway network element (GNE). The GNE routes the packet from the Ethernet network onto the SONET DCC. The packet is routed around the ring. The SONET network element is acting as an IS-IS router. The SONET DCC is the physical path. The SONET network element and GNE are IS-IS Level 1 routers. The standalone routers in the DCN perform the IS-IS Level 2 function. Notice that the DCC has become part of the DCN. The performance of the DCN is determined by all of the components.

Figure 2 Packet Flow in a DCN Network



Fundamental issues to address in designing a DCN today are the routing performance of the IS-IS routers and the bandwidth on the DCC. When designing the DCN network, the service provider must take into account the performance characteristic of all the routers, including the routing engine in the network element. Today, the routing engine in the network elements (NEs) can typically support a routing table of only 50 to 100 entries, so this limitation binds the Level 1 area size to 50 to 100 routers. The section DCC is used for management. The bandwidth of the section DCC is 192 KB. The D1 through D3 bytes of the section overhead DCC are used. A packet should not have to make more than seven hops on the DCC to enter the DCN because of bandwidth limitations and the performance of the router in the network element. As the size of the ring approaches 16 nodes, a second GNE must be added to the ring.

The first step for designing a DCN network is to gather information about a particular network environment. The natural geographic groupings of rings should be identified and a breakdown of the average central office size should be computed. This information is required for planning the OSI-based DCN.

Following are the questions that need to be answered before the design process is begun:

- What is the number of SONET nodes in the network today?
- What is the growth rate (number of nodes added per year) of the SONET/SDH network?
- What is the size of the Level 1 OSI area that the routing engine can support? In other words, how many Level 1 routers can be in an area?
- What is the size of the OSI domain that the Level 2 routing engine can support?
- How many network elements does the service provider want to place in an area to start with? Does the service provider want to leave room for growth within an area?
- How many central offices does the service provider have in the DCN?
- Does the service provider want to support a single GNE or dual GNEs?
- What is the average ring size?
- How many rings can be aggregated into a single area?
- How many SONET rings are in a large-sized central office?
- How many SONET rings are in a medium-sized central office?
- How many SONET rings are in a small-sized central office?

DCN Design with a Classic OSI Implementation

This document reviews a classic OSI design, and then reviews an improved design using multiareas. For purpose of example, answers to questions from a hypothetical large-sized service provider network are provided. This information is needed to design a network based on the three-tiered architecture.

- What is the number of SONET nodes in the network today?

  There are 25,000 SONET/SDH nodes deployed today.

- What is the growth rate (number of nodes added per year) of the SONET/SDH network?

  There are 4000 SONET/SDH nodes added per year.

- What is the size of the Level 1 OSI area that the routing engine can support? In other words, how many Level 1 routers can be in an area?

  The Level 1 area size is 50 routers.

- What is the size of the OSI domain that the Level 2 routing engine can support?

  The domain size is 500 Level 2 routers.

- How many network elements does the service provider want to place in an area to start with? Does the service provider want to leave room for growth within an area?

  The service provider wants to place 30 network elements in an area and leave address space for 20 additional network elements in an area.

- How many central offices does the service provider have in the DCN?

  There are 1700 central offices in the network.

- Does the service provider want to support a single GNE or dual GNEs?

  Most of the rings have a single GNE. The design will assume a single GNE per ring.

- What is the average ring size?

  Average ring size is ten.

- How many rings can be aggregated into a single area?

  A maximum of three SONET/SDH rings will be placed in an area.
- How many SONET rings are in a large-sized central office?

  The large-sized central office will have 36 SONET rings.
- How many SONET rings are in a medium-sized central office?

  The medium-sized central office will have ten SONET rings.
- How many SONET rings are in a small-sized central office?

  The small-sized central office will have one SONET ring.

To begin the network design, place the central offices in geographic areas. In this network design, there are five geographic areas. Within each geographic area, the service provider can determine the actual number of large-, medium-, and small-sized central offices. This network design example will use the following rules:

- A small-sized central office has 1 ring, a medium-sized central office has up to 10 rings, and a large-sized central office has up to 12 rings.
- The service provider has estimated the percentage of large-sized central offices to be 10 percent, medium-sized central offices to be 40 percent, and small-sized central offices to be 50 percent.
- Medium- and large-sized central offices will have redundant routers and redundant WAN links. Small central offices will have a single router and redundant WAN links.

An alternative to estimating the percentage of small-, medium- and large-sized central offices is for the service provider to count the number of central offices. Table 1 lists the central office breakdown by geographic area using the estimated percentages.

Table 1 Central Office Breakdown by Geographic Area

Geographic Location	Small-Sized Central Offices	Medium-Sized Central Offices	Large-Sized Central Offices	Total Number of Central Offices
Group 1	150	75	25	250
Group 2	300	150	50	500
Group 3	120	60	20	200
Group 4	360	180	60	600
Group 5	90	45	15	150
Totals	1020	510	170	1700

Next, determine the number of Level 2 routers required in each geographic area. Today in small-sized central offices, the service provider in the classic implementation of this network design would typically not have any SONET rings. The network design allows for one ring per office eventually, for growth. Because of the performance limitations of the SONET/SDH network elements, the design calls for many small areas. Remember that the network element routing engine can support only 50 entries in its routing table. Each area requires a Level 2 router, so the logical place for the Level 2 function to be performed is on a standalone router in each central office.

Placing the Level 2 function on the GNE will constrain the size of the routing domain because of performance limitations of the IS-IS routing engine in the GNE. The network design calls for every central office to have at least one OSI area. In this network, large-sized central offices have 36 rings, which equates to 12 Level 2 routers. Also remember that the design criteria questions indicated the

average ring size to be ten network elements, and that three rings should be placed in an area. This design will leave address space in an area to add network elements when the rings grow. The computation for the network design is as follows:

36 rings ÷ 3 rings per area = 12 Level 1 areas

The 36 SONET rings in a large-sized central office are split among 12 Level 1 areas. For every Level 1 area, a connection to the backbone is made through a standalone Level 1/Level 2 router, so 12 standalone routers are needed.

The medium-sized office has ten SONET/SDH rings per office. The new network design calls for three rings per OSI area. The computation for the network design is as follows:

10 rings ÷ 3 rings per area = 4 Level 1 areas (rounded up)

The small-sized central office has at most one SONET ring and requires one router per central office. Given these design parameters, the number of standalone routers that will be required are listed in Table 2.

Table 2 Standalone Router Requirements

Geographic Location	Total Number of Offices	Level 2 Small-Sized	Level 2 Medium-Sized	Level 2 Large-Sized	Level 2 Total	Total Number of Domains
Group 1	250	150	300	300	750	2
Group 2	500	300	600	600	1500	4
Group 3	200	120	240	240	600	2
Group 4	600	360	720	720	1800	4
Group 5	150	90	180	180	450	1
—	—	—	—	—	5100	13

To show how the numbers in Table 2 were derived from Table 1, look at Group 1: There are 150 small-sized central offices and one Level 1/Level 2 router per central office. In all, there are 150 Level 2 routers to support small-sized central offices for Group 1, as the following computation indicates:

Group 1 small-sized central offices:

150 small-sized central offices x 1 router per central office = 150 Level 2 routers

There are 75 medium-sized central offices in Group 1. Each medium-sized central office requires four Level 1/Level 2 routers as previously computed, so the total number of Level 1/ Level 2 routers for medium-sized central offices is as defined in the following equation:

Group 1 medium-sized central offices:

75 medium-sized central offices x 4 routers per central office = 300 Level 2 routers

There are 25 large-sized central offices in Group 1. A large-sized central office requires 12 Level 1/Level 2 routers, as computed in the first equation following Table 1. The following computation indicates the total number of Level 1/Level 2 routers required:

Group 1 large-sized central offices:

25 large-sized central offices x 12 routers per central office = 300 Level 2 routers

In Table 2, the number of standalone Level 2 routers is 5,100. The total number of domains for each group was computed as follows: The number of Level 2 routers in a group was divided by the domain size. The domain size was determined by the routing engine performance of the standalone router. In this design, the domain size is 500, and there would be a total of 13 domains for the network.

A number of obvious issues come up with this example: It is necessary to purchase a large number of standalone routers to provide the Level 2 functions. All of the routers must be monitored and maintained by a NOC. A method of routing between OSI domains is required, and either an interdomain routing protocol or static routes must be used.

IS-IS Multiarea DCN Architecture with SONET/SDH Deployment in All Central Offices

Now let us design the network using the Cisco IOS software IS-IS multiarea feature. Service providers deploying SDH rings today typically are managing all of their rings with OSI, and their network design option assumes that at least one OSI area should be supported in every central office, and that a Level 2 router is placed in every central office.

The following are the key assumptions for this network design:

- What is the number of SONET nodes in the network today?

  There are 25,000 SONET/SDH nodes deployed today.
- What is the growth rate (number of nodes added per year) of the SONET/SDH network?

  There are 4000 SONET/SDH nodes added per year.
- What is the size of the Level 1 OSI area that the routing engine can support? In other words, how many Level 1 routers can be in an area?

  The Level 1 area size is 50 routers.
- What is the size of the OSI domain that the Level 2 routing engine can support?

  The domain size is 500 Level 2 routers.
- How many network elements does the service provider want to place in an area to start with? Does the service provider want to leave room for growth within an area?

  The customer wants to place 30 network elements in an area and leave address space for 20 additional network elements in an area.
- How many central offices does the service provider have in the DCN?

  There are 1700 central offices in the network.
- Does the service provider want to support a single GNE or dual GNEs?

  Most of the rings have a single GNE.
- What is the average ring size?

  Average ring size is ten.
- How many rings can be aggregated into a single area?

  Three SONET/SDH rings per area 3 are required.
- How many SONET rings are in a large-sized central office?

  The large-sized central office will have 36 SONET rings.
- How many SONET rings are in a medium-sized central office?

The medium-sized central office will have ten SONET rings.

- How many SONET rings are in a small-sized central office?

  The small-sized central office will have one SONET ring.

There are five geographic areas, and within each geographic area the actual number of large-, medium-, and small-sized central offices must be determined. The central office size can be allocated as follows: 10 percent large-sized, 30 percent medium-sized, and 60 percent small-sized. Table 1 will be used again to represent the numbers of central offices per geographic area. The number of rings terminating in a differently sized central office can be as follows: A small-sized central office can have 1, a medium-sized central office can have 10, and a large-sized central office can have 36 rings. Small-sized central offices would have one SONET/SDH ring. Each central office will have at least one OSI area.

The next step is to compute the number of Level 2 routers required to implement the design. The design will use Cisco 3621 routers in small-sized central offices, which can support up to twelve Level 1 OSI areas. The assumption is that there will be only one OSI area per small-sized central office, and one Cisco 3621 router will be sufficient per small-sized central office. The Cisco 3631 router has two network modules that can be used for contact closure and serial connectivity.

Next, compute the number of small-sized routers for each group. In Group 1, there are 150 small-sized central offices and there is one Level 1/Level 2 router per central office. There are 150 Level 2 routers to support small-sized central offices for Group 1. The computations follow the totals that are listed in Table 3.

Table 3 Level 2 Router Requirements

Geographic Location	Total Number of Offices	Level 2 Small-Sized	Level 2 Medium-Sized	Level 2 Large-Sized	Level 2 Total	Total Number of Domains
Group 1	250	150	150	50	350	1
Group 2	500	300	300	100	700	2
Group 3	200	120	120	40	280	1
Group 4	600	360	360	120	840	2
Group 5	150	90	90	30	210	1
—	1700	—	—	—	2380	7

As Table 3 indicates, the number of Level 2 routers has still been substantially reduced over the classic DCN design. Use the following computations to understand how the reductions were made:

Group 1 small-sized central office:

150 small-sized central offices x 1 router per central office = 150 Level 2 routers

Group 2 small-sized central offices:

300 small-sized central offices x 1 router per central office = 300 Level 2 routers

Group 3 small-sized central offices:

120 small-sized central offices x 1 router per central office = 120 Level 2 routers

Group 4 small-sized central offices:

360 small-sized central offices x 1 router per central office = 360 Level 2 routers

Group 5 small-sized central offices:

90 small-sized central offices x 1 router per central office = 90 Level 2 routers

Next, compute the number of routers required for the medium-sized central offices. The network design uses Cisco 3631-DC-central office or Cisco 3662-DC-central office routers. Both of these routers support 12 Level 1 OSI areas with the IS-IS multiarea software. This design calls for ten OSI rings per central office. The original network design called for four Level 1 areas:

10 rings ÷ 3 rings per area = 4 Level 1 areas (rounded up)

One Cisco 3631 or Cisco 3662 router running the IS-IS multiarea software will support a medium-sized central office. The design calls for redundant IS-IS Level 1/Level 2 routers for medium- and large-sized offices. There are 75 medium-sized central offices in Group 1. Each medium-sized central office requires one Level 1/Level 2 router as previously computed, and a second router for backup. The total number of Level 1/ Level 2 routers for medium-sized central offices is as follows (see Table 3):

Group 1 medium-sized central offices:

75 medium-sized central offices x 2 routers per central office = 150 Level 2 routers

Group 2 medium-sized central offices:

150 medium-sized central offices x 2 routers per central office = 300 Level 2 routers

Group 3 medium-sized central offices:

60 medium-sized central offices x 2 routers per central office = 120 Level 2 routers

Group 4 medium-sized central offices:

180 medium-sized central offices x 2 routers per central office = 360 Level 2 routers

Group 5 medium-sized central offices:

45 medium-sized central offices x 2 routers per central office = 90 Level 2 routers

The computation of the large-sized central office numbers for Table 3 is the same process as previously outlined for the medium-sized central offices. (See Table 1 for the number of central offices.) The design uses Cisco 3631-DC-central office or Cisco 3662-DC-central office routers. Both of these routers support 12 Level 1 OSI areas with the IS-IS multiarea software. The design calls for 36 OSI rings per central office, as defined in the original network design computation:

36 rings ÷ 3 rings per area = 12 Level 1 areas

One Cisco 3631 or Cisco 3662 router running the IS-IS multiarea software will support a large-sized central office. The design calls for redundant IS-IS Level 1/Level 2 routers for medium- and large-sized offices. A second router will be placed in every large-sized office. There are 25 large-sized central offices in Group 1. The total number of Level 1/ Level 2 routers for large-sized central offices is as follows:

Group 1 large-sized central offices:

25 large-sized central offices x 2 routers per central office = 50 Level 2 routers.

The following examples show the remainder of the group's computations:

Group 2 large-sized central offices:

50 large-sized central offices x 2 routers per central office = 100 Level 2 routers.

Group 3 large-sized central offices:

20 large-sized central offices x 2 routers per central office = 40 Level 2 routers

Group 4 large-sized central offices:

60 large-sized central offices x 2 routers per central office = 120 Level 2 routers

Group 5 large-sized central offices:

15 large-sized central offices x 2 routers per central office = 30 Level 2 routers

The total number of Level 2 routers is listed in Table 3.

The network is divided into five geographic areas, and each geographic area is a logical grouping of central offices. The logical central office grouping will make up an OSI domain. (In IS-IS, a domain is a logical set of networks, unlike Internet domains that are general groupings of networks based on organization type or geography.) In this design, the performance characteristics of Level 2 routers allow the OSI domain to grow to 500 standalone routers. The domain size assumes that the routers have at least the performance capability of a Cisco 3662 or 3631 router. In Table 3, the number of Level 2 routers in Groups 2 and 4 exceeds 500, so these groups are split into two domains. A domain is made up of standalone access routers and standalone distribution routers; see Figure 3 and the next section.

The Cisco Three-Tiered DCN Network Architecture

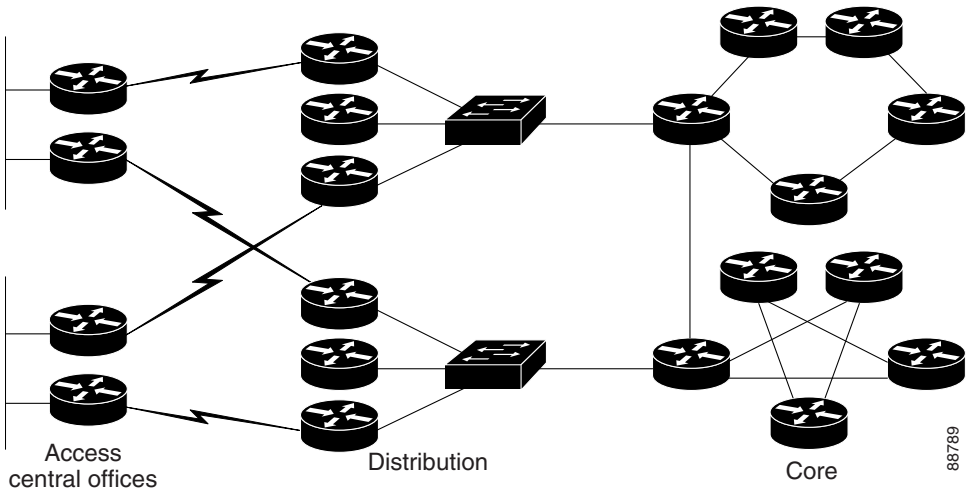
Service providers need a basic architecture for the DCN network. The recommended architecture is a three-tiered design. This design is described in the following sections:

Three-Tiered DCN Network Overview

A three-tiered DCN architecture design will ensure manageable and scalable networks with the ability to easily add network equipment with new features and new services as needed. At the core of the DCN are multiprotocol routers capable of transporting IP, OSI, and X.25.

A three-tiered architecture solution as shown in Figure 3 consists of core, distribution, and access elements. A backbone contains routers or WAN switches that form a core or transport utility. Switching centers equipped with distribution routers are located around the backbone to provide symmetric connectivity to central offices. At each central office, access routers provide connectivity into their respective switching and distribution center. Reliability is built into the DCN by designing in redundancy at each tier of the architecture. The access layer defines the DCN interface to the network elements located within the central office. The access routers are configured as Level 1/Level 2. The core and distribution routers are configured as Level 1/Level 2 or Level 2.

Figure 3 DCN Three-Tiered Architecture



The IS-IS routing protocol is run within the OSI domains. Static routes or an interdomain routing protocol can be run between the OSI domains. Cisco recommends running an interdomain routing protocol in the core. Cisco customers have traditionally used ISO-IGRP (the Interior Gateway Routing Protocol developed by Cisco Systems for ISO CLNS) as their interdomain routing protocol. Cisco has developed support for CLNS extensions within multiprotocol Border Gateway Protocol (BGP). The BGP work is based on Internet Engineering Task Force (IETF) RFC 2283. BGP is the mostly widely implemented interdomain routing protocol today.

When implementing the three-tier architecture, it is important to look at the bandwidth of the links and location of the NOC. Typically, the NOC or the data centers with the OSS are built as an additional access site in the architecture. The size of the links to the distribution center may be larger because of the amount of traffic. In the DCN environment, the flow of data is between the OSSs and the network elements, which are downstream from the central office. Typically, very little data is sent between network elements and central offices today, but there are applications that will create more traffic between central offices. These applications include remote login and signaling for bandwidth. Remote login allows a technician logged in to a network element to access another network element over the DCN. The remote login feature saves the technician from needing to be physically at a site to perform maintenance and troubleshooting tasks.

Bandwidth signaling applications are being defined as part of the following standards:

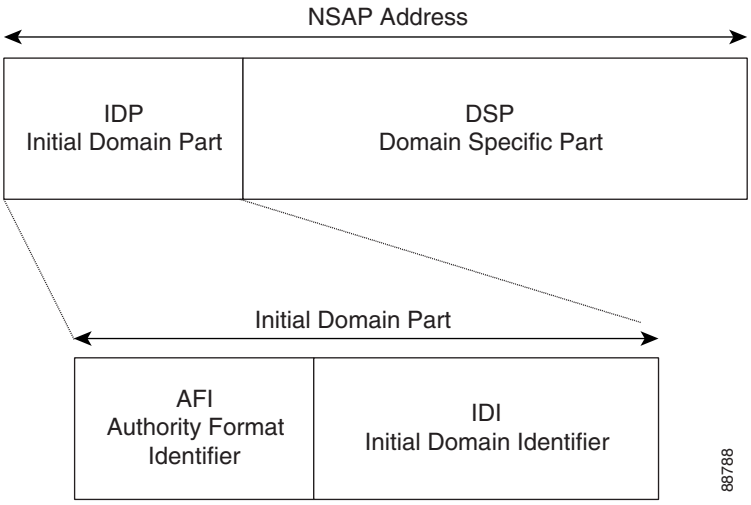
- ITU-T G.807—*Requirements for the Automatic Switched Transport Network (ASTN)*
- ITU-T G.8080—*Architecture for the Automatic Switched Optical Network (ASON)*
- Optical Internetworking Forum (OIF) *User Network Interface* (UNI) 1.0—This standard provides signaling between network elements, and between network elements and clients. It also provides signaling for both in-band and out-of-band or DCN networks, and for bandwidth.

OSI Addressing Issues and Suggestions

In ITU-T Recommendation X.213, *Data Networks and Open Systems Communications Open Systems Interconnections Service Definitions*, the network layer addressing is described in ANNEX A. The document is also referred to as ISO/IEC 8348:1996(E). Refer to ITU-T Recommendation X.213 for complete details about OSI addressing. This section focuses on basic address information used in the SONET/SDH environments.

The OSI network address is referred to as a network service access point (NSAP). The NSAP is assigned to the end system (ES) or intermediate system (IS) device. Unlike in IP, which has an address for every network interface, the OSI network device receives only one address, the NSAP address. The NSAP address has two parts, the Initial Domain Part (IDP) and Domain Specific Part (DSP), as shown in Figure 4.

Figure 4 NSAP Addresses



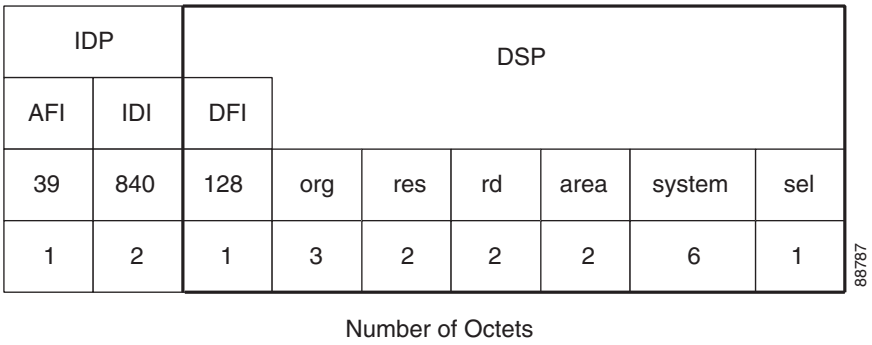
The IDP of the NSAP is assigned by address authorities. The address authorities allocate the bytes in the DSP. Six address authorities are currently defined, each briefly described as follows:

- ITU-T E.164—Specifies the initial domain identifier (IDI) as an ISDN number up to 15 digits long. This recommendation also specifies a PSTN up to 12 digits long.
- ITU-T F.69—Specifies the IDI as an international telex number up to eight digits long.
- ITU-T X.121—Specifies the IDI as an X.121 address for public X.25 networks, and is up to 14 digits long.
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Data Country Code (ISO DCC)—Specifies the IDI as a three-digit numeric code as defined by ISO 3166. An ISO member body within a country is assigned a three-digit code. The DSP is allocated by the ISO member body for a country.
- ISO 6523-ICD—Specifies the IDI as a four-digit International Code Designator (ICD) as defined by ISO 6523.
- Local—This address is the IDI and, if null, is used for local routing.

The SONET/SDH environments utilize the address authority defined by the ISO DCC. The AFI can have a value of 38 or 39. The value for the IDI is the country code. For the United States, the IDI is 840. The American National Standards Institute (ANSI) is the ISO body in the United States that assigns the 39.840 address space. The DSP addressing is defined in the American National Standard X3.216-1992, *Structure and Semantics of the Domain Specific Part of the Network Service Access Point Address*.

An ANSI-defined DSP is shown in Figure 5. The DSP is 17 binary octets long. The breakdown of the DSP is listed after the figure; the number of octets is shown under each category.

Figure 5 ANSI DSP Structure



- AFI—Authority format identifier value of 39 defines the NSAP type as ISO/IEC. The length is one binary octet.
- IDI—Initial domain identifier value of 840 defines the country as United States. The length is two binary octets.
- DFI—Domain Specific Part format identifier specifies the version of the ANSI X3.216. The decimal value is 128. Hexadecimal value is 80. The length is one binary octet.
- org—The organization is identified by the value that is assigned by ANSI. The length is three binary octets.
- res—A reserved field set to a value of 0. The length is two binary octets.
- rd—A routing domain prefix to be used for address summarization. This prefix allows the summarization of the multiple areas with one routing entry. The length is two binary octets.
- area—This portion of the NSAP identifies the unique Level 1 area. The length is two binary octets.
- system—This is the unique system identifier of an ES. There can only be one ES within an area with this unique identifier. There is no definition on how to assign the identifier. Implementors often use the MAC address off the first Ethernet port or a portion of the IP address. The length is six binary octets.
- sel—The NSAP selector is used to specify the network service user. The NSAP selector is used to differentiate multiple applications connections to the same ES. An analogous solution would be TCP/IP port numbers. The network layer is set to a value of 0, so a Cisco router is typically configured to a value of 0. The length is one binary octet.

In the Telcordia Specification GR-253-core, in Section 8 of the document, the NSAP address is described with reference to the DCN and SONET network elements. ISO DCC is the selected address format, and the AFI has a decimal value of 39 that is encoded in binary coded decimal. The AFI is configured into Cisco IOS software in decimal format. The AFI is broken down in Figure 6.

Figure 6 AFI Structure

	AFI	
Octets		1
Decimal	3	9
Binary	0011	1001
Cisco IOS entry	3	9

The ISO DCC in this example is for the United States, so the IDI decimal value is 840. The IDP portion of the NSAP is encoded in packed binary coded decimal format. The AFI and a portion of the IDI is shown in Figure 7.

Figure 7 AFI and IDI Structure

	AFI		IDI			IDI PAD
Octets	1		1.5			0.5
Decimal	3	9	8	4	0	None
Binary	0011	1001	1000	0100	0000	1111
Cisco IOS entry	3	9	8	4	0	F

The IDI shown in Figure 7 takes up 1.5 octets. The IDI has two octets set aside. The Telcordia GR-253 specification calls for filling the last four bits of the octet with ones. This process is referred to as the IDI PAD. Because there is no decimal value for the binary number 1111 in Binary Coded Decimal (BCD), the number is represented in hexadecimal as an F. The DSP portion of the NSAP is typically configured in hexadecimal. The DFI portion of the DSP has a decimal value of 128, a binary value of 1000 0000, and a hexadecimal value of 80; see Figure 8.

Figure 8 AFI, IDI , and DFI Structure

	AFI		IDI			IDI PAD	DFI	
Octets	1		1.5			0.5	1	
Decimal	3	9	8	4	0	None	128	
Binary	0011	1001	1000	0100	0000	1111	1000	0000
Cisco IOS entry	3	9	8	4	0	F	8	0

The next portion of the DSP, which is the organizational identifier, is assigned by ANSI. The organization identifier is made up of three octets that are entered into the Cisco IOS software as six hexadecimal characters.

The following example uses an organization identifier of 119999. The NSAP has the following format:

39.840f.80yy.yyyy.rrrr.dddd.aaaa.iiii.iiii.iiii.ss

and can be interpreted as follows:

- y—The organizational identifier as assigned by ANSI or other address authority for your region of the world.
- r—This portion of the NSAP is reserved and given a value of zero.
- d—The routing domain portion of the NSAP address. The routing domain is a collection of Level 1 areas. The routing domain allows the collection of Level 1 areas to be summarized among the Level 2 routers. The field can be provided in hexadecimal characters.
- a—The Level 1 area address as defined by ISO 10589. The field can be provided in hexadecimal characters.

- i—The individual system identifier. The structure of the format of the value is chosen by the customer. Customers typically input the MAC address of the first Ethernet port or a portion of the IP address.
- s—The NSAP selector. The value for a network entity title (NET) is zero.

Following is an example of the Cisco IOS software commands used to configure the NSAP on a Cisco router:

```
router isis DCN
net 39.840f.8011.9999.0000.0001.000b.00e0.f725.3338.00
```

OSI Addressing Implementation

This section describes how to implement an addressing plan based on the "OSI Addressing Issues and Suggestions" section on page 13. ANSI or the ISO DCC address authority in your geographic area of the world assigns the address space. ANSI can be contacted at http://ansi.org/.

Instructions for applying for a unique organizational identifier are included under the registration services portion of the ANSI website. In this example, the unique organizational identifier is 119999. The next portion of the DSP is marked reserved. The reserved portion of the NSAP is two octets. The NSAP up to this point looks like 39.840f.8011.9999.0000, and the format of the DSP is defined, but the service provider determines the assignment of the address space.

Because the remainder of the DSP is left up to the service provider, let us look at an example. In the example, the routing domain, the area, the individual system identifier, and NSAP selector will be filled out. The example has the following five OSI routing domains—domain 1111, domain 2222, domain 3333, domain 4444, and domain 5555. The first alternative has five OSI domains or routing domains. Each domain is two octets long. The key to laying out the address space is to allow summarization of domains, as follows:

OSI domain 1: 39.840f. 8011.9999.0000.1111

OSI domain 2: 39.840f. 8011.9999.0000.2222

OSI domain 3: 39.840f. 8011.9999.0000.3333

OSI domain 4: 39.840f. 8011.9999.0000.4444

OSI domain 5: 39.840f. 8011.9999.0000.5555

The area addressing can be created by adding the area addresses one at a time within a domain. Therefore, the first area within domain 1111 could be area address 0001, and the NSAP would be as follows:

39.840f.8011.9999.0000.1111.0001

The system identifier uniquely identifies the device within the area. To create this identifier, service providers often use the MAC address of the first Ethernet port on the router, which is displayed by entering the **show interface** EXEC command on the router (for purpose of example, the MAC address is shown in bold text):

```
Router# show interface ethernet 0/0

Ethernet0/0 is up, line protocol is down
  Hardware is AmdP2, address is 00d0.5872.9720 (bia 00d0.5872.9720)
  Internet address is 172.168.0.22/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 231/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
```

```
Last input never, output 00:00:08, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   0 packets input, 0 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 input packets with dribble condition detected
   12 packets output, 1009 bytes, 0 underruns
   12 output errors, 0 collisions, 2 interface resets
   0 babbles, 0 late collision, 0 deferred
   13 lost carrier, 0 no carrier
   0 output buffer failures, 0 output buffers swapped out
```

The following example shows how to use the MAC address 00d0.5872.9720 to create the area identifier:

39.840f.8011.9999.0000.1111.0001.00d0.5872.9720

It is also acceptable to use the IP address in the station identifier. In the following example, the IP address on the Ethernet interface is 172.168.0.22. Some service providers choose to use the IP address on the loopback interface, but for this example the Ethernet interface is used. The 172 portion of the IP address was left out and the remainder of the IP address was imbedded.

39.840f.8011.9999.0000.1111.0001.0168.0000.0022

The following example is another way to use the IP address to create the area address:

39.840f.8011.9999.0000.0001.1721.6800.0022

A final example would be to take the IP address and encode it in hexadecimal format. This action allows the entire IP address to be placed into the end system identifier, but recognizing the IP address is not as straightforward by doing so. The following list shows the loopback address 172.168.0.22 encoded as hexadecimal numbers:

- 172 = ac
- 168 = a8
- 0 = 00
- 22 = 16

Plugging the hexadecimal numbers into the end system identifier would result in the number 39.840f.8011.9999.0000.1111.0001.0000.aca8.0016. Notice that the first two octets of the system identifier are padded with 0s.

Note The NSAP selector is set to 00 for an IS-IS device. The following example shows what the NSAP of an IS-IS router would look like: 39.840f.8011.9999.0000.1111.0001.00d0.5872.9720.00.

Access Layer Configuration

This section focuses on the access layer of Cisco's three-tiered network architecture and contains these sections:

SONET/SDH Scaling Issues for Multiple OSI Areas

All SONET/SDH nodes on a ring are typically Level 1 routers, because of the performance issue described in the "DCN Design Considerations for OSI" section on page 5. SONET/SDH nodes on a ring should be in the same OSI area if the nodes are all Level 1. SONET/SDH devices must be organized into many small-sized OSI areas, as described in earlier sections about IS-IS multiarea DCN architecture. The IS-IS multiarea was added to the Cisco IOS feature set to improve the scaling of an IS-IS network in the SONET/SDH environments. The feature allows the configuration of up to 29 Level 1 IS-IS processes on Cisco routers.

Note The maximum number IS-IS process that can be configured is 29. However, the configuration of multiprotocol BGP (mBGP) CLNS and ISO-IGRP changes that number. If you configure mBGP CLNS, two IS-IS processes are used and you can configure only one instance of mBGP. On a router with mBGP CLNS configured, the user can only configure 27 IS-IS processes.

The configuration for ISO-IGRP takes two IS-IS processes. You can configure multiple ISO-IGRP processes and each ISO-IGRP process configured uses two IS-IS processes. If you configure two ISO-IGRP processes, then four IS-IS processes would be used. You have the ability to configure 25 IS-IS processes, which is 29 IS-IS processes minus the four IS-IS processes used by the two ISO-IGRP instances.

If you configure the mBGP CLNS process and one ISO-IGRP processes, you can configure 25 IS-IS processes. You start with 29 IS-IS processes and subtract the two IS-IS processes used by the one ISO-IGRP process and subtract the two IS-IS processes used by the mBGP CLNS process.

The number of IS-IS processes supported are specific to a platform, the architecture of the network, and the other tasks being performed on a platform. Specific base guidelines have been released for the Cisco 1800, 2600, and 3600 series platforms, as listed in Table 4.

Table 4 IS-IS Processes Supported on Cisco Router Platforms

Router Platform	IS-IS Processes
Cisco 1841	3
Cisco 2610, Cisco 2611, Cisco 2620, Cisco 2621, and Cisco 2651	3
Cisco 2691	8
Cisco 2811	8
Cisco 2821	8

Table 4 IS-IS Processes Supported on Cisco Router Platforms (continued)

Router Platform	IS-IS Processes
Cisco 2851	8
Cisco 3640	8
Cisco 3725	8
Cisco 3631	12
Cisco 3662	12
Cisco 3745	15
Cisco 3825	15
Cisco 3845	20

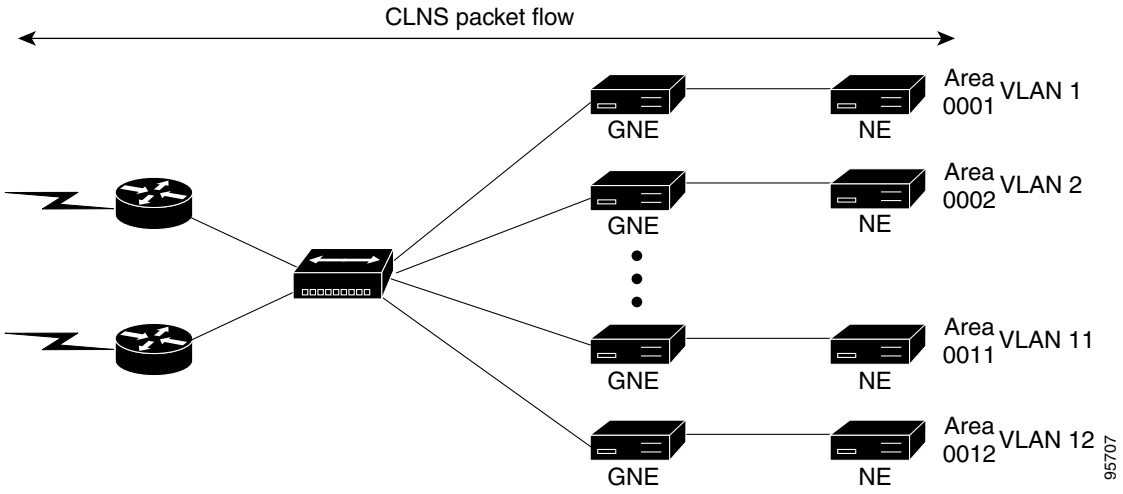
These numbers assume that the customer is implementing the three-tiered network architecture described in the "The Cisco Three-Tiered DCN Network Architecture" section on page 12. A flat network with many IS-IS adjacencies will not perform as well as the tiered network. For example, a poor design builds a Frame Relay cloud that peers all the sites together. As the number of sites in the Frame Relay network increase, the number of IS-IS adjacencies to maintain and the number of CPU cycles would also increase.

