CHAPTER 13

Management Network Connectivity

This chapter provides an overview of ONS 15454 data communications network (DCN) connectivity. Cisco Optical Networking System (ONS) network communication is based on IP, including communication between Cisco Transport Controller (CTC) computers and ONS 15454 nodes, and communication among networked ONS 15454 nodes. The chapter provides scenarios showing Cisco ONS 15454 nodes in common IP network configurations as well as information about provisionable patchcords, the IP routing table, external firewalls, and open gateway network element (GNE) networks.

Although ONS 15454 DCN communication is based on IP, ONS 15454 nodes can be networked to equipment that is based on the Open System Interconnection (OSI) protocol suites. This chapter also describes the ONS 15454 OSI implementation and provides scenarios that show how the ONS 15454 can be networked within a mixed IP and OSI environment.

Note This chapter does not provide a comprehensive explanation of IP networking concepts and procedures, nor does it provide IP addressing examples to meet all networked scenarios. For ONS 15454 networking setup instructions, refer to the "Turn Up a Node" chapter of the *Cisco ONS 15454 Procedure Guide*.

Chapter topics include:

Note To connect ONS 15454s to an IP network, you must work with a LAN administrator or other individual at your site who has IP networking training and experience.

13.1 IP Networking Overview

ONS 15454s can be connected in many different ways within an IP environment:

- They can be connected to LANs through direct connections or a router.
- IP subnetting can create multiple logical ONS 15454 networks within a single Class A, B, or C IP network. If you do not subnet, you will only be able to use one network from your Class A, B, or C network.
- Different IP functions and protocols can be used to achieve specific network goals. For example, Proxy Address Resolution Protocol (ARP) enables one LAN-connected ONS 15454 to serve as a gateway for ONS 15454s that are not connected to the LAN.
- Static routes can be created to enable connections among multiple CTC sessions with ONS 15454s that reside on the same subnet.
- ONS 15454s can be connected to Open Shortest Path First (OSPF) networks so that ONS 15454 network information is automatically communicated across multiple LANs and WANs.
- The ONS 15454 SOCKS (network proxy protocol) proxy server can control the visibility and accessibility between CTC computers and ONS 15454 element nodes.

13.2 IP Addressing Scenarios

ONS 15454 IP addressing generally has eight common scenarios or configurations. Use the scenarios as building blocks for more complex network configurations. Table 13-1 provides a general list of items to check when setting up ONS 15454 nodes in IP networks.

Table 13-1 General ONS 15454 IP Troubleshooting Checklist

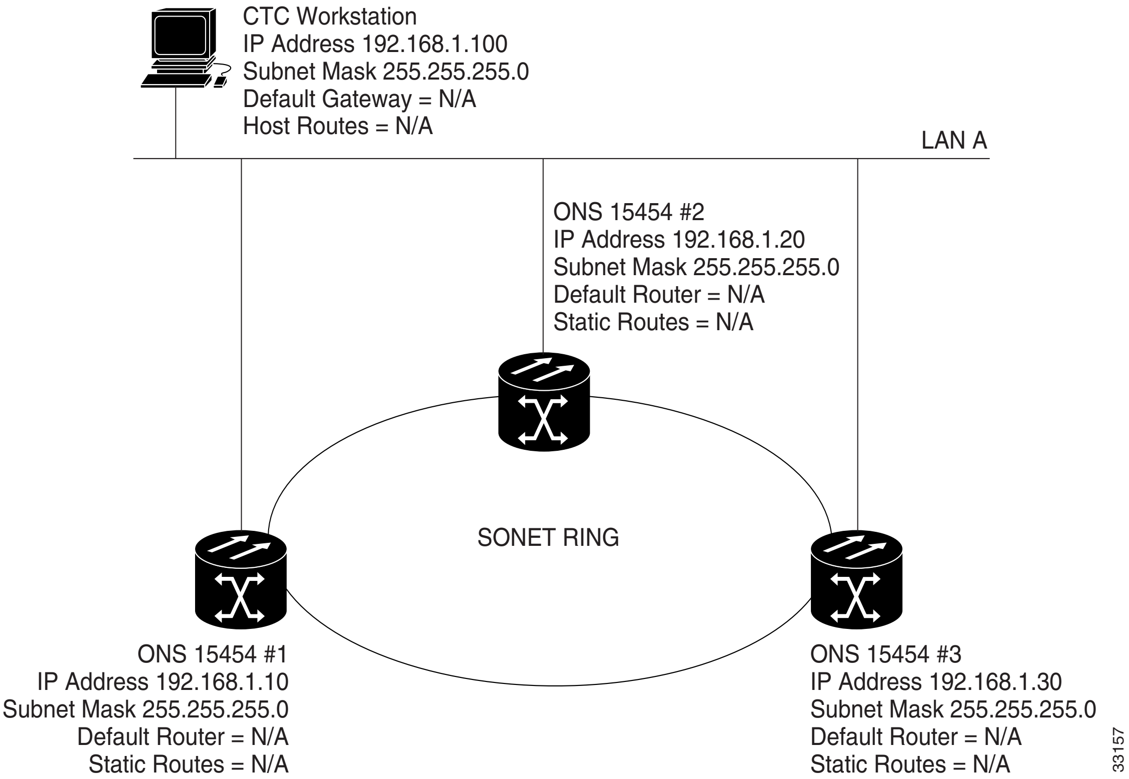
Item	What to Check
Link integrity	Verify that link integrity exists between: • CTC computer and network hub/switch • ONS 15454s (backplane wire-wrap pins or RJ-45 port) and network hub/switch • Router ports and hub/switch ports
ONS 15454 hub/switch ports	If connectivity problems occur, set the hub or switch port that is connected to the ONS 15454 to 10 Mbps half-duplex.
Ping	Ping the node to test connections between computers and ONS 15454s.
IP addresses/subnet masks	Verify that ONS 15454 IP addresses and subnet masks are set up correctly.
Optical connectivity	Verify that ONS 15454 optical trunk (span) ports are in service and that a DCC is enabled on each trunk port.

The TCC2P card secure mode option allows two IP addresses to be provisioned for the node: one for the backplane LAN port and one for the TCC2P LAN (TCP/IP) port. Secure mode IP addressing examples are provided in the "13.2.9 IP Scenario 9: IP Addressing with Secure Mode Enabled" section on page 13-20. IP addresses shown in the other scenarios assume that secure mode is not enabled. If secure mode is enabled, the IP addresses shown in the examples apply to the backplane LAN port. See the "13.2.9 IP Scenario 9: IP Addressing with Secure Mode Enabled" section on page 13-20 for information about secure mode, repeater (single IP address) mode, and configuration locks.

13.2.1 IP Scenario 1: CTC and ONS 15454s on Same Subnet

IP Scenario 1 shows a basic ONS 15454 LAN configuration (Figure 13-1). The ONS 15454s and CTC computer reside on the same subnet. All ONS 15454s connect to LAN A, and all ONS 15454s have DCC connections.