The CPU cycles on the router can be affected by other features enabled in the Cisco IOS software. Service providers often perform protocol translation on access routers. The router is translating between a TCP/IP session from the OSS and X.25 to the network element. Each packet is process-switched by the CPU, which affects the amount of CPU cycles available for maintaining IS-IS adjacencies.

Cisco routers are used to interconnect each Level 1 area or ring to the Level 2 backbone. A typical routing engine in a SONET network element can support only a routing table of 50 to 100 entries. This limitation bounds the area size to 50 Level 1 SONET routers. The service provider will need to check with their specific SONET/SDH vendors. Basic network designs were reviewed earlier in this document. Also, some SONET/SDH vendors have limitations on the number of ES adjacencies and Level 1 adjacencies that a GNE can support. The number of adjacencies has been as low as 15 on some SONET/SDH nodes. In early deployments, service providers were running into adjacency problems when implementing Ethernet hubs because they were putting multiple GNEs from different OSI areas on the same Ethernet hub, as shown in Figure 9. The GNEs in the different areas were forming ES adjacencies, which caused performance problems for the GNEs.

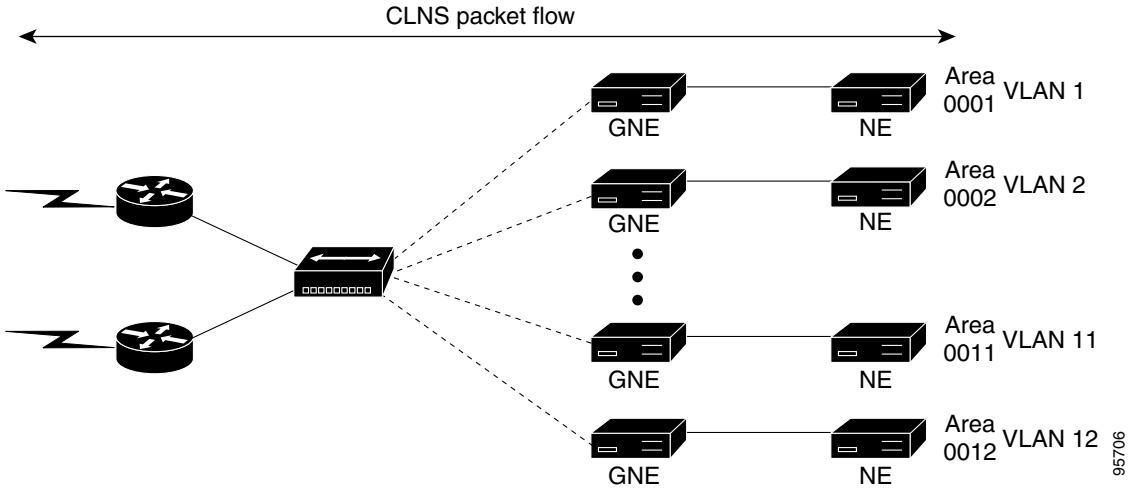
Note Gateway network elements are the network elements that are connected to the Ethernet and the optical ring or chain. The gateway network element is a gateway between the DCN and the in-band management channel, which is called the data communication channel (DCC).

Figure 9 GNEs Forming ES Adjacencies



Cisco's solution is shown in Figure 10. Cisco recommends installing an Ethernet switch and separating the GNEs, thereby placing all the GNEs in different OSI areas on a separate VLAN. Figure 10 shows 12 OSI areas that correspond to 12 VLANs.

Figure 10 GNEs Separated by an Ethernet Switch



SONET network elements communicate over a DCC in-band channel in the SONET ring at 192 KB. The in-band channel is used to access SONET nodes on the ring. Typically, there is only one GNE onto smaller rings deployed in a metropolitan setting. The DCC is often used to access the SONET node placed on a customer site or to access an optical amplifier in the fiber. Extending the DCN to these sites would not make sense from an economic or security standpoint. The limited 192 KB bandwidth of the DCC limits the size of the SONET/SDH ring. One method around the DCC bandwidth limitation is to add GNEs to the ring. The GNEs should be separated by four to seven hops. The service provider should consult the GNE vendor.

Defining IS-IS Multiareas with ISL Trunking

This section describes the configuration for an IS-IS multiarea with VLANs using Inter-Switch Link (ISL) trunking (a Cisco-proprietary protocol that maintains VLAN information as traffic flows between switches and routers). Typically, the multiarea feature is used at the access portion of the network. The OSS is located in the data center, and the CLNS packets are routed across the network to the central office router. Figure 11 shows a typical configuration.

Figure 11 IS-IS Multiarea Network Using ISL

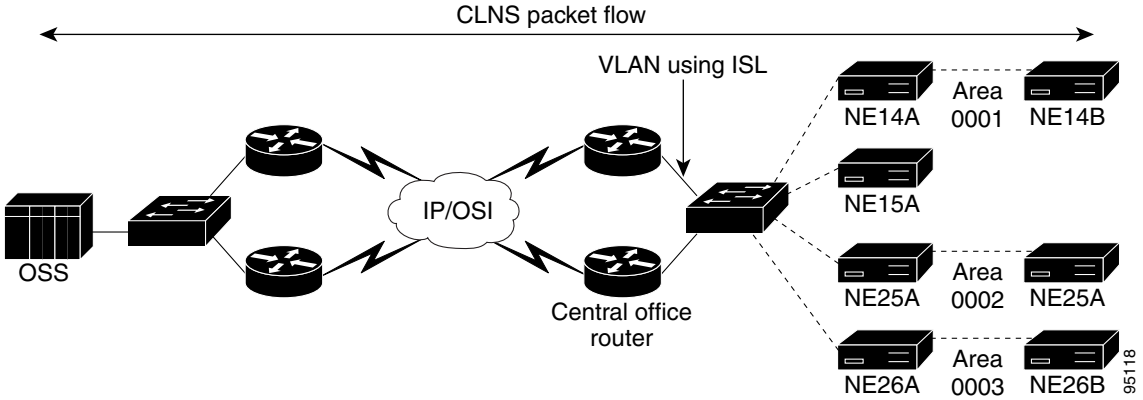


Figure 11 shows three IS-IS Level 1 areas. For purpose of example, the areas are small, with only two or three SONET or SDH network elements per area. A more typical area would have 30 to 50 network elements.

This configuration example uses a Cisco 3640 router and a Cisco Catalyst 2924XL switch. The IS-IS multiarea feature supports only one Level 1 or Level 2 IS-IS process per router. The router can be configured for up to 28 independent Level 1 processes and one Level 1/Level 2 process.

The number of IS-IS Level 1 processes supported depends upon the router platform. Each Level 1 IS-IS process must have a unique NSAP within an OSI area. The unique portion of the NSAP is the system identifier. The same unique system identifier must be used when creating multiple NSAPS on the Cisco 3640 router. In this example, the system identifier used is MAC address 0010.7bc7.ae40 from Ethernet port 0/0. See the "OSI Addressing Implementation" section on page 17 for more information about selecting system identifiers.

The MAC address is listed in the output of the **show interface** command, as the following example shows (text bolded for purpose of example):

```
3640A# show interface ethernet0/0

Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is 0010.7bc7.ae40 (bia 0010.7bc7.ae40)
  Internet address is 192.168.0.49/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:07, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   4 packets input, 533 bytes, 0 no buffer
   Received 3 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 input packets with dribble condition detected
   11 packets output, 786 bytes, 0 underruns
   0 output errors, 0 collisions, 4 interface resets
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier
   0 output buffer failures, 0 output buffers swapped out
```

Using address examples from the "OSI Addressing Implementation" section on page 17, the routing domain number is 1111. The following example configures the access router to handle the following three OSI areas:

39.840f.8011.9999.0000.1111.0001

39.840f.8011.9999.0000.1111.0002

39.840f.8011.9999.0000.1111.0003

The corresponding NSAPs for the Cisco 3640 router are built with a unique system identifier and a network selector value of 00. The network selector for the network layer is 00. The chosen system identifier for this example is the MAC address from Ethernet interface 0/0, so the NSAPs for the Cisco 3640 routers are as follows:

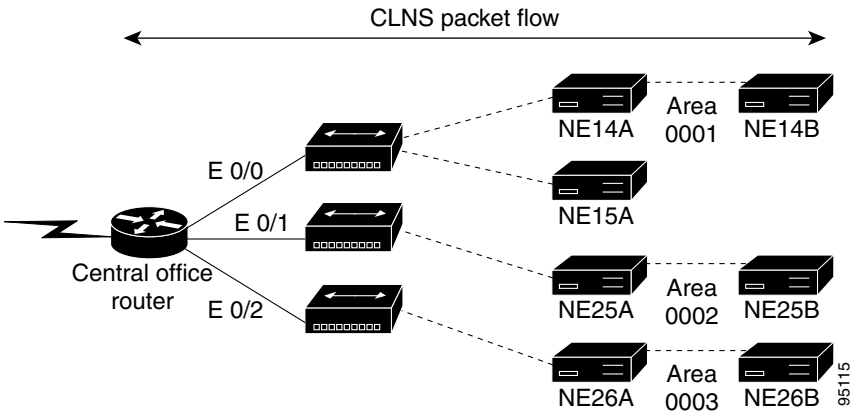
net 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00

net 39.840f.8011.9999.0000.1111.0002.0010.7bc7.ae40.00

net 39.840f.8011.9999.0000.1111.0003.0010.7bc7.ae40.00

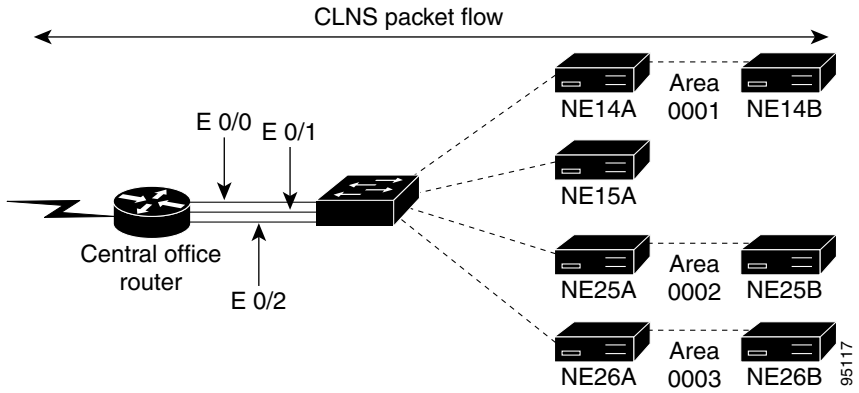
An interface can be associated with only one IS-IS processes. In the first solution that Cisco provided to service providers, a separate Ethernet interface was configured for every IS-IS process and LAN. Each LAN was on a separate hub, as shown in Figure 12.

Figure 12 IS-IS Multiarea Network Using Separate Ethernet Interfaces



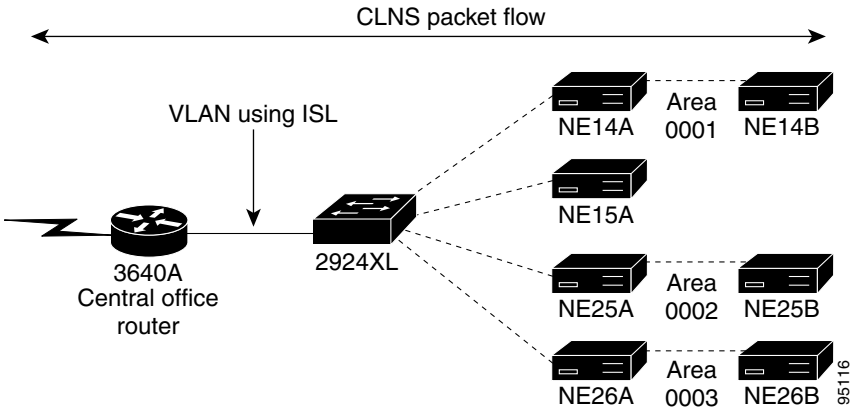
The next solution that Cisco provides makes it possible to consolidate the individual hubs into a Cisco Catalyst switch with VLANs. Each VLAN on the Cisco Catalyst switch had a separate Ethernet connection from the router, as shown in Figure 13.

Figure 13 IS-IS Multiarea Network Consolidating Hubs on a Switch (VLAN Trunking)



The number of physical Ethernet interfaces can be reduced by using VLAN trunking. A separate IS-IS process can be assigned to a subinterface. The example in this section focuses on implementing an IS-IS multiarea on an ISL trunk, as shown in Figure 14.

Figure 14 IS-IS Multiarea Network Using VLAN Trunking and ISL Encapsulation



Configuring an IS-IS Multiarea Network on a VLAN Using ISL Encapsulation

This section uses the network shown in Figure 14 as the basis for the configurations. The examples use a Cisco 3640 router with the Telco Feature Set running Cisco IOS Release 12.2(15)T.

Begin by enabling a CLNS routing and enabling TARP (assuming that TARP will be used). TARP is the target identifier (TID) Address Resolution Protocol, which is the name given to a piece of equipment by service providers in the United States. (TARP is an application that automates the mapping of CLNS addresses to TIDs, and will be described in more detail in the "Enabling TARP" section on page 60.)

The following example shows how to enable TARP and assign the router a TID using the router's host name; in this example, the assigned TID is 3640A for a Cisco 3640 router:

```
clns routing
tarp run
tarp tid 3640A
```

Next, create the IS-IS routing processes for the three areas shown in Figure 14. The first IS-IS routing process created can be a Level 1/Level 2, which is a circuit-type Level 1/Level 2. (Note that the circuit-type Level 1/Level 2 configuration will not show up in the system configuration output because "is-type level-1-2" is the default.) The remaining IS-IS processes will be Level 1, which is specified and identified in the Cisco IOS software as "is-type level-1." After the first Level 1/Level 2 IS-IS process is configured, the remaining processes will automatically be configured by the software as "is-type level-1."

Each IS-IS process has an identifier. In the examples, the IS-IS process identifiers are named after the OSI area. For example, the IS-IS process identifier area0001 is used for area 0001. (Note that the IS-IS process identifier name is arbitrary, but that area names are useful for troubleshooting. The service provider could have named the IS-IS processes after colors, for example.) The system identifier used in the example is the MAC address (0010.7bc7.ae40) from Ethernet port 0/0.

The following example shows how to configure the IS-IS routing processes for the three areas:

```
router isis area0001
 net 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
!
router isis area0002
 net 39.840f.8011.9999.0000.1111.0002.0010.7bc7.ae40.00
 is-type level-1
!
router isis area0003
 net 39.840f.8011.9999.0000.1111.0003.0010.7bc7.ae40.00
 is-type level-1
```

The IS-IS process area0001 is specified in the Cisco IOS software with the **is-type level-1-2** command, which is the Cisco IOS software default, but no **is-type** commands will be displayed in the configuration output. The area0001 process will provide connectivity back to the IS-IS backbone. There can be only one Level 2 IS-IS process, and each additional IS-IS process will be at Level 1. Each IS-IS process must be assigned to a separate interface. Fast Ethernet port 3/0 is configured for ISL trunking with three subinterfaces. The encapsulation on the interface is ISL (specified with the **encapsulation isl** command).

Designated IS Election Process on a LAN

Generally, service providers configure the Cisco access router to be the designated IS on the Ethernet interface. In IS-IS routing, a broadcast medium such as a LAN is not treated as a fully connected topology. Instead, a logical representation of the LAN is created called a *pseudonode*, which is generated by a Designated Intermediate System (DIS).

The DIS is responsible for creating and updating the pseudonode line-state packet (LSP) and flooding the LSPs over the LAN. On a broadcast medium such as Ethernet, one DIS is selected for Level 1 routers and a separate DIS is selected for Level 2 routers. There is no backup DIS. The election of a DIS can be preempted by a DIS with a higher priority. The routers on the LAN, including the DIS, form an adjacency with the pseudonode. A router elects itself the DIS based on interface priority. The priority range is from 0 (lowest) to 127 (highest). A priority of 64 is the default, and a priority of 127 sets the router to be elected as the DIS. If two routers have the same priority, the router with the highest subnetwork point of attachment (SNPA) wins the election.

The SNPA, which is the MAC address on the LAN or the data-link connection identifier (DLCI) on a Frame Relay network, is also used to configure a CLNS route for an interface. For the configuration example in this section, the SONET network elements are configured as Level 1 IS-IS routers. In real network implementations, service providers have found that forcing the Cisco router to be the DIS works best. Service providers are basically offloading the DIS functions onto the CPU of the standalone Cisco routers, as opposed to a SONET/SDH network element. This configuration is done by setting the IS-IS priority to 127 on the interface. A Level 1 IS-IS pseudonode is selected on each VLAN.

The Cisco router labeled “3640A” in Figure 14 is the DIS for each VLAN, and Fast Ethernet interface 3/0.1 is configured first. In the following example, the interface is configured with ISL encapsulation and VLAN 1 is assigned to the interface. IS-IS process area0001 is assigned to the interface using the **clns router isis area0001** command. The assignment of the IS-IS processes to the interfaces is shown in the following example. The IS-IS priority for selecting the DIS is modified to 127, from the default 64, to force the Cisco 3640 router to be the DIS. TARP is enabled on the interface. An IP subnet is assigned to VLAN 1 so that the network administrator can assign an IP address to the Cisco Catalyst 2924XL switch for management of the switch. The following example shows how to configure the Cisco router labeled “3640A” as the DIS for each VLAN. The IS-IS priority is set to 127 on the interface.

```
interface FastEthernet3/0
 no ip address
 duplex auto
 speed auto
 no cdp enable
!
interface FastEthernet3/0.1
 description IS-IS area 0001
 encapsulation isl 1
 ip address 192.168.2.61 255.255.255.192
 no ip redirects
 no cdp enable
 clns router isis area0001
 isis priority 127
 tarp enable
```

Fast Ethernet interface 3/0.2 is configured next. In the following example, the interface is configured with ISL encapsulation, and VLAN 2 is assigned to the interface. IS-IS process area0002 is assigned to the interface by the **clns router isis area0002** command. The assignment of the IS-IS processes to the interfaces is shown in the following example. The IS-IS priority for selecting the DIS is modified to 127 from the default 64, to force the Cisco 3640 router to be the DIS. TARP is enabled on the interface.

```
interface FastEthernet3/0.2
 description IS-IS area 0002
 encapsulation isl 2
 no cdp enable
 clns router isis area0002
 isis priority 127
 tarp enable
```

Fast Ethernet interface 3/0.3 is the third subinterface to be configured. As with the first two subinterfaces, this interface is configured with ISL encapsulation, and VLAN 3 is assigned to the interface. IS-IS process area0003 is assigned to the interface by the **clns router isis area0003** command. The assignment of the IS-IS processes to the interfaces is shown in the following example. The IS-IS priority for selecting the DIS is modified to 127 from the default 64, to force the Cisco 3640 router to be the DIS. TARP is enabled on the interface.

```
interface FastEthernet3/0.3
 description IS-IS area 0003
 encapsulation isl 3
 no cdp enable
 clns router isis area0003
 isis priority 127
 tarp enable
!
```

Verifying an IS-IS Multiarea Network Using VLAN Trunking and ISL Encapsulation

The next step is to verify that CLNS is operating on the router. Use the **show clns** EXEC command to verify that CLNS is running. The following example shows typical output of the **show clns** command:

```
3640A# show clns

Global CLNS Information:
  3 Interfaces Enabled for CLNS
  NET: 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
  NET: 39.840f.8011.9999.0000.1111.0002.0010.7bc7.ae40.00
  NET: 39.840f.8011.9999.0000.1111.0003.0010.7bc7.ae40.00
  Configuration Timer: 60, Default Holding Timer: 300, Packet Lifetime 64
  ERPDU's requested on locally generated packets
  Intermediate system operation enabled (CLNS forwarding allowed)
  IS-IS level-1-2 Router: area0001
    Routing for Area: 39.840f.8011.9999.0000.1111.0001
  IS-IS level-1 Router: area0002
    Routing for Area: 39.840f.8011.9999.0000.1111.0002
  IS-IS level-1 Router: area0003
    Routing for Area: 39.840f.8011.9999.0000.1111.0003
```

The sample output shows that the router has CLNS enabled on three interfaces. The three OSI NSAPs are listed. Notice that the system identifier—0010.7bc7.ae40—is the same for all three NSAPs. The three IS-IS processes are listed with their respective process identifiers—area0001, area0002, and area0003. The routing area assigned to each process is also listed.

The three interfaces running CLNS can be further examined using the **show clns interface** EXEC command. Sample command output for all three interfaces follows, starting with Fast Ethernet interface 3/0.1:

```
3640A# show clns interface fastethernet 3/0.1

FastEthernet3/0.1 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  RDPDUs enabled, min. interval 100 msec., Addr Mask enabled, last sent 00:47:38
  Congestion Experienced bit set at 4 packets
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 23 seconds
  Routing Protocol: IS-IS (area0001)
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 10, Priority: 127, Circuit ID: 3640A.01
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 2
    Level-2 Metric: 10, Priority: 127, Circuit ID: 3640A.01
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 0
    Next IS-IS LAN Level-1 Hello in 1 seconds
    Next IS-IS LAN Level-2 Hello in 2 seconds
```

In this sample output for Fast Ethernet interface 3/0.1, the interface is up and the line protocol is up. Notice that CLNS fast switching is enabled by default. The routing protocol is IS-IS and the associated IS-IS process identifier is area0001. The Circuit Type report indicates whether this circuit is Level 1, Level 2, or Level-1-2. In this case, the circuit type is Level-1-2. The IS-IS priority is 127 on the interface for the Cisco router labeled “3640A.” The Cisco 3640 router is the DIS and identified as the DIS in the Circuit ID field. In other words, the circuit identifier lists the designated router’s host name or system identifier if the routers do not know the host name. In this case, the designated router’s host name is

3640A. Remember that the Cisco 3640 router interface is set to IS-IS priority of 127, which is the highest value. There are two active Level 1 adjacencies. The adjacency numbers correspond to those shown in Figure 14. The Cisco router labeled “3640A” should have a Level 1 adjacency with the SONET/SDH nodes labeled “NE14A” and “NE15A.” The Level 2 routing metric is 10 and the IS-IS Level 2 priority is 127. The Circuit ID field lists 3640A as the designated router. There are no Level 2 IS-IS adjacencies on Fast Ethernet interface 3/.01. (Normally, the Level 2 adjacency would come from the WAN connection back to the distribution router, or to a Level 2 adjacency with a second Level-1-2 router in the central office configured for a different OSI area on the Level-1-2 IS-IS process.)

The following example shows sample output for Fast Ethernet interface 3/0.2:

```
3640A# show clns interface fastethernet 3/0.2

FastEthernet3/0.2 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  RDPDUs enabled, min. interval 100 msec., Addr Mask enabled
  Congestion Experienced bit set at 4 packets
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 40 seconds
  Routing Protocol: IS-IS (area0002)
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 10, Priority: 127, Circuit ID: 3640A.01
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 2 seconds
```

This sample output indicates the second VLAN is configured on Fast Ethernet interface 3/0.2. The interface is up and the line protocol is up. CLNS fast switching is enabled by default. The routing protocol is IS-IS and the associated IS-IS process identifier is area0002. The circuit type is Level-1-2 . Fast Ethernet interface 3/0.2 is a Level 1/Level 2 link. The IS-IS priority is 127 on the interface for the Cisco router labeled “3640A,” so 3640A is the DIS and is identified as the DIS in the Circuit ID report. There is one active Level 1 adjacency with SONET/SDH node NE25A.

The following example shows sample output for Fast Ethernet interface 3/0.3:

```
3640A# show clns interface fastethernet 3/0.3

FastEthernet3/0.3 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  RDPDUs enabled, min. interval 100 msec., Addr Mask enabled
  Congestion Experienced bit set at 4 packets
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 17 seconds
  Routing Protocol: IS-IS (area0003)
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 10, Priority: 127, Circuit ID: 3640A.01
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 1 seconds
```

The third VLAN is configured on Fast Ethernet interface 3/0.3. The interface is up and the line protocol is up. CLNS fast switching is enabled by default. The routing protocol is IS-IS, and the associated IS-IS process is area0003. The circuit type is Level-1-2. The IS-IS priority is 127 on the interface for the Cisco router labeled "3640A," so 3640A is the DIS and is identified as the DIS as part of the Circuit ID report. There is one active Level 1 adjacency with SONET/SDH node NE26A.

The next step is to examine the IS-IS adjacencies. Use the **show clns is-neighbor detail** EXEC command to see the adjacency to the SONET/SDH node NE14A:

```
3640A# show clns is-neighbor detail

Area area0001:
System Id      Interface   State  Type Priority  Circuit Id         Format
NE15A          Fa3/0.1     Up     L1   55        3640A.01           Phase V
  Area Address(es): 39.840f.8011.9999.0000.1111.0001
  Uptime: 00:04:16
NE14A          Fa3/0.1     Up     L1   64        3640A.01           Phase V
  Area Address(es): 39.840f.8011.9999.0000.1111.0001
  Uptime: 00:04:16

Area area0002:
System Id      Interface   State  Type Priority  Circuit Id         Format
NE25A          Fa3/0.2     Up     L1   64        3640A.01           Phase V
  Area Address(es): 39.840f.8011.9999.0000.1111.0002
  Uptime: 00:04:17

Area area0003:
System Id      Interface   State  Type Priority  Circuit Id         Format
NE26B          Fa3/0.3     Up     L1   64        3640A.01           Phase V
  Area Address(es): 39.840f.8011.9999.0000.1111.0003
  Uptime: 00:04:16
```

In this sample output, the three IS-IS processes running on the Cisco router are listed by process identifier. The IS-IS process identifiers are area0001, area0002, and area0003.

Examining the IS-IS process identifier area0001 in more detail indicates the following:

- IS-IS process identifier area0001 lists two system identifiers—NE14A and NE15A—on Fast Ethernet interface 3/0.1. The IS-IS adjacency state is up for both SONET network elements. The adjacency type is a Level 1.
- The priority advertised by device NE14A is 64 and the priority advertised by device NE15A is 55. The Circuit ID field uniquely identifies the interface on the IS-IS router with a one-octet number. On an Ethernet or multiaccess network, the circuit and system identifier of the DIS are concatenated to create the pseudonode (.3640A.01). The system identifier has been replaced with the host name by Cisco IOS software, so the pseudonode of IS-IS process area0001 is 3640A.01. The Circuit ID field in the output actually shows the pseudonode identifier.
- The neighbor considers the Cisco router labeled "3640A" to be the DIS. Router 3640A was selected as the DIS because its priority was set to 127, which is higher than the value of 64 advertised by device NE14A, or the value of 55 advertised by device NE15A.
- The adjacency type is Phase V OSI, as opposed to a Phase IV DECNet adjacency. SONET/SDH will always be Phase V.
- The area address is 39.840f.8011.9999.0000.1111.0001.
- The uptime is how long the adjacency has been up, which is a little over 4 minutes. Adjacency uptime is useful debugging information.

Configuring a Cisco Catalyst 2924XL VLAN Using ISL Encapsulation

This section reviews configuration for the Cisco Catalyst switch seen in Figure 14 on page 24. The example configures three VLANs, one VLAN for each OSI area. VLAN 1 is the default. For management of the switch interface, VLAN 1 is defined and assigned an IP address, as shown in the following example:

```
interface VLAN1
 ip address 192.168.12.50 255.255.255.0
 no ip route-cache
```

In the following example, Fast Ethernet ports 0/1 through 0/4 and 0/13 through 0/22 are assigned to VLAN 1:

```
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
```

The switch ports are configured as both access and for VLAN 1. VLAN 1 is the default and does not display in the Cisco IOS software configuration file. The OSI area 39.840f.8011.9999.0000.1111.0001 is assigned to IS-IS routers or network elements connected to VLAN 1. Device NE14A in Figure 14 on page 24 is connected to switch port 0/2. Device NE15A is connected to switch port 0/3.

In the following example, Fast Ethernet ports 0/5 through 0/8 are assigned to VLAN 2:

```
interface FastEthernet0/5
 switchport access vlan 2
!
interface FastEthernet0/6
 switchport access vlan 2
!
interface FastEthernet0/7
 switchport access vlan 2
!
interface FastEthernet0/8
 switchport access vlan 2
```

The switch ports are configured as both access and for VLAN 2. The OSI area 39.840f.8011.9999.0000.1111.0002 is assigned to IS-IS routers or network elements connected to VLAN 2. Device NE25A in Figure 14 on page 24 is connected to switch port 0/5.

In the following example, Fast Ethernet ports 0/9 through 0/12 are assigned to VLAN 3:

```
!
interface FastEthernet0/9
 switchport access vlan 3
!
interface FastEthernet0/10
 switchport access vlan 3
!
interface FastEthernet0/11
 switchport access vlan 3
!
interface FastEthernet0/12
 switchport access vlan 3
!
```

The switch ports are configured as both access and for VLAN 3. The OSI area 39.840f.8011.9999.0000.1111.0003 is assigned to IS-IS routers or network elements connected to VLAN 3. Device NE26A in Figure 14 is connected to switch port 0/10.

In the following example, switch ports 0/23 and 0/24 are configured as trunks with ISL encapsulation. The Cisco IOS software default trunk encapsulation type is ISL.

```
interface FastEthernet0/23
 switchport mode trunk
!
interface FastEthernet0/24
 switchport mode trunk
```

Verifying the Cisco Catalyst 2924XL VLAN Configuration Using ISL Encapsulation

To verify port assignment to the VLANs, use the **show vlan brief** EXEC command:

```
Router-2924XL# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4,
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16,
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20,
                                                Fa0/21, Fa0/22
2    VLAN0002                         active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
3    VLAN0003                         active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Status of a specific port such as the device NE14A connection can be verified using the **show interface** EXEC command:

```
Router-2924XL# show interface fastethernet 0/3

FastEthernet0/3 is up, line protocol is up
  Hardware is Fast Ethernet, address is 00d0.796c.acc3 (bia 00d0.796c.acc3)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive not set
  Full-duplex, 100Mb/s, 100BaseTX/FX
```

```
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 2000 bits/sec, 0 packets/sec
5 minute output rate 7000 bits/sec, 2 packets/sec
   2186 packets input, 1256415 bytes, 0 no buffer
   Received 1535 broadcasts, 0 runts, 0 giants, 0 throttles
   105 input errors, 105 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   0 watchdog, 1528 multicast
   0 input packets with dribble condition detected
   12421 packets output, 5859914 bytes, 0 underruns
   0 output errors, 0 collisions, 1 interface resets
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier
   0 output buffer failures, 0 output buffers swapped out
```

Defining IS-IS Multiareas with IEEE 802.1Q Trunking

This section describes the requirements for implementing an IS-IS multiarea using IEEE 802.1Q encapsulation, instead of the ISL encapsulation used in the "Defining IS-IS Multiareas with ISL Trunking" section. In this configuration, which is shown in Figure 15, the network is basically the same as that used in the ISL example—the OSS is located in the data center and the CLNS packets are routed across the network to the central office router. The difference is that IEEE 802.1Q encapsulation will be used for the VLAN trunks.

Figure 15 IS-IS Multiarea Network with an IEEE 802.1Q Trunk

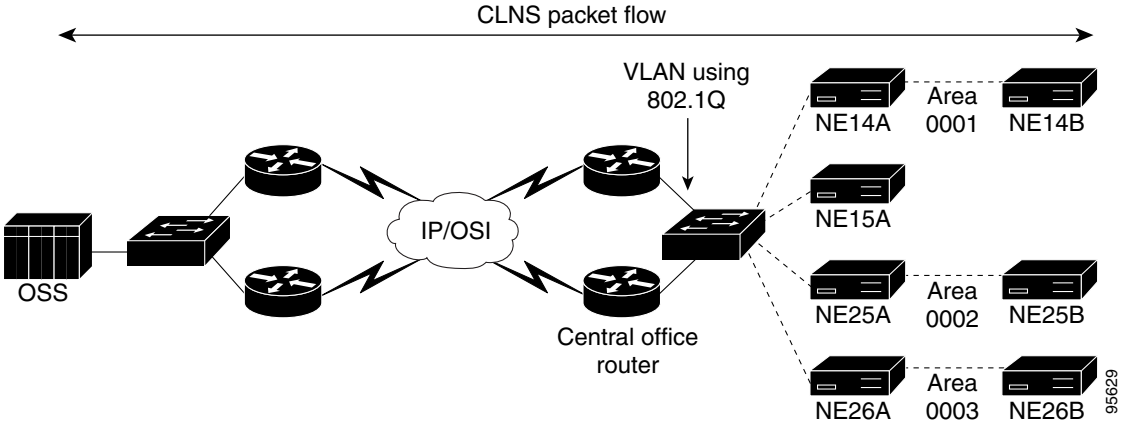
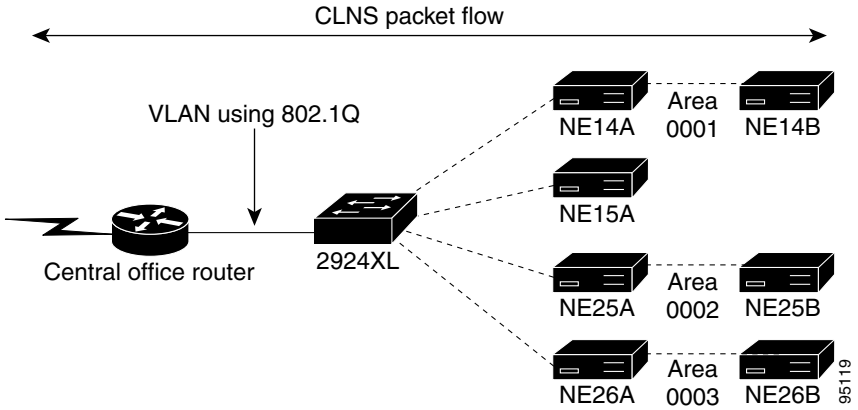


Figure 16 shows three IS-IS Level 1 areas. For the purpose of example, the areas are small, with only two or three SONET/SDH network elements per area. A typical area would have 30 to 50 network elements. This configuration is done using a Cisco 3640 router and Cisco Catalyst 2924XL switch.

Figure 16 IS-IS Multiarea Network Using VLAN Trunking and IEEE 802.1Q Encapsulation



Configuring an IEEE 802.1Q Trunk Router

The following configuration shows the IEEE 802.1Q encapsulation changes on the Cisco router interfaces. The configuration is the same as that seen in the "Configuring an IS-IS Multiarea Network on a VLAN Using ISL Encapsulation" section except for the encapsulation scheme. The **encapsulation dot1q** command is used on the three subinterfaces, which enables IEEE 802.1Q encapsulation.

```
interface FastEthernet3/0.1
 description IS-IS area 0001
 encapsulation dot1Q 1 native
 ip address 192.168.12.24 255.255.255.0
 no ip redirects
 no cdp enable
 clns router isis area0001
 isis priority 127
 tarp enable
!
interface FastEthernet3/0.2
 description IS-IS area 0002
 encapsulation dot1Q 2
 no ip redirects
 no cdp enable
 clns router isis area0002
 isis priority 127
 tarp enable
!
interface FastEthernet3/0.3
 description IS-IS area 0003
 encapsulation dot1Q 3
 no ip redirects
 no cdp enable
 clns router isis area0003
 isis priority 127
 tarp enable
```

Configuring a Cisco Catalyst 2924XL VLAN with IEEE 802.1Q Encapsulation

This section describes the changes required for the Cisco Catalyst switch configuration using the ISL implementation shown in Figure 14 on page 24, to using the IEEE 802.1Q implementation shown in Figure 15 on page 32. The configuration is the same as that in the "Configuring a Cisco Catalyst 2924XL VLAN Using ISL Encapsulation" section except for the VLAN encapsulation scheme. The VLAN

trunking encapsulation changes from ISL to IEEE 802.1Q encapsulation. Fast Ethernet port 0/23 is set up as the switch trunk port in both examples. In the following example, the **switchport trunk encapsulation dot1q** command is used on the switch port trunk, which enables IEEE 802.1Q encapsulation:

```
interface FastEthernet0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

Verifying a Cisco Catalyst 2924XL VLAN with IEEE 802.1Q Encapsulation

To verify port assignments of the VLANs, use the **show vlan brief** EXEC command:

```
Router# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4,
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16,
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20,
                                                Fa0/21, Fa0/22
2    VLAN0002                         active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
3    VLAN0003                         active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Status of a specific port, such as the device NE14A connection, can be verified using the **show interface** EXEC command:

```
Router# show interface fastethernet 0/10

FastEthernet0/10 is up, line protocol is up
  Hardware is Fast Ethernet, address is 00d0.796c.accb (bia 00d0.796c.accb)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive not set
  Half-duplex, 10Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 1 packets/sec
     1 packets input, 64 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     72 packets output, 4039 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Defining Multiple Areas with Manual Area Addressing

The designers of the ISO IS-IS protocol realized that there would be situations when the network would need to be readdressed. A provision was made in ISO 10589 to allow multiple area addresses to be associated with one area. ISO 10589 defines a management parameter for manual area addresses. A manual area address parameter is set in each IS-IS router that contains a list of all of the area addresses. The list of area addresses is distributed in the Level 1 LSP. The area comprises the union of all of the area addresses advertised, and the Level 2 router creates a composite list. All of the IS-IS routers, according to ISO 10589, must support at least three area addresses within an area. Two IS-IS routers must have at least one area address in common for an adjacency to be formed.

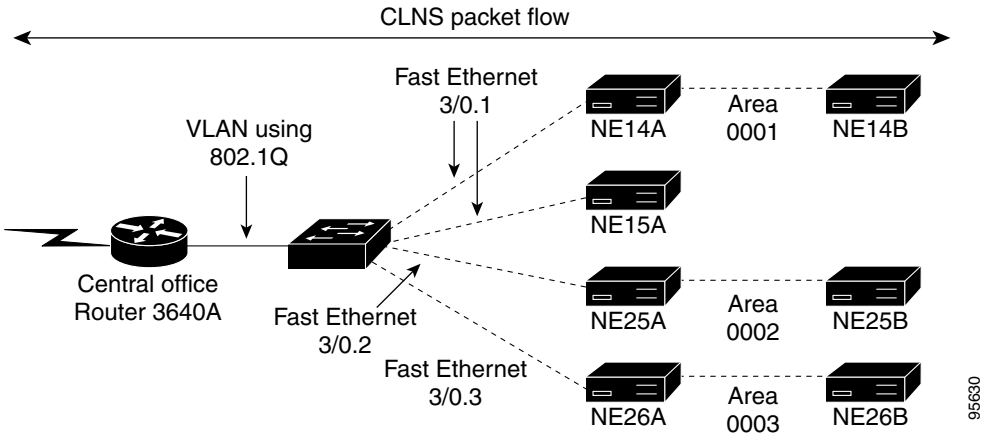
Originally, the Cisco IOS software supported only three area addresses within an area. Cisco changed this limit to support a minimum of three and a maximum of 254 addresses. The change was made to accommodate the SONET/SDH environment.

Caution The number of manual area addresses that are configured should match between two IS-IS routers. Cisco routers will not form an adjacency if the number of areas do not match. Therefore, changing the number of manual area addresses in a live network can cause a loss of connectivity.

Service providers have used manual area addressing as a tool to expand their networks without readdressing the network. Manual area addressing was used before the IS-IS multiarea feature was available. Incumbent local exchange carriers (ILECs) and PTTs typically deploy large numbers of small-sized SONET/SDH rings or chains. The rings and chains grow over time. Service providers did not want to readdress the network as it grew in size, so they would split the rings into groups and assign an area address. As SONET/SDH nodes were added to the rings or chains in the group, the overall area grew in size. The number of Level 1 IS-IS routers also grew. Eventually, the area size needed to be split. When a new standalone router was added to the area, one of the groups was migrated to the new router, and the NET was removed from the old group. This technique is used less frequently since the introduction of the IS-IS multiarea feature.

The configuration to add the manual area addressing is based on the network shown in Figure 17. NETs will be added to IS-IS process area 0001.

Figure 17 Sample Network for Configuring Manual Area Addresses



The following example shows the configuration before manual area addresses are added:

```
router isis area0001
 net 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
```

Configuring Manual Area Addressing

This section shows how to configure manual area addresses using the **max-area-addresses** router configuration command. The default value for this command is three addresses (which will *not* appear in router configurations).

The following example shows how to change the maximum number of manual area addresses to four, and configure four corresponding NETs:

```
3640A(config)# router isis area0001
3640A(config-router)# max-area-addresses 4
3640A(config-router)# net 39.840f.8011.9999.0000.1111.0004.0010.7bc7.ae40.00
3640A(config-router)# net 39.840f.8011.9999.0000.1111.0005.0010.7bc7.ae40.00
3640A(config-router)# net 39.840f.8011.9999.0000.1111.0006.0010.7bc7.ae40.00
3640A(config-router)# net 39.840f.8011.9999.0000.1111.0007.0010.7bc7.ae40.00
%The maximum allowed addresses already configured
```

The IS-IS router configured for manual area addressing with multiple areas will have multiple NETs associated with one IS-IS process. There will still be one IS-IS process and one IS-IS area.

Note Do not confuse this configuration with the IS-IS multiarea configuration, which has multiple IS-IS processes and areas.

The following example displays the new IS-IS portion of the configuration. Under IS-IS process area0001, there are now four NET statements; one area will advertise the multiple NETs.

```
router isis area0001
 max-area-addresses 4
 net 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
 net 39.840f.8011.9999.0000.1111.0004.0010.7bc7.ae40.00
 net 39.840f.8011.9999.0000.1111.0005.0010.7bc7.ae40.00
 net 39.840f.8011.9999.0000.1111.0006.0010.7bc7.ae40.00
!
router isis area0002
 net 39.840f.8011.9999.0000.1111.0002.0010.7bc7.ae40.00
 is-type level-1
!
router isis area0003
 net 39.840f.8011.9999.0000.1111.0003.0010.7bc7.ae40.00
 is-type level-1
```

Use the **show clns** EXEC command to display all the NETs that are configured:

```
3640A# show clns

Global CLNS Information:
  3 Interfaces Enabled for CLNS
  NET: 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
  NET: 39.840f.8011.9999.0000.1111.0004.0010.7bc7.ae40.00
  NET: 39.840f.8011.9999.0000.1111.0005.0010.7bc7.ae40.00
  NET: 39.840f.8011.9999.0000.1111.0006.0010.7bc7.ae40.00
  NET: 39.840f.8011.9999.0000.1111.0002.0010.7bc7.ae40.00
  NET: 39.840f.8011.9999.0000.1111.0003.0010.7bc7.ae40.00
  Configuration Timer: 60, Default Holding Timer: 300, Packet Lifetime 64
  ERPDU's requested on locally generated packets
```

```
  Intermediate system operation enabled (CLNS forwarding allowed)
  IS-IS level-1-2 Router: area0001
    Routing for Area: 39.840f.8011.9999.0000.1111.0001
  IS-IS level-1 Router: area0002
    Routing for Area: 39.840f.8011.9999.0000.1111.0002
  IS-IS level-1 Router: area0003
    Routing for Area: 39.840f.8011.9999.0000.1111.0003
```

The **show clns protocol** EXEC command provides useful information about the manual area addresses configured. The following example displays the system identifier and the IS type as Level-1-2. There are four manual area addresses and four areas are listed. This example displays one area, but all area addresses would be advertised. An adjacent host still needs to be configured for the same number of manual area addresses and matching NETs to form balanced adjacencies.

```
3640A# show clns protocol

IS-IS Router: area0001
  System Id: 0010.7BC7.AE40.00  IS-Type: level-1-2
  Maximum nr of area adresses in this area is 4
  Manual area address(es):
        39.840f.8011.9999.0000.1111.0001
        39.840f.8011.9999.0000.1111.0004
        39.840f.8011.9999.0000.1111.0005
        39.840f.8011.9999.0000.1111.0006
  Routing for area address(es):
        39.840f.8011.9999.0000.1111.0001
        39.840f.8011.9999.0000.1111.0004
        39.840f.8011.9999.0000.1111.0005
        39.840f.8011.9999.0000.1111.0006
  Interfaces supported by IS-IS:
        FastEthernet3/0.1 - OSI
  Redistribute:
    static (on by default)
  Distance for L2 CLNS routes: 110
  RRR level: none
  Generate narrow metrics: level-1-2
  Accept narrow metrics:   level-1-2
  Generate wide metrics:   none
  Accept wide metrics:     none

IS-IS Router: area0002
  System Id: 0010.7BC7.AE40.00  IS-Type: level-1
  Manual area address(es):
        39.840f.8011.9999.0000.1111.0002
  Routing for area address(es):
        39.840f.8011.9999.0000.1111.0002
  Interfaces supported by IS-IS:
        FastEthernet3/0.2 - OSI
  Redistribute:
    static (on by default)
  Distance for L2 CLNS routes: 110
  RRR level: none
  Generate narrow metrics: level-1-2
  Accept narrow metrics:   level-1-2
  Generate wide metrics:   none
  Accept wide metrics:     none

IS-IS Router: area0003
  System Id: 0010.7BC7.AE40.00  IS-Type: level-1
  Manual area address(es):
        39.840f.8011.9999.0000.1111.0003
  Routing for area address(es):
        39.840f.8011.9999.0000.1111.0003
```

```
Interfaces supported by IS-IS:
      FastEthernet3/0.3 - OSI
Redistribute:
  static (on by default)
Distance for L2 CLNS routes: 110
RRR level: none
Generate narrow metrics: level-1-2
Accept narrow metrics:   level-1-2
Generate wide metrics:   none
Accept wide metrics:     none
```

Verifying Adjacencies in a Network with Manual Area Addresses

Use the **show clns neighbors** EXEC command to verify that adjacencies are being formed. The following example indicates that an adjacency is up for IS-IS process area0001. The adjacency type is IS but the protocol is End System-Intermediate System (ES-IS) (see bold text), so an IS-IS adjacency is not being formed for IS-IS process area0001:

```
3640A# show clns neighbors

Area area0001:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
NE15A          Fa3/0.1     0010.7bd8.c7d0  Up     263       IS   ES-IS
NE14A          Fa3/0.1     00e0.b064.4325  Up     293       IS   ES-IS

Area area0002:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
NE25A          Fa3/0.2     00e0.b064.434e  Up     22        L1   IS-IS

Area area0003:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
NE26A          Fa3/0.3     00d0.5872.9720  Up     28        L1   IS-IS
```

Troubleshooting Adjacencies in a Network with Manual Area Addresses

Use the **debug isis adj-packets** command to debug IS-IS adjacency packets. In the following example, an IS-IS Hello (IIH) message comes in on Fast Ethernet interface 3/0.1 and causes a maximum area address mismatch error report to be displayed. (In the following output, text is in bold for purpose of example.) The network element with MAC address 00e0.b064.4325, which is device NE14A, is sending an IIH. The IIH has a different number of maximum area addresses than router 3640A. The number of maximum area addresses needs to be changed to match router 3640A. The change also needs to be made to device NE15A.

```
3640A# debug isis adj-packets

IS-IS Adjacency related packets debugging is on
3640A#
00:45:07: ISIS-Adj (area0001): Rec L1 IIH from 00e0.b064.4325 (FastEthernet3/0.1), cir
type L1, cir id 00E0.B064.4324.02, length 147
00:45:07: ISIS-Adj (area0001): Max-area-addresses mismatch, in L1 IIH from
FastEthernet3/0.1
```

In the network configuration, the maximum number of manual area addresses has been changed to four on devices NE14A, NE14B, and NE15A. The **show clns neighbors** command now indicates that the adjacency is up and the protocol being used is IS-IS:

```
3640A# show clns neighbors

Area area0001:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
```

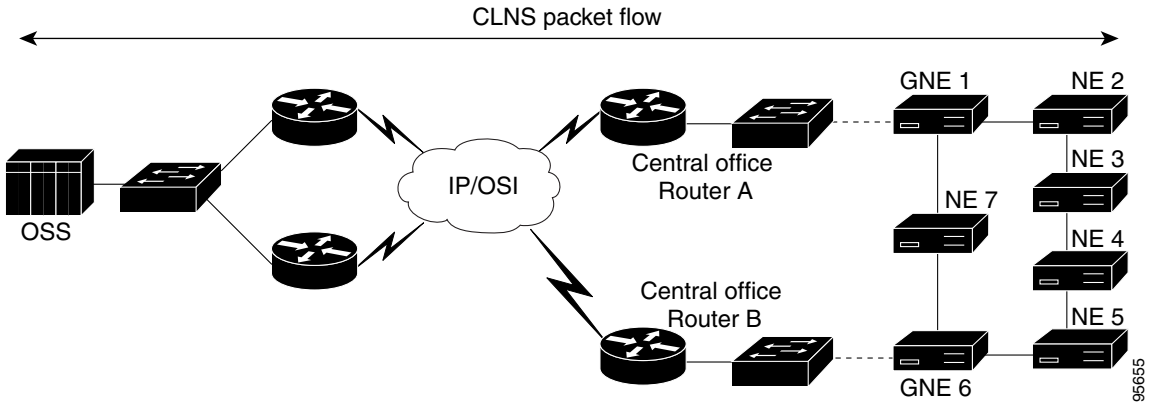
```
NE15A          Fa3/0.1     0010.7bd8.c7d0      Up     27         L1   IS-IS
NE14A          Fa3/0.1     00e0.b064.4325      Up     24         L1   IS-IS

Area area0002:
System Id      Interface   SNPA                State  Holdtime   Type Protocol
NE25A          Fa3/0.2     00e0.b064.434e      Up     22         L1   IS-IS

Area area0003:
System Id      Interface   SNPA                State  Holdtime   Type Protocol
NE26A          Fa3/0.3     00d0.5872.9720      Up     23         L1   IS-IS
```

Using Generic Routing Encapsulation Tunnels to Prevent Area Partitions

A GNE provides a gateway between the DCN LAN and the SONET DCC. The DCC is the embedded operations channel. There are two DCCs in the SONET/SDH frame: the section DCC and the line DCC. The section DCC is embedded in the section overhead and is made up of three bytes that create a 192-kbps data path. The section DCC has been standardized in TMN for management of the downstream SONET network elements. The line DCC is made up of nine bytes that create a 576-kbps data channel. The standards have carved out the bandwidth in the line DCC, but the TMN standards do not define *use* of the line DCC. Therefore, vendors have implemented proprietary uses for the line DCC.

Figure 18 shows the flow of CLNS packets across the network. For a CLNS packet to move from the OSS to device NE3, the packet must be routed across the DCN to the LAN in central office Router A or Router B. For purpose of example, assume that the packet arrives at the LAN in central office Router A. Device GNE 1 routes the packet from the LAN to the DCC and forward the packet across the section DCC to device NE2. Device NE2 forwards the packet across the section DCC to device NE3. The action of routing packets between the DCN and the section DCC is the definition of a GNE.

Figure 18 Typical GNE Configuration



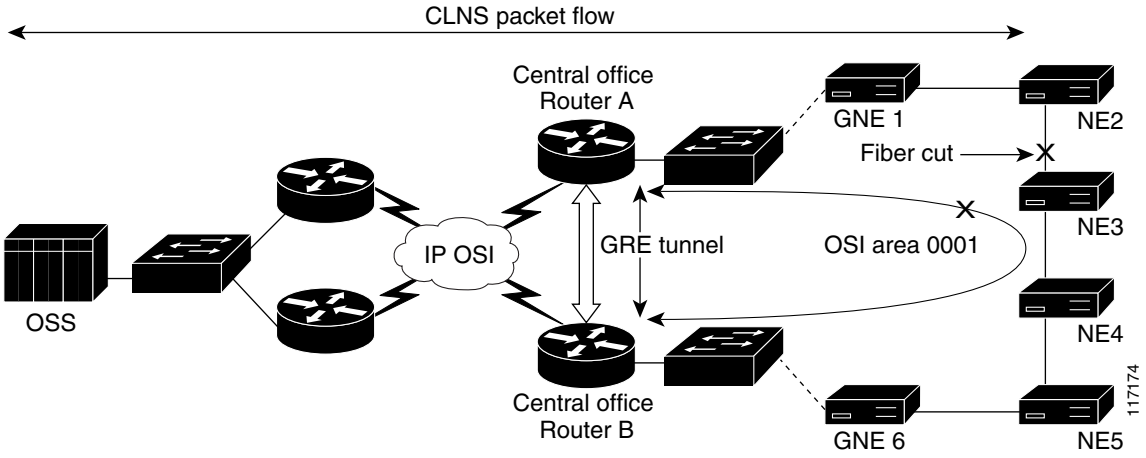
The service provider will typically implement one GNE per SONET/SDH ring on small-sized rings. The definition of small is typically six network elements or fewer. ILECs and PTTs typically have many small-sized rings or chains to extend services out from the central office to businesses. The service provider will build large collector rings to aggregate bandwidth from the small-sized rings. The larger rings typically have multiple GNEs to add redundancy to ring access, as shown in Figure 18. This section describes generic routing encapsulation (GRE) tunnels and the IS-IS default Originate features, both of which can be used to improve redundancy.

CLNS over GRE Tunnels

Traditionally the SONET/SDH technology is deployed in ring topologies for redundancy. In the event of a fiber cut (see Figure 19), the ring will wrap and the traffic will be either path switched or line switched onto the protected portion of the fiber. The DCC will be preserved as well.

There are times when it may be necessary to deploy fiber-optic cable in a long chain without the geographic diversity shown in Figure 19.

Figure 19 GRE Tunnel over CLNS with Cut Fiber Link



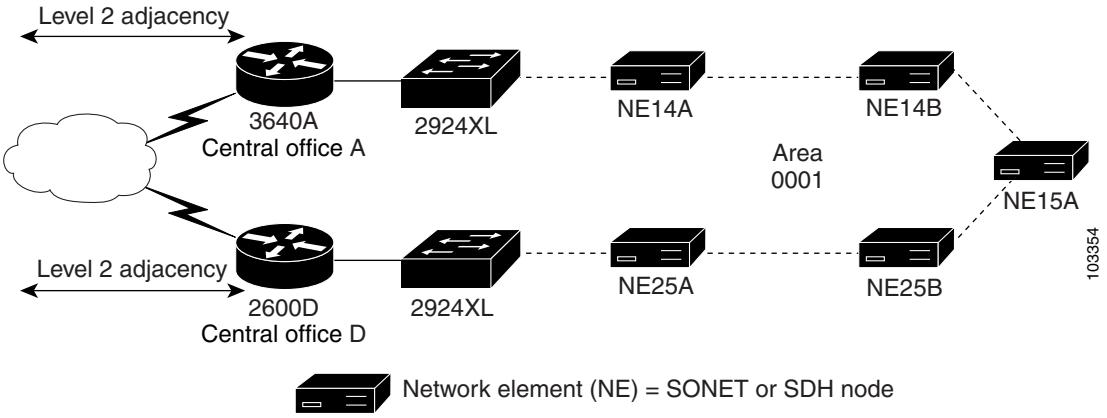
If the fiber gets cut, the OSI area will become partitioned and the OSS will not be able to communicate with some of the network elements.

One solution to the partitioned Level 1 area is to build a GRE tunnel between the Cisco routers for CLNS. The GRE tunnel will pass the IS-IS traffic between the partitioned parts of the network, as shown in Figure 19.

Configuring a GRE Tunnel

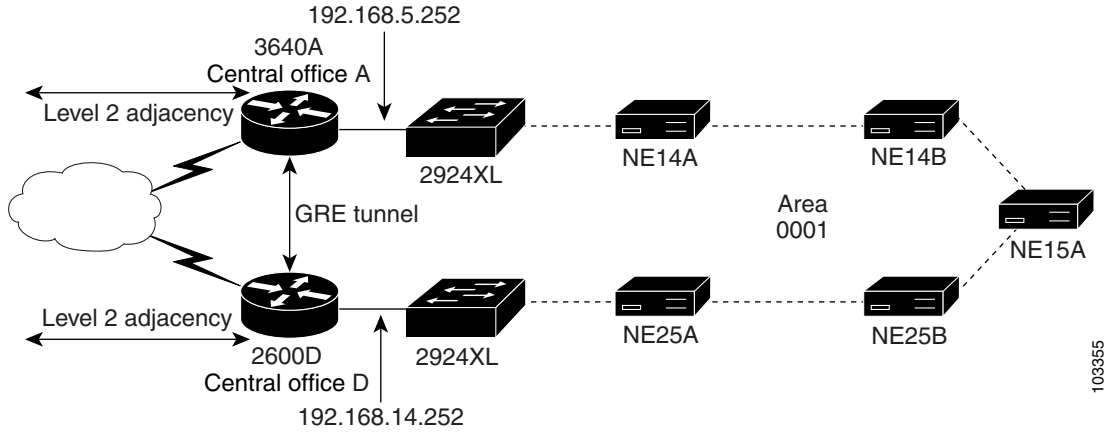
This section describes a sample GRE configuration. The sample network is shown in Figure 20 and depicts the following scenario: Router 3640A is in central office A and router 2600D is in central office D. The two central offices have a SONET/SDH chain running between them. The SONET/SDH network elements are all Level 1 routers. Network elements NE14A and NE25A are both GNEs to the SONET/SDH chain, which is in area 00001. The routers 3640A and 2600D are both Level 1/Level 2 access routers. A fiber cut between the network elements would partition area 0001.

Figure 20 Typical Network Before GRE Tunnel Configuration



The configuration builds a GRE tunnel between router 3640A and router 2600D. The GRE tunnel and the IP addresses that are used in the tunnel are shown in Figure 21.

Figure 21 GRE Tunnel Configuration



The following configuration example for the GRE tunnel shows that the router labeled 2600D in Figure 21 is configured for IS-IS routing in area 0001:

```
router isis area0001
 net 39.840f.8011.9999.0000.1111.0001.00e0.1ee3.c720.00
```

Router 2600D is connected to the SONET/SDH device NE25A over Ethernet interface 0/0:

```
interface Ethernet0/0
 ip address 192.168.5.189 255.255.255.192
 half-duplex
 clns router isis area0001
```

A loopback interface has been created for the GRE tunnel to terminate on router 2600D:

```
interface Loopback0
 ip address 192.168.5.252 255.255.255.192
```

The source of the GRE tunnel on router 2600D is the loopback address 192.168.5.252. The tunnel destination is the loopback IP address 192.168.14.252 on the router labeled 3640A in Figure 21. The routing metric assigned to the GRE tunnel is 30. Some service providers prefer to use the tunnel only in the event of an outage. IS-IS routing for CLNS has been turned up on the tunnel. The IS-IS metric can range from 1 to 63, with 63 being the worst route. The GRE keepalive feature is implemented in the example. The keepalive feature will take down the GRE tunnel interface if the far end of the tunnel becomes unavailable. See the following example:

```
interface Tunnel1
 no ip address
 keepalive 3 3
 clns router isis area0001
 isis metric 30
 tunnel source 192.168.5.252
 tunnel destination 192.168.14.252
 tarp enable
```

The following example shows how to configure router 3640A for IS-IS routing in area 0001:

```
router isis area0001
 net 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
```

In the following example, router 3640A is connected to SONET/SDH device NE14A over Fast Ethernet interface 3/0.1:

```
interface FastEthernet3/0.1
 description ISIS area 0001
 encapsulation dot1Q 1 native
 ip address 192.168.12.24 255.255.255.0
 no ip redirects
 no cdp enable
 clns router isis area0001
 isis priority 127
 tarp enable
```

The following example creates a loopback interface for the GRE tunnel to terminate on router 3640A:

```
interface Loopback0
 ip address 192.168.14.252 255.255.255.192
```

The source of the GRE tunnel on router 3640A is the loopback 0 IP address 192.168.14.252. The tunnel destination is loopback IP address 192.168.5.252 on router 2600D. The routing metric assigned to the GRE tunnel is 30. The GRE keepalive feature is implemented. See the following example:

```
interface Tunnel1
 no ip address
 keepalive 3 3
 clns router isis area0001
 isis metric 30
 tunnel source 192.168.5.252
 tunnel destination 192.168.14.252
 tarp enable
```

Note The source and destination IP addresses must match on each end of the tunnel. If the IP addresses do not match, the tunnel line protocol will not come up. If you choose to use a source or destination interface when configuring the tunnel, the IP address of the interface of the tunnel will be used.

The status of the tunnel can be examined with the **show interface** command. In the following example, tunnel 1 is up and line protocol is up. The keepalive option is set to send keepalives every 3 seconds, and set to retry three times before marking the interface line protocol down.

```
3640A# show interface tunnel 1

Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 28/255, rxload 28/255
  Encapsulation TUNNEL, loopback not set
  Keepalive set (3 sec), retries 3
  Tunnel source 192.168.14.252, destination 192.168.5.252
  Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
  Tunnel TTL 255
  Checksumming of packets disabled,  fast tunneling enabled
  Last input 00:00:07, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 29
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 1000 bits/sec, 0 packets/sec
  5 minute output rate 1000 bits/sec, 0 packets/sec
     1767 packets input, 705632 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     1945 packets output, 712879 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Use the **debug tunnel** command to debug the tunnel. The following example shows the **debug tunnel** command output:

```
3640A# debug tunnel

Tunnel Interface debugging is on
3640A#

01:11:24: Tunnel1: GRE/IP to decaps 192.168.5.252->192.168.14.252 (len=1537 ttl=253)
01:11:24: Tunnel1: GRE decapsulated CLNS packet
01:11:24: Tunnel1: GRE/IP encapsulated 192.168.14.252->192.168.5.252 (linktype=7, len=48)
01:11:24: Tunnel1: GRE/IP to decaps 192.168.5.252->192.168.14.252 (len=24 ttl=252)
01:11:25: Tunnel1: GRE/IP encapsulated 192.168.14.252->192.168.5.252 (linktype=25,
len=1537)
01:11:27: Tunnel1: GRE/IP encapsulated 192.168.14.252->192.168.5.252 (linktype=7, len=48)
01:11:27: Tunnel1: GRE/IP to decaps 192.168.5.252->192.168.14.252 (len=24 ttl=252)
01:11:30: Tunnel1: GRE/IP encapsulated 192.168.14.252->192.168.5.252 (linktype=7, len=48)
01:11:30: Tunnel1: GRE/IP to decaps 192.168.5.252->192.168.14.252 (len=24 ttl=252)
01:11:31: Tunnel1: GRE/IP to decaps 192.168.5.252->192.168.14.252 (len=1537 ttl=253)
01:11:31: Tunnel1: GRE decapsulated CLNS packet
```

Use the **debug tunnel keepalive** command to debug the tunnel keepalive. In the following example, notice that the keepalive packets are being sent every 3 seconds:

```
3640A# debug tunnel keepalive

Tunnel keepalive debugging is on
3640A#

01:12:27: Tunnel1: sending keepalive, 192.168.5.252->192.168.14.252 (len=24 ttl=255),
counter=1
01:12:27: Tunnel1: keepalive received, 192.168.5.252->192.168.14.252 (len=24 ttl=252),
resetting counter
01:12:30: Tunnel1: sending keepalive, 192.168.5.252->192.168.14.252 (len=24 ttl=255),
counter=1
01:12:30: Tunnel1: keepalive received, 192.168.5.252->192.168.14.252 (len=24 ttl=252),
resetting counter
```

```
01:12:33: Tunnel1: sending keepalive, 192.168.5.252->192.168.14.252 (len=24 ttl=255),
counter=1
01:12:33: Tunnel1: keepalive received, 192.168.5.252->192.168.14.252 (len=24 ttl=252),
resetting counter
01:12:36: Tunnel1: sending keepalive, 192.168.5.252->192.168.14.252 (len=24 ttl=255),
counter=1
01:12:36: Tunnel1: keepalive received, 192.168.5.252->192.168.14.252 (len=24 ttl=252),
resetting counter
01:12:39: Tunnel1: sending keepalive, 192.168.5.252->192.168.14.252 (len=24 ttl=255),
counter=1
01:12:39: Tunnel1: keepalive received, 192.168.5.252->192.168.14.252 (len=24 ttl=252),
resetting counter
01:12:42: Tunnel1: sending keepalive, 192.168.5.252->192.168.14.252 (len=24 ttl=255),
counter=1
01:12:42: Tunnel1: keepalive received, 192.168.5.252->192.168.14.252 (len=24 ttl=252),
resetting counter
01:12:45: Tunnel1: sending keepalive, 192.168.5.252->192.168.14.252 (len=24 ttl=255),
counter=1
01:12:45: Tunnel1: keepalive received, 192.168.5.252->192.168.14.252 (len=24 ttl=252),
resetting counter
```

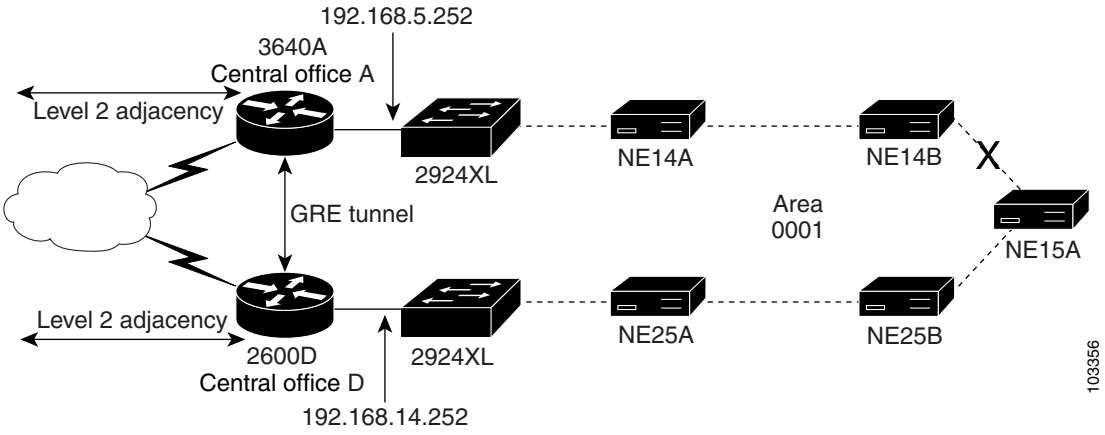
The next step is to look at the IS-IS topology after breaking the link between SONET/SDH nodes. The following example shows the IS-IS topology with the GRE tunnel up and the SONET/SDH chain in place:

```
3640A# show isis topology

Area area0001:
IS-IS IP paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
3640A                --
NE15A                30         NE14A                Fa3/0.1     00e0.b064.4325
NE25B                40         NE14A                Fa3/0.1     00e0.b064.4325
NE14B                20         NE14A                Fa3/0.1     00e0.b064.4325
2600D                30         2600D                Tu1         *Tunnel*
NE14A                10         NE14A                Fa3/0.1     00e0.b064.4325
NE25A                40         2600D                Tu1         *Tunnel*

IS-IS IP paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
3640A                --
2600D                30         2600D                Tu1         *Tunnel*
```

All of the network elements can be reached within the area from router 3640A, even though the IS-IS metric was raised to 30 on the tunnel. The tunnel is still the preferred path to router 2600D and network element device NE25A. The traffic could be forced out of the tunnel and onto the SONET/SDH DCC by raising the IS-IS metric.

The next part of this example breaks the connection between devices NE14B and NE15A, as shown in Figure 22. The example after the figure displays the new IS-IS topology after the connection break. All of the network elements and routers are still listed, and the connection to devices NE15A and NE25B has moved to the tunnel.

Figure 22 GRE Tunnel with Broken Connection




```
3640A# show isis topology

Area area0001:
IS-IS IP paths to level-1 routers
System Id            Metric     Next-Hop            Interface   SNPA
3640A                --
NE15A                60         2600D               Tu1         *Tunnel*
NE25B                50         2600D               Tu1         *Tunnel*
NE14B                20         NE14A               Fa3/0.1     00e0.b064.4325
2600D                30         2600D               Tu1         *Tunnel*
NE14A                10         NE14A               Fa3/0.1     00e0.b064.4325
NE25A                40         2600D               Tu1         *Tunnel*
```

Without the tunnel connection, routers 3640A and 2600D would not be able to see the entire IS-IS area 0001. Devices may not be able to communicate, depending upon where the devices sit in the network. The loss of connectivity can be demonstrated by shutting down the tunnel interface.

The following example displays the new IS-IS topology and indicates that packets reaching router 3640A from the network cloud could be forwarded only to devices NE14A and NE14B.

```
3640A# show isis topology

Area area0001:
IS-IS IP paths to level-1 routers
System Id            Metric     Next-Hop            Interface   SNPA
3640A                --
NE15A                **
NE25B                **
NE14B                20         NE14A               Fa3/0.1     00e0.b064.4325
2600D                **
NE14A                10         NE14A               Fa3/0.1     00e0.b064.4325
NE25A                **
```

IS-IS Attach-Bit Control Feature

Routing traffic between Level 1 areas is done by Level 2 routers. Level 1 routers forward the packets to their nearest Level 1/Level 2 router. Typically located at the access layer of the network, the Level 1/Level 2 routers are standalone Cisco routers, and Level 1 routers are SONET/SDH network elements.

The Level 1/Level 2 Cisco router identifies itself by setting the attach-bit in the link-state packets (LSPs). Often service providers have more than one Level 1/Level 2 router per area for redundancy. On large rings, there may be multiple GNEs with access to separate Level 1/Level 2 routers. A Level 1/Level 2 router can lose connectivity to the area with the OSS or the network backbone. If a Level 1/Level 2 Cisco router is configured for IS-IS multiarea, the Level 1/Level 2 router will set the attach bit. If there are multiple Level 1/ Level 2 routers in the same central office networked to share the WAN link, these two routers would form a Level 2 adjacency. The Level 2 attach bit would be set. In either case, the central office Level 1/Level 2 routers will not have access to the OSS systems in the NOC if the WAN link is down. Packets forwarded to the Level 1/Level 2 router destined for the NOC will be discarded. The service provider wants the packets to be sent out the alternate GNE to an alternate central office.

There is a solution to this problem. For purpose of example, we will use a router named "3640A" (see Figure 23) to show the configurations and verifications. Router 3640A will continue to set the attach-bit when it has another Level 2 adjacency or the Cisco IOS IS-IS Multiarea feature is configured. In other words, router 3640A will set the attach-bit if it can reach multiple areas. The Level 1 routers nearest router 3640A will continue to forward traffic to router 3640A. Traffic sent to router 3640A is most likely destined for the area containing the OSS. The traffic, which is usually alarms destined for the NOC and alarm packets, will be dropped.

Cisco developed the IS-IS Attach-Bit Control feature to provide the network administrator with more control in setting the attach-bit. The feature is modeled after the IP **default-information originate** *route-map* router subcommand. The new command, **set-attach-bit**, is an IS-IS CLNS router subcommand and its syntax is as follows:

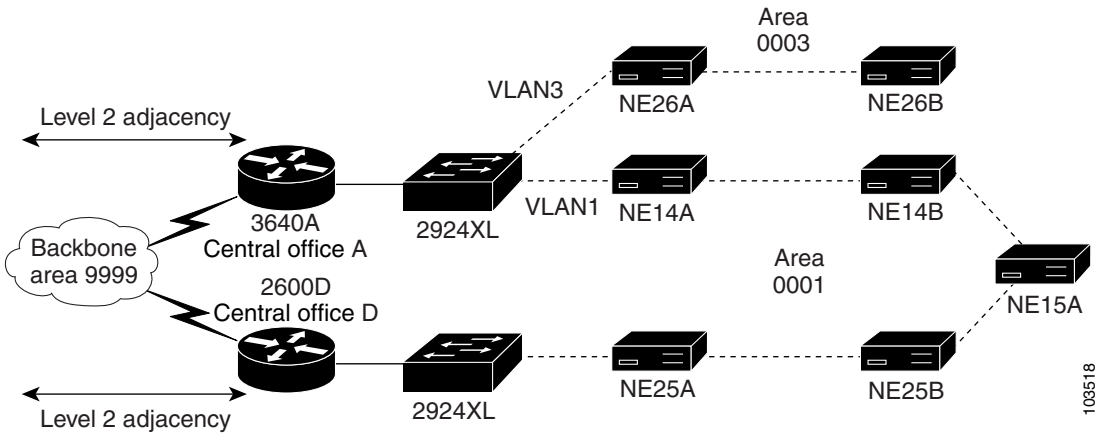
router isis
set-attach-bit {**always** | **never** | **route-map** *mapname*}

The **route-map** keyword can be used to specify multiple CLNS routes or prefixes. If one of the routes or prefixes is matched in the Level 2 CLNS routing table, the Level 1/Level 2 router sets the attach bit in the LSP.

The following example contains five SONET/SDH network elements in a chain between central office A and central office D. NE14A and router 3640A are located in central office A. NE14A is a GNE between the SONET/SDH DCC and the Ethernet. Device NE14A forwards traffic destined for another area to the nearest Level 2 router, which is router 3640A.

Located in central office D is the Level 1/Level 2 router labeled 2600D and GNE NE25A. The other three SONET/SDH network elements are located is separate central offices. All of these devices are configured for area 0001. Router 3640A is configured for IS-IS multiarea and is located in area 0003. Figure 23 shows the network and the connections to the backbone, which is area 9999.

Figure 23 Network with IS-IS Attach-Bit Control Configured



Verifying IS-IS Attach-Bit Control

To verify that the IS-IS Attach-Bit Control feature is configured, first display a baseline configuration without the IS-IS Attach-Bit Control feature configured. The network administrator can look at the attach-bit settings using the **show isis database** EXEC command. The following example shows output for router 3640A. In the IS-IS process called area000, router 3640A's attach-bit is set to 1 in the Level-1 link state database. The attach-bit field is labeled "ATT." The router is configured to run two IS-IS processes, area0001 and area0003.