Figure 13-1 IP Scenario 1: CTC and ONS 15454s on Same Subnet

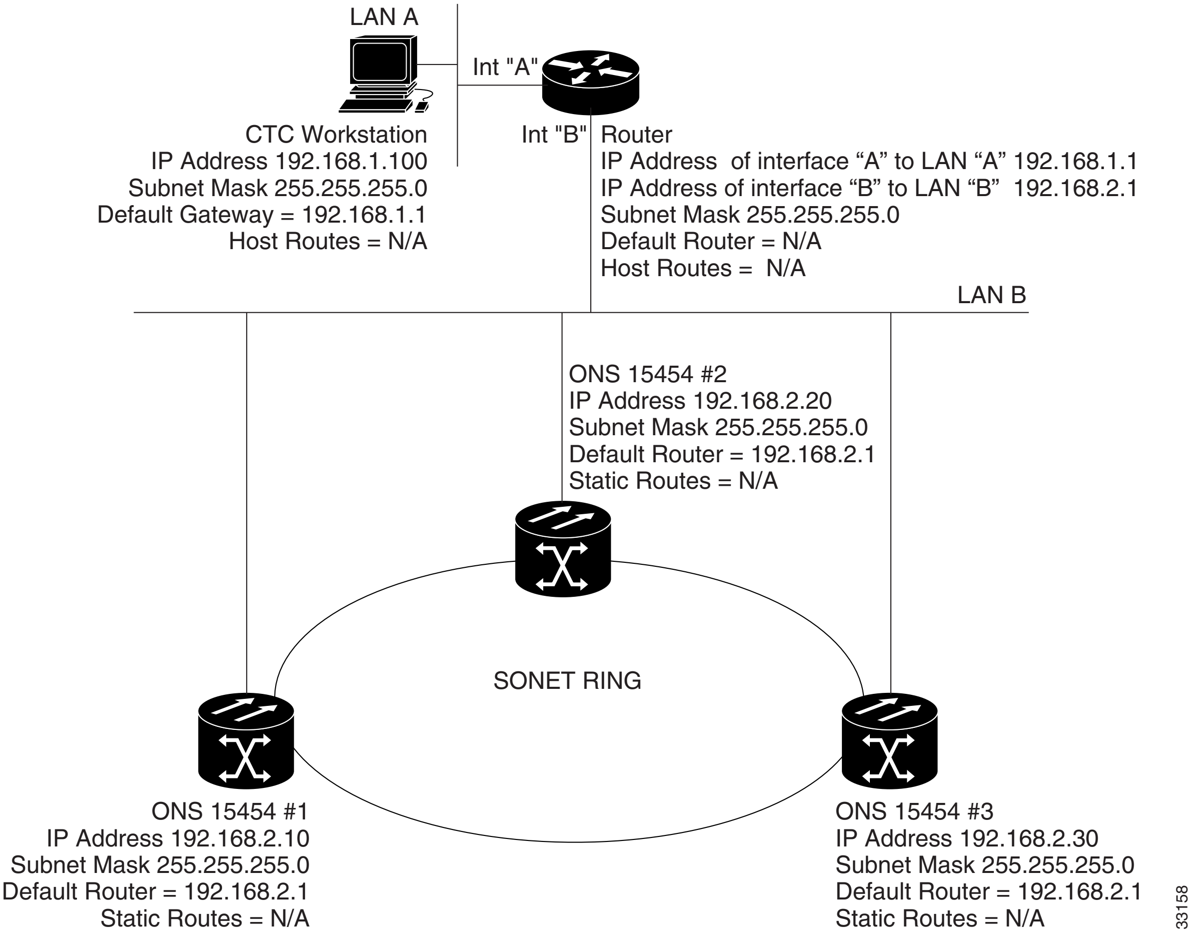


13.2.2 IP Scenario 2: CTC and ONS 15454 Nodes Connected to a Router

In IP Scenario 2 the CTC computer resides on a subnet (192.168.1.0) and attaches to LAN A (Figure 13-2). The ONS 15454s reside on a different subnet (192.168.2.0) and attach to LAN B. A router connects LAN A to LAN B. The IP address of router interface A is set to LAN A (192.168.1.1), and the IP address of router interface B is set to LAN B (192.168.2.1).

On the CTC computer, the default gateway is set to router interface A. If the LAN uses Dynamic Host Configuration Protocol (DHCP), the default gateway and IP address are assigned automatically. In the Figure 13-2 example, a DHCP server is not available.

Figure 13-2 IP Scenario 2: CTC and ONS 15454 Nodes Connected to a Router


LAN A
Int "A"
CTC Workstation
IP Address 192.168.1.100
Subnet Mask 255.255.255.0
Default Gateway = 192.168.1.1
Host Routes = N/A
Int "B"
Router
IP Address of interface “A” to LAN “A” 192.168.1.1
IP Address of interface “B” to LAN “B” 192.168.2.1
Subnet Mask 255.255.255.0
Default Router = N/A
Host Routes = N/A
LAN B
ONS 15454 #2
IP Address 192.168.2.20
Subnet Mask 255.255.255.0
Default Router = 192.168.2.1
Static Routes = N/A
SONET RING
ONS 15454 #1
IP Address 192.168.2.10
Subnet Mask 255.255.255.0
Default Router = 192.168.2.1
Static Routes = N/A
ONS 15454 #3
IP Address 192.168.2.30
Subnet Mask 255.255.255.0
Default Router = 192.168.2.1
Static Routes = N/A
33158

13.2.3 IP Scenario 3: Using Proxy ARP to Enable an ONS 15454 Gateway

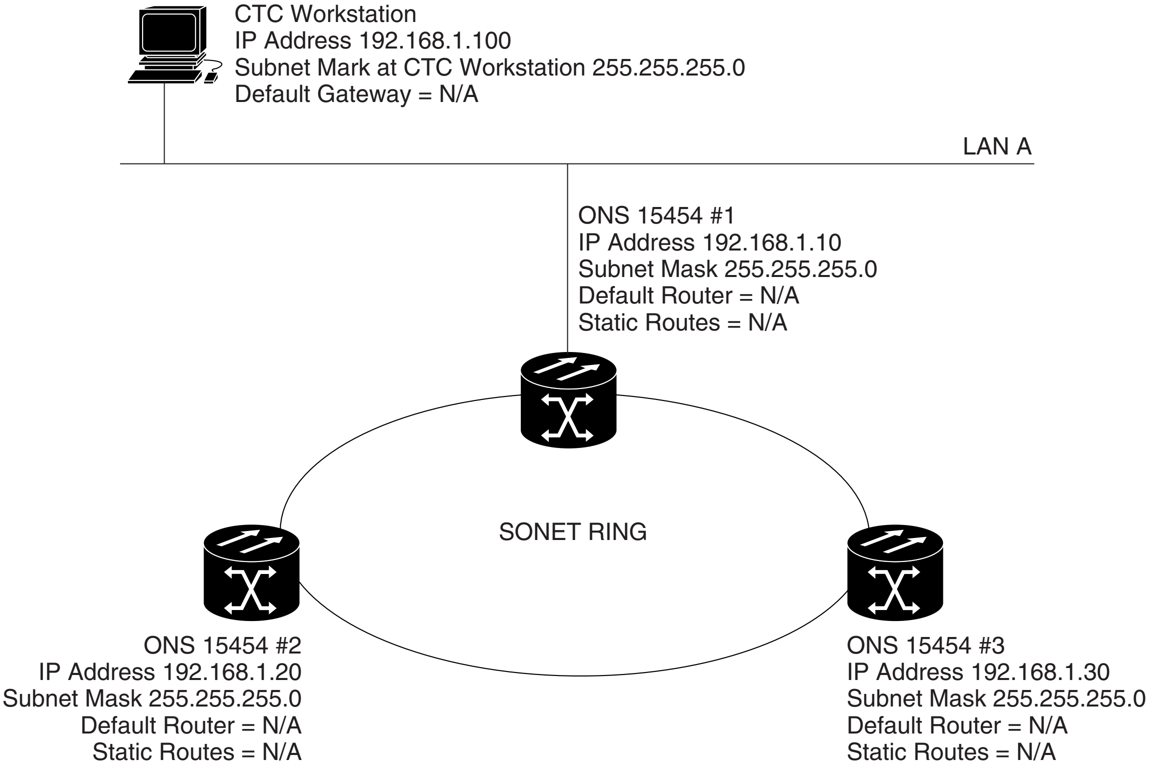
ARP matches higher-level IP addresses to the physical addresses of the destination host. It uses a lookup table (called ARP cache) to perform the translation. When the address is not found in the ARP cache, a broadcast is sent out on the network with a special format called the ARP request. If one of the machines on the network recognizes its own IP address in the request, it sends an ARP reply back to the requesting host. The reply contains the physical hardware address of the receiving host. The requesting host stores this address in its ARP cache so that all subsequent datagrams (packets) to this destination IP address can be translated to a physical address.

Proxy ARP enables one LAN-connected ONS 15454 to respond to the ARP request for ONS 15454s not connected to the LAN. (ONS 15454 proxy ARP requires no user configuration.) For this to occur, the DCC-connected ONS 15454s must reside on the same subnet. When a LAN device sends an ARP request to an ONS 15454 that is not connected to the LAN, the gateway ONS 15454 returns its MAC address to the LAN device. The LAN device then sends the datagram for the remote ONS 15454 to the MAC address of the proxy ONS 15454. The proxy ONS 15454 uses its routing table to forward the datagram to the non-LAN ONS 15454.

IP Scenario 3 is similar to IP Scenario 1, but only one ONS 15454 (1) connects to the LAN (Figure 13-3). Two ONS 15454s (2 and 3) connect to ONS 15454 1 through the SONET DCC. Because all three ONS 15454s are on the same subnet, proxy ARP enables ONS 15454 1 to serve as a gateway for ONS 15454 2 and 3.

Note This scenario assumes all CTC connections are to Node 1. If you connect a laptop to either ONS 15454 2 or 3, network partitioning occurs; neither the laptop nor the CTC computer can see all nodes. If you want laptops to connect directly to end network elements, you must create static routes (see "13.2.5 IP Scenario 5: Using Static Routes to Connect to LANs" section on page 13-7) or enable the ONS 15454 SOCKS proxy server (see "13.2.7 IP Scenario 7: Provisioning the ONS 15454 SOCKS Proxy Server" section on page 13-12).