```
3640A# show isis database

Area area0001:
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
3640A.00-00         * 0x00000009   0x7AB5        758               1/0/0
3640A.03-00         * 0x00000007   0x6705        649               0/0/0
NE15A.00-00           0x00000009   0x88E2        520               0/0/0
NE25B.00-00           0x0000000A   0x1DB6        660               0/0/0
NE25B.02-00           0x00000007   0x2941        871               0/0/0
NE14B.00-00           0x00000008   0xF840        744               0/0/0
NE14B.02-00           0x00000007   0x622C        794               0/0/0
2600D.00-00           0x0000000A   0xC715        758               1/0/0
NE14A.00-00           0x00000008   0x7C68        578               0/0/0
NE14A.01-00           0x00000007   0x8232        735               0/0/0
NE25A.00-00           0x00000007   0x8E92        563               0/0/0
NE25A.01-00           0x00000007   0x95E2        745               0/0/0
NE25A.02-00           0x00000007   0x69E3        578               0/0/0
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
BackBoneR1.00-00      0x0000000D   0x6BEF        599               0/0/0
3640A.00-00         * 0x0000000A   0x8457        758               0/0/0
3640A.02-00         * 0x00000007   0xC0AC        886               0/0/0
2600D.00-00           0x00000009   0xDE1C        765               0/0/0
2600D.02-00           0x00000007   0xFA61        847               0/0/0

Area area0003:
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
3631A.00-00           0x00000008   0x33D5        827               0/0/0
NE26B.00-00           0x00000009   0xAFE0        652               0/0/0
NE26B.02-00           0x00000007   0x87A3        554               0/0/0
3640A.00-00         * 0x00000008   0x52DE        564               1/0/0
```

```
3640A.01-00         * 0x00000007   0x5325        532               0/0/0
NE26A.00-00           0x00000009   0xA756        668               0/0/0
NE26A.02-00           0x00000008   0x8904        1128              0/0/0
```

Next, use the **ping clns** and **show clns route** EXEC commands to verify connectivity. Following is the output of ping to an IS-IS router in the area backbone:

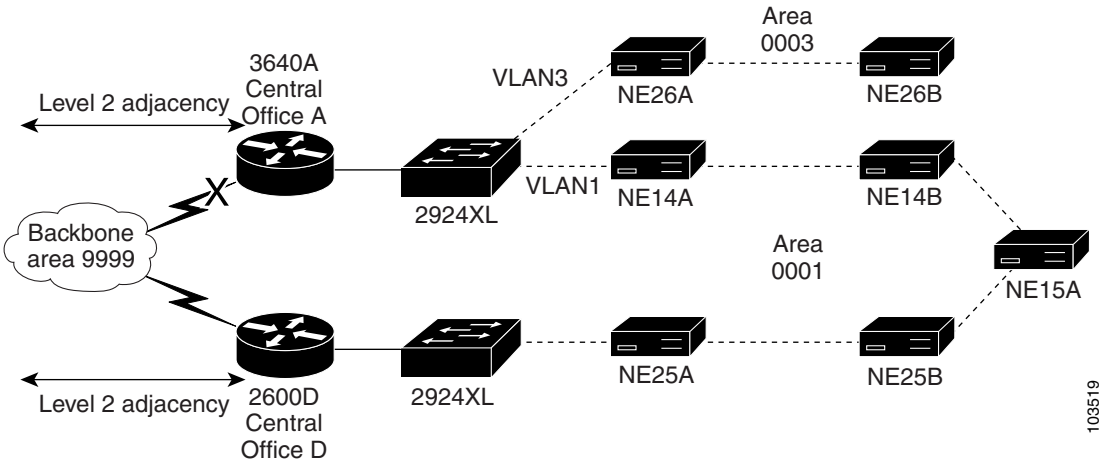
```
3640A# ping clns 39.840f.8011.9999.0000.1111.9999.000d.bc2e.6d80.00

Type escape sequence to abort.
Sending 5, 100-byte CLNS Echos with timeout 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

The following example shows the CLNS routing table with a route to backbone area 9999 (text in bold is for purpose of example only and indicates the backbone route):

```
3640A# show clns route

Codes: C - connected, S - static, d - DecnetIV
       I - ISO-IGRP,  i - IS-IS,  e - ES-IS
       B - BGP,       b - eBGP-neighbor

C  39.840f.8011.9999.0000.1111.0003 [2/0], Local IS-IS Area
C  39.840f.8011.9999.0000.1111.0001 [2/0], Local IS-IS Area
C  39.840f.8011.9999.0000.1111.0003.0010.7bc7.ae40.00 [1/0], Local IS-IS NET
C  39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00 [1/0], Local IS-IS NET

i  39.840f.8011.9999.0000.1111.9999 [110/10]
      via BackBoneR1, Ethernet0/1
```

Disconnect the connection to the backbone from router 3640A as shown in Figure 24, and display the IS-IS database again using the **show isis database** EXEC command.

Figure 24 Broken Network Link with IS-IS Attach-Bit Control Configured



Router 3640A still has the attach-bit set because the router is configured for the IS-IS Multiarea feature, so router 3640A can reach multiple areas. (You can determine the attach-bit setting by looking at the ATT field in the **show isis database** command output. The attach-bit is set when the value is 1.)

```
3640A# show isis database
```

```
Area area0001:
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
3640A.00-00         * 0x00000004   0x84B0        1181              1/0/0
3640A.03-00         * 0x00000002   0x71FF        1180              0/0/0
NE15A.00-00           0x00000004   0x92DD        612               0/0/0
NE25B.00-00           0x00000004   0x29B0        491               0/0/0
NE25B.02-00           0x00000003   0x313D        1165              0/0/0
NE14B.00-00           0x00000003   0x033B        417               0/0/0
NE14B.02-00           0x00000002   0x6C27        537               0/0/0
NE14A.00-00           0x00000005   0x8265        1179              0/0/0
NE14A.01-00           0x00000003   0x8A2E        1170              0/0/0
NE25A.00-00           0x00000003   0x46FD        1056              0/0/0
NE25A.02-00           0x00000002   0x73DE        409               0/0/0
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
3640A.00-00         * 0x00000001   0x4A75        1173              0/0/0

Area area0003:
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
3631A.00-00           0x00000003   0x3DD0        503               0/0/0
NE26B.00-00           0x00000004   0xB9DB        576               0/0/0
NE26B.02-00           0x00000003   0x8F9F        538               0/0/0
3640A.00-00         * 0x00000005   0x58DB        1177              1/0/0
3640A.01-00         * 0x00000004   0x5922        1177              0/0/0
NE26A.00-00           0x00000005   0xAF52        1178              0/0/0
NE26A.02-00           0x00000003   0x93FE        1166              0/0/0
```

The CLNS routing table displayed by the **show clns route** EXEC command shows that no connection to the backbone is available. There are only routes for areas 39.840f.8011.9999.0000.1111.0003 and 39.840f.8011.9999.1111.0001. The backbone route 39.840f.8011.9999.0000.1111.9999 has dropped out of the routing table. Packets destined to the backbone are dropped by router 3640A.

```
3640A# show clns route

Codes: C - connected, S - static, d - DecnetIV
       I - ISO-IGRP,  i - IS-IS,  e - ES-IS
       B - BGP,       b - eBGP-neighbor

C  39.840f.8011.9999.0000.1111.0003 [2/0], Local IS-IS Area
C  39.840f.8011.9999.0000.1111.0001 [2/0], Local IS-IS Area
C  39.840f.8011.9999.0000.1111.0003.0010.7bc7.ae40.00 [1/0], Local IS-IS NET
C  39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00 [1/0], Local IS-IS NET
```

The following example configures the **set-attach-bit** command. The **route-map** command sets conditions for setting the attach-bit. The **route-map** name or map tag assigned for the example is BackBone_Connection. The **match clns** command names the **clns filter** command that contains the NSAP address to match in the route table. In this example, the focus is on connectivity to the backbone.

```
clns filter-set BackBone_Area permit 39.840f.8011.9999.0000.1111.9999
!
router isis area0001
 net 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
 set-attached-bit route-map BackBone_Connection
!
route-map BackBone_Connection permit 10
 match clns address BackBone_Area
```

The following example reexamines the IS-IS database and the CLNS routing table after the **set-attach-bit** command is configured. The Level 1 database for the IS-IS area process area0001 shows that router 3640A is no longer setting the attach bit. The ATT field is set to zero for the LSP from router 3640A. Router 2600D is setting the attach-bit and providing access to the backbone. The ATT field is set to 1 for the LSP from router 2600D.

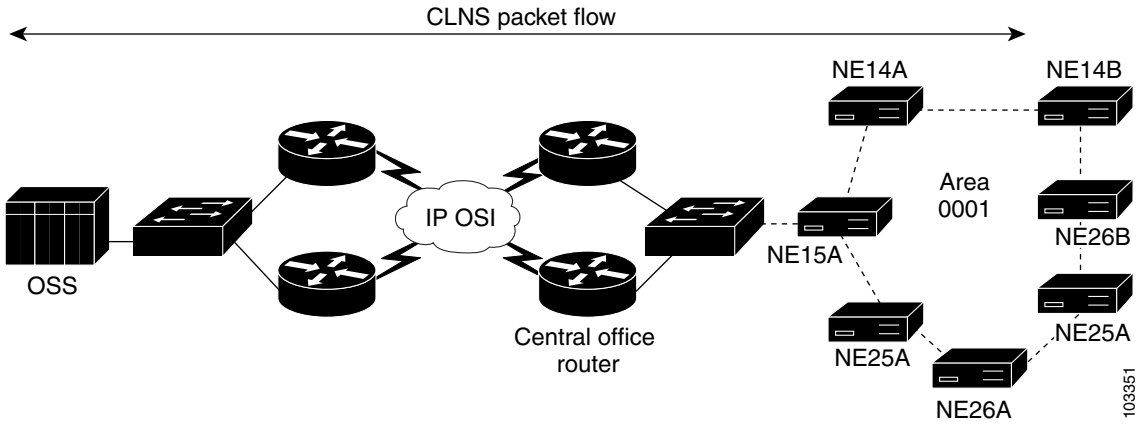
```
3640A# show isis database

Area area0001:
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
3640A.00-00         * 0x00000011   0x62CD        1143              0/0/0
3640A.03-00         * 0x0000000E   0x590C        557               0/0/0
NE15A.00-00           0x00000011   0x78EA        910               0/0/0
NE25B.00-00           0x0000000F   0x13BB        766               0/0/0
NE25B.02-00           0x0000000E   0x1B48        671               0/0/0
NE14B.00-00           0x0000000F   0xEA47        700               0/0/0
NE14B.02-00           0x0000000E   0x5433        512               0/0/0
2600D.00-00           0x00000011   0xB91C        1013              1/0/0
NE14A.00-00           0x0000000F   0x6E6F        647               0/0/0
NE14A.01-00           0x0000000F   0x723A        1106              0/0/0
NE25A.00-00           0x0000000E   0x8099        879               0/0/0
NE25A.01-00           0x0000000F   0x85EA        917               0/0/0
NE25A.02-00           0x0000000F   0x59EB        1140              0/0/0
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
BackBoneR1.00-00      0x00000010   0x65F2        426               0/0/0
3640A.00-00         * 0x00000010   0x2C84        1131              0/0/0
3640A.02-00         * 0x0000000E   0xB2B3        541               0/0/0
2600D.00-00           0x0000000F   0xD222        454               0/0/0
2600D.02-00           0x0000000F   0xEA69        818               0/0/0

Area area0003:
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
3631A.00-00           0x0000000F   0x25DC        491               0/0/0
NE26B.00-00           0x00000010   0xA1E7        523               0/0/0
NE26B.02-00           0x0000000F   0x77AB        975               0/0/0
3640A.00-00         * 0x0000000F   0x44E5        562               1/0/0
3640A.01-00         * 0x0000000E   0x452C        510               0/0/0
NE26A.00-00           0x00000011   0x975E        1151              0/0/0
NE26A.02-00           0x0000000F   0x7B0B        1144              0/0/0
3640A#
```

Additional information on the IS-IS Attach-Bit Control feature can be found on CCO. Refer also to the Cisco IOS Product Marketing Application Note, *Using the IS-IS Attach-Bit Control Feature*.

Using IP over CLNS Tunnels to Access Remote Devices

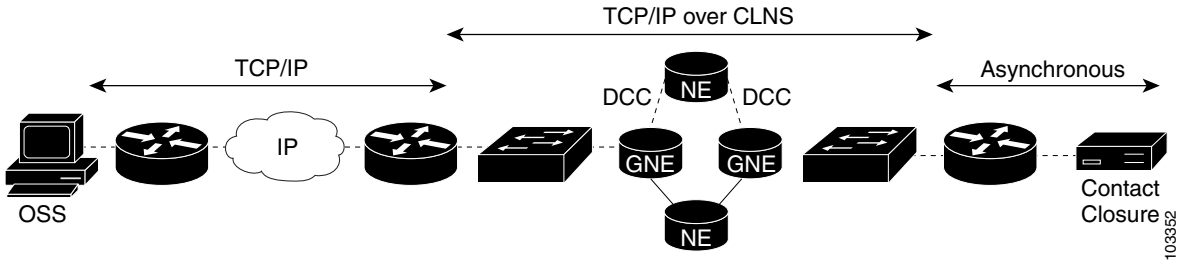
The SONET/SDH DCC is an extension of the telco DCN. Service providers do not want to build the DCN out to every SONET/SDH location. Figure 25 shows a typical telco network where each of the network elements are located at different physical locations. The DCC is used to communicate to remote SONET/SDH add/drop multiplexers (ADMs) on the ring.

Figure 25 Typical Telco Network with Network Elements at Different Locations



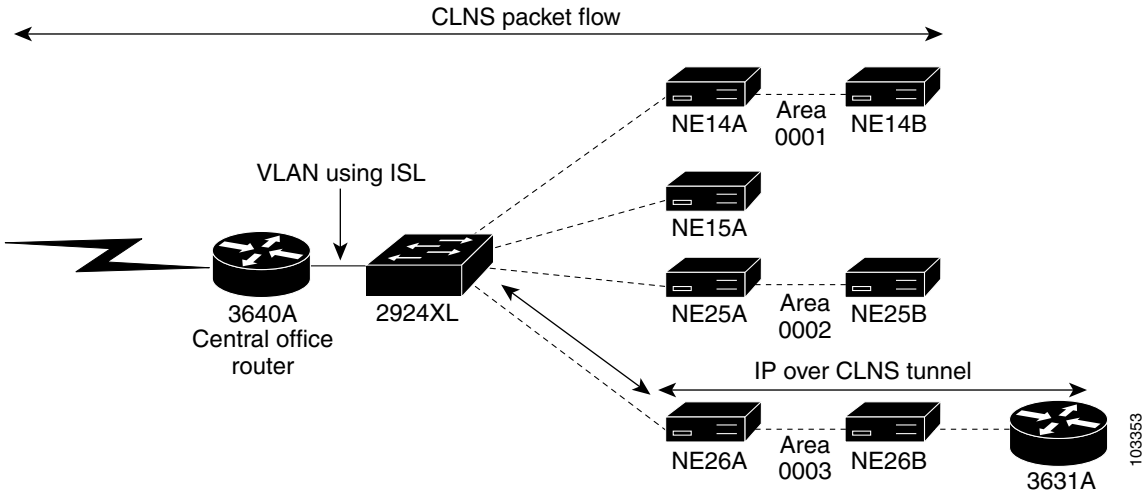
Service providers need to reach asynchronous and IP devices in the same location as the SONET/SDH nodes. Typically, the service providers are trying to access a contact closure device, as shown in Figure 26. Service providers can use the DCC by tunneling IP over CLNS. The router located in the central office in front of the GNE is usually the one used to create the tunnel. The router in the remote location usually terminates the CLNS tunnel and the TCP/IP session. The data is sent out the asynchronous connection to the contact closure device.

Figure 26 Telco Network Data Flow to a Contact Closure Device



Cisco has developed a contact closure device, which is a network module called the NM-AIC-64 that can be installed in the Cisco 2600, 3600, and 3700 series routers. The tunneling examples in this section use a Contact Closure device (the NM-AIC-64) embedded in router 3631A shown in Figure 27.

Figure 27 Telco Network with Cisco Contact Closure Device



Configuring a Tunnel Using IP over CLNS

In Figure 27, the IP over CLNS tunnel is created from the Cisco 3640A router to the Cisco 3631A router. The following example shows the CLNS tunnel configuration for the two routers:

Cisco 3640A Router Configuration

```
interface CTunnel1
 description connection remote site with 3631A
 ip address 192.168.10.1 255.255.255.252
 ctunnel destination 39.840f.8011.9999.0000.1111.0003.0001.6444.3410.cc
!
router isis area0003
 net 39.840f.8011.9999.0000.1111.0003.0010.7bc7.ae40.00
 is-type level-1
```

Cisco 3631A Router Configuration

```
clns routing
!
interface CTunnel1
 ip address 192.168.10.2 255.255.255.252
 ctunnel destination 39.840f.8011.9999.0000.1111.0003.0010.7bc7.ae40.cc
!
router isis area0003
 net 39.840f.8011.9999.0000.1111.0003.0001.6444.3410.00
 is-type level-1
```

Verifying the IP over CLNS Tunnel Configuration

The tunnel is actually configured as an interface and the status of the tunnel can be checked with the **show interfaces ctunnel1** command, as follows:

```
3640A# show interfaces ctunnel1

CTunnel1 is up, line protocol is up
  Hardware is CTunnel
  Description: connection remote site with 3631A
  Internet address is 192.168.10.1/30
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
```

```
   reliability 255/255, txload 56/255, rxload 28/255
Encapsulation TUNNEL, loopback not set
Keepalive set (10 sec)
Tunnel destination 39.840f.8011.9999.0000.1111.0003.0001.6444.3410.cc
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 1000 bits/sec, 3 packets/sec
5 minute output rate 2000 bits/sec, 2 packets/sec
   217 packets input, 13104 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   177 packets output, 33658 bytes, 0 underruns
   0 output errors, 0 collisions, 0 interface resets
   0 output buffer failures, 0 output buffers swapped out
```

The report shows that the CLNS tunnel is physically up. The “line protocol is up” report indicates that the router has a route to the CLNS tunnel destination. The hardware report indicates the interface type is CTunnel. The tunnel destination is 39.840f.8011.9999.0000.1111.0003.0001.6444.3410.cc, which is the NET for the Cisco 3631A router. Additional information about the **show interfaces ctunnel** command can be found in the Cisco IOS Software Release 12.1T *IP over a CLNS Tunnel* feature module at the following URL:
http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1834/products_feature_guide09186a0080080382.html

Note Cisco released the IP over CLNS Tunnel feature before an industry standard existed. An RFC has been created to tunnel IPv4 and IPv6 over CLNS. Cisco supports the feature beginning in Cisco IOS Release 12.3(7)T. The default tunnel mode is the original Cisco solution. An option on the tunnel interface allows the tunnel to be set to GRE. The Cisco IOS Release 12.3(7)T document describing the *CLNS Support for GRE Tunneling of IPv4 and IPv6 Packets in CLNS Networks* feature module at the following URL:
http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_feature_guide09186a00801ffb3d.html

Configuring a Contact Closure Device

The tunnel in the previous configuration example was created to access the Contact Closure device (the NM-AIC-64) in the Cisco 3631 router. The NM-AIC-64 is installed in the second network module slot and communicates across the PCI bus in the router. The NM-AIC-64 requires an IP address to access it, and must be assigned an IP address and a static route that points to the IP address of the NM-AIC-64. The static route should be redistributed into the IP routing protocol.

The following example shows the basic configuration for the NM-AIC-64:

```
alarm-interface 2
 ip address 192.168.10.5
!
ip route 192.168.10.5 255.255.255.255 Serial2/0
!
router ospf 795
 log-adjacency-changes
 redistribute static subnets
 network 192.168.0.0 0.0.255.255 area 0
```

Verifying the Contact Closure Device Configuration

The following example shows the report from issuing the **show ip route** command on the Cisco 3631A router. The static route to reach NM-AIC-64 is highlighted in bold text for purpose of example. Notice that the NM-AIC-64 looks like a serial device connected to the router.

```
3631A# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O    192.168.12.0/24 [110/11112] via 192.168.10.1, 00:10:51, CTunnel1
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/30 is directly connected, CTunnel1
S       192.168.10.5/32 is directly connected, Serial2/0
O    192.168.0.0/24 [110/11121] via 192.168.10.1, 00:10:51, CTunnel1
     192.168.2.0/26 is subnetted, 2 subnets
O       192.168.2.64 [110/11112] via 192.168.10.1, 00:10:51, CTunnel1
O       192.168.2.128 [110/11112] via 192.168.10.1, 00:10:51, CTunnel1
     192.168.3.0/26 is subnetted, 1 subnets
O       192.168.3.128 [110/11122] via 192.168.10.1, 00:10:52, CTunnel1
```

The following example shows the report from issuing the **show ip route** command on the Cisco 3640A router. The static route to reach the NM-AIC-64 is highlighted in bold text for purpose of example, and looks like an external route learned over OSPF.

```
3640A# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

C    192.168.12.0/24 is directly connected, FastEthernet3/0.1
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/30 is directly connected, CTunnel1
O E2    192.168.10.5/32 [110/20] via 192.168.10.2, 00:09:48, CTunnel1
C    192.168.0.0/24 is directly connected, Ethernet0/0
     12.0.0.0/32 is subnetted, 1 subnets
R       12.222.16.0 [120/1] via 192.168.0.1, 00:00:16, Ethernet0/0
     192.168.2.0/26 is subnetted, 2 subnets
C       192.168.2.64 is directly connected, FastEthernet3/0.2
C       192.168.2.128 is directly connected, FastEthernet3/0.3
     192.168.3.0/26 is subnetted, 1 subnets
O       192.168.3.128 [110/11] via 192.168.2.190, 00:09:48, FastEthernet3/0.3
R*   0.0.0.0/0 [120/1] via 192.168.0.1, 00:00:16, Ethernet0/0
```

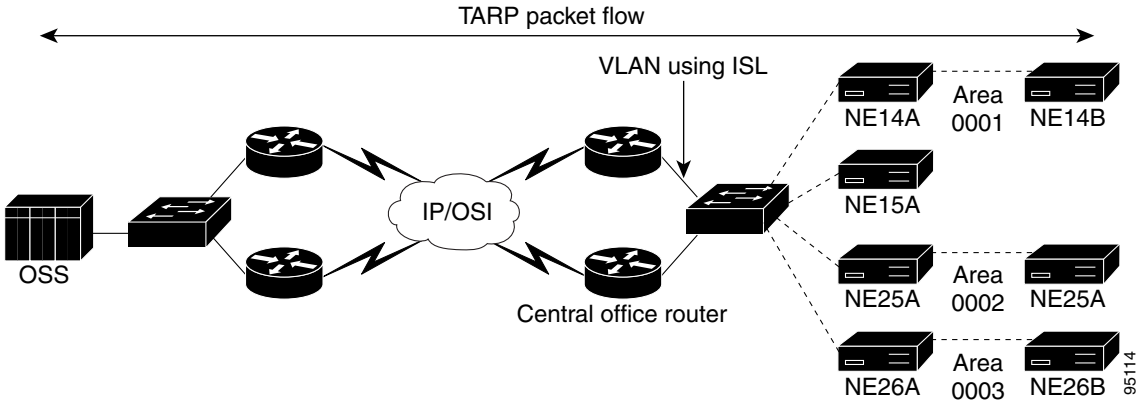
For more information about configuring the NM-AIC-64, refer to the document *NM-AIC-64, Contact Closure Network Module*.

Mapping NSAPs to Device Names Using TARP

This section describes a method of mapping NSAPs to device names. In North America, ILECs and long distance carriers use a TID—a network-wide unique *target identifier*—to name a piece of equipment. The TID is a string of up to 20 case-sensitive characters. Service providers needed a dynamic method to map TIDs to NSAPs or network entity titles (NETs)—the terms NSAP and NET are often used interchangeably within the telco industry—and TARP serves that purpose. TARP runs over the Connectionless Network Protocol (CLNP), as defined in ISO 8473, and all Cisco routers that support CLNS routing support TARP. TARP is documented in GR-253-Core section 8. Additional documentation about TARP can be found on the ATIS website at www.atis.org. TARP was developed as part of the SONET Interoperability Forum (SIF).

TARP was developed to map the name for a network element (NE) to an NSAP. The OSS administrator typically knows the network element TID when building a profile for the device, but often does not know the NSAP. TARP was designed to dynamically map the TID to the NSAP. TARP was implemented on the router to facilitate the mapping across a network. Typically, the service provider has an OSS in the data center that needs to communicate with a network element in the central office, as shown in Figure 28.

Figure 28 Typical TARP Configuration and Packet Flow



A router can be configured to participate in TARP. The router is actually assigned a TID. The NET of a router is associated with the TID.

Note The network layer for a device cannot have an address in OSI; instead, the device must have an NET. The NET at the network layer is actually an NSAP with a selector value of 00. IS-IS routers are assigned NETs. The TARP cache maps the NET of the IS-IS router to the TID.

The following example shows how to configure the IS-IS router to assign the NET (notice that the NET is the NSAP with a network selector value of 00):

```
router isis area0001
 net 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
```

In OSI, File Transfer, Access, and Management (FTAM) and other applications have a specific network selector (also called N-selector) value that identifies the application. The network selector value for the TARP application are the hexadecimal digits AF. The network selector is analogous to a TCP port number.

TARP uses five types of protocol data units (PDUs):

- Type 1 PDU is a request for the NSAP with a specific TID value within a Level 1 routing area. The type 1 PDU is propagated to all of the IS-IS Level 1 adjacencies and ES-IS adjacencies. A separate type 1 PDU is sent to every adjacency. A type 1 packet can be issued from a Cisco router using the **tarp resolve tid** or **tarp resolve tid 1** EXEC command.
- Type 2 PDU is a request for the NSAP with a specific TID value within a Level 2 routing area. A type 2 request PDU is propagated by an individual type 2 PDU being sent to all of the IS-IS and ES-IS adjacencies in the IS-IS router. A type 2 packet can be issued from a Cisco router using the **tarp resolve tid 2** EXEC command. The **tarp resolve tid** EXEC command issues a type 2 packet after the type 1 fails.
- Type 3 PDU is a response to a TARP request. The TARP request could be a type 1, type 2, or type 5 PDU. The type 3 packet is a unicast PDU, and a single PDU is sent directly back to the originator.
- Type 4 PDU is a notification of an NSAP address change or a TID change. The type 4 PDU is propagated through the entire network. The type 4 PDU is sent to all of the adjacencies of the network element.
- Type 5 PDU is a request for a TID that matches a specific NSAP. The type 5 PDU is sent directly to a specific NSAP. A type 5 PDU can be issued from a Cisco router using the **tarp query** EXEC command.

In a traditional IS-IS implementation, a single IS-IS process is configured. The TARP application uses the NET in the single process for creating the NSAP. If the router is configured with an IS-IS multiarea, TARP will behave as follows:

- The router uses the NET of the Level 2 area if a Level 2 process is configured, so that the NSAP for the TID will be the NET of the Level 2 process with a selector value of AF.
- If no Level 2 process is configured and multiple Level 1 processes are configured, the first active Level 1 process NET will be used.

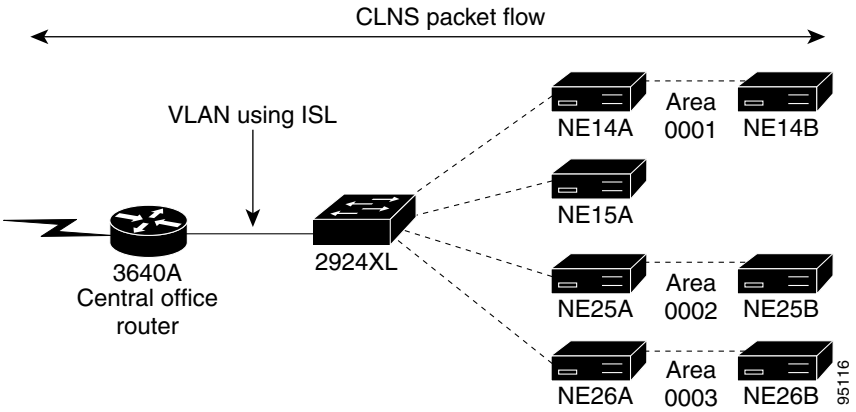
Note Multiple Level 1 processes are sorted by the process name alphanumerically, and capital letters are sorted ahead of lowercase letters.

If a Level 1 process is added or removed, the NSAP associated with the TID can change at the next reload of the router.

- Type 1 PDUs received are processed as normal. The TARP data cache is checked for an entry. If no entry is present, the type 1 PDU is propagated to all Level 1 IS-IS and ES-IS adjacencies in the same Level 1 area.
- Type 2 PDUs received are processed as normal. The TARP data cache is checked for an entry. If no entry is present, the type 2 PDU is propagated to all IS-IS and ES-IS adjacencies. If the PDU originated in a different Level 1 IS-IS area, the TID and NET of the source will be cached in the TARP data cache.
- Type 4 PDUs are forwarded to all ES-IS and IS-IS adjacencies.
- Type 3 and type 5 PDUs are sent to a specific NSAP and are therefore routed. The type 3 PDU is a response to a type 1 or type 2 PDU originated at a specific address.

The Cisco router labeled “3640A” in Figure 29 is configured with multiple IS-IS processes.

Figure 29 IS-IS Multiarea Network Using VLAN Trunking and ISL Encapsulation



Use the **show tarp tid-cache** EXEC command to examine the TARP TID cache. The following is sample output from this command:

```
3640A# show tarp tid-cache

TID ('*' : static; & : local)                    NSAP

& 3640A                        39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
3640A#
```

The following example lists the configuration for the Cisco 3640 router. The first IS-IS process listed is area0001. The NET associated with the process area0001 is 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00, which matches the NET listed in the TARP TID cache for the Cisco router labeled "3640A." (Remember the rule that the NET of the Level 2 IS-IS process would be associated with the TID.)

```
3640A# show configuration

Using 2849 out of 129016 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3640A
!
boot system slot1:
boot system flash
boot system rom
boot system slot0:
logging queue-limit 100
!
ip subnet-zero
clns routing
mpls ldp logging neighbor-changes
no ftp-server write-enable
!
!
!
!
interface Ethernet0/0
 ip address 192.168.0.49 255.255.255.0
```

```
 half-duplex
 no cdp enable
!
interface Ethernet0/1
 no ip address
 shutdown
 half-duplex
 no cdp enable
!
interface Ethernet0/2
 no ip address
 shutdown
 half-duplex
 no cdp enable
!
interface Ethernet0/3
 ip address 10.19.250.33 255.255.255.248
 shutdown
 half-duplex
 no cdp enable
!
interface Serial1/0
 no ip address
 clockrate 9600
 no cdp enable
!
interface Serial1/1
 no ip address
 shutdown
 no cdp enable
!
interface Serial1/2
 no ip address
 clockrate 9600
 no cdp enable
!
interface Serial1/3
 no ip address
 clockrate 9600
 no cdp enable
!
interface FastEthernet3/0
 no ip address
 duplex auto
 speed auto
 no cdp enable
!
interface FastEthernet3/0.1
 description ISIS area 0001
 encapsulation dot1Q 1 native
 ip address 192.168.12.24 255.255.255.0
 no ip redirects
 no cdp enable
 clns router isis area0001
 isis priority 127
 tarp enable
!
interface FastEthernet3/0.2
 description ISIS area 0002
 encapsulation dot1Q 2
 ip address 192.168.2.125 255.255.255.192
 no ip redirects
 no cdp enable
 clns router isis area0002
```

```
 isis priority 127
 tarp enable
!
interface FastEthernet3/0.3
 description ISIS area 0003
 encapsulation dot1Q 3
 ip address 192.168.2.189 255.255.255.192
 no ip redirects
 no cdp enable
 clns router isis area0003
 isis priority 127
 tarp enable
!
router ospf 795
 no log-adjacency-changes
 network 192.168.0.0 0.0.255.255 area 0
!
router isis area0001
 net 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
!
router isis area0002
 net 39.840f.8011.9999.0000.1111.0002.0010.7bc7.ae40.00
 is-type level-1
!
router isis area0003
 net 39.840f.8011.9999.0000.1111.0003.0010.7bc7.ae40.00
 is-type level-1
!
router rip
 network 192.168.0.0
!
no ip http server
no ip classless
ip route 0.0.0.0 0.0.0.0 172.31.232.17
!
!
no cdp run
clns host NE14A 39.840f.8011.9999.0000.1111.0001.00e0.b064.4324.00
clns host NE14B 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00
clns host NE25A 39.840f.8011.9999.0000.1111.0002.00e0.b064.434e.00
clns host NE25B 39.840f.8011.9999.0000.1111.0002.0030.94e2.6ce0.00
clns host NE26A 39.840f.8011.9999.0000.1111.0003.00d0.5872.9720.00
clns host NE26B 39.840f.8011.9999.0000.1111.0003.0010.7b17.f880.00
clns host NE15A 39.840f.8011.9999.0000.1111.0001.0010.7bd8.c7d0.00
clns host 3640A 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
!
tftp-server slot1:
tarp run
tarp tid 3640A
!
line con 0
 password cisco
line aux 0
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
line vty 5 99
 login
!
end
```

Enabling TARP

The following example shows the **tarp run** and **tarp tid** global configuration commands used to enable TARP on a central office router:

```
tarp run
tarp tid 3640A
```

TARP must be enabled on an interface in order for TARP packets to be forwarded. TARP is enabled on the Cisco router labeled "3640A," shown in Figure 30 on page 62. The configuration for Fast Ethernet interface 3/0.1 is listed in the following example; the **tarp enable** interface configuration command is the last command listed.

```
interface FastEthernet3/0.1
 description ISIS area 0001
 encapsulation dot1Q 1 native
 ip address 192.168.12.24 255.255.255.0
 no ip redirects
 no cdp enable
 clns router isis area0001
 isis priority 127
 tarp enable
```

Use the **show tarp** EXEC command to display the global TARP configuration information on a router:

```
3640A# show tarp

Global TARP information:
  TID of this station is "3640A"
  Timer T1 (timer for response to TARP Type 1 PDU) is 15 seconds
  Timer T2 (timer for response to TARP Type 2 PDU) is 25 seconds
  Timer T3 (timer for response to ARP request) is 40 seconds
  Timer T4 (timer that starts when T2 expires) is 15 seconds
  Loop Detection Buffer entry timeout : 300 seconds
  Loop Detection Buffer zero sequence timer is 300 seconds
  TID cache entry timeout : 3600 seconds
  This station will propagate TARP PDUs
  This station will originate TARP PDUs
  TID<->NET cache is enabled
  Sequence number that next packet originated by this station will have : 1
  Update remote cache (URC) bit is 0
  Packet lifetime : 100 hops
  Protocol type used in outgoing packets : "FE"
  N-Selector used in TARP PDU's : "AF"
```

Use the following information to interpret the report:

- TID of this station is 3640A. (Remember that the TID is case-sensitive.)
- Timers T1, T2, T3, and T4 are set at the default values defined in GR-253-Core Section 8:
  - Timer T1 is the time that the router waits for a response to a TARP type 1 PDU. Timer T1 can be altered with the **tarp t1-response-timer** *seconds* global configuration command. The range of seconds is from 0 to 3600 with a default of 15.
  - Timer T2 is the time that the router waits for a response to a TARP type 2 PDU. Timer T2 can be altered with the **tarp t2-response-timer** *seconds* global configuration command. The range of seconds is from 0 to 3600 with a default of 25.
  - Timer T3 is the time that the router waits for a response to an address resolution request, which is a TARP type 5 PDU. Timer T3 can be altered with the **tarp arp-request-timer** *seconds* global configuration command. The range of seconds is from 0 to 3600 with a default of 40.