Figure 13-3 IP Scenario 3: Using Proxy ARP

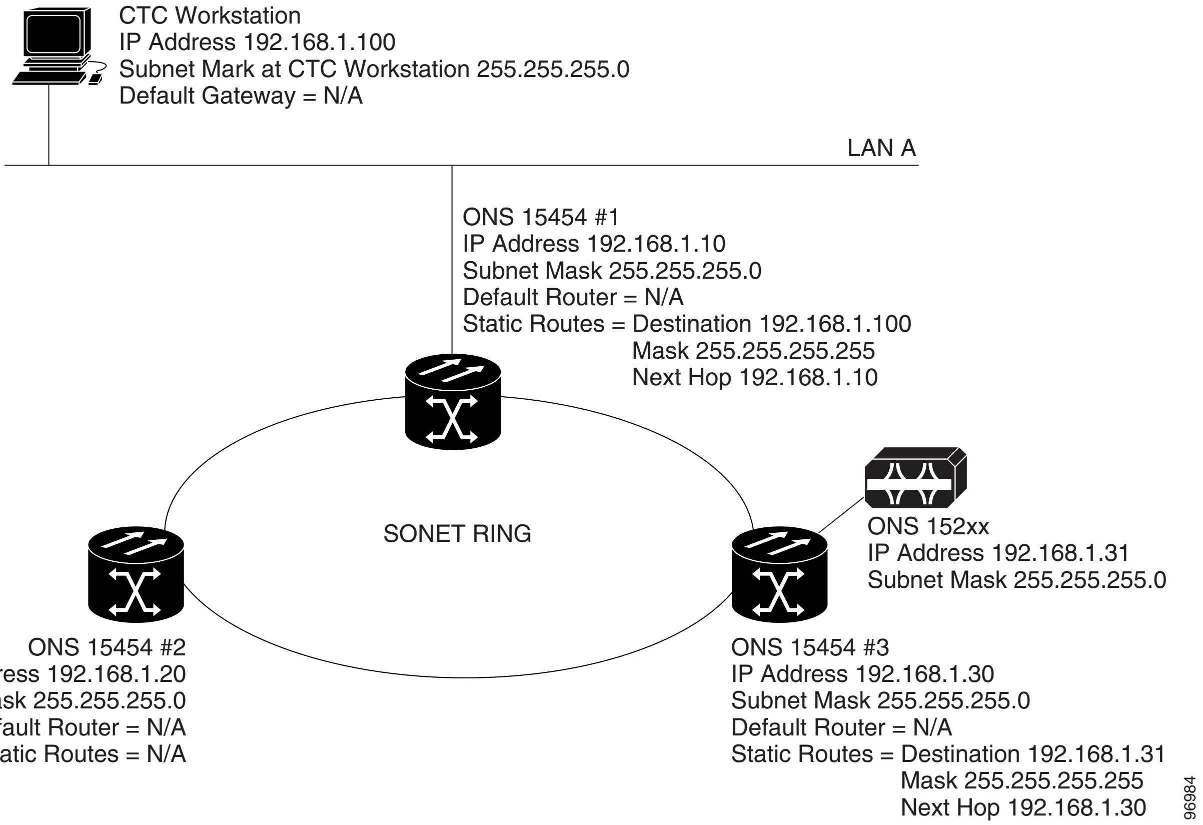


You can also use proxy ARP to communicate with hosts attached to the craft Ethernet ports of DCC-connected nodes (Figure 13-4). The node with an attached host must have a static route to the host. Static routes are propagated to all DCC peers using OSPF. The existing proxy ARP node is the gateway for additional hosts. Each node examines its routing table for routes to hosts that are not connected to the DCC network but are within the subnet. The existing proxy server replies to ARP requests for these additional hosts with the node MAC address. The existence of the host route in the routing table ensures that the IP packets addressed to the additional hosts are routed properly. Other than establishing a static route between a node and an additional host, no provisioning is necessary. The following restrictions apply:

- Only one node acts as the proxy ARP server for any given additional host.
- A node cannot be the proxy ARP server for a host connected to its Ethernet port.

In Figure 13-4, Node 1 announces to Node 2 and 3 that it can reach the CTC host. Similarly, Node 3 announces that it can reach the ONS 152xx. The ONS 152xx is shown as an example; any network element (NE) can be set up as an additional host.

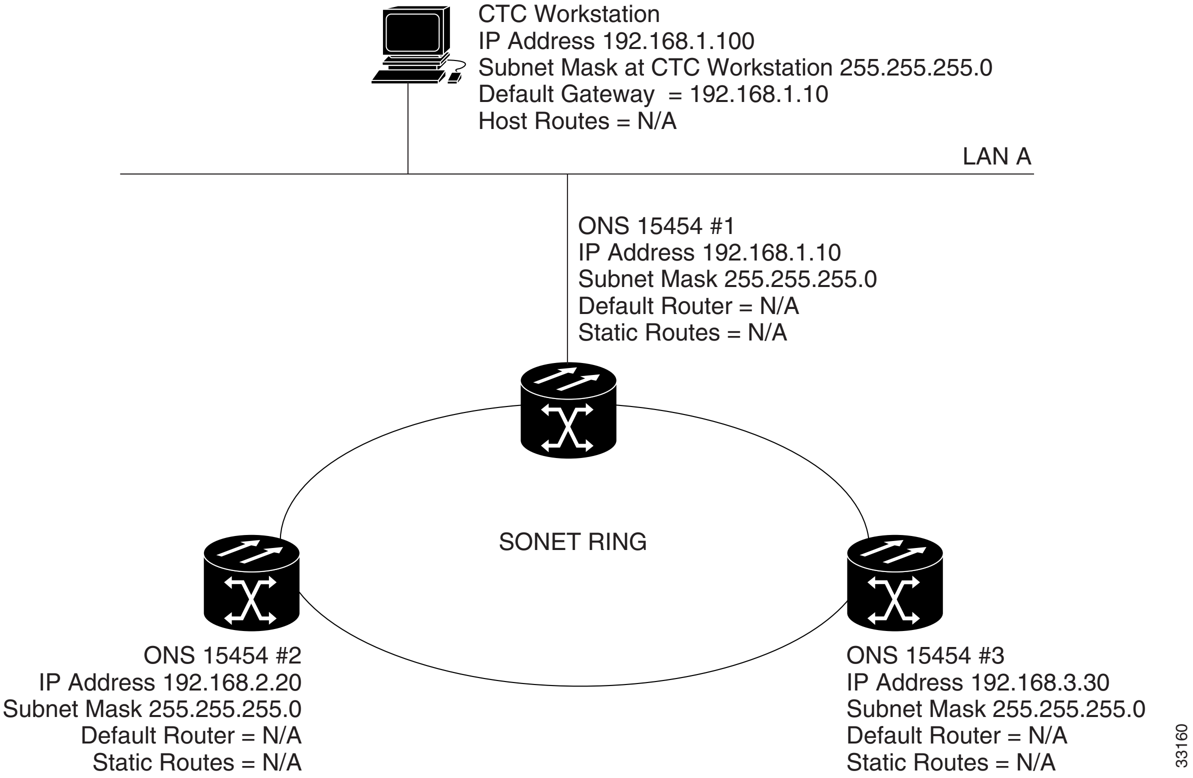
Figure 13-4 IP Scenario 3: Using Proxy ARP with Static Routing



13.2.4 IP Scenario 4: Default Gateway on a CTC Computer

IP Scenario 4 is similar to IP Scenario 3, but Nodes 2 and 3 reside on different subnets, 192.168.2.0 and 192.168.3.0, respectively (Figure 13-5). Node 1 and the CTC computer are on subnet 192.168.1.0. Proxy ARP is not used because the network includes different subnets. For the CTC computer to communicate with Nodes 2 and 3, Node 1 is entered as the default gateway on the CTC computer.

Figure 13-5 IP Scenario 4: Default Gateway on a CTC Computer



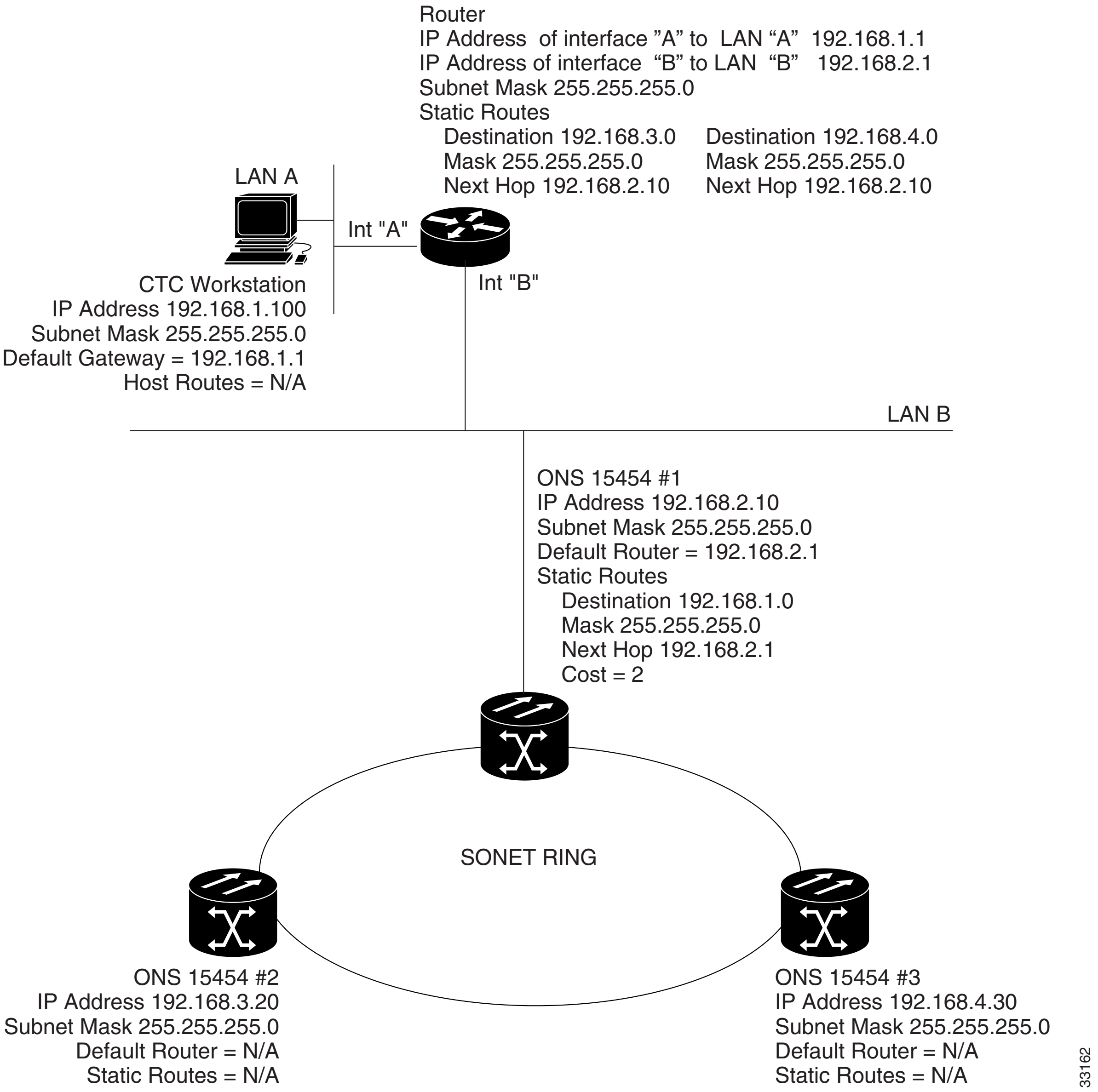
13.2.5 IP Scenario 5: Using Static Routes to Connect to LANs

Static routes are used for two purposes:

- To connect ONS 15454s to CTC sessions on one subnet connected by a router to ONS 15454s residing on another subnet. (These static routes are not needed if OSPF is enabled. "13.2.6 IP Scenario 6: Using OSPF" section on page 13-10 shows an OSPF example.)
- To enable multiple CTC sessions among ONS 15454s residing on the same subnet.

In Figure 13-6, one CTC residing on subnet 192.168.1.0 connects to a router through interface A. (The router is not set up with OSPF.) ONS 15454s residing on different subnets are connected through Node 1 to the router through interface B. Because Nodes 2 and 3 are on different subnets, proxy ARP does not enable Node 1 as a gateway. To connect to the CTC computer on LAN A (subnet 192.168.1.0), you must create a static route on Node 1. You must also manually add static routes between the CTC computer on LAN A and Nodes 2 and 3 because these nodes are on different subnets.

Figure 13-6 IP Scenario 5: Static Route With One CTC Computer Used as a Destination

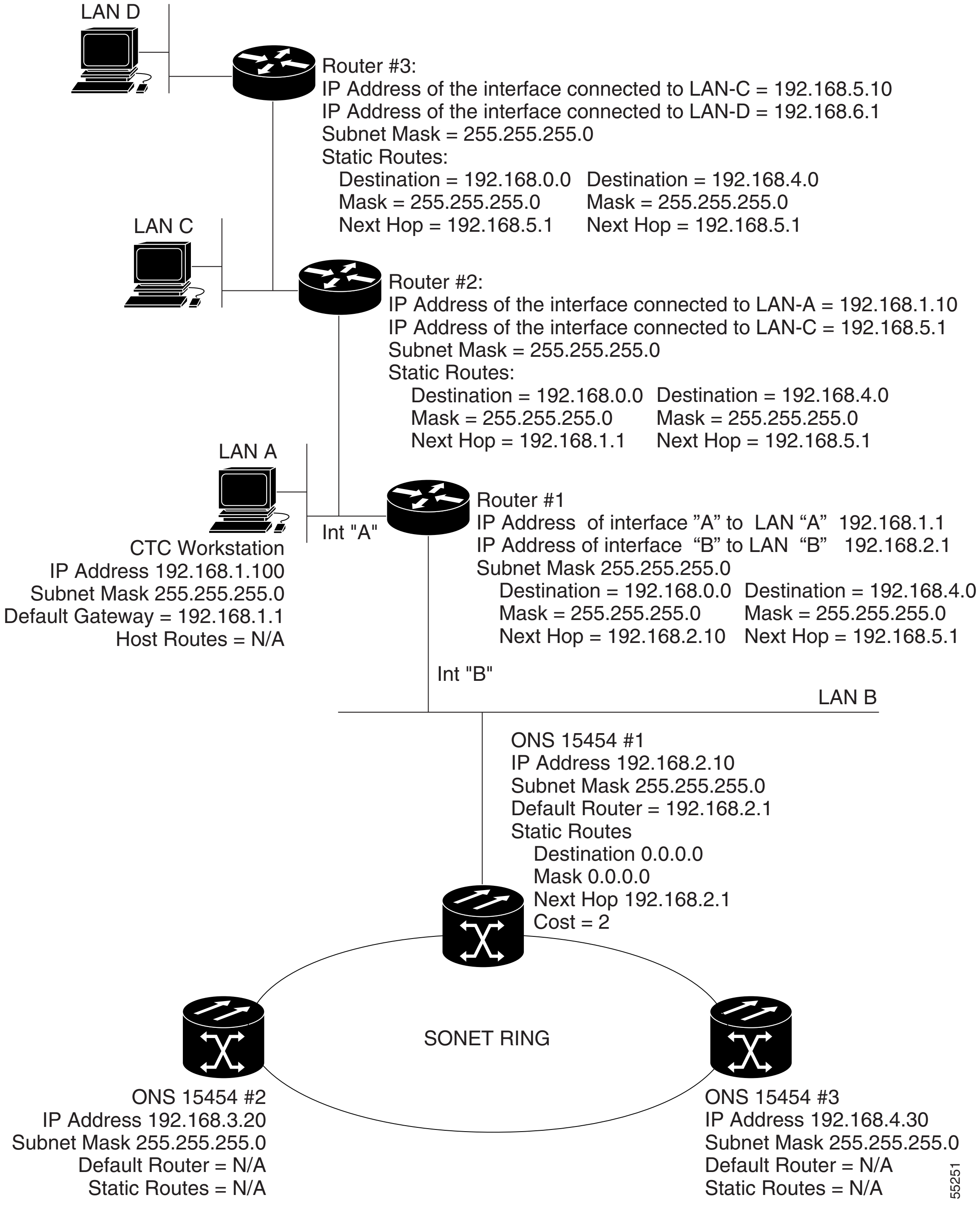


The destination and subnet mask entries control access to the ONS 15454s:

- If a single CTC computer is connected to a router, enter the complete CTC "host route" IP address as the destination with a subnet mask of 255.255.255.255.
- If CTC computers on a subnet are connected to a router, enter the destination subnet (in this example, 192.168.1.0) and a subnet mask of 255.255.255.0.
- If all CTC computers are connected to a router, enter a destination of 0.0.0.0 and a subnet mask of 0.0.0.0. Figure 13-7 shows an example.

The IP address of router interface B is entered as the next hop, and the cost (number of hops from source to destination) is 2. You must manually add static routes between the CTC computers on LAN A, B, and C and Nodes 2 and 3 because these nodes are on different subnets.

Figure 13-7 IP Scenario 5: Static Route With Multiple LAN Destinations


LAN D
Router #3:
IP Address of the interface connected to LAN-C = 192.168.5.10
IP Address of the interface connected to LAN-D = 192.168.6.1
Subnet Mask = 255.255.255.0
Static Routes:
Destination = 192.168.0.0 Destination = 192.168.4.0
Mask = 255.255.255.0 Mask = 255.255.255.0
Next Hop = 192.168.5.1 Next Hop = 192.168.5.1
LAN C
Router #2:
IP Address of the interface connected to LAN-A = 192.168.1.10
IP Address of the interface connected to LAN-C = 192.168.5.1
Subnet Mask = 255.255.255.0
Static Routes:
Destination = 192.168.0.0 Destination = 192.168.4.0
Mask = 255.255.255.0 Mask = 255.255.255.0
Next Hop = 192.168.1.1 Next Hop = 192.168.5.1
LAN A
Router #1
IP Address of interface ”A” to LAN “A” 192.168.1.1
IP Address of interface “B” to LAN “B” 192.168.2.1
Subnet Mask 255.255.255.0
Destination = 192.168.0.0 Destination = 192.168.4.0
Mask = 255.255.255.0 Mask = 255.255.255.0
Next Hop = 192.168.2.10 Next Hop = 192.168.5.1
Int "A"
CTC Workstation
IP Address 192.168.1.100
Subnet Mask 255.255.255.0
Default Gateway = 192.168.1.1
Host Routes = N/A
Int "B"
LAN B
ONS 15454 #1
IP Address 192.168.2.10
Subnet Mask 255.255.255.0
Default Router = 192.168.2.1
Static Routes
Destination 0.0.0.0
Mask 0.0.0.0
Next Hop 192.168.2.1
Cost = 2
SONET RING
ONS 15454 #2
IP Address 192.168.3.20
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A
ONS 15454 #3
IP Address 192.168.4.30
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A
55251

13.2.6 IP Scenario 6: Using OSPF

Open Shortest Path First (OSPF) is a link state Internet routing protocol. Link state protocols use a "hello protocol" to monitor their links with adjacent routers and to test the status of their links to their neighbors. Link state protocols advertise their directly connected networks and their active links. Each link state router captures the link state "advertisements" and puts them together to create a topology of the entire network or area. From this database, the router calculates a routing table by constructing a shortest path tree. Routes are recalculated when topology changes occur.

ONS 15454s use the OSPF protocol in internal ONS 15454 networks for node discovery, circuit routing, and node management. You can enable OSPF on the ONS 15454s so that the ONS 15454 topology is sent to OSPF routers on a LAN. Advertising the ONS 15454 network topology to LAN routers eliminates the need to manually enter static routes for ONS 15454 subnetworks. Figure 13-8 shows a network enabled for OSPF. Figure 13-9 shows the same network without OSPF. Static routes must be manually added to the router for CTC computers on LAN A to communicate with Nodes 2 and 3 because these nodes reside on different subnets.

OSPF divides networks into smaller regions, called areas. An area is a collection of networked end systems, routers, and transmission facilities organized by traffic patterns. Each OSPF area has a unique ID number, known as the area ID. Every OSPF network has one backbone area called "area 0." All other OSPF areas must connect to area 0.

When you enable an ONS 15454 OSPF topology for advertising to an OSPF network, you must assign an OSPF area ID in decimal format to the ONS 15454 network. Coordinate the area ID number assignment with your LAN administrator. All DCC-connected ONS 15454s should be assigned the same OSPF area ID.