  - Timer T4 starts when timer T2 expires. The timer is used for error recovery, and can be altered with the **tarp post-t2-response-timer** *seconds* global configuration command. The range of seconds is from 0 to 3600 with a default of 15.

- The Loop Detection Buffer helps prevent TARP type 1, type 2, and type 4 packets from looping throughout the network. The entry timeout value determines the amount of time that mapping data will be stored in the loop detection database.
- The Loop Detection Buffer zero sequence timer starts when a TARP packet with a value of 0 (zero) is received. Additional TARP packets with a sequence value of 0 that are received before the timer expires are discarded. The timer value displayed in the example is set to 5 minutes (300 seconds).
- TID cache entry timeout indicates the amount of time the TID-to-NSAP maps will be cached in the router, which in this example is 3600 seconds (1 hour). The TID cache timer is configurable with the **tarp cache-timer** *seconds* global configuration command. The caching of the TID can be turned on or off with the **tarp allow-caching** global configuration command. TID caching is on by default.
- "This station will propagate TARP PDUs" indicates that the router can forward TARP PDUs.
- "This station will originate TARP PDUs" indicates that the router can originate TARP PDUs.
- "TID<->NET cache is enabled" indicates that the TID-to-NSAP maps will be cached by the router. The cache timer is set to 3600 seconds (1 hour). The cache value can range from 30 to 86400 seconds (24 hours).
- "Sequence number that the next TARP packet originated by this router will have" indicates a value of 1; the value can range from 0 to 65535. The sequence number prevents broadcast storms and is the next outgoing TARP packet. The sequence number can be changed with the **tarp sequence-number** *number* global configuration command.
- An update remote cache (URC) bit value of 0 (zero) indicates that remote routers should store the TARP type 3 packet in their cache. A value of 1 would tell the remote hosts not to store the packet in the remote router's cache. The URC value can be changed using the **tarp urc** {**0** | **1**} global configuration command.
- Packet lifetime is the number of hops that the packet can live. Each IS-IS router the packet traverses is counted as one hop. The default hop number is 100, and the range is from 0 to 65535.
- Protocol type "FE" is used to identify the CLNP, as specified in GR-253-CORE section 8. This parameter can be configured using Cisco IOS software. The protocol type can be specified in outgoing TARP PDUs with the **tarp protocol hex-digit** global configuration command.
- N-selector is the network selector value used in TARP PDUs. In this example, the network selector value are the hexadecimal digits AF, which designates the TARP application as specified in GR-253-CORE section 8. This parameter can be configured using Cisco IOS software. The N-selector value generated with the TARP PDU can be changed with the **tarp selector hex-digit** global configuration command.

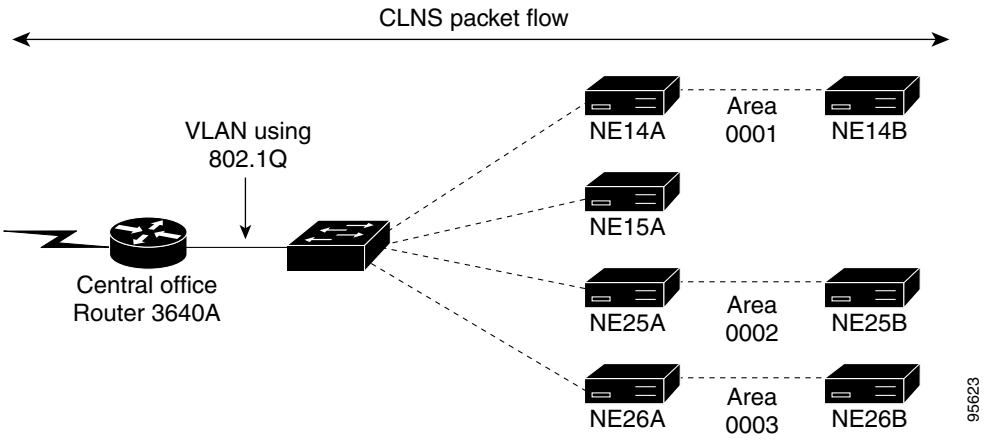
Using TARP with Remote Login Applications

One reason TARP was developed was to assist remote login applications. Central office technicians may not know the NSAP of the device that they want to log in to remotely, but they can determine the name of the equipment or the TID.

Network monitoring applications such as Telcordia's Network Management Application (NMA) or Provision applications such as Fujitsu's Flexr can also take advantage of TARP as a dynamic method to map TIDs to NSAPs or NETs. The system administrator would have to type in only the TID for the device that was to be monitored or provisioned, which is much easier than typing the NSAP. The OSS application would then issue a TARP type 1 or type 2 packet to learn the NET.

To issue a TARP type 1 or type 2 request on a Cisco router, use the **tarp resolve tid** EXEC command. Use Figure 30 as an example network for interpreting the reports displayed.

Figure 30 Sample Network for Interpreting TARP Reports



Issue a TARP type 1 request for the NET for device NE15A using the **tarp resolve tid** EXEC command:

```
3640A# tarp resolve tid NE15A

Type escape sequence to abort.
Sending TARP type 1 PDU, timeout 15 seconds ...

 NET corresponding to TID NE15A is 39.840f.8011.9999.0000.1111.0001.0010.7bd8.c7d0.00
```

The request returns a message indicating that a TARP type 1 PDU was sent out. The software will wait for 15 seconds for a reply (the default time value for the T1 timer). If no response is received after 15 seconds, a type 2 PDU would be sent out to all of the IS-IS and ES-IS nodes that support TARP.

In this example, the network element with the TID value of NE15A did respond with a TARP type 3 PDU, and the software picked up and displayed the NET on the screen. The NET is 39.840f.8011.9999.0000.1111.0001.0010.7bd8.c7d0.00. The TID-to-NET map will be stored in the router's TARP data cache.

To display the contents of the TARP data cache, use the **show tarp tid-cache** EXEC command. The TID for router 3640A and device NE15A is listed in the TARP data cache.

```
3640A# show tarp tid-cache

TID ('*' : static; & : local)                   NSAP

& 3640A                       39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
  NE15A                       39.840f.8011.9999.0000.1111.0001.0010.7bd8.c7d0.00
```

To clear the TARP cache, use the **clear tarp tid-cache** command:

```
3640A# clear tarp tid-table
```

Check the TARP TID cache after clearing it to verify that only the Cisco router labeled "3640A" is listed:

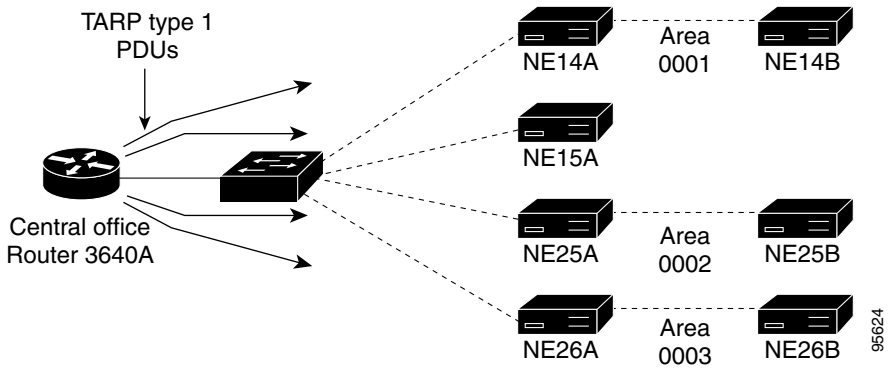
```
3640A# show tarp tid-cache

TID ('*' : static; & : local)                   NSAP

& 3640A                       39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
```

It is possible to watch the propagation of the TARP PDUs, for example, to watch router 3640A generate a TARP type 1 PDU for every adjacency. Use the **show clns neighbors** EXEC command to show all of the adjacencies:

```
3640A# show clns neighbors

Area area0001:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
NE15A          Fa3/0.1     0010.7bd8.c7d0  Up     27        L1   IS-IS
NE14A          Fa3/0.1     00e0.b064.4325  Up     21        L1   IS-IS

Area area0002:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
NE25A          Fa3/0.2     00e0.b064.434e  Up     22        L1   IS-IS

Area area0003:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
NE26A          Fa3/0.3     00d0.5872.9720  Up     21        L1   IS-IS
```

Four adjacencies are listed and all are of type Level 1. Figure 30 has been redrawn in Figure 31 with an arrow depicting each of the TARP type 1 PDUs being sent out. One important point to note is that TARP is not a broadcast protocol. A type 1 packet is generated and sent out to each of the IS-IS adjacencies. Sending separate PDUs to each adjacency will generate more network traffic than a single broadcast packet.

Figure 31 Transmission of TARP Type 1 PDUs



TARP **debug** commands can also help track the packets that are being sent. Before the **debug** command is issued, a list of the system identifiers will help analyze the command output:

```
3640A system id 0010.7bc7.ae40
NE14A system is 00e0.b064.4324
NE14B system id 0050.7363.7b40
NE25A system id 00e0.b064.434e
NE25B system is 0030.94e2.6ce0
NE26A system id 00d0.5872.9720
NE26B system id 0010.7b17.f880
NE15A system id 0010.7bd8.c7d0
```

To verify the TARP type 1 PDUs that are being sent out, issue the **debug tarp packet** command. In addition, issue the **debug tarp events** command to track additional TARP PDU activity.

```
3640A# debug tarp packets
TARP packet info debugging is on
3640A# debug tarp events
TARP events debugging is on
```

Next issue the **tarp resolve tid** EXEC command for device NE15A. In the following example, the router will wait 15 seconds for a response before issuing a TARP type 2 PDU. Device NE15A responds within 15 seconds with its NET, which is the NSAP address and selector value of 00.

```
3640A# tarp resolve tid NE15A

Type escape sequence to abort.
Sending TARP type 1 PDU, timeout 15 seconds ...

 NET corresponding to TID NE15A is 39.840f.8011.9999.0000.1111.0001.0010.7bd8.c7d0.00
```

The **debug tarp packets** command output shows a TARP type 1 PDU being sent to each of the four IS-IS adjacencies over the Fast Ethernet interface connection; four type 1 PDU packet will be sent out. The first type 1 packet is sent to device NE15A (0010.7bd8.c7d0) from the Cisco router labeled "3640A" (0010.7bc7.ae40):

```
3640A#
00:16:50: TARP-PA: Propagated TARP packet, type 1, out on FastEthernet3/0.1
00:16:50:        Lft = 100, Seq = 7, Prot type = 0xFE, URC = TRUE
00:16:50:        Dtid len = 5, Stid len = 5, Prot addr len = 20
00:16:50:        Destination NSAP : 39.840f.8011.9999.0000.1111.0001.0010.7bd8.c7d0.00
00:16:50:        Originator's NSAP : 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
00:16:50:        Target TID : NE15A
00:16:50:        Originator's TID : 3640A
```

The **debug tarp packets** output continues by showing the second type 1 packet being sent to device NE14A (00e0.b064.4324) from the Cisco router labeled "3640A" (0010.7bc7.ae40):

```
00:16:50: TARP-PA: Propagated TARP packet, type 1, out on FastEthernet3/0.1
00:16:50:        Lft = 100, Seq = 7, Prot type = 0xFE, URC = TRUE
00:16:50:        Dtid len = 5, Stid len = 5, Prot addr len = 20
00:16:50:        Destination NSAP : 39.840f.8011.9999.0000.1111.0001.00e0.b064.4324.00
00:16:50:        Originator's NSAP : 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
00:16:50:        Target TID : NE15A
00:16:50:        Originator's TID : 3640A
```

The **debug tarp packets** output continues by showing the third type 1 packet being sent to device NE25A (00e0.b064.434e) from the Cisco router labeled "3640A" (0010.7bc7.ae40):

```
00:16:50: TARP-PA: Propagated TARP packet, type 1, out on FastEthernet3/0.2
00:16:50:        Lft = 100, Seq = 7, Prot type = 0xFE, URC = TRUE
00:16:50:        Dtid len = 5, Stid len = 5, Prot addr len = 20
00:16:50:        Destination NSAP : 39.840f.8011.9999.0000.1111.0002.00e0.b064.434e.00
00:16:50:        Originator's NSAP : 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
00:16:50:        Target TID : NE15A
00:16:50:        Originator's TID : 3640A
```

The **debug tarp packets** output shows a fourth type 1 packet being sent to device NE26A (00d0.5872.9720) from the Cisco router labeled "3640A" (0010.7bc7.ae40):

```
00:16:50: TARP-PA: Propagated TARP packet, type 1, out on FastEthernet3/0.3
00:16:50:        Lft = 100, Seq = 7, Prot type = 0xFE, URC = TRUE
00:16:50:        Dtid len = 5, Stid len = 5, Prot addr len = 20
00:16:50:        Destination NSAP : 39.840f.8011.9999.0000.1111.0003.00d0.5872.9720.00
00:16:50:        Originator's NSAP : 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
00:16:50:        Target TID : NE15A
00:16:50:        Originator's TID : 3640A
```

Next, the **debug tarp packets** output shows a type 3 packet being received on Fast Ethernet interface 3/0.1 by router 3640A (0010.7bc7.ae40) from device NE15A (0010.7bd8.c7d0):

```
00:16:50: TARP-PA: Received TARP type 3 PDU on interface FastEthernet3/0.1
00:16:50:        Lft = 100, Seq = 3, Prot type = 0xFE, URC = TRUE
```

```
00:16:50:        Ttid len = 0, Stid len = 5, Prot addr len = 20
00:16:50:        Packet sent/propagated by
39.840f.8011.9999.0000.1111.0001.0010.7bd8.c7d0.af
00:16:50:        Originator's NSAP : 39.840f.8011.9999.0000.1111.0001.0010.7bd8.c7d0.00
00:16:50:        Originator's TID : NE15A
```

Finally, the **debug tarp events** output shows a TARP cache entry being created. A value is set for the loop detection buffer (LDB). The loop detection buffer is a method of deterring packets from propagating TARP packets that the IS-IS router has already seen.

```
00:16:50: TARP-PA: Created new DYNAMIC cache entry for NE15A
00:16:50: TARP-EV: Packet from 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
discarded - sequence
00:16:50:        number (7) <= that in LDB cache entry (7)
00:16:50: TARP-EV: Packet from 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
discarded - sequence
00:16:50:        number (7) <= that in LDB cache entry (7)
```

Notice that the TARP application generated a separate unicast packet for every adjacency instead of a single broadcast packet.

Controlling TARP Propagation Using Split Horizon

The original implementations of TARP had type 1, type 2, and type 4 packets forwarded to IS-IS and ES-IS adjacencies. Service providers were experiencing problems with TARP PDUs looping through the network and causing congestion. One of the first things that Cisco did to control the propagation of TARP packets was to implement split horizon, so that a TARP packet would not be forwarded on the same interface that the packet was received on. The problem was worse on Ethernet interfaces: A router or other device on an Ethernet interface would receive a type 2 PDU. A separate type 2 PDU would be sent to all of the router adjacencies, and these devices should have already received the packet.

This section steps through an example of the network elements without split horizon. Figure 32 shows a TARP type 1 PDU being generated from router 3640A. Router 3640A will generate a type 1 PDU to all of its Level 1 adjacencies. The arrows in Figure 32 depict the Type 1 PDUs that are being sent out to all of router 3640A's Level 1 adjacencies.

Figure 32 TARP Propagation Control Using Split Horizon

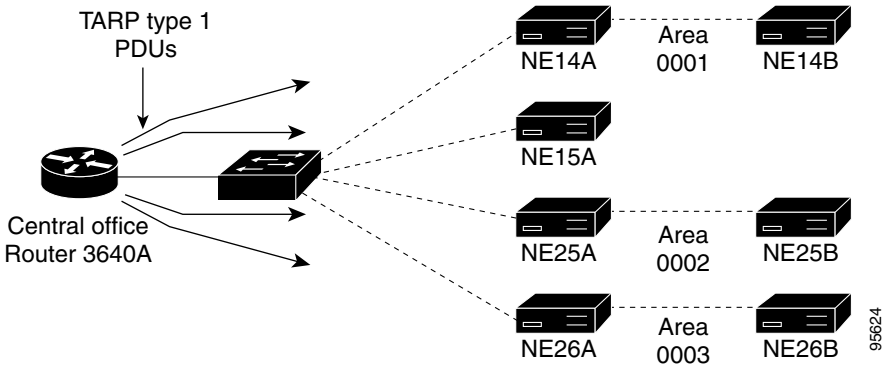
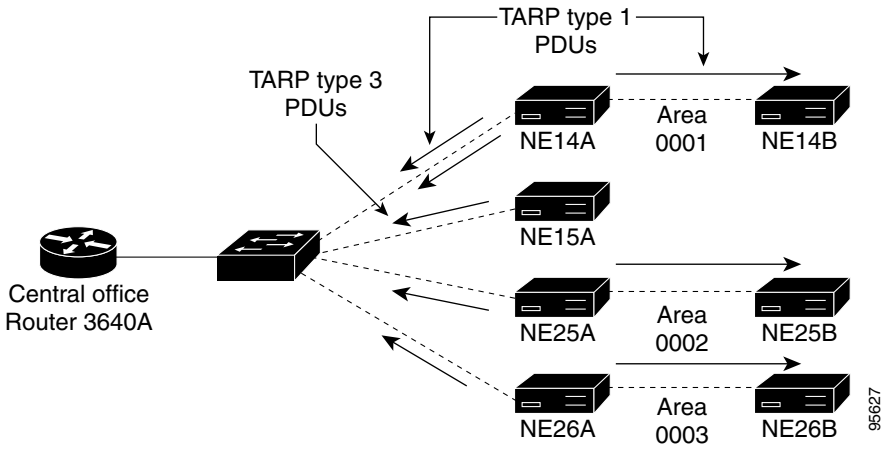


Figure 33 shows how the early implementations of TARP would respond to the type 1 PDUs sent out in Figure 32. Type 1 PDUs would be forwarded out the interface that the type 1 PDU had arrived on. Device NE 14A has an adjacency with devices NE14B, NE15A, and router 3640A, so device NE14A would send out three type 1 PDUs, which are represented by the three arrows coming out of device NE14A. Device NE15A is the object of the type 1 PDU, and device NE15A responds with a TARP type 3 PDU directly

to router 3640A. Device NE25A has two Level 1 IS-IS adjacencies, which are router 3640A and device NE25B, and two type 1 packets are forwarded out, as shown in Figure 33 by the two parallel arrows. Similarly, device NE26A has two Level-1 IS-IS adjacencies, which are router 3640A router and device NE26B, and Figure 33 shows two TARP type 1 packets being forwarded out.

Figure 33 Split Horizon Not Implemented on a Network Element

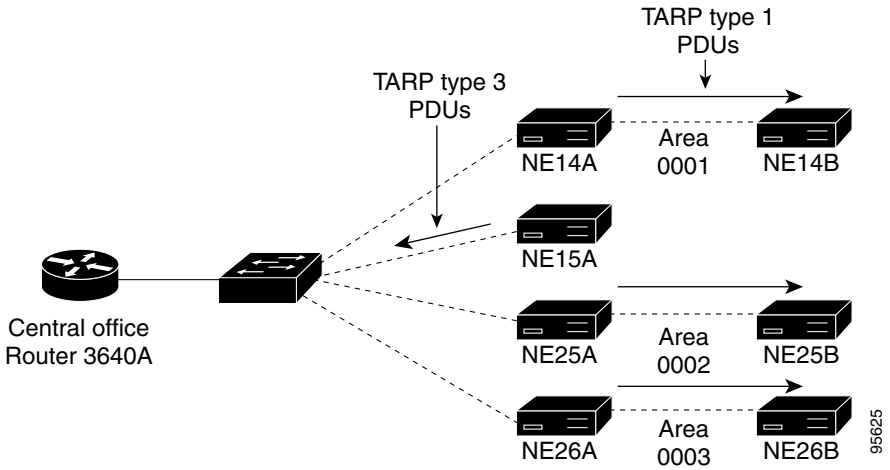


The point is that TARP packets can multiply quickly on the network. Split horizon is only one method that Cisco implemented to control the number of TARP packets.

At this point, router 3640A has received a type 3 response to the type 1 query; however, numerous packets have been launched. Without split horizon implemented, router 3640A would respond to each of the incoming type 1 PDUs and send back a type 1 packet to each of the adjacencies on the Ethernet interface. Eventually, the packets would expire due to the time-to-live field, but in the meantime much bandwidth has been expended.

Figure 34 shows what happens when split horizon is implemented on the network elements and the router. Device NE15A responds with a type 3 PDU. Device NE14A sends a type 1 PDU out on the DCC, but not on the Ethernet interface. Remember that split horizon does not allow the device to send a type 1 packet on the same interface that the packet arrived on. With split horizon configured, devices NE15A and NE26A send a type 1 PDU out on the DCC, but not on the Ethernet interface.

Figure 34 Split Horizon Implemented on Network Elements and Router 3640A

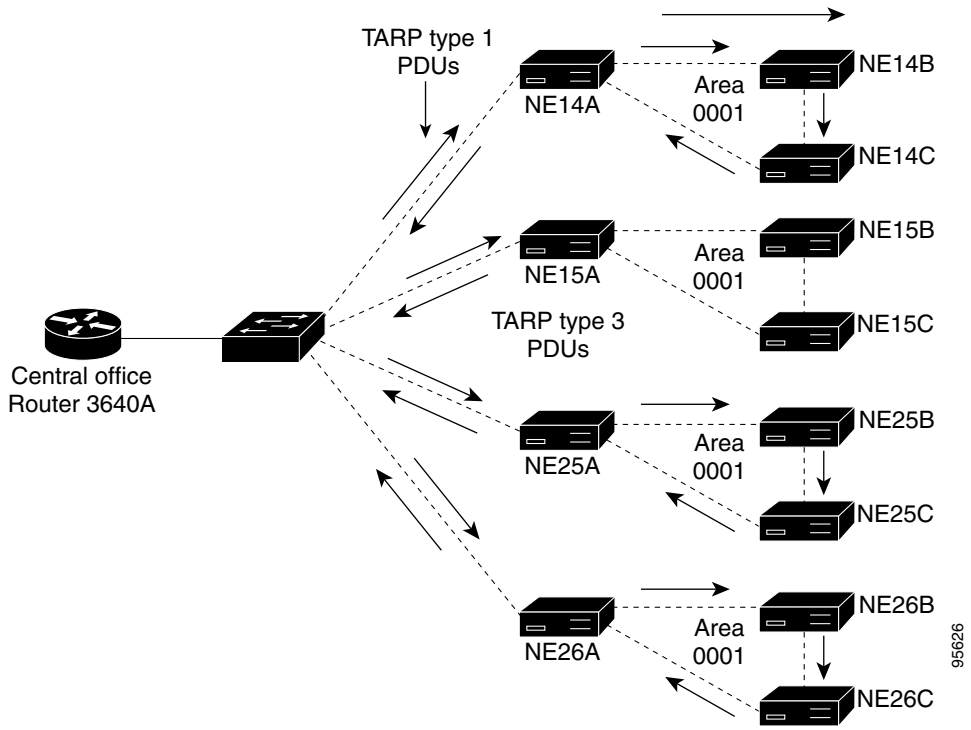


The problem of looping TARP PDUs has also been addressed by the SONET Interoperability Forum, which is discussed in the next section.

Additional Methods of Controlling the Propagation of TARP Packets

In the original TARP implementation, traffic multiplied exponentially. Cisco developed split horizon to help customers reduce this traffic, which can be implemented by placing all the network elements in the same OSI area. In Figure 35, the area is designated 0001.

Figure 35 Split Horizon and All Network Elements in the Same Area



The SONET Interoperability forum later developed a loop detection procedure using the loop detection buffer on the IS-IS router. Upon receiving a type 1, type 2, or type 4 PDU, the IS-IS router checks the loop detection buffer for a match. If there is no match, an entry is created with the system identifier that originated the packet and its sequence number.

Use the **show tarp ldp** EXEC command to display the TARP loop detection database on a Cisco router. The output lists the TARP sequence number and the time until the entry is aged out.

In the following example, any new TARP PDUs arriving from system identifier 0010.7BC7.AE40 with a sequence number of 9 or less will be discarded for the next 287 seconds. Any new TARP PDUs arriving from system identifier 0010.7BD8.C7D0 with a sequence number of 5 or less will be discarded for the next 287 seconds.

```
3640A# show tarp ldb

   System ID        Sequence Number    Expiration (sec)    Zero-sequence timer
 0010.7BC7.AE40               9            287              0
 0010.7BD8.C7D0               5            287              0
```

In the following example, the output from the **debug tarp events** command indicates that the TARP entries in the LDB are being aged:

```
3640A# debug tarp events

01:56:18: TARP-EV: Aging LDB entry for 0010.7BC7.AE40
01:56:18: TARP-EV: Aging LDB entry for 0010.7BD8.C7D0
```

A TARP type 4 packet is used to notify the network of changes. The type 4 packet is used to notify IS-IS and ES devices of TID changes or address changes. The TARP type 4 packet is used to reset the TARP sequence number to 0 (zero).

TARP PDU Packet Propagation Control Configuration Commands

Cisco has developed software commands that help control the propagation of type 1, type 2, and type 4 TARP PDU packets throughout the network. The **tarp route-static** global configuration command provides the ability to statically map the propagation of TARP packets across the network, and is issued as follows:

tarp route-static *nsap* [**all** | **message-type** *type-number* [*type-number*] [*type-number*]]

This command creates a manual adjacency to forward the TARP packet. The command can also be used to forward the TARP packets across IS-IS routers that do not support the TARP application. Use this command to forward TARP packets across the core of the network, yet control the propagation of the packets. The **tarp route-static** command can be implemented by a TARP packet type and is valid for the packet types 1, 2, and 4. TARP type 3 and 5 packets are unicast and sent to only one address; there is no need to apply the **tarp route-static** command to type 3 and 5 packets.

To control the propagation of TARP packets, use the **no tarp propagate** interface configuration command:

no tarp propagate [**all** | **message-type** *type-number* [*type-number*] [*type-number*]]

This command turns off the propagation by TARP packet type. The **no tarp propagate** command can be implemented by individual TARP packet type, and types 1, 2, and 4 are valid for the command.

Note If both the **tarp route-static** and the **no tarp propagate** commands are issued for type 4 PDUs on the router, the **tarp route-static** global configuration command takes precedence and the type 4 packets will be unicast to the specified NSAP.

Maintaining and Troubleshooting the IS-IS Network

The Cisco IOS software provides commands to help determine the topology and connectivity of the network, and that are useful for verifying and troubleshooting the IS-IS network. The following EXEC commands are described in this section:

- **clns host**
- **debug clns esis packets**
- **debug isis adjacency**
- **debug isis adj-packets**
- **debug tarp events**
- **debug tarp packets**
- **ping**
- **ping clns**
- **show clns interface**
- **show clns isis neighbor**
- **show clns neighbor**
- **show isis route**
- **show isis topology**
- **tarp query**
- **tarp resolve**
- **traceroute**
- **which-route**

Caution Take care in issuing the Cisco IOS **debug** commands, because they can consume CPU cycles and interfere with the normal operation of the network.

Mapping NSAPs to CLNS Host Names

Managing and troubleshooting the networks using NSAP addresses can be cumbersome, because the system identifier in the NSAP is typically in hexadecimal format. This format makes monitoring the IS-IS adjacencies, the ES-IS adjacencies, the IS-IS database, and other information a difficult task. Issuing debugging commands such as the **ping clns** EXEC command and TARP commands can also be cumbersome. One solution is to statically map NSAPs to host names. In the Cisco IOS software, this mapping can be done using the **clns host** command. The following example shows how to map CLNS hosts to IS-IS devices:

```
clns host 3640A 39.840f.8011.9999.0000.1111.0003.00d0.5872.9720.00
clns host NE14A 39.840f.8011.9999.0000.1111.0001.00e0.b064.4325.00
```

```
clns host NE14B 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00
clns host NE25A 39.840f.8011.9999.0000.1111.0002.00e0.b064.434e.00
clns host NE25B 39.840f.8011.9999.0000.1111.0002.0030.94e2.6ce0.00
clns host NE26A 39.840f.8011.9999.0000.1111.0003.00d0.5872.9720.00
clns host NE26B 39.840f.8011.9999.0000.1111.0003.00d0.5872.9720.00
clns host NE15A 39.840f.8011.9999.0000.1111.0001.0010.7bd8.c7d0.00
```

Using TLV 137 to Correlate Router and Host Names

The maintenance of the CLNS host statements in every IS-IS router and CLNS host in the network can be cumbersome in a large-sized network. A dynamic solution has been developed as part of the IS-IS protocol. A new type, length, value (TLV) has been defined in Informational RFC 2763, *Dynamic Hostname Exchange Mechanism for IS-IS*. IS-IS, originally designed for OSI routing, uses TLV parameters to carry information in link-state packets. The new TLV type 137, dynamic host name, and its value field contain the name of the router originating the link-state packet. The feature was introduced in Cisco IOS Release 12.0(4)T, and the **show clns neighbors** EXEC command uses TLV 137 or the **clns host** command to correlate router and host name.

Following is sample output from the **show clns neighbors** command showing the system identifier with the host name:

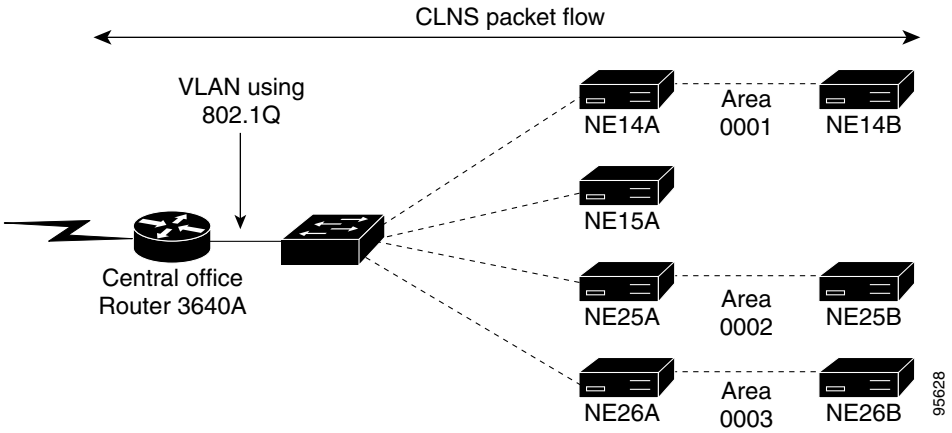
```
3640A# show clns neighbors

Area area0001:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
NE15A          Fa3/0.1     0010.7bd8.c7d0  Up     24        L1   IS-IS
NE14A          Fa3/0.1     00e0.b064.4325  Up     25        L1   IS-IS

Area area0002:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
NE25A          Fa3/0.2     00e0.b064.434e  Up     23        L1   IS-IS

Area area0003:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
NE26B          Fa3/0.3     00d0.5872.9720  Up     26        L1   IS-IS
```

Note The IS-IS router must support TLV type 137 for the names to be propagated. This technique will become more valuable as more SONET and SDH vendors support TLV type 137.

Displaying IS-IS Network Topology

This section describes how to use Cisco IOS software commands to determine network topology. Use Figure 36 as a reference for the command examples.

Figure 36 Sample Network for Determining IS-IS Network Topology



Use the **show isis topology** EXEC command to list the topology of the IS-IS network. The following example lists the topology as shown in Figure 36:

```
3640A# show isis topology

Area area0001:
IS-IS IP paths to level-1 routers
System Id            Metric     Next-Hop            Interface   SNPA
3640A                --
NE15A                10         NE15A               Fa3/0.1     0010.7bd8.c7d0
NE14B                20         NE14A               Fa3/0.1     00e0.b064.4325
NE14A                10         NE14A               Fa3/0.1     00e0.b064.4325

IS-IS IP paths to level-2 routers
System Id            Metric     Next-Hop            Interface   SNPA
3640A                --

Area area0002:
IS-IS IP paths to level-1 routers
System Id            Metric     Next-Hop            Interface   SNPA
3640A                --
NE25B                20         NE25A               Fa3/0.2     00e0.b064.434e
NE25A                10         NE25A               Fa3/0.2     00e0.b064.434e

Area area0003:
IS-IS IP paths to level-1 routers
System Id            Metric     Next-Hop            Interface   SNPA
NE26B                20         NE26A               Fa3/0.3     00d0.5872.9720
3640A                --
NE26A                10         NE26A               Fa3/0.3     00d0.5872.9720
```

In Figure 36, the IS-IS Level 1 area0001 contains the IS-IS Level 1/Level 2 Cisco 3640 router and the IS-IS Level 1 devices NE15A, NE14B, and NE14A. Device NE15A is directly connected using Fast Ethernet interface 3/0.1 to router 3640A, and has a routing metric of 10. The SNPA for device NE15A is 0010.7bd8.c7d0. On an Ethernet interface, the SNPA is the MAC address. Device NE14B is one hop away from router 3640A; therefore, the routing metric is 20 and the next hop IS-IS router is device NE14A. Device NE14A is connected using Fast Ethernet interface 3/0.1. The SNPA is the MAC address (00e0.b064.4325) of device NE14A, the next hop device. Device NE14A is directly connected to Fast Ethernet 3/0.1 and has a routing metric of 10. The SNPA or MAC address of device NE14A is 00e0.b064.4325.

In IS-IS area 0002, there are three system identifiers—router 3640A and devices NE25B and NE25A—as seen in Figure 36. Device NE25B can be reached one hop away through device NE25A on Fast Ethernet interface 3/0.2. The routing metric is 20 because device NE25B is one hop away. The SNPA for the next hop device, NE25A, is 00e0.b064.434e. Device NE25A is directly connected with a routing metric of 10.

In IS-IS area 0003, there are three system identifiers—router 3640A and devices NE26B and NE26A, as seen in Figure 36. Device NE26B can be reached one hop away through device NE26A on Fast Ethernet interface 3/0.3. The routing metric is 20. The SNPA for the next hop device, NE26A, is 00d0.5872.9720. Device NE26A is directly connected with a routing metric of 10.