Figure 13-8 IP Scenario 6: OSPF Enabled

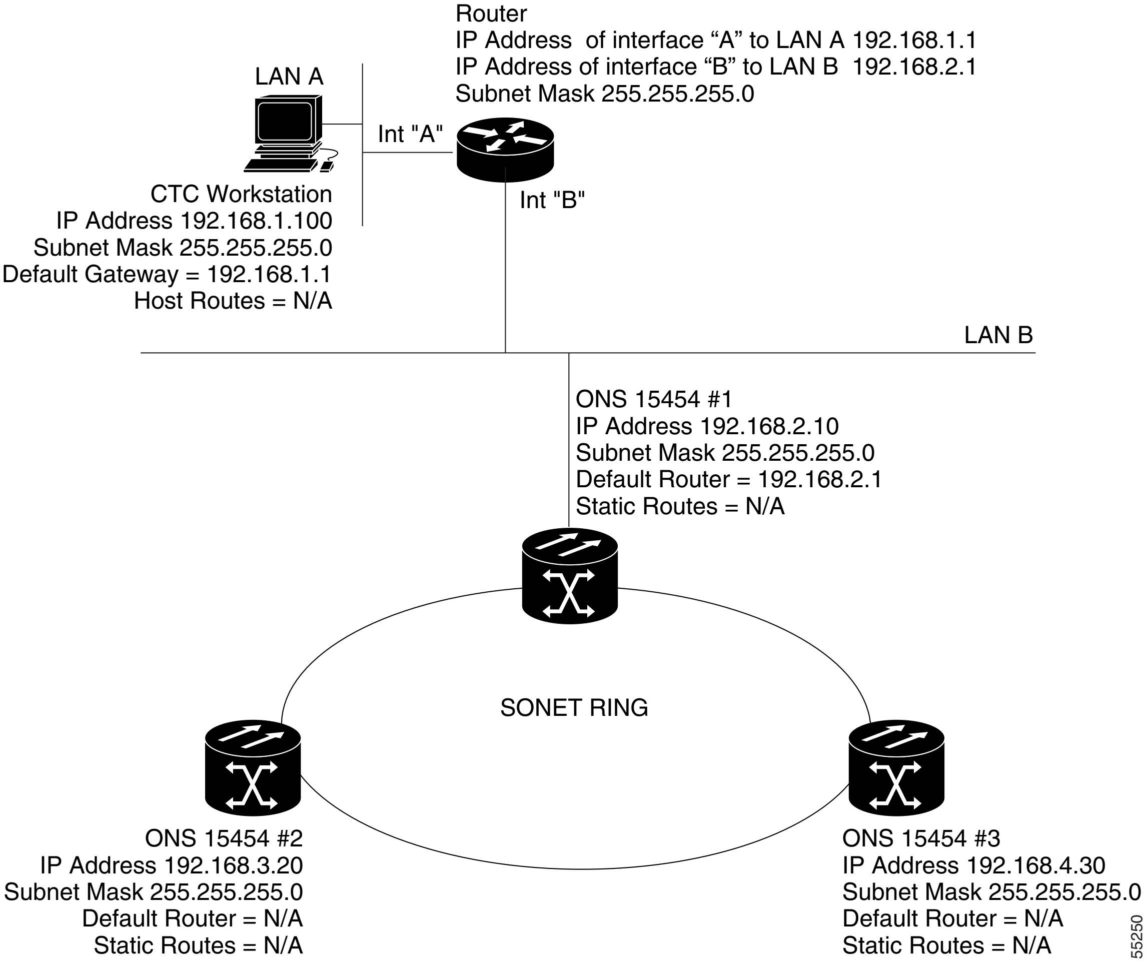
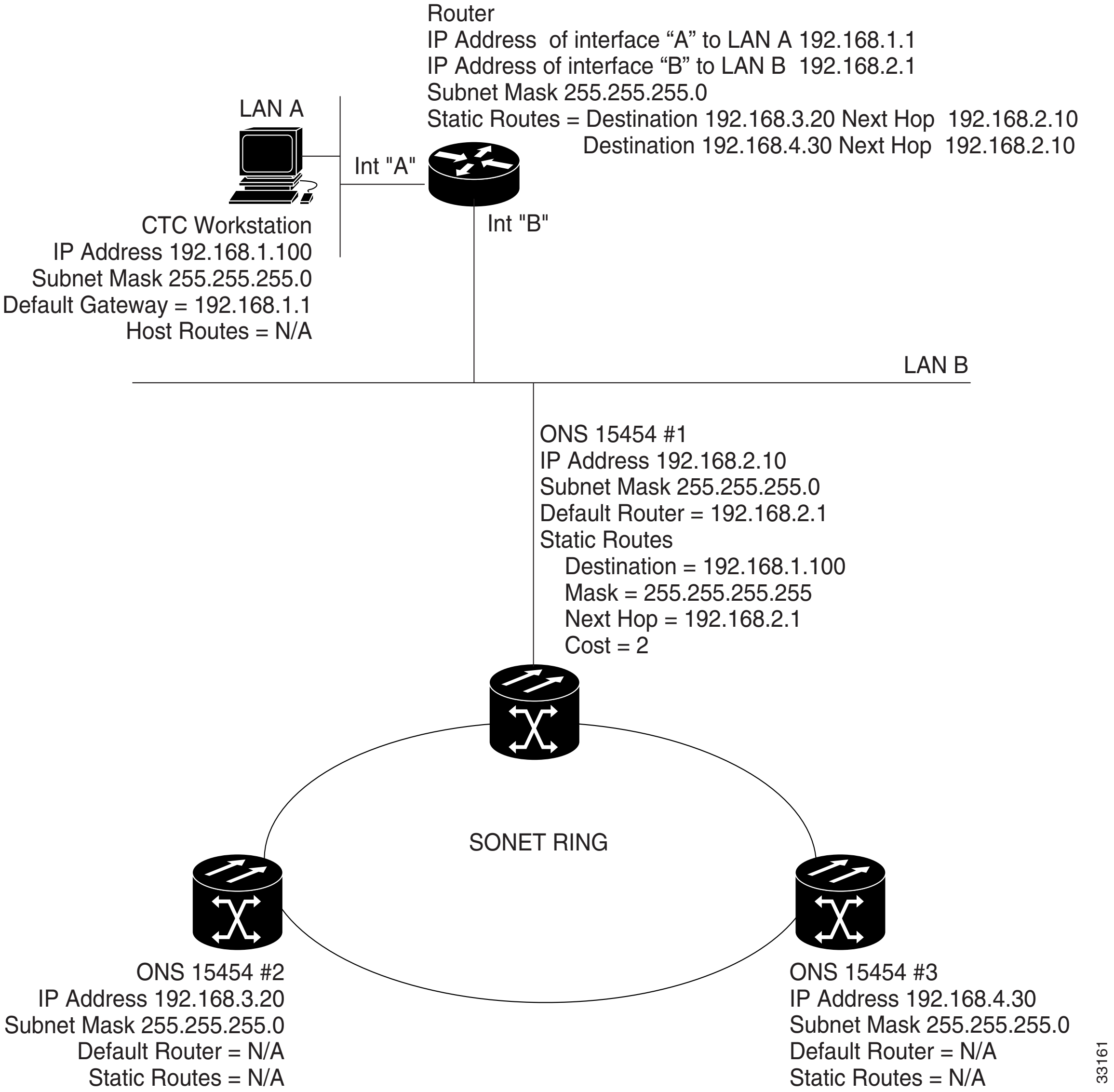


Figure 13-9 IP Scenario 6: OSPF Not Enabled


Router
IP Address of interface “A” to LAN A 192.168.1.1
IP Address of interface “B” to LAN B 192.168.2.1
Subnet Mask 255.255.255.0
Static Routes = Destination 192.168.3.20 Next Hop 192.168.2.10
Destination 192.168.4.30 Next Hop 192.168.2.10
LAN A
Int "A"
Int "B"
CTC Workstation
IP Address 192.168.1.100
Subnet Mask 255.255.255.0
Default Gateway = 192.168.1.1
Host Routes = N/A
LAN B
ONS 15454 #1
IP Address 192.168.2.10
Subnet Mask 255.255.255.0
Default Router = 192.168.2.1
Static Routes
Destination = 192.168.1.100
Mask = 255.255.255.255
Next Hop = 192.168.2.1
Cost = 2
SONET RING
ONS 15454 #2
IP Address 192.168.3.20
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A
ONS 15454 #3
IP Address 192.168.4.30
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A
33161