Similar network topology information can be gathered from the **show isis route** EXEC command. The information is similar to that displayed by the **show isis topology** command, except for an additional field that indicates the state of the adjacency to the next hop IS-IS router. The following example output shows the information displayed by the **show isis route** command:

```
3640A# show isis route

Area area0001:
IS-IS Level-1 Routing Table - version 5
System Id       Next-Hop        Interface   SNPA            Metric  State
3640A           --
NE15A           NE15A           Fa3/0.1     0010.7bd8.c7d0  10      Up
NE14B           NE14A           Fa3/0.1     00e0.b064.4325  20      Up
NE14A           NE14A           Fa3/0.1     00e0.b064.4325  10      Up

Area area0002:
IS-IS Level-1 Routing Table - version 5
System Id       Next-Hop        Interface   SNPA            Metric  State
3640A           --
NE25B           NE25A           Fa3/0.2     00e0.b064.434e  20      Up
NE25A           NE25A           Fa3/0.2     00e0.b064.434e  10      Up

Area area0003:
IS-IS Level-1 Routing Table - version 4
System Id       Next-Hop        Interface   SNPA            Metric  State
3640A           --
NE26B           NE26A           Fa3/0.3     00d0.5872.9720  20      Up
NE26A           NE26A           Fa3/0.3     00d0.5872.9720  10      Up
```

The **show isis route** EXEC command can be used to specify the next hop to a specific IS-IS router. The following example shows the route to device NE14B:

```
3640A# show isis route NE14B

Area area0001:
System Id       Next-Hop        Interface   SNPA            Metric  State
NE14B           NE14A           Fa3/0.1     00e0.b064.4325  20      Up

Area area0002:
No IS-IS Level-1 route to NE14B found

Area area0003:
No IS-IS Level-1 route to NE14B found
```

The **which-route** EXEC command displays the next hop in the route for the packet and specific information about the hop, and is better suited to display the route to device NE14B. The command displays the routing table where the CLNS address is found in the router. The command can also be useful if you are running multiple routing processes on the router.

```
3640A# which-route NE14B
```

```
Route look-up for destination 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00, NE14B
  Found route in IS-IS level-1 routing table

Adjacency entry used:
System Id      Interface   SNPA           State  Holdtime  Type Protocol
NE14A          Fa3/0.1     00e0.b064.4325      Up     23        L1   IS-IS
  Area Address(es): 39.840f.8011.9999.0000.1111.0001
  Uptime: 01:11:57
```

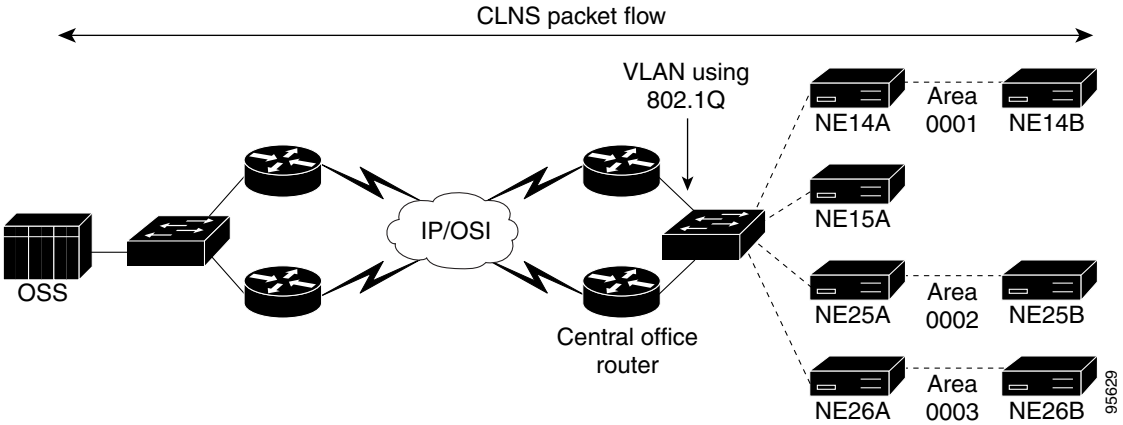
In this display:

- The NET for device NE14B is 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00, and is found in the Level 1 routing table for the Cisco router labeled “3640A” in Figure 36 on page 71.
- The system identifier of the adjacent IS-IS router is device NE14A. (The **clns host** command was used to translate the system identifier to the host identifier.)
- Device NE14A is accessed using Fast Ethernet interface 3/0.1.
- The MAC address or SNPA for device NE14A is 00e0.b064.4325.
- The state of the Level 1 IS-IS adjacency is up and, therefore, device NE14A is reachable.
- The hold time represents the time until the Level 1 adjacency times out, and in this example is 23 seconds. If an IS-IS hello message is not received within 23 seconds, the IS-IS adjacency will be torn down.
- The IS-IS adjacency type is Level 1.
- Protocol: The adjacency was learned from the IS-IS protocol.
- The IS-IS area address is 39.840f.8011.9999.0000.1111.0001 and the area has been available for 1 hour, 11 minutes, and 57 seconds. The uptime report is useful while troubleshooting the length of time that the area has been available.

Verifying IS-IS Adjacency Formation

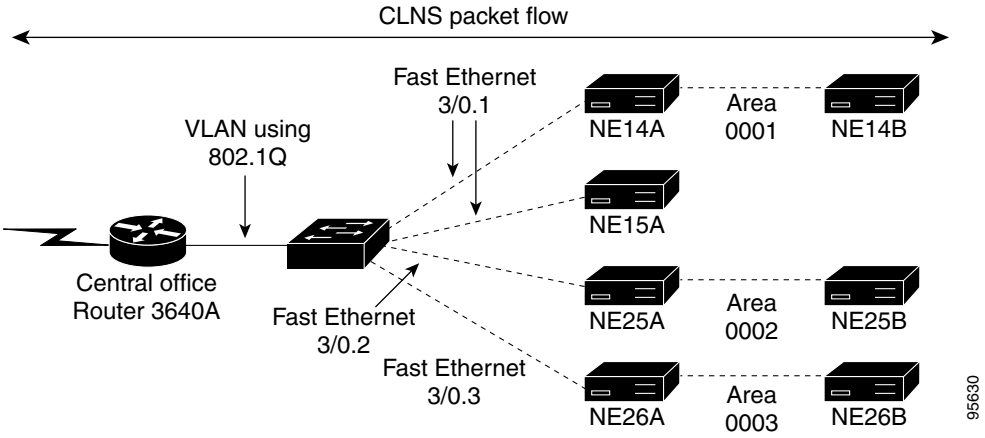
This section describes how to determine whether two IS-IS router devices are forming IS-IS adjacencies. If the devices are not forming adjacencies, it will be necessary to determine why not. Cisco has found from working with service providers that typically the SONET/SDH nodes do not have a robust debugging capability. Figure 37 shows a typical operational IS-IS network.

Figure 37 Operational IS-IS Network



The portion of the network that this section focuses on debugging is shown in Figure 38, and examines the access router in the central office that supports the Level-1-2 adjacency to the network elements.

Figure 38 Access Router in the Central Office that Supports the Level 1-2 Adjacency to the Network Elements



The Cisco IOS software provides commands that determine the status of the IS-IS adjacency between the Cisco router labeled "3640A" in Figure 38 and the network elements. All of the network elements in the example are set up as Level 1 IS-IS routers. Devices NE14A and NE15A are in OSI area 0001, and there should be two Level 1 adjacencies established on Fast Ethernet interface 3/.01.

The **show clns interface** EXEC command displays the number adjacencies on the interface (report displayed in bold text for purpose of example).

```
3640A# show clns interface FastEthernet3/0.1

FastEthernet3/0.1 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  RDPDUs enabled, min. interval 100 msec., Addr Mask enabled, last sent 00:00:40
  Congestion Experienced bit set at 4 packets
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 38 seconds
  Routing Protocol: IS-IS (area0001)
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 10, Priority: 127, Circuit ID: 3640A.01
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 2
    Level-2 Metric: 10, Priority: 127, Circuit ID: 3640A.01
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 0
    Next IS-IS LAN Level-1 Hello in 254 milliseconds
    Next IS-IS LAN Level-2 Hello in 2 seconds
```

The output of the command shows that there are two Level 1 adjacencies. There are no Level 2 adjacencies, which corresponds to the configuration seen in Figure 38 on page 74.

The ES-IS protocol works with the IS-IS protocol. When a router is configured for IS-IS, ES-IS is automatically enabled. End systems and routers send End System Hello (ESH) and Intermediate System Hello (ISH) messages to determine the network addresses of adjacent neighbors. On a LAN, the ESHs

are sent to a broadcast address of 09-00-2b-00-00-05 to reach the routers. The ISHs are sent to a broadcast address of 09-00-2b-00-00-04 to reach the end systems. The IS-IS adjacencies are formed IS-IS Hello (IIH) messages and there are three types, as follows:

- IIH message for point-to-point links
- Level 1 LAN IIH message
- Level 2 LAN IIH message

Examine the adjacencies coming up on a working network using Figure 38 on page 74 as an example. This task requires the MAC address or SNPA for debugging the IIH messages. One method of quickly determining the system identifier is to use the **show clns neighbors** EXEC command.

In the following example, when the **show clns neighbors** EXEC command is issued, the host name is displayed instead of the actual system identifier. The host name will be displayed when static host name assignments have been made in the Cisco router, or when the SONET/SDH nodes support dynamic host assignment. Static and dynamic host assignment are explained in the "Mapping NSAPs to CLNS Host Names" section on page 69.

```
3640A# show clns neighbors

Area area0001:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
NE15A          Fa3/0.1     0010.7bd8.c7d0  Up     22        L1   IS-IS
NE14A          Fa3/0.1     00e0.b064.4325  Up     20        L1   IS-IS

Area area0002:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
NE25A          Fa3/0.2     00e0.b064.434e  Up     23        L1   IS-IS

Area area0003:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
NE26B          Fa3/0.3     00d0.5872.9720  Up     29        L1   IS-IS
```

Examining IS-IS Adjacency Formation

The next step is to look at how IS-IS adjacencies are formed. Use the **debug isis adj-packets** EXEC command to watch the IIHs being sent. In the following example, the Fast Ethernet interface has been turned down and then brought up after debugging was turned on to capture the entire process. (Key reports are in bold text for purpose of example.)

```
3640A# debug isis adj-packets
```

The Fast Ethernet interface comes up:

```
00:05:44: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet3/0, changed state
to up
```

Router 3640A in Figure 38 on page 74 sends Level 1 and Level 2 IIHs:

```
00:05:44: ISIS-Adj (area0001): Sending L1 LAN IIH on FastEthernet3/0.1, length 1497
00:05:44: ISIS-Adj (area0001): Sending L2 LAN IIH on FastEthernet3/0.1, length 1497
00:05:44: ISIS-Adj (area0002): Sending L1 LAN IIH on FastEthernet3/0.2, length 1497
00:05:44: ISIS-Adj (area0003): Sending L1 LAN IIH on FastEthernet3/0.3, length 1497
00:05:52: ISIS-Adj (area0003): Sending L1 LAN IIH on FastEthernet3/0.3, length 1497
00:05:53: ISIS-Adj (area0001): Sending L1 LAN IIH on FastEthernet3/0.1, length 1497
00:05:53: ISIS-Adj (area0002): Sending L1 LAN IIH on FastEthernet3/0.2, length 1497
00:05:53: ISIS-Adj (area0001): Sending L2 LAN IIH on FastEthernet3/0.1, length 1497
00:06:00: ISIS-Adj (area0003): Sending L1 LAN IIH on FastEthernet3/0.3, length 1497
00:06:02: ISIS-Adj (area0001): Sending L1 LAN IIH on FastEthernet3/0.1, length 1497
00:06:02: ISIS-Adj (area0002): Sending L1 LAN IIH on FastEthernet3/0.2, length 1497
00:06:03: ISIS-Adj (area0001): Sending L2 LAN IIH on FastEthernet3/0.1, length 1497
```

```
00:06:08: ISIS-Adj (area0003): Sending L1 LAN IIH on FastEthernet3/0.3, length 1497
00:06:10: ISIS-Adj (area0001): Sending L1 LAN IIH on FastEthernet3/0.1, length 1497
```

Router 3640A receives a Level 1 IIH from MAC address 0010.7bd8.c7d0, which is device NE15A. The Level 1 adjacency comes up between router 3640A and device NE15A.

```
00:06:10: ISIS-Adj (area0001): Rec L1 IIH from 0010.7bd8.c7d0 (FastEthernet3/0.1), cir
type L1, cir id 0010.7BD8.C7D0.01, length 147
00:06:10: ISIS-Adj (area0001): New adjacency, level 1 for 0010.7bd8.c7d0
```

Router 3640A receives a Level 1 IIH from MAC address 00e0.b064.4325, which is device NE14A. The Level 1 adjacency comes up between router 3640A and device NE14A.

```
00:06:10: ISIS-Adj (area0001): Rec L1 IIH from 00e0.b064.4325 (FastEthernet3/0.1), cir
type L1, cir id 00E0.B064.4324.02, length 147
00:06:10: ISIS-Adj (area0001): New adjacency, level 1 for 00e0.b064.4325
.
.
.
00:06:11: ISIS-Adj (area0001): Sending L1 LAN IIH on FastEthernet3/0.1, length 1497
```

Router 3640A receives a second IIH from device NE15A. The Cisco 3640A router's Level 1 adjacency count goes to 1 and the adjacency state is up.

```
00:06:11: ISIS-Adj (area0001): Rec L1 IIH from 0010.7bd8.c7d0 (FastEthernet3/0.1), cir
type L1, cir id 0010.7BC7.AE40.01, length 147
00:06:11: ISIS-Adj (area0001): L1 adj count 1
00:06:11: ISIS-Adj (area0001): Adjacency state goes to Up
```

Router 3640A and device NE15A are going through the designated router selection. The system identifier of the designated router is 0001.0010.7bc7.AE40, which is router 3640A.

```
00:06:11: ISIS-Adj (area0001): Run level-1 DR election for FastEthernet3/0.1
00:06:11: ISIS-Adj (area0001): New level-1 DR 0010.7BC7.AE40 on FastEthernet3/0.1
00:06:11: ISIS-Adj (area0001): Didn't purge DR LSP--not fully elected
```

Router 3640A receives a second Level 1 IIH from device NE14A. The Level 1 adjacency count goes to 2. The adjacency state between router 3640A and device NE14A goes to up.

```
00:06:11: ISIS-Adj (area0001): Rec L1 IIH from 00e0.b064.4325 (FastEthernet3/0.1), cir
type L1, cir id 0010.7BC7.AE40.01, length 147
00:06:11: ISIS-Adj (area0001): L1 adj count 2
00:06:11: ISIS-Adj (area0001): Adjacency state goes to Up
```

The designated router election process runs again. Router 3640A remains the designated router.

```
00:06:11: ISIS-Adj (area0001): Run level-1 DR election for FastEthernet3/0.1
00:06:11: ISIS-Adj (area0001): No change (it's us)
```

The normal sending and receiving of IIHs in area 0001 is shown in the following example:

```
00:06:12: ISIS-Adj (area0001): Sending L1 LAN IIH on FastEthernet3/0.1, length 1497
00:06:12: ISIS-Adj (area0001): Rec L1 IIH from 0010.7bd8.c7d0 (FastEthernet3/0.1), cir
type L1, cir id 0010.7BC7.AE40.01, length 147
00:06:12: ISIS-Adj (area0002): Sending L1 LAN IIH on FastEthernet3/0.2, length 1497
00:06:12: ISIS-Adj (area0001): Sending L2 LAN IIH on FastEthernet3/0.1, length 1497
00:06:14: ISIS-Adj (area0001): Sending L1 LAN IIH on FastEthernet3/0.1, length 1497
```

The same procedure for establishing adjacency in area 0002 and area 0003 takes place. The start of the process of sending and receiving IIHs for both areas is shown in the following example:

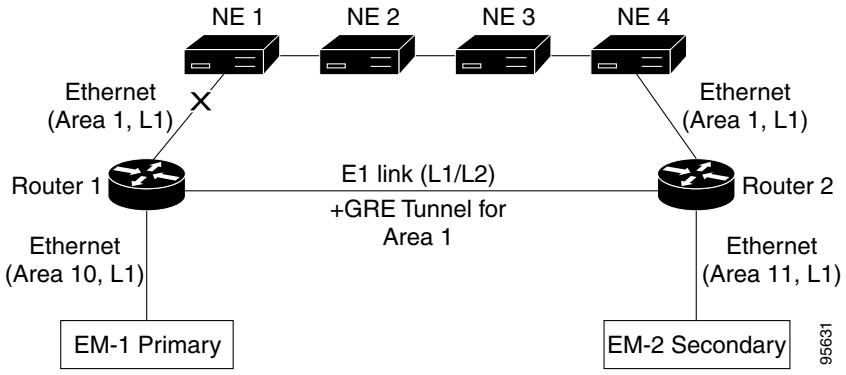
```
00:06:16: ISIS-Adj (area0003): Rec L1 IIH from 00d0.5872.9720 (FastEthernet3/0.3), cir
type L1, cir id 00D0.5872.9720.01, length 147
00:06:16: ISIS-Adj (area0003): New adjacency, level 1 for 00d0.5872.9720
00:06:16: ISIS-Adj (area0003): Sending L1 LAN IIH on FastEthernet3/0.3, length 1497
```

```
00:06:16: ISIS-Adj (area0002): Rec L1 IIH from 00e0.b064.434e (FastEthernet3/0.2), cir
type L1, cir id 00E0.B064.434E.01, length 147
00:06:16: ISIS-Adj (area0002): New adjacency, level 1 for 00e0.b064.434e
```

Sample Adjacency Debugging Scenario

In Figure 39, Nodes 1 through 4 are TN-16s and are SDH network elements that are connected over a fiber-optic link. The GNEs and Cisco routers are located in the Router 1 and Router 2 central offices. The problem is that NE 1 cannot establish a Level 1 adjacency with the Cisco router. The result is that the service provider will have connectivity problems reaching NE 1 from Element Manager System EM-1 Primary. The network elements are configured as Level 1 IS-IS routers. The Cisco routers are configured as Level-1-2 IS-IS routers.

Figure 39 Sample Network for Troubleshooting IS-IS Adjacency Problems



The first problem encountered is that the IS-IS adjacency will not come up between Router 1 and NE 1. One way to solve this problem is to determine if the Cisco router interface is up. Use the **show clns interface** EXEC command to do so (key reports shown in bold text for purpose of example):

```
Router1# show clns interface Ethernet0

Ethernet0 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  RDPDUs enabled, min. interval 100 msec., Addr Mask enabled
  Congestion Experienced bit set at 4 packets
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 47 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 10, Priority: 64, Circuit ID: 0000.0000.60B1.01
    Number of active level-1 adjacencies: 0
    Level-2 Metric: 10, Priority: 64, Circuit ID: 0000.0000.60B1.01
    Number of active level-2 adjacencies: 0
    Next IS-IS LAN Level-1 Hello in 2 seconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
```

The report indicates that the interface is up and the line protocol is up and that the next ESH/ISH will be sent in 47 seconds. The IS-IS routing protocol is turned on and the circuit type is Level-1-2. The number of Level 1 adjacencies is 0 (zero) and the number of Level 2 adjacencies is 0 in the following output. On

the Ethernet interface, according to Figure 39 on page 77, there should be an adjacency with Node 1. The adjacency type should be Level 1 because Node 1 can be configured as only Level 1. The interface is advertising Level 1 and Level 2 IS-IS hello messages.

The next step would be to examine the IS-IS adjacency formation using the **debug isis adjacency** command. In the following example, Router 1 is sending Level 1 and Level 2 IIHs. The **debug** command output indicates that the Cisco router is sending out the Level 1 IIH packets and the Level 2 IIH packets on Ethernet interface 0. Router 1 is not receiving the IIHs from NE 1 on Ethernet interface 0.

```
Router1# debug isis adjacency

IS-IS Adjacency related packets debugging is on
Router1#
ISIS-Adj: Sending L2 IIH on Ethernet0
ISIS-Adj: Sending L1 IIH on Ethernet0
ISIS-Adj: Sending L2 IIH on Ethernet0
ISIS-Adj: Sending L1 IIH on Ethernet0
```

It is also recommended that the Ethernet interface be verified as operational. In this example, the problem was with the software on the SDH network element. The SDH node had to be rebooted for the IS-IS to come up and send the IIH.

Take another look at the problems described previously for Figure 39 on page 77; that is, the IS-IS adjacency will not come up between Router 1 and NE 1. A report from the **show clns interface** EXEC command indicates that the interface is up, but no Level 1 adjacency is formed because the value is 0 (report shown in bold text for purpose of example):

```
Router1# show clns interface Ethernet 0

Ethernet0 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  RDPDUs enabled, min. interval 100 msec., Addr Mask enabled
  Congestion Experienced bit set at 4 packets
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 32 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 10, Priority: 64, Circuit ID: 0000.0000.60B1.01
    Number of active level-1 adjacencies: 0
    Level-2 Metric: 10, Priority: 64, Circuit ID: 0000.0000.60B1.01
    Number of active level-2 adjacencies: 0
    Next IS-IS LAN Level-1 Hello in 2 seconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
```

Next, enter the **debug isis adjacency** command on Router 1. In the following example, Router 1 is sending Level 1 and Level 2 IIHs, and receives an IIH from system identifier 0010.7bc7.ae41, which is the NE 1. The circuit type is Level 1. The circuit identifier is 0000.0000.0130.01, which is the view NE 1 has of the DIS (key reports shown in bold text text for purpose of example).

```
ISIS-Adj: Sending L1 IIH on Ethernet0
ISIS-Adj: Sending L2 IIH on Ethernet0
ISIS-Adj: Rec L1 IIH from 0010.7bc7.ae41 (Ethernet0), cir type 1, cir id 0000.0000.0130.01
ISIS-Adj: Area mismatch, level 1 IIH on Ethernet0
ISIS-Adj: Sending L1 IIH on Ethernet0
ISIS-Adj: Sending L2 IIH on Ethernet0
```

The report by the **debug isis adjacency** command lists an area mismatch for Level 1 IIH. The IS-IS router NE 1 and Router 1 do not have the same area identifier. The NSAP for both devices needs to be checked.

In the following example, the Cisco router is running an IS-IS multiarea, so the IS-IS process associated with Ethernet interface 0 must be checked. The report indicates that IS-IS process area_02 was assigned to Ethernet interface 0.

```
router isis area_02
 net 39.840f.8011.9999.0000.1111.0200.0000.0000.0130.00
```

To prevent the mismatch, IS-IS process area_01 should have been assigned to Ethernet interface 0:

```
router isis area_01
 net 39.840f.8011.9999.0000.1111.0100.0000.0000.0130.00
```

The following example shows how to verify that the IS-IS adjacency shown in Figure 39 on page 77 is coming up correctly after the change. NE 1 is configured as Level 1 IS-IS. Router 1 is configured as a Level 1 and Level 2 router. The debugging is being done on Router 1. Router 1 is sending Level 1 and Level 2 IIHs. Router 1 is receiving Level 1 IIHs from NE 1. The IS-IS adjacencies are coming up correctly.

```
Router1# debug isis adjacency

IS-IS Adjacency related packets debugging is on
Router1#
ISIS-Adj: Sending L2 IIH on Ethernet0
ISIS-Adj: Sending L1 IIH on Ethernet0
ISIS-Adj: Sending L2 IIH on Ethernet0
ISIS-Adj: Sending L1 IIH on Ethernet0
ISIS-Adj: Sending L2 IIH on Ethernet0
ISIS-Adj: Sending L1 IIH on Ethernet0
ISIS-Adj: Sending L2 IIH on Ethernet0
ISIS-Adj: Rec L1 IIH from 00e0.b064.4325 (Ethernet0), cir type 1, cir id 0000.0000.60B1.01
ISIS-Adj: Sending L1 IIH on Ethernet0
ISIS-Adj: Sending L2 IIH on Ethernet0
```

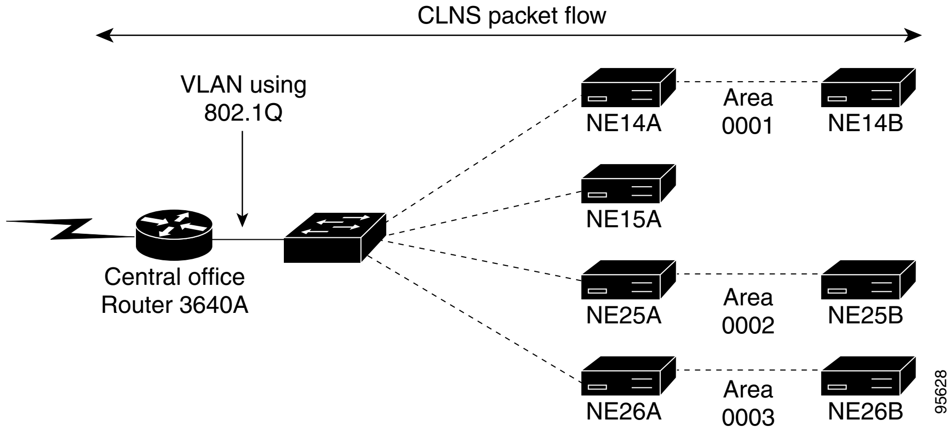
In the following example output from the **show clns isis neighbors** command, Router 1 and TN-16 Node 1 have formed a Level 1 adjacency. The designated Level 1 IS on the LAN is circuit identifier 0000.0000.60B1 according to the system identifier 0000.0000.0F0F.

```
Router1# show clns isis neighbors

System Id      Interface   State  Type Priority  Circuit Id         Format
0000.0000.0F0F Et0         Up     L1   64        0000.0000.60B1.01  Phase V
```

Verifying IS-IS Network Connectivity Using the ping and traceroute Commands

The route to a specific network element can be traced with the **traceroute** command. The **traceroute** command uses the Time to Live (TTL) field in an IP datagram to cause routers in the path to send back error messages. The IP version of the **traceroute** command is the default, and there is a CLNS version of the command. The following example shows a route traced to device NE14B for the sample network shown in Figure 40.

Figure 40 Sample Network for Determining IS-IS Network Topology




```
3640A# traceroute clns NE14B

Type escape sequence to abort.
Tracing the route to NE14B (39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00)

  1 NE14A(39.840f.8011.9999.0000.1111.0001.00e0.b064.4324.00) 0 msec ! 0 msec ! 4 msec !
  2 NE14B(39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00) 0 msec ! 0 msec ! 0 msec !
```

The **ping clns** EXEC command is another method to determine connectivity to an IS-IS router or ES. The following example shows sample output of the **ping clns** EXEC command to device NE14B:

```
3640A# ping clns NE14B

Type escape sequence to abort.
Sending 5, 100-byte CLNS Echos with timeout 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

The following example shows **debug** command output from the CLNS packets sent from the **ping clns** command. The ping originates from the Cisco 3640 router with NET 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00, to device NE14B with NET 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00.

```
3640A#

00:03:45: CLNS: Originating packet, size 100
00:03:45:       from 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
      to 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00
      via 00E0.B064.4324 (FastEthernet3/0.1 00e0.b064.4325)
00:03:45: CLNS: Echo Reply PDU received on FastEthernet3/0.1!
00:03:45: CLNS: Originating packet, size 100
00:03:45:       from 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
      to 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00
      via 00E0.B064.4324 (FastEthernet3/0.1 00e0.b064.4325)
00:03:45: CLNS: Echo Reply PDU received on FastEthernet3/0.1!
00:03:45: CLNS: Originating packet, size 100
00:03:45:       from 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
      to 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00
      via 00E0.B064.4324 (FastEthernet3/0.1 00e0.b064.4325)
00:03:45: CLNS: Echo Reply PDU received on FastEthernet3/0.1!
00:03:45: CLNS: Originating packet, size 100
00:03:45:       from 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
      to 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00
```

```
      via 00E0.B064.4324 (FastEthernet3/0.1 00e0.b064.4325)
00:03:45: CLNS: Echo Reply PDU received on FastEthernet3/0.1!
00:03:45: CLNS: Originating packet, size 100
00:03:45:       from 39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00
      to 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00
      via 00E0.B064.4324 (FastEthernet3/0.1 00e0.b064.4325)
00:03:45: CLNS: Echo Reply PDU received on FastEthernet3/0.1!
```

The Cisco IOS **ping** EXEC command does not require the **clns** keyword in the command string. It is possible to enter the **ping** command with the CLNS host identifier or the NET and get the same results. The following examples show sample reports from both command strings:

```
3640A# ping 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00

Translating "39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00"...domain server
(255.255.255.255)

Type escape sequence to abort.
Sending 5, 100-byte CLNS Echos with timeout 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

3640A# ping NE14B

Translating "NE14B"...domain server (255.255.255.255)

Type escape sequence to abort.
Sending 5, 100-byte CLNS Echos with timeout 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Troubleshooting Network Connections Using the ping clns Command

A typical service provider network is shown in Figure 41. In this troubleshooting example, the OSS cannot access device NE26B. The technician at the network operations center (NOC) has connectivity to the central office router.

Figure 41 Typical Service Provider Network

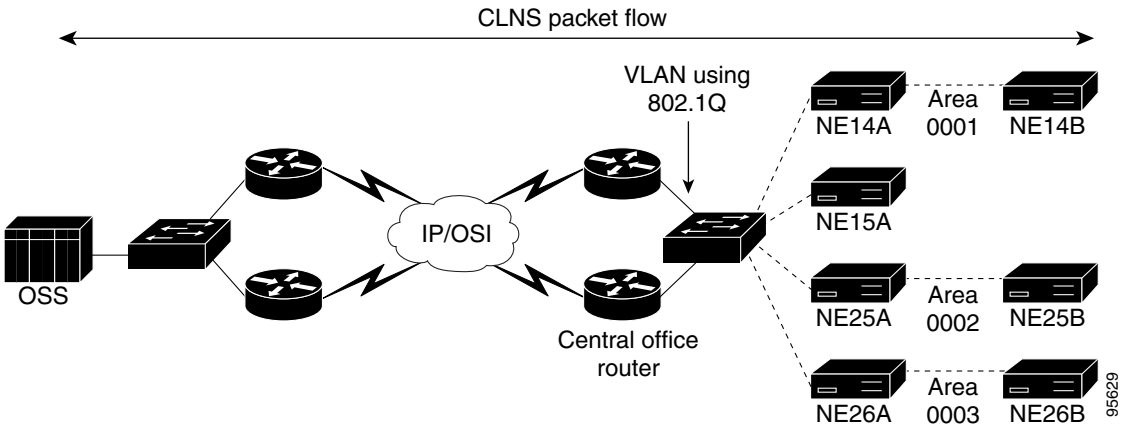
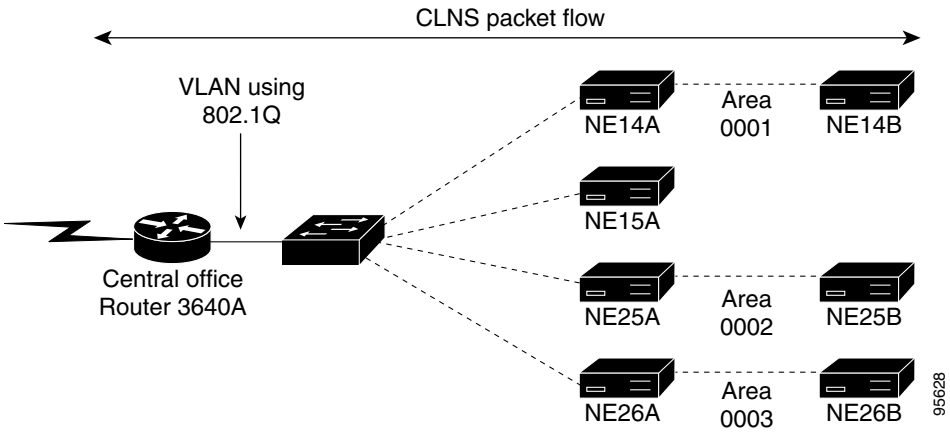


Figure 42 shows router 3640A and connections to the network elements in the central office. The NOC technician has telnetted to router 3640A and is troubleshooting the OSI connectivity to network element device NE26B.

Figure 42 Troubleshooting OSI Connectivity



The first part of the example uses the **ping clns** EXEC command to try a connection to device NE26B.

Note Not all network elements in the network support the **ping clns** EXEC command; check with your network element vendor.

In the following example, the **ping clns** command was not successful at making the connection:

```
3640A# ping clns NE26B

Type escape sequence to abort.
Sending 5, 100-byte CLNS Echos with timeout 2 seconds

CLNS: cannot send ECHO.
CLNS: cannot send ECHO.
CLNS: cannot send ECHO.
CLNS: cannot send ECHO.
CLNS: cannot send ECHO.
Success rate is 0 percent (0/5)
```

Next, issue the **ping clns** EXEC command to try a connection to the GNE. In the following example, the network element supports the **ping clns** command and a successful connection is made:

```
3640A# ping clns NE26A

Type escape sequence to abort.
Sending 5, 100-byte CLNS Echos with timeout 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

The router is configured with **clns host** command statements for the network elements, so the technician did not have to type out the whole NSAP address; see the section "Mapping NSAPs to CLNS Host Names" section on page 69.

The next step is to determine whether the IS-IS adjacency is coming up between router 3640A and device NE26A. Use the **show clns interface** EXEC command to see that the number of Level 1 IS-IS adjacencies is 0 (text in bold for purpose of example):

```
3640A# show clns interface fastethernet 3/0.3

FastEthernet3/0.3 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
```

```
  ERPDUs enabled, min. interval 10 msec.
  RDPDUs enabled, min. interval 100 msec., Addr Mask enabled
  Congestion Experienced bit set at 4 packets
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 21 seconds
  Routing Protocol: IS-IS (area0003)
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 10, Priority: 127, Circuit ID: 3640A.01
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 0
    Next IS-IS LAN Level-1 Hello in 51 milliseconds
```

The next step is to check processes in area 0003. Use the **show clns neighbors** EXEC command to display the areas. In the following example, the system identifier for device NE26A is listed and is on Fast Ethernet interface 3/0.3. The protocol that is coming up is ES-IS; therefore, one of the systems is configured as an ES on this interface.

```
3640A# show clns neighbors

Area area0001:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
NE15A          Fa3/0.1     0010.7bd8.c7d0  Up     21        L1   IS-IS
NE14A          Fa3/0.1     00e0.b064.4325  Up     25        L1   IS-IS

Area area0002:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
NE25A          Fa3/0.2     00e0.b064.434e  Up     24        L1   IS-IS

Area area0003:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
NE26A          Fa3/0.3     00d0.5872.9720  Up     278       IS   ES-IS
```

Use the **debug isis adjacency** command to watch IS-IS adjacencies come up. IIHs are being received by router 3640A on Fast Ethernet interfaces 3/0.2 and 3/0.1. IIHs are being sent by router 3640A on Fast Ethernet interfaces 3/0.1, 3/0.2, and 3/0.3. The problem is with device NE26A; it is not sending Level 1 IIHs on Fast Ethernet interface 3/0.3.

```
3640A# debug isis adjacency

IS-IS Adjacency related packets debugging is on

3640A#
01:23:04: ISIS-Adj (area0002): Rec L1 IIH from 00e0.b064.434e (FastEthernet3/0.2), cir
type L1, cir id 0010.7BC7.AE40.01, length 147
01:23:05: ISIS-Adj (area0001): Rec L1 IIH from 00e0.b064.4325 (FastEthernet3/0.1), cir
type L1, cir id 0010.7BC7.AE40.01, length 147
01:23:06: ISIS-Adj (area0001): Sending L2 LAN IIH on FastEthernet3/0.1, length 1497
01:23:06: ISIS-Adj (area0003): Sending L1 LAN IIH on FastEthernet3/0.3, length 1497
01:23:07: ISIS-Adj (area0001): Sending L1 LAN IIH on FastEthernet3/0.1, length 1497
01:23:07: ISIS-Adj (area0002): Sending L1 LAN IIH on FastEthernet3/0.2, length 1497
01:23:09: ISIS-Adj (area0001): Rec L1 IIH from 0010.7bd8.c7d0 (FastEthernet3/0.1), cir
type L1, cir id 0010.7BC7.AE40.01, length 147
01:23:09: ISIS-Adj (area0001): Sending L1 LAN IIH on FastEthernet3/0.1, length 1497
01:23:09: ISIS-Adj (area0003): Sending L1 LAN IIH on FastEthernet3/0.3, length 1497
01:23:10: ISIS-Adj (area0002): Sending L1 LAN IIH on FastEthernet3/0.2, length 1497
01:23:12: ISIS-Adj (area0001): Sending L1 LAN IIH on FastEthernet3/0.1, length 1497
01:23:12: ISIS-Adj (area0003): Sending L1 LAN IIH on FastEthernet3/0.3, length 1497
01:23:12: ISIS-Adj (area0002): Sending L1 LAN IIH on FastEthernet3/0.2, length 1497
01:23:13: ISIS-Adj (area0001): Rec L1 IIH from 00e0.b064.4325 (FastEthernet3/0.1), cir
type L1, cir id 0010.7BC7.AE40.01, length 147
```

```
01:23:14: ISIS-Adj (area0002): Rec L1 IIH from 00e0.b064.434e (FastEthernet3/0.2), cir
type L1, cir id 0010.7BC7.AE40.01, length 147
01:23:14: ISIS-Adj (area0001): Sending L2 LAN IIH on FastEthernet3/0.1, length 1497
01:23:15: ISIS-Adj (area0001): Sending L1 LAN IIH on FastEthernet3/0.1, length 1497
01:23:15: ISIS-Adj (area0002): Sending L1 LAN IIH on FastEthernet3/0.2, length 1497
01:23:15: ISIS-Adj (area0003): Sending L1 LAN IIH on FastEthernet3/0.3, length 1497
01:23:18: ISIS-Adj (area0001): Sending L1 LAN IIH on FastEthernet3/0.1, length 1497
01:23:18: ISIS-Adj (area0001): Rec L1 IIH from 0010.7bd8.c7d0 (FastEthernet3/0.1), cir
type L1, cir id 0010.7BC7.AE40.01, length 147
01:23:18: ISIS-Adj (area0002): Sending L1 LAN IIH on FastEthernet3/0.2, length 1497
01:23:18: ISIS-Adj (area0003): Sending L1 LAN IIH on FastEthernet3/0.3, length 1497
01:23:21: ISIS-Adj (area0001): Sending L1 LAN IIH on FastEthernet3/0.1, length 1497
01:23:21: ISIS-Adj (area0003): Sending L1 LAN IIH on FastEthernet3/0.3, length 1497
01:23:21: ISIS-Adj (area0002): Sending L1 LAN IIH on FastEthernet3/0.2, length 1497
01:23:22: ISIS-Adj (area0001): Rec L1 IIH from 00e0.b064.4325 (FastEthernet3/0.1), cir
type L1, cir id 0010.7BC7.AE40.01, length 147
01:23:23: ISIS-Adj (area0002): Rec L1 IIH from 00e0.b064.434e (FastEthernet3/0.2), cir
type L1, cir id 0010.7BC7.AE40.01, length 147
```

The next step is to debug the ES-IS protocol using the **debug clns esis packets** command. The following example shows a configuration error by the technician:

```
3640A# debug clns esis packets

ES-IS packets debugging is on

3640A#
01:32:22: ES-IS: ISH from 00e0.b064.4325 (FastEthernet3/0.1), HT 300
01:32:26: ES-IS: ISH from 00e0.b064.434e (FastEthernet3/0.2), HT 300
01:32:30: ES-IS: ISH sent to All ESs (FastEthernet3/0.1): NET
39.840f.8011.9999.0000.1111.0001.0010.7bc7.ae40.00, HT 300, HLEN 30
01:32:35: ES-IS: ISH from 00d0.5872.9720 (FastEthernet3/0.3), HT 300
```

Router 3640A first receives an IS Hello (ISH) from device NE14A (SNPA 00e0.b064.4325) on Fast Ethernet interface 3/0.1. The holdtime is 300 seconds before discarding. Router 3640A receives an ISH from device NE25A (SNPA 00e0.b064.434e) on Fast Ethernet interface 3/0.2. An ISH was sent to all end systems on Fast Ethernet interface 3/0.1 with a hold time of 300 seconds. The packet header length is 30 bytes. The last packet is an ISH from device NE26A (SNPA 00d.0.5872.9720) with a hold time of 300 seconds. Device NE26A has only the ES-IS protocol turned up. Router 3640A is sending out ESHs on all the Fast Ethernet interfaces. Device NE26A is sending an ISH. Device NE26A is configured only to support ES-IS, which was determined because ISHs were being sent, but not IIH.

Once device NE26A is correctly configured for IS-IS routing, verify the correct adjacency using the **show clns neighbors** EXEC command. The following example shows the report displayed:

```
3640A# show clns neighbors

Area area0001:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
NE15A          Fa3/0.1     0010.7bd8.c7d0  Up     23        L1   IS-IS
NE14A          Fa3/0.1     00e0.b064.4325  Up     22        L1   IS-IS

Area area0002:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
NE25A          Fa3/0.2     00e0.b064.434e  Up     24        L1   IS-IS

Area area0003:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
NE26A          Fa3/0.3     00d0.5872.9720  Up     22        L1   IS-IS
```

The following example shows the results of **ping clns** commands:

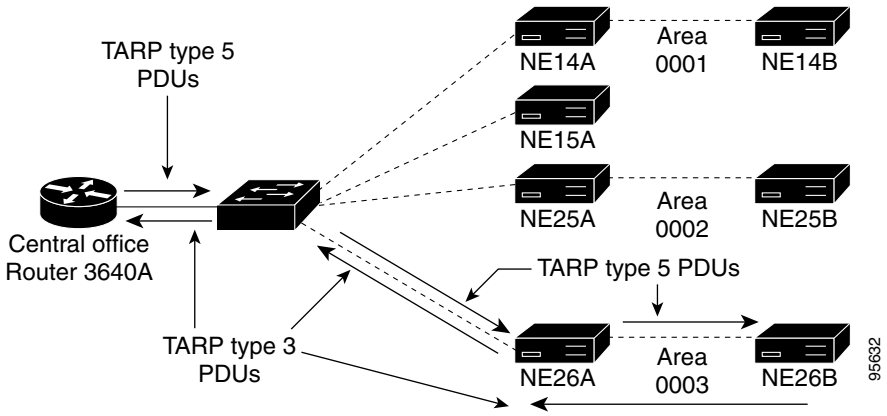
```
3640A# ping clns NE26A

Type escape sequence to abort.
Sending 5, 100-byte CLNS Echos with timeout 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

3640A# ping clns NE26B

Type escape sequence to abort.
Sending 5, 100-byte CLNS Echos with timeout 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Successful connection indicates that the network is up and working.

Troubleshooting Network Connections Using TARP PDUs

A TARP type 5 PDU can be used to troubleshoot the network. (See the "Mapping NSAPs to Device Names Using TARP" section on page 55 for more information about TARP.) The type 5 PDU is sent to a specific NSAP address requesting the TID. The analogy would be sending an IP **ping** command in an IP network. The Cisco IOS software provides a **ping clns** EXEC command, but not all network vendors of SONET/SDH equipment have implemented support for the CLNS **ping** command. In Figure 43, a TARP type 5 PDU is being sent from router 3640A to device NE26B. Figure 43 also shows that the response is a type 3 PDU.

Figure 43 TARP Type 5 PDU Transmissions



The following example shows how to issue the **debug tarp packets** and **debug tarp events** commands and interpret the output:

```
3640A# debug tarp packets
TARP packet info debugging is on
3640A# debug tarp events
TARP events debugging is on

The tarp query is issued for 39.840f.8011.9999.0000.1111.0003.0010.7b17.f880.00

3640A# tarp query 39.840f.8011.9999.0000.1111.0003.0010.7b17.f880.00

Type escape sequence to abort.
Sending TARP type 5 PDU, timeout 40 seconds ...
```

```
 TID corresponding to NET 39.840f.8011.9999.0000.1111.0003.0010.7b17.f880.00 is NE26B
```

The **debug tarp packets** command output shows the type 5 PDU being sent to its destination:

```
3640A#
00:15:22: TARP-PA: Originated TARP packet, type 5, to
        destination 39.840f.8011.9999.0000.1111.0003.0010.7b17.f880.00
00:15:22: TARP-EV: Packet from 39.840f.8011.9999.0000.1111.0003.0010.7b17.f880.00 has a
00:15:22:        sequence number (4) > that in LDB cache entry (3)
00:15:22:        - updating cache entry
```

A type 3 PDU is received on Fast Ethernet interface 3/0.3. The PDU is the response from device NE26B for the type 5 PDU.

```
00:15:22: TARP-PA: Received TARP type 3 PDU on interface FastEthernet3/0.3
00:15:22:        Lft = 100, Seq = 4, Prot type = 0xFE, URC = TRUE
00:15:22:        Ttid len = 0, Stid len = 5, Prot addr len = 20
00:15:22:        Packet sent/propagated by
39.840f.8011.9999.0000.1111.0003.0010.7b17.f880.af
00:15:22:        Originator's NSAP : 39.840f.8011.9999.0000.1111.0003.0010.7b17.f880.00
00:15:22:        Originator's TID : NE26B
```

The **debug tarp event** command output indicates that device NE26B is entered into the TARP data cache:

```
00:15:22: TARP-PA: Created new DYNAMIC cache entry for NE26B
```

The **tarp query** command issues a TARP type 5 PDU, which is sent to a specific network and requests the TID or name of the network element.

The following example shows a TARP query being sent to device NE14B with NET 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00. The TID is device NE14B. Note that the CLNS host name and the TID were both set to device NE14B, which was chosen by the system administrator.

```
3640A# tarp query 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00

Type escape sequence to abort.
Sending TARP type 5 PDU, timeout 40 seconds ...

 TID corresponding to NET 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00 is NE14B
```

Cisco IOS **debug** commands allow packets issued from a **tarp query** command to be examined. The following examples show output from the **debug tarp events** and **debug tarp packets** EXEC commands. The **debug** command output is based on the **tarp query** command. (Bold text highlights key parts of the report for purpose of example.)

```
3640A# debug tarp events
TARP events debugging is on
3640A# debug tarp packets
TARP packet info debugging is on

3640A#
00:33:23: TARP-PA: Originated TARP packet, type 5, to
        destination 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00
00:33:23: TARP-PA: Received TARP type 3 PDU on interface FastEthernet3/0.1
00:33:23:        Lft = 100, Seq = 2, Prot type = 0xFE, URC = TRUE
00:33:23:        Ttid len = 0, Stid len = 5, Prot addr len = 20
00:33:23:        Packet sent/propagated by
39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.af
00:33:23:        Originator's NSAP : 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00
00:33:23:        Originator's TID : NE14B
00:33:23: TARP-PA: Created new DYNAMIC cache entry for NE14B
```

The output indicates a TARP type 5 PDU is sent to NET 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00. The packet that was receive is a type 3 PDU and was sent by NSAP 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.af. The network selector on the NSAP is "af," which designates the TARP application. The output also reports the originator's NSAP as 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00. More accurately, this label should be the originator's NET. The originator's TID is listed as NE14B.

If the NSAP or NET of the IS-IS router is not known but the TID is known, use the **tarp resolve** EXEC command to test connectivity between devices. The following example shows sample output:

```
3640A# tarp resolve NE14B

Type escape sequence to abort.
Sending TARP type 1 PDU, timeout 15 seconds ...

 NET corresponding to TID NE14B is 39.840f.8011.9999.0000.1111.0001.0050.7363.7b40.00
```

In the output, the router will wait 15 seconds for a response before issuing a TARP type 2 PDU. Device NE14B responds within 15 seconds with its NET, which is the NSAP address and selector value of 00.

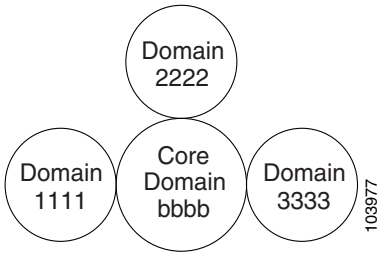
Distribution Layer Configuration

This section focuses on the distribution layer of Cisco's three-tiered network architecture and contains these sections:

Configuring the Distribution Network

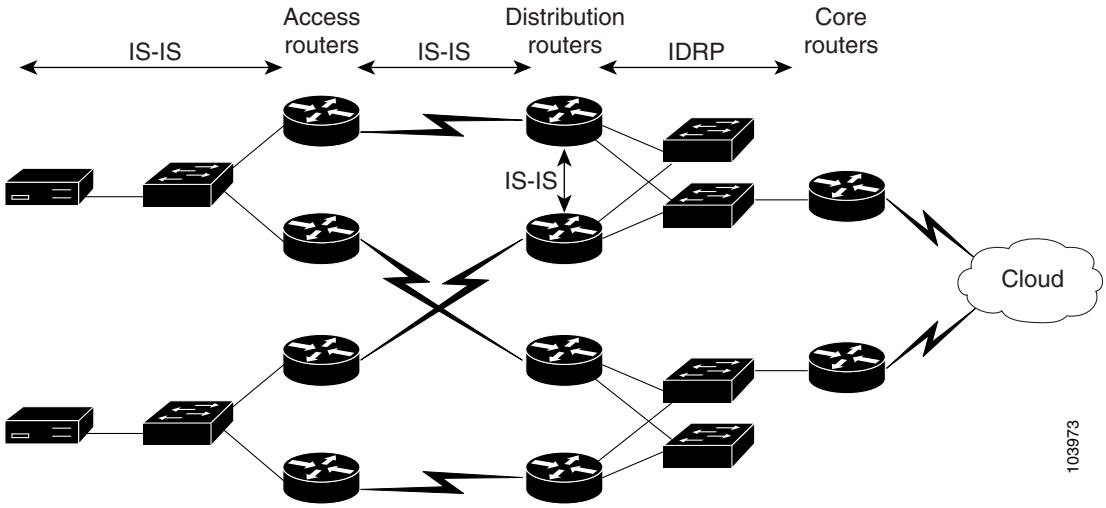
The hypothetical network that will be used in this section assumes the network is laid out in three geographic areas. Each geographic area will be a separate Open System Interconnection (OSI) domain. The core routers will be placed in a separate domain in the center. Figure 44 shows the concept; domain designations have also been provided.

Figure 44 OSI Domains for the Distribution Network



As previously mentioned in this document, Cisco recommends that customers implement a three-tiered architecture in the data communications network (DCN) (see "The Cisco Three-Tiered DCN Network Architecture" section on page 12). The network shown in Figure 45 has the access layer and distribution routers in the same OSI domain.

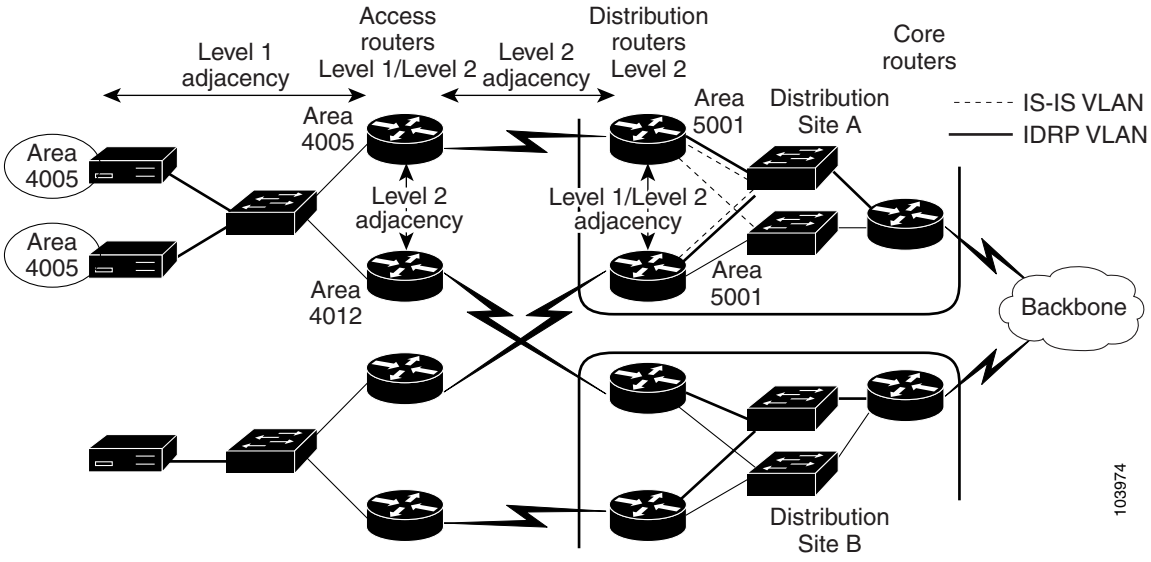
Figure 45 Three-Tiered Architecture with Routing Protocols and Domains



The IS-IS routing protocol is running within the OSI domain. The core routers have been placed in a separate OSI domain. An Interdomain Routing Protocol (IDRP) is running between the distribution and core routers. The Level 2 routers within a domain must be connected contiguously to provide access throughout the domain. In Figure 45, the distribution routers are connected with Ethernet, and IS-IS is run over the Ethernet. The IDRP runs over a separate Ethernet network, as shown in Figure 45. The two Ethernet networks could also be configured using VLANs. A redundant alternative would be to install two switches and configure a separate VLAN for IS-IS and the IDRP on each switch. The service provider should not configure IS-IS and the IDRP on the same VLAN if the IDRP is ISO-IGRP.

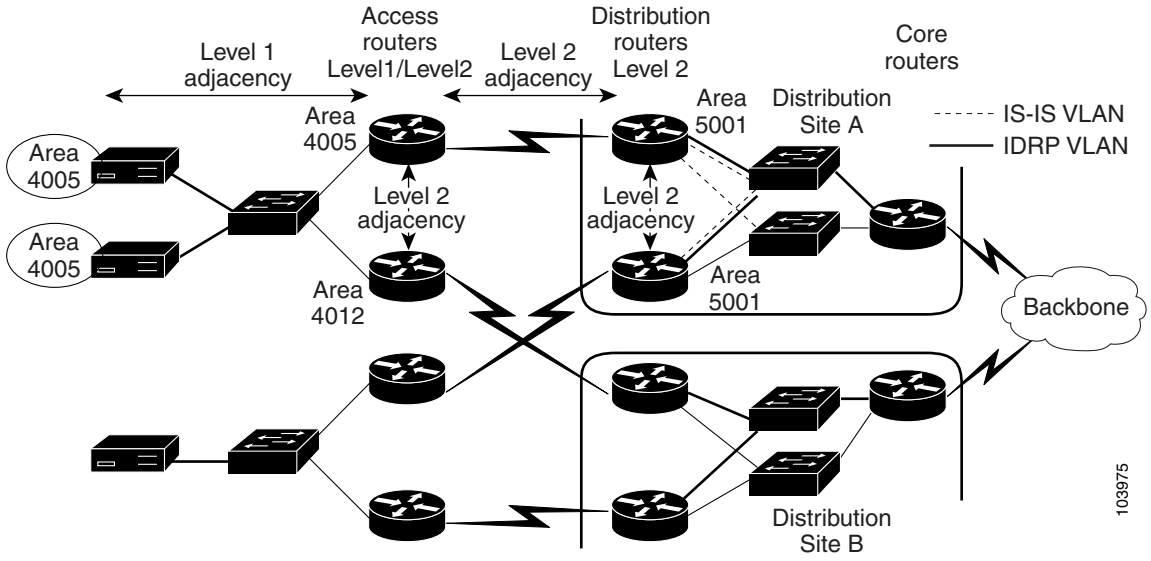
The distribution routers should be configured in one IS-IS area that is shared by only the distribution routers in this site. The distribution routers can be configured as Level 1/Level 2 routers. The distribution routers will form a Level 2 adjacency to the access routers over the WAN links, because the access routers in the central office will be in a separate OSI area. The distribution routers will form a Level 1/Level 2 adjacency over the LAN connecting the routers at the distribution site. The service provider should make sure the routers have redundant LANs tiering the area together. The Level 1 area must stay contiguous. In Figure 46, there is a separate VLAN configured for IS-IS on each switch. Figure 46 also shows the adjacencies.

Figure 46 Three-Tiered Architecture with Level 1/Level 2 Adjacencies



An alternative method is to configure the distribution routers as Level 2 routers only. Use the **is-type level-2-only** command to do so. The service provider would still place all the distribution routers at site A in the same OSI area. The advantage of configuring the routers as Level 2 is that the router needs to maintain only one set of adjacencies and one database. In other words, the Level 1 database and the Level 1 adjacencies are eliminated, which lowers the overhead on the router. The adjacencies are shown in Figure 47.

Figure 47 Three-Tiered Architecture with Level 2 Adjacencies



Distribution Network Configuration Example

In the following sample configuration, the distribution router is in domain 3333 and area0003. The Connectionless Network Service (CLNS) configuration for a distribution router in Distribution site A is listed. The host name of the router is 7507A. Ethernet interfaces 0/0 and 0/1 are connected to two separate LANs, which make up the redundant LANs in the distribution center. Serial interfaces 1/0 through 6/7 are connected using a DS1 link to a separate access site or central office. A second distribution site is recommended for redundancy, as shown in Figure 47. The second distribution routers would be connected to the same access sites with a DS1. The configuration would be very similar.

```
hostname Access7507A
!
clns routing
!
!
interface Ethernet0/0
clns router isis area0003
 tarp enable
!
interface Ethernet0/1
clns router isis area0003
 tarp enable

!
interface Serial1/0
 description DS1 City1
  clns router isis area0003
 tarp enable
!
interface Serial1/1
 description DS1 City2
 clns router isis area0003
 tarp enable
!
interface Serial1/2
 description DS1 City3
 clns router isis area0003
 tarp enable
!
interface Serial1/3
 description DS1 City4
 clns router isis area0003
 tarp enable
!
interface Serial1/4
 description DS1 City5
 clns router isis area0003
 tarp enable
!
interface Serial1/5
 description DS1 City6
 clns router isis area0003
 tarp enable
!
interface Serial1/6
 description DS1 City7
 clns router isis area0003
 tarp enable
!
interface Serial1/7
 description DS1 City8
 clns router isis area0003
```

```
 tarp enable
!
interface Serial4/0
 description DS1 City9
 clns router isis area0003
 tarp enable
!
interface Serial4/1
 description DS1 City10
 clns router isis area0003
 tarp enable
!
interface Serial4/2
 description DS1 City11
 clns router isis area0003
 tarp enable
!
interface Serial4/3
 description DS1 City12
 clns router isis area0003
 tarp enable
!
interface Serial4/4
 description DS1 City13
 clns router isis area0003
 tarp enable
!
interface Serial4/5
 description DS1 City14
 clns router isis area0003
 tarp enable
!
interface Serial4/6
 description DS1 North1
 clns router isis area0003
 tarp enable
!
interface Serial4/7
 description T1 City15
 clns router isis area0003
 tarp enable
!
interface Serial5/0
 description DS1 City16
 clns router isis area0003
 tarp enable
!
interface Serial5/1
 description DS1 City17
 clns router isis area0003
 tarp enable
!
interface Serial5/2
 description City18
 clns router isis area0003
 tarp enable
!
interface Serial5/3
 description DS1 City19
 clns router isis area0003
 tarp enable
!
interface Serial5/4
 description DS1 Main1
```

```
 clns router isis area0003
 tarp enable
!
interface Serial5/5
 description DS1 City20
 clns router isis area0003
 tarp enable
!
interface Serial5/6
 description DS1 City21
 clns router isis area0003
 tarp enable
!
interface Serial5/7
 description DS1 City22
 clns router isis area0003
 tarp enable
!
interface Serial6/0
 description DS1 City23
 clns router isis area0003
 tarp enable
!
interface Serial6/1
 description DS1 City24
 clns router isis area0003
 tarp enable
!
interface Serial6/2
 description DS1 City25
 clns router isis area0003
 tarp enable
!
interface Serial6/3
 description DS1 City26
 clns router isis area0003
 tarp enable
!
interface Serial6/4
 description DS1 City27
 clns router isis area0003
 tarp enable
!
interface Serial6/5
 description DS1 City28
 clns router isis area0003
 tarp enable
!
interface Serial6/6
 description DS1 City29
 clns router isis area0003
 tarp enable
!
interface Serial6/7
 description DS1 City30
 clns router isis area0003
 tarp enable
!
router isis area0003
 net 39.840f.8011.9999.0000.3333.0003.1234.0c15.86a3.00
!
tarp run
tarp tid Access7507A
```

Core Layer Configuration

The following sections describe how to configure the core portion of the OSI network:

OSI Domains and the Core

A large OSI network is made up of multiple OSI domains. The recommended architectural design for a large OSI network is to place the core in an OSI domain. The individual OSI domains are connected to the core at two points. Figure 48 illustrates this concept. The core configuration can be configured with static routes, ISO-IGRP, or multiprotocol BGP. Multiprotocol BGP configuration is described in the feature module titled *Multiprotocol BGP (MP-BGP) Support for CLNS*.

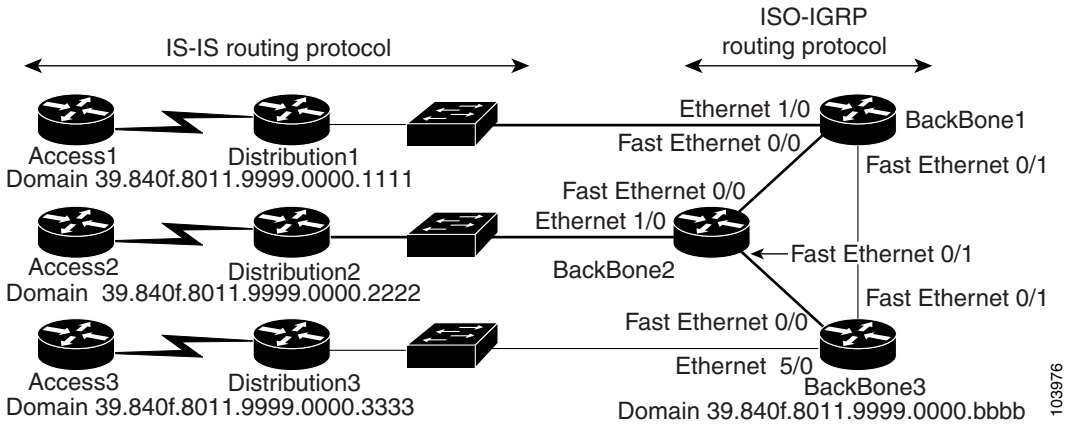
ISO-IGRP can be used in the core to link the three OSI domains. The IS-IS routing protocol will be run in each of the three IS-IS domains, as shown in Figure 48. The IS-IS routing protocol will be run on the access routers and the distribution routers. The core routers will be the boundary between the IS-IS domains and the ISO-IGRP domain, and the core routers will run the IS-IS and ISO-IGRP routing protocols. The ISO-IGRP routes will be redistributed directly into IS-IS. IS-IS should not be redistributed directly into ISO-IGRP. The routes injected into ISO-IGRP should be summarized. The domain can be summarized with a single static route that can be injected into the core.

Configuring the Core Network

The example network used in this section is based on a lab network. The lab network sample configurations will have only one core, instead of the recommended two cores. This section will describe some configuration tricks to implement a second core. The lab network has three routers in the core, which will connect together using Ethernet. In a real network, WAN links, rather than Ethernet, would be used to make the connections. The core routers are connected using Ethernet to distribution routers as shown in Figure 48. The four domains are addressed as follows:

```
39.840f.8011.9999.0000.1111
39.840f.8011.9999.0000.2222
39.840f.8011.9999.0000.3333
39.840f.8011.9999.0000.bbbb
```

Figure 48 Sample Core Network



In the lab network, each backbone router is connected using an Ethernet connection to a distribution router. The distribution router is connected using Ethernet to an access router. To simplify the example, the access site is not redundant and is sufficient for examining the core.

Core Network Configuration Examples

This section contains the following configuration examples:

Configuring the First Core Router

Start configuration of the core routers with the router named BackBone1. The router will be configured to participate in both IS-IS domain 1111 and area 9999. The IS-IS process identifier is area9999. Remember that the process identifier is similar in concept to a UNIX process identifier.

```
!
router isis area9999
 net 39.840f.8011.9999.0000.1111.9999.000d.bc2e.6d80.00
 redistribute iso-igrp backbone
```

The backbone has been assigned its own domain bbbb and all three core routers have been placed in area 1001. The ISO-IGRP process identifier is called backbone.

The following example shows the ISO-IGRP configuration:

```
router iso-igrp backbone
 net 39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d80.00
 redistribute static
```

The challenge is to summarize the domain into the core using a static route. The route is summarized with the following **clns route** command. The following **clns route** command configures a path to domain 1111 or 39.840f.8011.9999.0000.1111. The route can be accessed using Ethernet interface 1/0 on router BackBone1.

```
clns route 39.840f.8011.9999.0000.1111 Ethernet1/0 000d.bc2e.6d90
```

Ethernet interface 1/0 is the BackBone1 interface connected to the distribution router, which is labeled Distribution1. The MAC address of Ethernet interface 1/0 on the BackBone1 router is 000d.bc2e.6d90. Use the **show interfaces** command, as the following sample output shows, to confirm the MAC address.

```
BackBone1# show interfaces ethernet 1/0

Ethernet1/0 is up, line protocol is down
  Hardware is AmdP2, address is 000d.bc2e.6d90 (bia 000d.bc2e.6d90)
  Internet address is 192.168.10.1/26
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 128/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     254 packets output, 18476 bytes, 0 underruns
     254 output errors, 0 collisions, 4 interface resets
     0 babbles, 0 late collision, 0 deferred
     255 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Figure 48 on page 94 shows that router BackBone1 on Fast Ethernet interface 0/0 is connected to router BackBone2 on Fast Ethernet interface 0/0. Router BackBone1 on FastEthernet interface 0/1 is connected to router BackBone3 on Fast Ethernet interface 0/1. ISO-IGRP is turned up on these interfaces. For purpose of example, the following configuration shows the routing processes for ISO-IGRP in bold text. The ISO-IGRP process is called backbone. TARP is enabled on the backbone.

```
interface FastEthernet0/0
 ip address 192.168.20.1 255.255.255.252
 speed auto
 half-duplex
 clns router iso-igrp backbone
 tarp enable

interface FastEthernet0/1
 ip address 192.168.20.5 255.255.255.252
 speed auto
 half-duplex
 clns router iso-igrp backbone
 tarp enable
```

Figure 48 on page 94 shows that BackBone1 router Ethernet interface 1/0 is connected to the distribution router Distribution1. The IS-IS routing protocol is run over the Ethernet interface 1/0 connection between router BackBone1 and router Distribution1. The core router BackBone1 participates in domain 1111 and the backbone domain bbbb. The following example shows the configuration for Ethernet interface 1/0:

```
interface Ethernet1/0
 ip address 192.168.10.1 255.255.255.192
 half-duplex
 clns router isis area9999
```

Verifying the First Core Router Configuration

Use the **show clns** EXEC command to check interface configuration for the core router. The following example shows three interfaces configured for CLNS. Two NETs are shown, one NET for ISO-IGRP and a second for IS-IS.

```
BackBone1# show clns

Global CLNS Information:
  3 Interfaces Enabled for CLNS
  NET: 39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d80.00
  NET: 39.840f.8011.9999.0000.1111.9999.000d.bc2e.6d80.00
  Configuration Timer: 60, Default Holding Timer: 300, Packet Lifetime 64
  ERPDU's requested on locally generated packets
  Intermediate system operation enabled (CLNS forwarding allowed)
  ISO-IGRP level-1 Router: backbone
    Routing for Domain: 39.840F.8011.9999.0000.BBBB, Area: 1001
  ISO-IGRP level-2 Router: DOMAIN_backbone
    Routing for Domain: 39.840F.8011.9999.0000.BBBB
  IS-IS level-1-2 Router: area9999
    Routing for Area: 39.840f.8011.9999.0000.1111.9999
```

Use the **show clns neighbors** EXEC command to verify that there are three neighbors. BackBoneR1 has a Level 1 ISO-IGRP adjacency on Fast Ethernet interface 0/1 with BackBoneR3. The router Distribution1 has a Level 1/Level 2 adjaceny on Ethernet interface 1/0. BackBoneR2 has a Level 1 ISO-IGRP adjacency on Fast Ethernet interface 0/0 with BackBoneR3. The following **show clns neighbors** command output matches the configuration listed earlier and in Figure 48 on page 94.

```
BackBoneR1# show clns neighbors

System Id      Interface   SNPA            State  Holdtime  Type Protocol
BackBoneR3     Fa0/1       0010.7bd8.c7d1  Up     39        L1   ISO-IGRP
Distribution1  Et1/0       0010.7b17.f880  Up     9         L1L2 IS-IS
BackBoneR2     Fa0/0       000d.bc2e.6d40  Up     50        L1   ISO-IGRP
```

Use the **show clns neighbors detail** EXEC command to show additional detail about the neighbors.

```
BackBoneR1# show clns neighbors detail

System Id      Interface   SNPA            State  Holdtime  Type Protocol
BackBoneR3     Fa0/1       0010.7bd8.c7d1  Up     36        L1   ISO-IGRP
  Area Address(es): 39.840f.8011.9999.0000.bbbb.1001
  Uptime: 01:32:07
Distribution1  Et1/0       0010.7b17.f880  Up     7         L1L2 IS-IS
  Area Address(es): 39.840f.8011.9999.0000.1111.9999
  Uptime: 01:32:08
  NSF capable
BackBoneR2     Fa0/0       000d.bc2e.6d40  Up     47        L1   ISO-IGRP
  Area Address(es): 39.840f.8011.9999.0000.bbbb.1001
  Uptime: 01:32:08
```

Configuring a Second Core Router

The configuration for a second core router named BackBone2 in the example network is next. The router will be configured to participate in both IS-IS domain 2222 and area 0002. The IS-IS process identifier is area0002. Remember the process identifier is similar in concept to a UNIX process identifier. In the following example, notice the command to redistribute the routes in ISO-IGRP back into IS-IS. The number of routes will be small, because each domain is summarized with a static route into ISO-IGRP.

```
!
router isis area0002
 net 39.840f.8011.9999.0000.2222.0002.000d.bc2e.6d40.00
 redistribute iso-igrp backbone
```

Configuring the ISO IGRP Routing Protocol

This section describes how to configure the ISO-IGRP routing protocol. The backbone has been assigned its own domain as bbbb, and all three core routers have been placed in area 1001. In the following ISO-IGRP configuration example, notice the **redistribute static** command that redistributes the static route that summarizes domain 2222 into ISO-IGRP:

```
router iso-igrp backbone
 net 39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d40.00
 redistribute static
```

The challenge is to summarize the domain into the core on a static route. The route is summarized with the **clns route** command, as shown in the following example. The **clns route** command configures a path to domain 2222 or 39.840f.8011.9999.0000. 2222. The route can be accessed using Ethernet interface 1/0, on router BackBone1.

```
clns route 39.840f.8011.9999.0000.2222 Ethernet1/0 000d.bc2e.6d50
```

Ethernet interface 0/1 is connected to the distribution router labeled Distribution1. The MAC address of Ethernet interface 1/0 on the BackBone1 router is 000d.bc2e.6d50. Use the **show interfaces** command, as the following sample output shows, to confirm the MAC address.