13.2.7 IP Scenario 7: Provisioning the ONS 15454 SOCKS Proxy Server

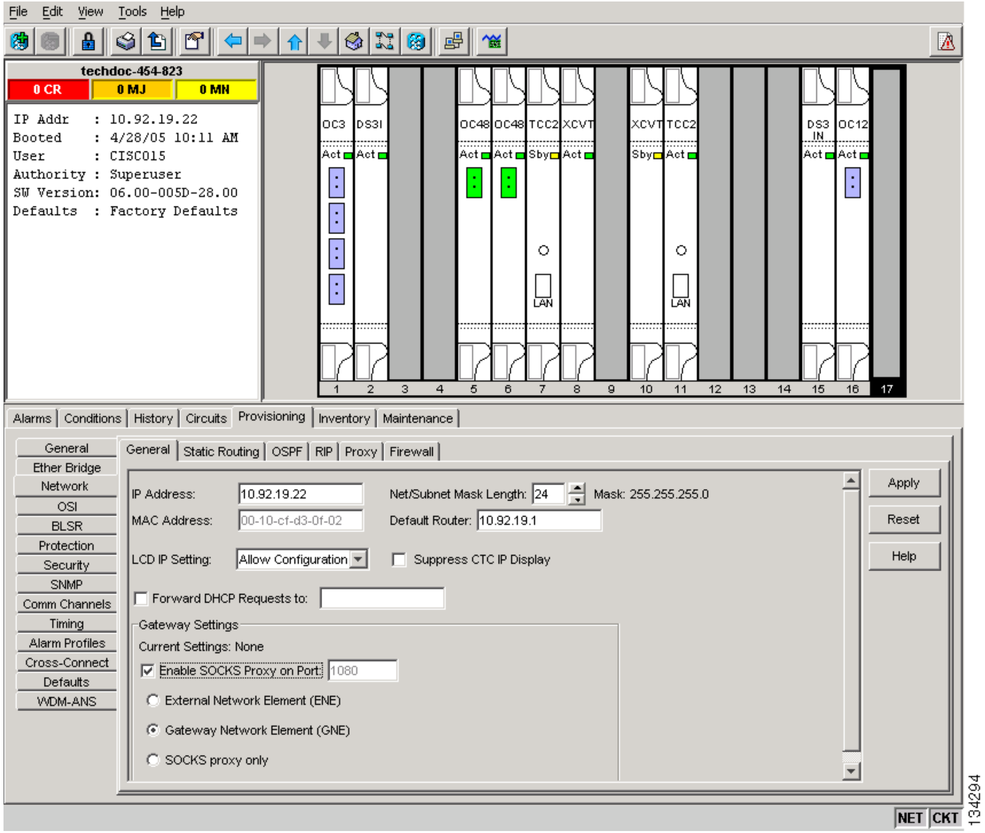
The ONS 15454 SOCKS proxy is an application that allows an ONS 15454 node to serve as an internal gateway between a private enterprise network and the ONS 15454 network. (SOCKS is a standard proxy protocol for IP-based applications developed by the Internet Engineering Task Force.) Access is allowed from the private network to the ONS 15454 network, but access is denied from the ONS 15454 network to the private network. For example, you can set up a network so that field technicians and network operations center (NOC) personnel can both access the same ONS 15454s while preventing the field technicians from accessing the NOC LAN. To do this, one ONS 15454 is provisioned as a gateway network element (GNE) and the other ONS 15454s are provisioned as end network elements (ENEs). The GNE ONS 15454 tunnels connections between CTC computers and ENE ONS 15454s, providing management capability while preventing access for non-ONS 15454 management purposes.

The ONS 15454 gateway setting performs the following tasks:

- Isolates DCC IP traffic from Ethernet (craft port) traffic and accepts packets based on filtering rules. The filtering rules (see Table 13-3 on page 13-17 and Table 13-4 on page 13-18) depend on whether the packet arrives at the ONS 15454 DCC or the TCC2/TCC2P Ethernet interface.
- Processes Simple Network Time Protocol (SNTP) and Network Time Protocol (NTP) requests. ONS 15454 ENEs can derive time-of-day from an SNTP/NTP LAN server through the GNE ONS 15454.
- Processes Simple Network Management Protocol version 1 (SNMPv1) traps. The GNE ONS 15454 receives SNMPv1 traps from the ENE ONS 15454s and forwards or relays the traps to SNMPv1 trap destinations or ONS 15454 SNMP relay nodes.

The ONS 15454 SOCKS proxy server is provisioned using the Enable SOCKS proxy server on port check box on the Provisioning > Network > General tab (Figure 13-10).

Figure 13-10 SOCKS Proxy Server Gateway Settings



```
IP Addr   : 10.92.19.22
Booted    : 4/28/05 10:11 AM
User      : CISCO15
Authority : Superuser
SW Version: 06.00-005D-28.00
Defaults  : Factory Defaults
```

IP Address: 10.92.19.22
MAC Address: 00-10-cf-d3-0f-02
Net/Subnet Mask Length: 24 Mask: 255.255.255.0
Default Router: 10.92.19.1
LCD IP Setting: Allow Configuration
□ Suppress CTC IP Display
□ Forward DHCP Requests to:

Gateway Settings
Current Settings: None
☑ Enable SOCKS Proxy on Port: 1080
○ External Network Element (ENE)
● Gateway Network Element (GNE)
○ SOCKS proxy only

If checked, the ONS 15454 serves as a proxy for connections between CTC clients and ONS 15454s that are DCC-connected to the proxy ONS 15454. The CTC client establishes connections to DCC-connected nodes through the proxy node. The CTC client can connect to nodes that it cannot directly reach from the host on which it runs. If not selected, the node does not proxy for any CTC clients, although any established proxy connections continue until the CTC client exits. In addition, you can set the SOCKS proxy server as an ENE or a GNE:

- External Network Element (ENE)—If set as an ENE, the ONS 15454 neither installs nor advertises default or static routes. CTC computers can communicate with the ONS 15454 using the TCC2/TCC2P craft port, but they cannot communicate directly with any other DCC-connected ONS 15454.

  In addition, firewall is enabled, which means that the node prevents IP traffic from being routed between the DCC and the LAN port. The ONS 15454 can communicate with machines connected to the LAN port or connected through the DCC. However, the DCC-connected machines cannot communicate with the LAN-connected machines, and the LAN-connected machines cannot communicate with the DCC-connected machines. A CTC client using the LAN to connect to the firewall-enabled node can use the proxy capability to manage the DCC-connected nodes that would otherwise be unreachable. A CTC client connected to a DCC-connected node can only manage other DCC-connected nodes and the firewall itself.
- Gateway Network Element (GNE)—If set as a GNE, the CTC computer is visible to other DCC-connected nodes and firewall is enabled.
- Proxy-only—If Proxy-only is selected, firewall is not enabled. CTC can communicate with any other DCC-connected ONS 15454s.

Note If you launch CTC against a node through a Network Address Translation (NAT) or Port Address Translation (PAT) router and that node does not have proxy enabled, your CTC session starts and initially appears to be fine. However, CTC never receives alarm updates and disconnects and reconnects every two minutes. If the proxy is accidentally disabled, it is still possible to enable the proxy during a reconnect cycle and recover your ability to manage the node, even through a NAT/PAT firewall.

Note ENEs that belong to different private subnetworks do not need to have unique IP addresses. Two ENEs that are connected to different GNEs can have the same IP address. However, ENEs that connect to the same GNE must always have unique IP addresses.

Figure 13-11 shows an ONS 15454 SOCKS proxy server implementation. A GNE ONS 15454 is connected to a central office LAN and to ENE ONS 15454s. The central office LAN is connected to a NOC LAN, which has CTC computers. Both the NOC CTC computer and the craft technicians must be able to access the ONS 15454 ENEs. However, the craft technicians must be prevented from accessing or seeing the NOC or central office LANs.

In the example, the ONS 15454 GNE is assigned an IP address within the central office LAN and is physically connected to the LAN through its LAN port. ONS 15454 ENEs are assigned IP addresses that are outside the central office LAN and are given private network IP addresses. If the ONS 15454 ENEs are collocated, the craft LAN ports could be connected to a hub. However, the hub should have no other network connections.

Figure 13-11 IP Scenario 7: ONS 15454 SOCKS Proxy Server with GNE and ENEs on the Same Subnet

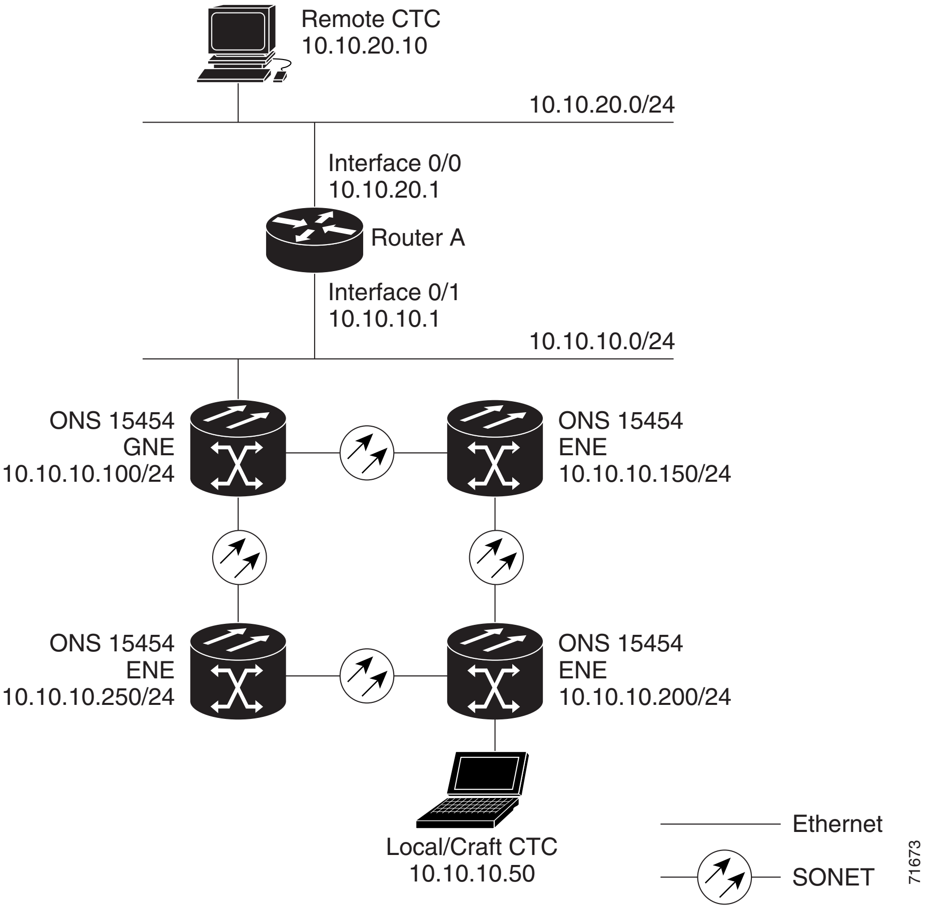


Table 13-2 shows recommended settings for ONS 15454 GNEs and ENEs in the configuration shown in Figure 13-11.