```
BackBoneR2# show interfaces ethernet 1/0

Ethernet1/0 is up, line protocol is up
  Hardware is AmdP2, address is 000d.bc2e.6d50 (bia 000d.bc2e.6d50)
  Internet address is 192.168.50.1/26
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 8000 bits/sec, 1 packets/sec
  5 minute output rate 4000 bits/sec, 0 packets/sec
     2273 packets input, 2301496 bytes, 0 no buffer
     Received 2266 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     1048 packets output, 816754 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Figure 48 on page 94 shows that BackBone2 Fast Ethernet interface 0/0 is connected to the BackBone1 router, and BackBone2 Fast Ethernet interface 0/1 is connected to the BackBone3 router. ISO-IGRP is turned up on these interfaces. For purpose of example, the following sample configuration shows the routing process for ISO-IGRP in bold text. The ISO-IGRP process is called backbone. TARP is enabled on the backbone.

```
interface FastEthernet0/0
 ip address 192.168.20.2 255.255.255.252
 speed auto
 half-duplex
 clns router iso-igrp backbone
 tarp enable
!
interface FastEthernet0/1
 ip address 192.168.20.10 255.255.255.252
 speed auto
 half-duplex
 clns router iso-igrp backbone
 tarp enable
```

Figure 48 on page 94 shows Ethernet interface 1/0 is connected to the distribution router labeled Distribution1. The IS-IS routing protocol is run over the Ethernet interface 1/0 connection between router BackBone2 and router Distribution2. The core router BackBone2 participates in domain 2222 and the backbone domain bbbb. The following example shows the configuration for Ethernet interface 1/0:

```
interface Ethernet1/0
 ip address 192.168.50.1 255.255.255.192
 half-duplex
 clns router isis area0002
 tarp enable
```

Configuring a Third Core Router

Following is the configuration for the BackBone3 router, without step-by-step explanation. See the "Configuring the First Core Router" and "Verifying the First Core Router Configuration" sections for more details on core router configuration and verification.

```
router iso-igrp backbone
 redistribute static
 net 39.840f.8011.9999.0000.bbbb.1001.0010.7bd8.c7d0.00
!
router isis area0033
 redistribute iso-igrp backbone
 net 39.840f.8011.9999.0000.3333.0033.0010.7bd8.c7d0.00
!
clns route 39.840f.8011.9999.0000.3333 Ethernet5/0 0010.7bd8.c821
!
interface FastEthernet0/0
 ip address 192.168.20.9 255.255.255.252
 duplex auto
 speed auto
 clns router iso-igrp backbone
 tarp enable
!
interface FastEthernet0/1
 ip address 192.168.20.6 255.255.255.252
 duplex auto
 speed auto
 clns router iso-igrp backbone
 tarp enable
```

```
!
interface Ethernet5/0
 ip address 192.168.100.1 255.255.255.252
 half-duplex
 clns router isis area0033
```

Verifying the Routing Table

To verify the routing table created on the BackBoneR1 router, use the **show clns route** EXEC command. You will see the static route to domain 39.840f.8011.9999.0000.1111. The routes to domains 39.840f.8011.9999.0000.2222 and 39.840f.8011.9999.0000.3333 are learned from the ISO-IGRP routing protocol. You will also see the IS-IS routes to areas within domain 39.840f.8011.9999.0000.1111.

```
BackBoneR1# show clns route

ISO-IGRP Routing Table for Domain 39.840F.8011.9999.0000.BBBB, Area 1001
System Id       Next-Hop        SNPA                Interface   Metric   State
BackBoneR3      BackBoneR3      0010.7bd8.c7d1      Fa0/1       110      Up
BackBoneR2      BackBoneR2      000d.bc2e.6d40      Fa0/0       110      Up
BackBoneR1      0000.0000.0000  --                  --          0        Up

ISO-IGRP Routing Table for Domain 39.840F.8011.9999.0000.BBBB
Area Id         Next-Hop        SNPA                Interface   Metric   State
1001            0000.0000.0000  --                  --          0        Up

Codes: C - connected, S - static, d - DecnetIV
       I - ISO-IGRP,  i - IS-IS,  e - ES-IS
       B - BGP,       b - eBGP-neighbor

C  39.840f.8011.9999.0000.1111.9999 [2/0], Local IS-IS Area
C  39.840f.8011.9999.0000.bbbb [2/0], Local ISO-IGRP Domain
C  39.840f.8011.9999.0000.1111.9999.000d.bc2e.6d80.00 [1/0], Local IS-IS NET
C  39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d80.00 [1/0], Local ISO-IGRP NET

i  39.840f.8011.9999.0000.1111.0003 [110/20]
      via Distribution1, Ethernet1/0
S  39.840f.8011.9999.0000.1111 [10/0]
      via Ethernet1/0
I  39.840f.8011.9999.0000.2222 [100/110]
      via BackBoneR2, FastEthernet0/0
I  39.840f.8011.9999.0000.3333 [100/110]
      via BackBoneR3, FastEthernet0/1
```

Verifying Network Connectivity

To verify network connectivity, use the **clns ping** and **trace** EXEC commands.

In the following example, the ping is from access router Access1 in domain 1111 to access router Access2 in domain 2222:

```
Access2# ping clns Access1

Type escape sequence to abort.
Sending 5, 100-byte CLNS Echos with timeout 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/12 ms
```

The following example traces the route from Access2 to Access1; the route matches what is shown in Figure 48 on page 94.

```
Access2# trace clns Access1

Type escape sequence to abort.
Tracing the route to Access1 (39.840f.8011.9999.0000.1111.0003.00d0.5872.9720.00)

  1 Distribution2(39.840f.8011.9999.0000.2222.0002.0030.94e2.6ce0.00) 0 msec ! 0 msec ! 0
msec !
  2 BackBoneR2(39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d40.00) 4 msec ! 4 msec ! 4
msec !
  3 BackBoneR1(39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d80.00) 4 msec ! 4 msec ! 4
msec !
  4 Distribution1(39.840f.8011.9999.0000.1111.9999.0010.7b17.f880.00) 4 msec ! 4 msec ! 4
msec !
  5 Access1(39.840f.8011.9999.0000.1111.0003.00d0.5872.9720.00) 4 msec ! 4 msec ! 4 msec !
Access2#
```

Adding Redundancy to the Core

When considering redundancy in the core portion of the network, most service providers will implement more redundancy than has been shown in the examples in this document. The first place the service providers will increase redundancy is between the core router and the distribution router, and the service provider will do so by building redundant LANs. Therefore, a second static route would need to be added for the second LAN. An earlier example in this document configured a single static route for a router designated BackBone1; this configuration is listed again in the following example. A second route would be almost identical, except that the route statement (**clns route** command) would reflect the appropriate Ethernet interface and its equivalent MAC address.

```
clns route 39.840f.8011.9999.0000.1111 Ethernet1/0 000d.bc2e.6d90
```

To continue adding redundancy, add a second core and a second set of distribution sites. In an ISO-IGRP configuration, one core must be a primary route and the second core a secondary or backup. The primary and secondary routes are designated by the length of the route specified in the static routes. The Cisco IOS software prefers the path with the longest route. Examine the route statements for the primary core using the following example:

```
! BackBone1 Router
clns route 39.840f.8011.9999.0000.1111 Ethernet1/0 000d.bc2e.6d90

! BackBone2 Router
clns route 39.840f.8011.9999.0000.2222 Ethernet1/0 000d.bc2e.6d50

! BackBone3 Router
clns route 39.840f.8011.9999.0000.3333 Ethernet5/0 0010.7bd8.c821
```

The second core will be made up of routers BackBone1A, BackBone2A and BackBone3A. The following examples show the static route for each of the secondary core routers, by router.

```
! BackBone1A Router
clns route 39.840f.8011.9999.0000.11 Ethernet1/1 000d.bc2e.7d90

! BackBone2A Router
clns route 39.840f.8011.9999.0000.22 Ethernet1/1 000d.bc2e.7d50

! BackBone3A Router
clns route 39.840f.8011.9999.0000.33 Ethernet4/1 0010.7bd8.d421
```

Notice that the route is shorter in length for the secondary routers. For example, router BackBone1 has a static route configured for 39.840f.8011.9999.0000.1111 and router BackBone1A has a static route configured for 39.840f.8011.9999.0000.11. The distribution routers have both routes in their routing tables. The distribution routers will choose the longer route or more significant route to forward packets to.

Tunneling Across the Core

Some service providers will have routers in the core that do not route CLNS. So tunnels must be built across the core. Cisco recommends that you route up to the distribution router and build a small number of tunnels across the core between the distribution routers.

Completing the Core Router Configurations

The following sections provide the configurations for the remaining routers in the sample lab network shown in Figure 48 on page 94:

- Configuring Router Access1, page 101
- Configuring Router Access2, page 103
- Configuring Router Access3, page 104
- Configuring Router Distribution1, page 106
- Configuring Router Distribution2, page 108
- Configuring Router Distribution3, page 109

Configuring Router Access1

The following example shows the relevant CLNS configuration commands for the router designated Access1 in Figure 48 on page 94:

```
Access1# show configuration

hostname Access1
!
clns routing
!
interface Ethernet0/0
 ip address 192.168.10.66 255.255.255.192
 half-duplex
 clns router isis area0003
 tarp enable
!
interface BRI0/0
 no ip address
 shutdown
!
router isis area0003
 net 39.840f.8011.9999.0000.1111.0003.00d0.5872.9720.00
!
clns host BackBoneR1 39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d80.00
clns host BackBoneR2 39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d40.00
clns host BackBoneR3 39.840f.8011.9999.0000.bbbb.1001.0010.7bd8.c7d0.00
clns host Distribution2 39.840f.8011.9999.0000.2222.0002.0030.94e2.6ce0.00
clns host Distribution1 39.840f.8011.9999.0000.1111.9999.0010.7b17.f880.00
clns host Access1 39.840f.8011.9999.0000.1111.0003.00d0.5872.9720.00
!
```

```
tarp run
tarp tid Access1
!
```

Verifying the Configuration

The following examples display output from the **show clns** and **show clns neighbors** EXEC commands for router Access1. The commands display global information about CLNS and the router. The routing area is identified as 39.840f.8011.9999.0000.1111.0003.

```
Access1# show clns

Global CLNS Information:
  2 Interfaces Enabled for CLNS
  NET: 39.840f.8011.9999.0000.1111.0003.00d0.5872.9720.00
  Configuration Timer: 60, Default Holding Timer: 300, Packet Lifetime 64
  ERPDU's requested on locally generated packets
  Intermediate system operation enabled (CLNS forwarding allowed)
  IS-IS level-1-2 Router: area0003
    Routing for Area: 39.840f.8011.9999.0000.1111.0003

Access1# show clns neighbors

System Id      Interface   SNPA            State  Holdtime  Type Protocol
3640A          Et0/0       0010.7bc7.ae41  Up     26        L2   IS-IS
Distribution1  Et0/1       0010.7b17.f881  Up     28        L2   IS-IS
```

The following example displays information from the **show clns route** EXEC command:

```
Access1# show clns route
Codes: C - connected, S - static, d - DecnetIV
       I - ISO-IGRP,  i - IS-IS,  e - ES-IS
       B - BGP,       b - eBGP-neighbor

C  39.840f.8011.9999.0000.1111.0003 [2/0], Local IS-IS Area
C  39.840f.8011.9999.0000.1111.0003.00d0.5872.9720.00 [1/0], Local IS-IS NET

i  39.840f.8011.9999.0000.1111.0001 [110/10]
      via 3640A, Ethernet0/0
i  39.840f.8011.9999.0000.1111 [110/30]
      via Distribution1, Ethernet0/1
i  39.840f.8011.9999.0000.2222 [110/20]
      via Distribution1, Ethernet0/1
i  39.840f.8011.9999.0000.3333 [110/20]
      via Distribution1, Ethernet0/1
i  39.840f.8011.9999.0000.1111.9999 [110/10]
      via Distribution1, Ethernet0/1
i  39.840f.8011.9999.0000.bbbb [110/20]
      via Distribution1, Ethernet0/1
```

The following example shows how to test connectivity by issuing the **ping clns** command to a backbone router:

```
Access1# ping clns BackBoneR3

Type escape sequence to abort.
Sending 5, 100-byte CLNS Echos with timeout 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/5 ms
```

The following example shows how to trace a route to another router:

```
Access1# trace clns Distribution2
```

```
Type escape sequence to abort.
Tracing the route to Distribution2 (39.840f.8011.9999.0000.2222.0002.0030.94e2.)

  1 Distribution1(39.840f.8011.9999.0000.1111.9999.0010.7b17.f880.00) 0 msec ! !
  2 BackBoneR1(39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d80.00) 0 msec ! 0 m!
  3 BackBoneR2(39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d40.00) 0 msec ! 0 m!
  4 Distribution2(39.840f.8011.9999.0000.2222.0002.0030.94e2.6ce0.00) 4 msec ! !
```

Configuring Router Access2

The following example shows the relevant CLNS configuration commands for the router designated Access2 in Figure 48 on page 94:

```
Access2# show configuration

clns routing
!
interface Ethernet0
 ip address 192.168.5.190 255.255.255.192
 no ip route-cache
 no ip mroute-cache
 clns router isis area0012
 tarp enable
!
interface Ethernet1
 ip address 192.168.50.66 255.255.255.252
 no ip route-cache
 no ip mroute-cache
 clns router isis area0012
 tarp enable
!
router isis area0012
 net 39.840f.8011.9999.0000.2222.0012.00e0.b064.434e.00
!
clns host BackBoneR1 39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d80.00
clns host BackBoneR2 39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d40.00
clns host BackBoneR3 39.840f.8011.9999.0000.bbbb.1001.0010.7bd8.c7d0.00
clns host Distribution2 39.840f.8011.9999.0000.2222.0002.0030.94e2.6ce0.00
clns host Distribution1 39.840f.8011.9999.0000.1111.9999.0010.7b17.f880.00
clns host Access1 39.840f.8011.9999.0000.1111.0003.00d0.5872.9720.00
clns host Access2 39.840f.8011.9999.0000.2222.0012.00e0.b064.434e.00
!
tarp run
tarp tid Access2
end
```

Verifying the Configuration

The following examples display output from the **show clns** and **show clns neighbors** EXEC commands for router Access2. The commands display global information about CLNS and the router. The routing area is identified as 39.840f.8011.9999.0000.2222.0012.

```
Access2# show clns

Global CLNS Information:
  2 Interfaces Enabled for CLNS
  NET: 39.840f.8011.9999.0000.2222.0012.00e0.b064.434e.00
  Configuration Timer: 60, Default Holding Timer: 300, Packet Lifetime 64
  ERPDU's requested on locally generated packets
  Intermediate system operation enabled (CLNS forwarding allowed)
  IS-IS level-1-2 Router: area0012
    Routing for Area: 39.840f.8011.9999.0000.2222.0012
```

```
Access2# show clns neighbors

System Id      Interface   SNPA            State  Holdtime  Type Protocol
Distribution2  Et1         0030.94e2.6ce0  Up     23        L2   IS-IS
Access2#show clns  neighbors detail

System Id      Interface   SNPA            State  Holdtime  Type Protocol
Distribution2  Et1         0030.94e2.6ce0  Up     23        L2   IS-IS
  Area Address(es): 39.840f.8011.9999.0000.2222.0002
  Uptime: 01:49:34
```

The following example shows the routing table for router Access2. The routes are listed to the backbone domain and the other two domains.

```
Access2# show clns route

Codes: C - connected, S - static, d - DecnetIV
       I - ISO-IGRP,  i - IS-IS,  e - ES-IS

C  39.840f.8011.9999.0000.2222.0012 [2/0], Local IS-IS Area
C  39.840f.8011.9999.0000.2222.0012.00e0.b064.434e.00 [1/0], Local IS-IS NET

i  39.840f.8011.9999.0000.2222.0002 [110/10]
      via Distribution2, Ethernet1
i  39.840f.8011.9999.0000.1111 [110/20]
      via Distribution2, Ethernet1
i  39.840f.8011.9999.0000.2222 [110/30]
      via Distribution2, Ethernet1
i  39.840f.8011.9999.0000.3333 [110/20]
      via Distribution2, Ethernet1
i  39.840f.8011.9999.0000.bbbb [110/20]
      via Distribution2, Ethernet1
```

Configuring Router Access3

The following example shows the relevant CLNS configuration commands for the router designated Access3 in Figure 48 on page 94:

```
Access3# show configuration
!
hostname Access3
!
enable password cisco
!
clns routing
!
interface Ethernet0/0
 ip address 192.168.3.62 255.255.255.192
 half-duplex
 tarp enable
!
interface Ethernet0/1
 ip address 192.168.101.66 255.255.255.192
 half-duplex
 clns router isis area0035
 tarp enable
!
router isis area0035
 net 39.840f.8011.9999.0000.3333.0035.0050.7363.7b40.00
!
clns host Distribution3 39.840f.8011.9999.0000.3333.0035.00e0.1ee3.c720.00
clns host BackBoneR2 39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d40.00
clns host BackBoneR3 39.840f.8011.9999.0000.bbbb.1001.0010.7bd8.c7d0.00
```

```
clns host BackBoneR1 39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d80.00
clns host Distribution2 39.840f.8011.9999.0000.2222.0002.0030.94e2.6ce0.00
clns host Distribution1 39.840f.8011.9999.0000.1111.9999.0010.7b17.f880.00
clns host Access1 39.840f.8011.9999.0000.1111.0003.00d0.5872.9720.00
clns host Access2 39.840f.8011.9999.0000.2222.0012.00e0.b064.434e.00
clns host Access3 39.840f.8011.9999.0000.3333.0035.0050.7363.7b40.00
!
tarp run
tarp tid Access3
!
```

Verifying the Configuration

The following examples display output from the **show clns**, **show clns neighbors**, and **show clns neighbors detail** EXEC commands for router Access3. The commands display global information about CLNS and the router. The routing area is identified as 39.840f.8011.9999.0000.3333.0035.

```
Access3# show clns

Global CLNS Information:
  1 Interfaces Enabled for CLNS
  NET: 39.840f.8011.9999.0000.3333.0035.0050.7363.7b40.00
  Configuration Timer: 60, Default Holding Timer: 300, Packet Lifetime 64
  ERPDU's requested on locally generated packets
  Intermediate system operation enabled (CLNS forwarding allowed)
  IS-IS level-1-2 Router: area0035
    Routing for Area: 39.840f.8011.9999.0000.3333.0035

Access3# show clns neighbors

System Id      Interface   SNPA            State  Holdtime  Type Protocol
Distribution3  Et0/1       00e0.1ee3.c721  Up     9         L1L2 IS-IS

Access3# show clns neighbors detail

System Id      Interface   SNPA            State  Holdtime  Type Protocol
Distribution3  Et0/1       00e0.1ee3.c721  Up     9         L1L2 IS-IS
  Area Address(es): 39.840f.8011.9999.0000.3333.0035
Uptime: 00:05:32
```

The following example displays information from the **show clns route** EXEC command:

```
Access3# show clns route

Codes: C - connected, S - static, d - DecnetIV
       I - ISO-IGRP,  i - IS-IS,  e - ES-IS
       B - BGP,       b - eBGP-neighbor

C  39.840f.8011.9999.0000.3333.0035 [2/0], Local IS-IS Area
C  39.840f.8011.9999.0000.3333.0035.0050.7363.7b40.00 [1/0], Local IS-IS NET

i  39.840f.8011.9999.0000.3333.0033 [110/20]
      via Distribution3, Ethernet0/1
i  39.840f.8011.9999.0000.1111 [110/20]
      via Distribution3, Ethernet0/1
i  39.840f.8011.9999.0000.2222 [110/20]
      via Distribution3, Ethernet0/1
i  39.840f.8011.9999.0000.3333 [110/30]
      via Distribution3, Ethernet0/1
i  39.840f.8011.9999.0000.bbbb [110/20]
      via Distribution3, Ethernet0/1
```

The following example shows how to test connectivity by issuing the **ping clns** command to router Access1:

```
Access3# ping clns Access1

Type escape sequence to abort.
Sending 5, 100-byte CLNS Echos with timeout 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/9 ms
```

The following example shows how to trace a route to another router:

```
Access3# trace clns Access1

Type escape sequence to abort.
Tracing the route to Access1 (39.840f.8011.9999.0000.1111.0003.00d0.5872.9720.00)

  1 Distribution3(39.840f.8011.9999.0000.3333.0035.00e0.1ee3.c720.00) 4 msec ! 0 msec ! 0
msec !
  2 BackBoneR3(39.840f.8011.9999.0000.bbbb.1001.0010.7bd8.c7d0.00) 0 msec ! 0 msec ! 0
msec !
  3 BackBoneR1(39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d80.00) 0 msec ! 0 msec ! 0
msec !
  4 Distribution1(39.840f.8011.9999.0000.1111.9999.0010.7b17.f880.00) 4 msec ! 4 msec ! 4
msec !
  5 Access1(39.840f.8011.9999.0000.1111.0003.00d0.5872.9720.00) 4 msec ! 4 msec ! 4 msec !
```

Configuring Router Distribution1

The following example shows the relevant CLNS configuration commands for the router designated Distribution1 in Figure 48 on page 94:

```
Distribution1# show configuration

hostname Distribution1
!
enable password cisco
!
clns routing
!
interface Ethernet0/0
 ip address 192.168.10.2 255.255.255.252
 no ip mroute-cache
 half-duplex
 clns router isis area9999
 tarp enable
!
interface Ethernet0/1
 ip address 192.168.10.65 255.255.255.192
 no ip mroute-cache
 half-duplex
 clns router isis area9999
 tarp enable
!
router isis area9999
 net 39.840f.8011.9999.0000.1111.9999.0010.7b17.f880.00
!
clns host BackBoneR1 39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d80.00
clns host BackBoneR2 39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d40.00
clns host BackBoneR3 39.840f.8011.9999.0000.bbbb.1001.0010.7bd8.c7d0.00
clns host Distribution1 39.840f.8011.9999.0000.1111.9999.0010.7b17.f880.00
clns host Distribution2 39.840f.8011.9999.0000.2222.0002.0030.94e2.6ce0.00
clns host Access1 39.840f.8011.9999.0000.1111.0003.00d0.5872.9720.00
!
```

```
tarp run
tarp tid Distribution1
```

Verifying the Configuration

The following examples display output from the **show clns**, **show clns neighbors**, and **show clns neighbors detail** EXEC commands for router Distribution1. The commands display global information about CLNS and the router. The routing area is identified as 39.840f.8011.9999.0000.1111.9999.

```
Distribution1# show clns

Global CLNS Information:
  2 Interfaces Enabled for CLNS
  NET: 39.840f.8011.9999.0000.1111.9999.0010.7b17.f880.00
  Configuration Timer: 60, Default Holding Timer: 300, Packet Lifetime 64
  ERPDU's requested on locally generated packets
  Intermediate system operation enabled (CLNS forwarding allowed)
  IS-IS level-1-2 Router: area9999
    Routing for Area: 39.840f.8011.9999.0000.1111.9999

Distribution1# show clns neighbors

System Id      Interface   SNPA            State  Holdtime  Type Protocol
Access1        Et0/1       00d0.5872.9721  Up     9         L2   IS-IS
BackBoneR1     Et0/0       000d.bc2e.6d90  Up     25        L1L2 IS-IS

Distribution1# show clns neighbors detail

System Id      Interface   SNPA            State  Holdtime  Type Protocol
Access1        Et0/1       00d0.5872.9721  Up     8         L2   IS-IS
  Area Address(es): 39.840f.8011.9999.0000.1111.0003
  Uptime: 00:03:20
BackBoneR1     Et0/0       000d.bc2e.6d90  Up     29        L1L2 IS-IS
  Area Address(es): 39.840f.8011.9999.0000.1111.9999
  Uptime: 02:16:45
NSF capable
```

The following example displays information from the **show clns route** EXEC command:

```
Distribution1# show clns route

Codes: C - connected, S - static, d - DecnetIV
       I - ISO-IGRP,  i - IS-IS,  e - ES-IS
       B - BGP,       b - eBGP-neighbor

C  39.840f.8011.9999.0000.1111.9999.0010.7b17.f880.00 [1/0], Local IS-IS NET
C  39.840f.8011.9999.0000.1111.9999 [2/0], Local IS-IS Area

i  39.840f.8011.9999.0000.1111.0001 [110/20]
      via Access1, Ethernet0/1
i  39.840f.8011.9999.0000.1111.0003 [110/10]
      via Access1, Ethernet0/1
i  39.840f.8011.9999.0000.1111 [110/20]
      via BackBoneR1, Ethernet0/0
i  39.840f.8011.9999.0000.2222 [110/10]
      via BackBoneR1, Ethernet0/0
i  39.840f.8011.9999.0000.bbbb [110/10]
      via BackBoneR1, Ethernet0/0
```

Configuring Router Distribution2

The following example shows the relevant CLNS configuration commands for the router designated Distribution2 in Figure 48 on page 94:

```
Distribution2# show configuration

hostname Distribution2
!
interface Ethernet0/0
 ip address 192.168.50.65 255.255.255.252
 no ip mroute-cache
 half-duplex
 clns router isis area0002
 tarp enable
!
interface Ethernet0/1
 ip address 192.168.50.2 255.255.255.192
 no ip mroute-cache
 half-duplex
 clns router isis area0002
!
router isis area0002
 net 39.840f.8011.9999.0000.2222.0002.0030.94e2.6ce0.00
!
clns host BackBoneR1 39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d80.00
clns host BackBoneR2 39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d40.00
clns host BackBoneR3 39.840f.8011.9999.0000.bbbb.1001.0010.7bd8.c7d0.00
clns host Distribution2 39.840f.8011.9999.0000.2222.0002.0030.94e2.6ce0.00
clns host Distribution1 39.840f.8011.9999.0000.1111.9999.0010.7b17.f880.00
clns host Access1 39.840f.8011.9999.0000.1111.0003.00d0.5872.9720.00
clns host Access2 39.840f.8011.9999.0000.2222.0012.00e0.b064.434e.00
!
tarp run
tarp tid Distribution2
!
```

Verifying the Configuration

The following examples display output from the **show clns, show clns neighbors**, and **show clns neighbors detail** EXEC commands for router Distribution2. The commands display global information about CLNS and the router. The routing area is identified as 39.840f.8011.9999.0000.2222.0002.

```
Distribution2# show clns

Global CLNS Information:
  2 Interfaces Enabled for CLNS
  NET: 39.840f.8011.9999.0000.2222.0002.0030.94e2.6ce0.00
  Configuration Timer: 60, Default Holding Timer: 300, Packet Lifetime 64
  ERPDU's requested on locally generated packets
  Intermediate system operation enabled (CLNS forwarding allowed)
  IS-IS level-1-2 Router: area0002
    Routing for Area: 39.840f.8011.9999.0000.2222.0002

Distribution2# show clns neighbors

System Id      Interface   SNPA            State  Holdtime  Type Protocol
Access2        Et0/0       00e0.b064.434f  Up     8         L2   IS-IS
BackBoneR2     Et0/1       000d.bc2e.6d50  Up     27        L1L2 IS-IS

Distribution2# show clns neighbors detail

System Id      Interface   SNPA            State  Holdtime  Type Protocol
Access2        Et0/0       00e0.b064.434f  Up     7         L2   IS-IS
```

```
  Area Address(es): 39.840f.8011.9999.0000.2222.0012
  Uptime: 01:48:26
BackBoneR2     Et0/1       000d.bc2e.6d50      Up     23        L1L2 IS-IS
  Area Address(es): 39.840f.8011.9999.0000.2222.0002
  Uptime: 01:48:26
  NSF capable
```

The following example displays CLNS route information:

```
Distribution2# show clns route

Codes: C - connected, S - static, d - DecnetIV
       I - ISO-IGRP,  i - IS-IS,  e - ES-IS
       B - BGP,       b - eBGP-neighbor

C  39.840f.8011.9999.0000.2222.0002 [2/0], Local IS-IS Area
C  39.840f.8011.9999.0000.2222.0002.0030.94e2.6ce0.00 [1/0], Local IS-IS NET

i  39.840f.8011.9999.0000.2222.0012 [110/10]
      via Access2, Ethernet0/0
i  39.840f.8011.9999.0000.1111 [110/10]
      via BackBoneR2, Ethernet0/1
i  39.840f.8011.9999.0000.2222 [110/20]
      via BackBoneR2, Ethernet0/1
i  39.840f.8011.9999.0000.3333 [110/10]
      via BackBoneR2, Ethernet0/1
i  39.840f.8011.9999.0000.bbbb [110/10]
      via BackBoneR2, Ethernet0/1
```

Configuring Router Distribution3

The following example shows the relevant CLNS configuration commands for the router designated Distribution3 in Figure 48 on page 94:

```
Distribution3# show configuration

Using 3873 out of 29688 bytes
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Distribution3
!
boot-start-marker
boot system flash
boot system rom
boot-end-marker
!
!
enable password cisco
!
clock timezone EST -5
no aaa new-model
ip subnet-zero
ip domain name compgen.com
ip host 1d12RAA-2600 172.20.220.61
ip host 1d12RAB-2600 172.20.220.60
ip host 1d38RAE-7200 172.20.221.65
ip host 1d38RAF-7200 172.20.221.66
ip host 1d12RAC-2600 172.20.220.62
ip name-server 172.30.4.11
```

```
clns routing
no ftp-server write-enable
x25 routing
!
!
stun peer-name 172.25.192.47
stun protocol-group 103 basic
!
!
interface Loopback0
 ip address 192.168.5.252 255.255.255.192
!
interface Ethernet0/0
 ip address 192.168.100.2 255.255.255.192
 half-duplex
 clns router isis area0035
 tarp enable
!
interface Ethernet0/1
 ip address 192.168.5.61 255.255.255.192
 half-duplex
 clns router isis area0035
 tarp enable
!
interface Serial1/0
 mtu 1562
 no ip address
 encapsulation x25 dce
 no ip mroute-cache
 x25 ltc 5
 x25 ips 512
 x25 ops 512
 x25 threshold 1
 x25 pvc 1 rbp local port 10000
 clockrate 9600
!
router ospf 795
 log-adjacency-changes
 network 192.168.0.0 0.0.255.255 area 0
!
router isis area0035
 net 39.840f.8011.9999.0000.3333.0035.00e0.1ee3.c720.00
!
clns host Distribution3 39.840f.8011.9999.0000.3333.0035.00e0.1ee3.c720.00
clns host BackBoneR2 39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d40.00
clns host BackBoneR3 39.840f.8011.9999.0000.bbbb.1001.0010.7bd8.c7d0.00
clns host BackBoneR1 39.840f.8011.9999.0000.bbbb.1001.000d.bc2e.6d80.00
clns host Distribution2 39.840f.8011.9999.0000.2222.0002.0030.94e2.6ce0.00
clns host Distribution1 39.840f.8011.9999.0000.1111.9999.0010.7b17.f880.00
clns host Access1 39.840f.8011.9999.0000.1111.0003.00d0.5872.9720.00
clns host Access2 39.840f.8011.9999.0000.2222.0012.00e0.b064.434e.00
!
tarp run
tarp tid Distribution3
!
```

Verifying the Configuration

The following examples display output from the **show clns**, **show clns neighbors**, and **show clns neighbors detail** EXEC commands for router Distribution3. The commands display global information about CLNS and the router. The routing area is identified as 39.840f.8011.9999.0000.3333.0035.

```
Distribution3# show clns
```

```
Global CLNS Information:
  2 Interfaces Enabled for CLNS
  NET: 39.840f.8011.9999.0000.3333.0035.00e0.1ee3.c720.00
  Configuration Timer: 60, Default Holding Timer: 300, Packet Lifetime 64
  ERPDU's requested on locally generated packets
  Intermediate system operation enabled (CLNS forwarding allowed)
  IS-IS level-1-2 Router: area0035
    Routing for Area: 39.840f.8011.9999.0000.3333.0035

Distribution3# show clns neighbors

System Id      Interface   SNPA            State  Holdtime  Type Protocol
BackBoneR3     Et0/0       0010.7bd8.c821  Up     29        L2   IS-IS
NE14B          Et0/1       0050.7363.7b41  Up     26        L1L2 IS-IS

Distribution3# show clns neighbors detail

System Id      Interface   SNPA            State  Holdtime  Type Protocol
BackBoneR3     Et0/0       0010.7bd8.c821  Up     23        L2   IS-IS
  Area Address(es): 39.840f.8011.9999.0000.3333.0033
  Uptime: 00:52:12
NE14B          Et0/1       0050.7363.7b41  Up     26        L1L2 IS-IS
  Area Address(es): 39.840f.8011.9999.0000.3333.0035
  Uptime: 00:17:36
```

The following example displays information from the **show clns route** EXEC command:

```
Distribution3# show clns route

Codes: C - connected, S - static, d - DecnetIV
       I - ISO-IGRP,  i - IS-IS,  e - ES-IS
       B - BGP,       b - eBGP-neighbor

C  39.840f.8011.9999.0000.3333.0035 [2/0], Local IS-IS Area
C  39.840f.8011.9999.0000.3333.0035.00e0.1ee3.c720.00 [1/0], Local IS-IS NET

i  39.840f.8011.9999.0000.3333.0033 [110/10]
      via BackBoneR3, Ethernet0/0
i  39.840f.8011.9999.0000.1111 [110/10]
      via BackBoneR3, Ethernet0/0
i  39.840f.8011.9999.0000.2222 [110/10]
      via BackBoneR3, Ethernet0/0
i  39.840f.8011.9999.0000.3333 [110/20]
      via BackBoneR3, Ethernet0/0
i  39.840f.8011.9999.0000.bbbb [110/10]
      via BackBoneR3, Ethernet0/0
```

Additional References

This section provides the following additional reference information:

- Related Documents, page 112
- Standards, page 113
- Technical Assistance, page 113

Related Documents

Related Topic	Document Title
Bandwidth signaling applications	• ITU-T G.807, *Requirements for the Automatic Switched Transport Network (ASTN)* • ITU-T G.8080, *Architecture for the Automatic Switched Optical Network (ASON)* • Optical Internetworking Forum (OIF) *User Network Interface* (UNI) 1.0
Cisco IS-IS technical support	Integrated Intermediate System-to-Intermediate System (IS-IS) Cisco IOS support page
CLNS tunnel configuration	• *IP over a CLNS Tunnel*, Cisco IOS Release 12.1(5)T feature module • *CLNS Support for GRE Tunneling of IPv4 and IPv6 Packets in CLNS Networks*, Cisco IOS Release 12.3(7)T feature module
IP requirements for a DCN	ITU-T G.7712/Y.1703, *Architecture and Specification of the Data Communication Networ*k
IS-IS attach-bit	*Using the IS-IS Attach-Bit Control Feature,* Cisco IOS Product Marketing Application Note
NM-AIC-64 configuration	*NM-AIC-64, Contact Closure Network Module*, Cisco IOS Release 12.2(8)T feature module
NSAP address structure	American National Standard X3.216-1992, *Structure and Semantics of the Domain Specific Part of the Network Service Access Point Address*
NSAP IDP structure	• ITU-T E.164 • ITU-T F.69 • ITU-T X.121 • ISO DCC • ISO 6523-ICD
Optical internetworking	Optical Internetworking Forum (OIF) *User Network Interface* (UNI) 1.0
OSI addressing issues	ITU-T X.213, *Data Networks and Open Systems Communications Open Systems Interconnections Service Definitions*
SONET requirements for a DCN	• Telcordia Specification, Issue 3 of GR-253-CORE, *Synchronous Optical Network (SONET) Transport Systems: Common Criteria* • M.3010, *Principles for a Telecommunications Management Network*
Telcordia SONET transport systems	Telcordia Specification, Issue 3 of GR-253-CORE, *Synchronous Optical Network (SONET) Transport Systems: Common Criteria*, Section 8

Standards

Standard	Title
RFC 2763	*Dynamic Hostname Exchange Mechanism for IS-IS* (Informational)
ITU-T G.7712/Y.1703	*Architecture and Specification of the Data Communication Network*
ITU-T G.807	*Requirements for the Automatic Switched Transport Network (ASTN)*
ITU-T G.8080	*Architecture for the Automatic Switched Optical Network (ASON)*
ITU-T M.3010	*Principles for a Telecommunications Management Network*
ITU-T X.213	*Data Networks and Open Systems Communications Open Systems Interconnections Service Definitions*
American National Standard X3.216-199	*Structure and Semantics of the Domain Specific Part of the Network Service Access Point Address*

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Glossary

ADMs—add/drop multiplexers

AFI—authority and format identifier

ANSI—American National Standards Institute

BCD—Binary Coded Decimal

CLECs—competitive local exchange carriers

CLNP—Connectionless Network Protocol

DCC—data communications channel

DCN—data communications network

DFI—Domain Specific Part format identifier

DIS—Designated Intermediate System

DLCI—data-link connection identifier

DSLAMs—digital subscriber line access multiplexers

DSP—Domain Specific Part

ES—end system

ESH—End System Hello

FTAM—File Transfer, Access, and Management

GNE—gateway network element

GRE—generic routing encapsulation

IDI—initial domain identifier

IDP—Initial Domain Part

IEEE—Institute of Electrical and Electronics Engineers

IETF—Internet Engineering Task Force

IIH—IS-IS Hello message

ILECs—incumbent local exchange carriers

ISH—Intermediate System Hello

IS—intermediate system

IS-IS—Intermediate System-to-Intermediate System

ISL—Inter-Switch Link

ISO CLNS—International Standards Organization Connectionless Network Service

ISO DCC—Data Country Code

ISO/IEC—International Organization for Standardization/International Electrotechnical Commission

ISO-IGRP—Interior Gateway Routing Protocol developed by Cisco Systems for ISO CLNS)

ITU—International Telecommunication Union

IXC—inter-exchange carriers

LDB—loop detection buffer

LSP—line-state packet and link-state packet

MAC—Media Access Control

NET—network entity title

NMA—Network Management Application

NOC—network operations center

NSAP—network service access point

OAM&P—operations, administration, maintenance, and provisioning

OSI—Open System Interconnection

PDUs—protocol data units

PSTN—public switched telephone network

PTT—Post, Telephone and Telegraph

RBOCs—regional Bell operating companies

SDH—Synchronous Digital Hierarchy

SNPA—subnetwork point of attachment

SONET—Synchronous Optical Network

TARP—Target Identifier Address Resolution Protocol

TDM—time-division multiplexing

TID—target identifier

TMN—Telecommunications Management Network

TTL—Time-to-Live field

URC—update remote cache

VLAN—virtual LAN