Table 13-2 ONS 15454 Gateway and End NE Settings

Setting	ONS 15454 Gateway NE	ONS 15454 End NE
OSPF	Off	Off
SNTP server (if used)	SNTP server IP address	Set to ONS 15454 GNE IP address
SNMP (if used)	SNMPv1 trap destinations	Set SNMPv1 trap destinations to ONS 15454 GNE, port 391

Figure 13-12 shows the same SOCKS proxy server implementation with ONS 15454 ENEs on different subnets. Figure 13-13 on page 13-17 shows the implementation with ONS 15454 ENEs in multiple rings. In each example, ONS 15454 GNEs and ENEs are provisioned with the settings shown in Table 13-2.

Figure 13-12 IP Scenario 7: ONS 15454 SOCKS Proxy Server with GNE and ENEs on Different Subnets

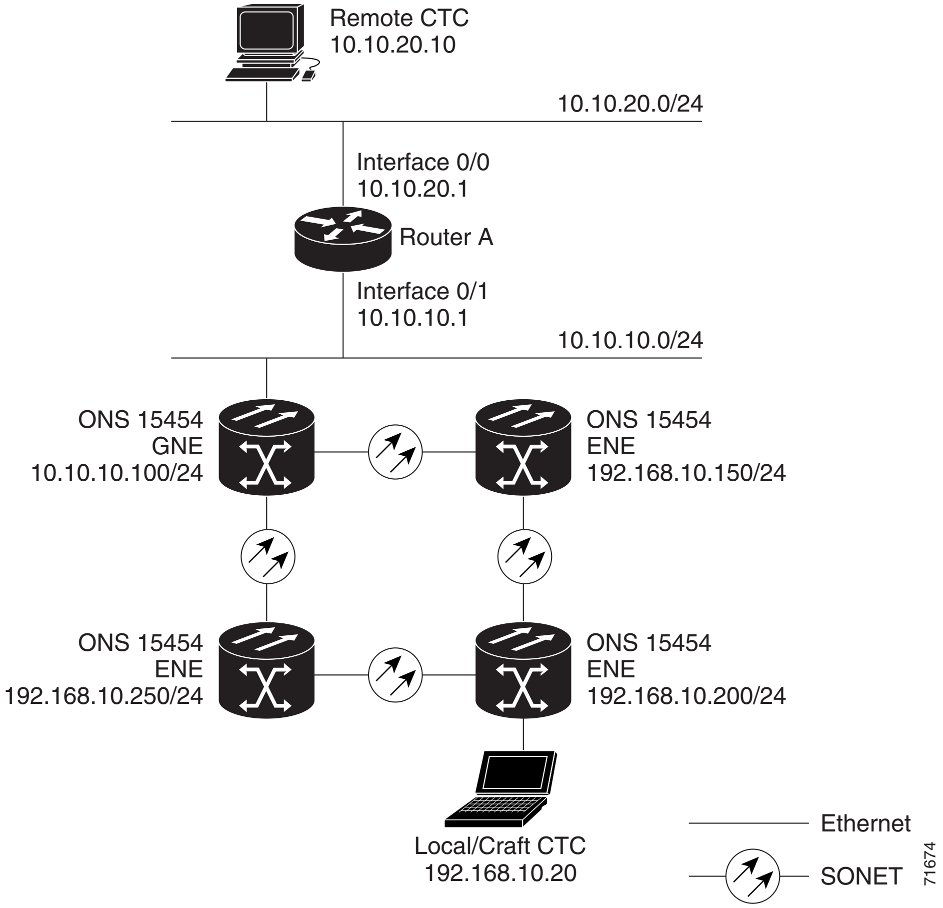


Figure 13-13 IP Scenario 7: ONS 15454 SOCKS Proxy Server With ENEs on Multiple Rings

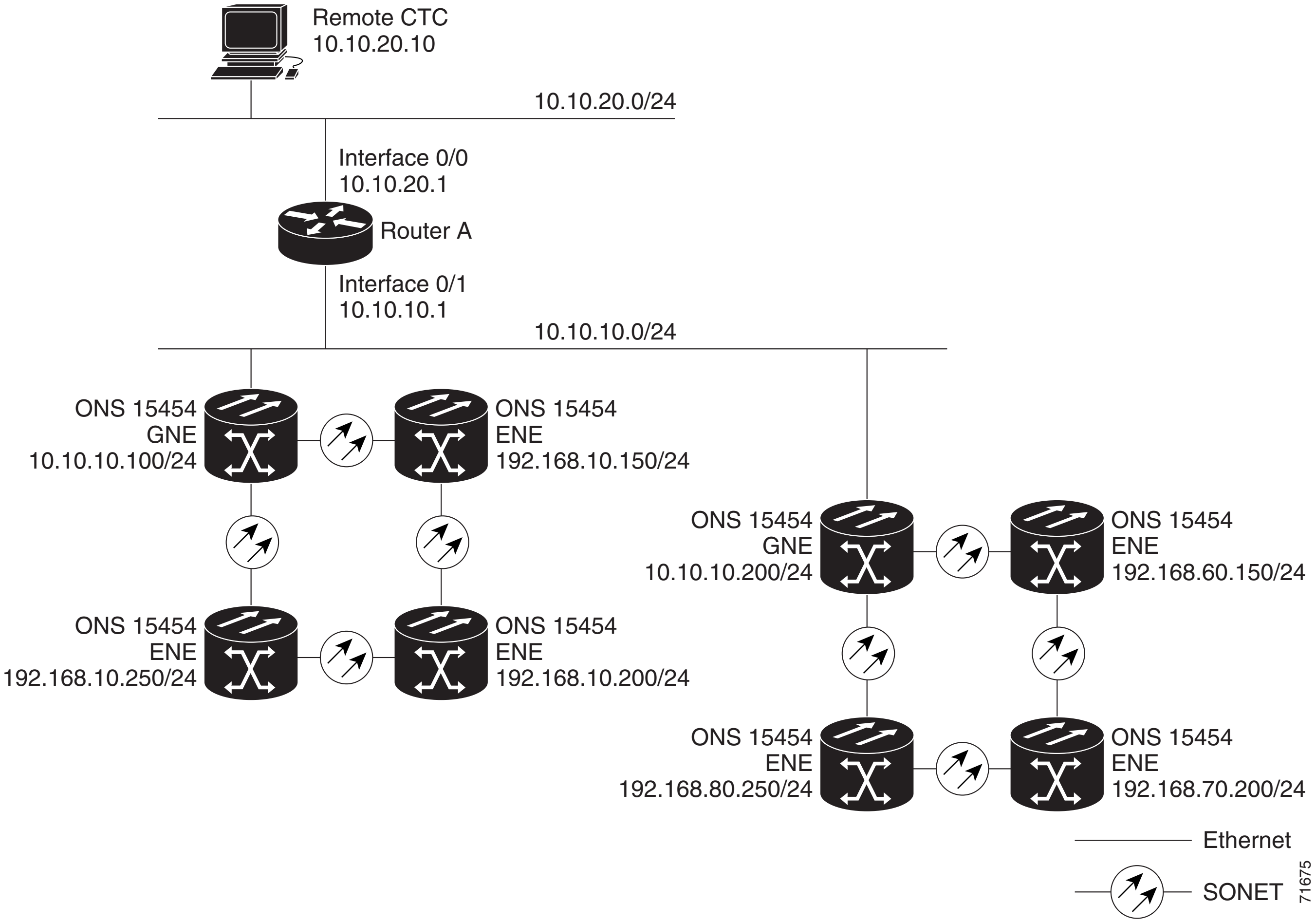


Table 13-3 shows the rules that the ONS 15454 follows to filter packets for the firewall when nodes are configured as ENEs and GNEs.

Table 13-3 SOCKS Proxy Server Firewall Filtering Rules

Packets Arriving At:	Are Accepted if the Destination IP Address is:
TCC2/TCC2P Ethernet interface	• The ONS 15454 node itself • The ONS 15454 node's subnet broadcast address • Within the 224.0.0.0/8 network (reserved network used for standard multicast messages) • Subnet mask = 255.255.255.255
DCC interface	• The ONS 15454 node itself • Any destination connected through another DCC interface • Within the 224.0.0.0/8 network

If the packet is addressed to the ONS 15454 node, additional rules, shown in Table 13-4, are applied. Rejected packets are silently discarded.

Table 13-4 SOCKS Proxy Server Firewall Filtering Rules When Packet Addressed to the ONS 15454

Packets Arriving At	Accepts	Rejects
TCC2/TCC2P Ethernet interface	• All UDP[1] packets except those in the Rejected column	• UDP packets addressed to the SNMP trap relay port (391)
DCC interface	• All UDP packets • All TCP[2] protocols except packets addressed to the Telnet and SOCKS proxy server ports • OSPF packets • ICMP[3] packets	• TCP packets addressed to the Telnet port • TCP packets addressed to the SOCKS proxy server port • All packets other than UDP, TCP, OSPF, ICMP

[1] UDP = User Datagram Protocol

[2] TCP = Transmission Control Protocol

[3] ICMP = Internet Control Message Protocol

If you implement the SOCKS proxy server, note that all DCC-connected ONS 15454s on the same Ethernet segment must have the same gateway setting. Mixed values produce unpredictable results, and might leave some nodes unreachable through the shared Ethernet segment.

If nodes become unreachable, correct the setting with one of the following actions:

- Disconnect the craft computer from the unreachable ONS 15454. Connect to the ONS 15454 through another network ONS 15454 that has a DCC connection to the unreachable ONS 15454.
- Disconnect all DCCs to the node by disabling them on neighboring nodes. Connect a CTC computer directly to the ONS 15454 and change its provisioning.

13.2.8 IP Scenario 8: Dual GNEs on a Subnet

The ONS 15454 provides GNE load balancing, which allows CTC to reach ENEs over multiple GNEs without the ENEs being advertised over OSPF. This feature allows a network to quickly recover from the loss of a GNE, even if the GNE is on a different subnet. If a GNE fails, all connections through that GNE fail. CTC disconnects from the failed GNE and from all ENEs for which the GNE was a proxy, and then reconnects through the remaining GNEs. GNE load balancing reduces the dependency on the launch GNE and DCC bandwidth, both of which enhance CTC performance. Figure 13-14 shows a network with dual GNEs on the same subnet.

Figure 13-14 IP Scenario 8: Dual GNEs on the Same Subnet

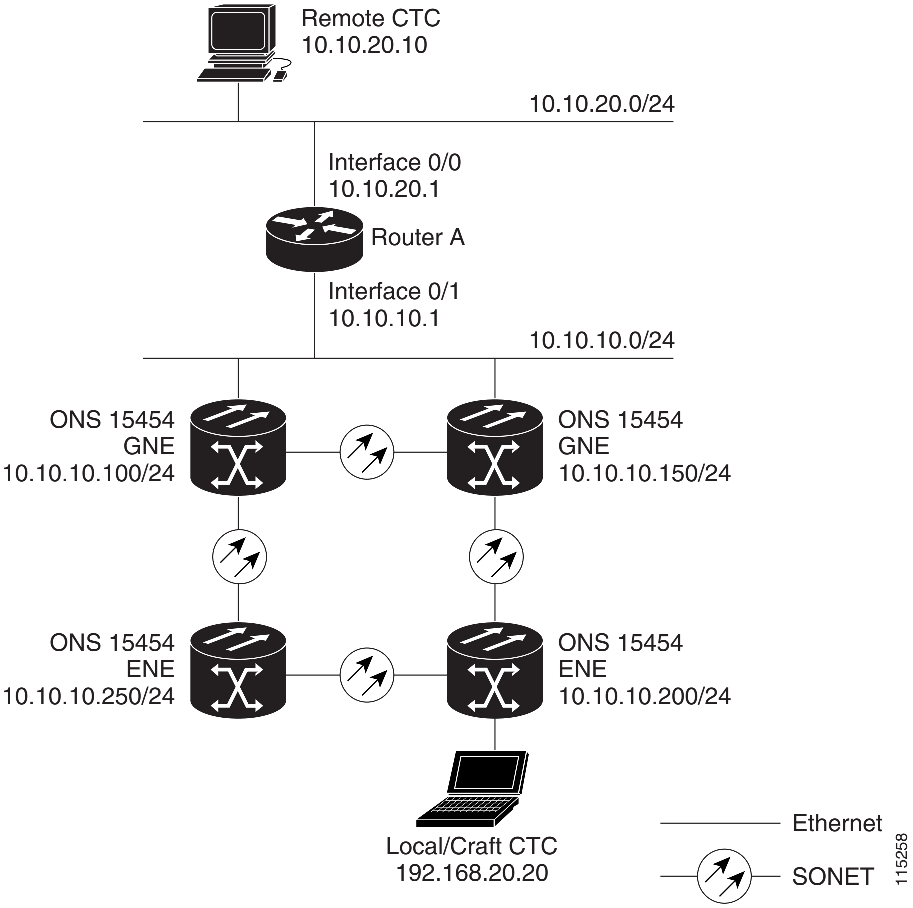
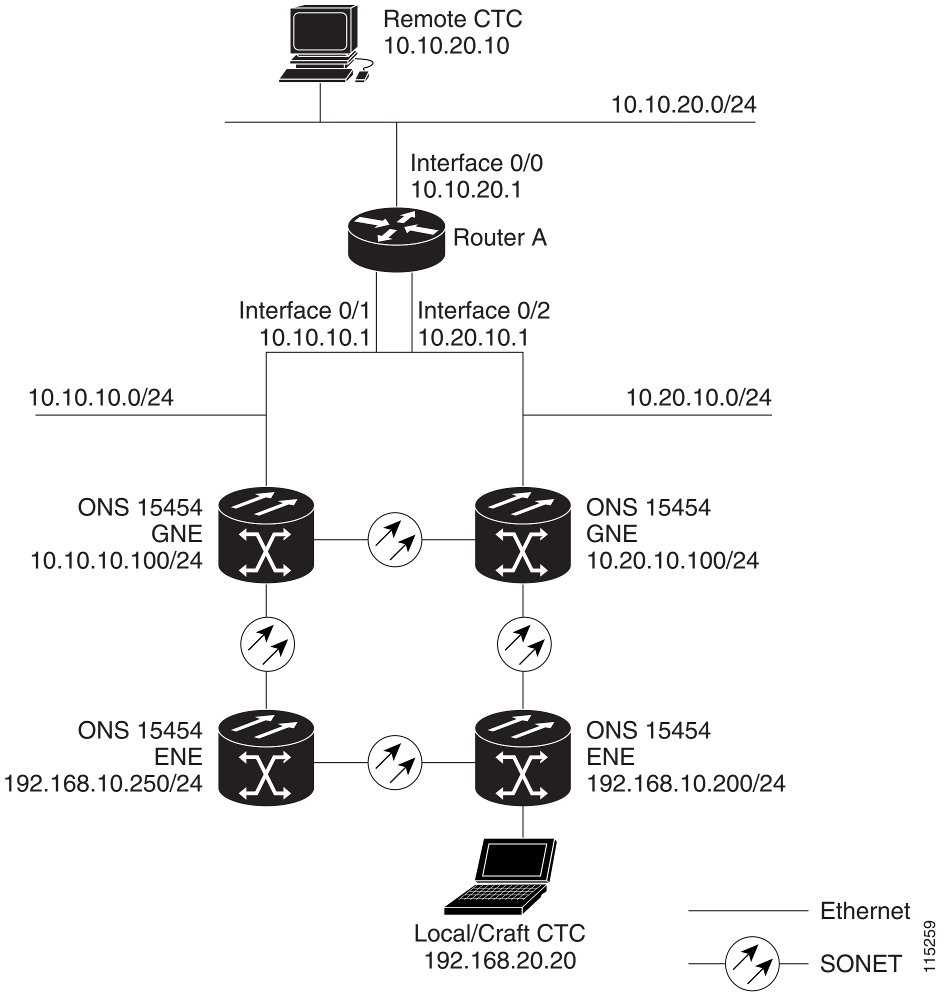


Figure 13-15 shows a network with dual GNEs on different subnets.

Figure 13-15 IP Scenario 8: Dual GNEs on Different Subnets



13.2.9 IP Scenario 9: IP Addressing with Secure Mode Enabled

The TCC2 card and TCC2P card both default to nonsecure mode. In this mode, the front and back Ethernet (LAN) ports share a single MAC address and IP address. TCC2P cards allow you to place a node in secure mode, which prevents a front-access craft port user from accessing the LAN through the backplane port. Secure mode can be locked, which prevents the mode from being altered. To place a node in secure mode or to lock secure node, refer to the "Change Node Settings" chapter in the *Cisco ONS 15454 Procedure Guide*.

13.2.9.1 Secure Mode Behavior

Changing a TCC2P node from repeater mode to secure mode allows you to provision two IP addresses for the ONS 15454 and causes the node to assign the ports different MAC addresses. In secure mode, one IP address is provisioned for the ONS 15454 backplane LAN port, and the other IP address is provisioned for the TCC2P Ethernet port. Both addresses reside on different subnets, providing an additional layer of separation between the craft access port and the ONS 15454 LAN. If secure mode is enabled, the IP addresses provisioned for both TCC2P TCP/IP LAN ports must follow general IP addressing guidelines and must reside on different subnets from each other and the default router IP address.

In secure mode, the IP address assigned to the front LAN (Ethernet) port becomes a private address, while the backplane connects the node to an Operations Support System (OSS) through a central office LAN or private enterprise network. A superuser can configure the node to hide or reveal the backplane's LAN IP address in CTC, the routing table, or autonomous message reports.

In nonsecure mode, a node can be a GNE or ENE. Placing the node into secure mode automatically turns on SOCKS proxy and defaults the node to GNE status. However, the node can be changed back to an ENE. In nonsecure mode, an ENE’s SOCKS proxy can be disabled—effectively isolating the node beyond the LAN firewall—but it cannot be disabled in secure mode.To change a node’s GNE or ENE status and disable the SOCKS proxy, refer to the “Turn Up a Node” chapter in the *Cisco ONS 15454 Procedure Guide*.

Caution Enabling secure mode causes the TCC2P card to reboot; a TCC2P card reboot affects traffic.

Note The secure mode option does not appear in CTC if TCC2 cards are installed. If one TCC2 and one TCC2P card are installed in a node, secure mode will appear in CTC but it cannot be modified.

Note If both front and backplane access ports are disabled in an ENE and the node is isolated from DCC communication (due to user provisioning or network faults), the front and backplane ports are automatically reenabled.

Figure 13-16 on page 13-22 shows an example of secure-mode ONS 15454 nodes with front-access Ethernet port addresses that reside on the same subnet.

Figure 13-16 IP Scenario 9: ONS 15454 GNE and ENEs on the Same Subnet with Secure Mode Enabled

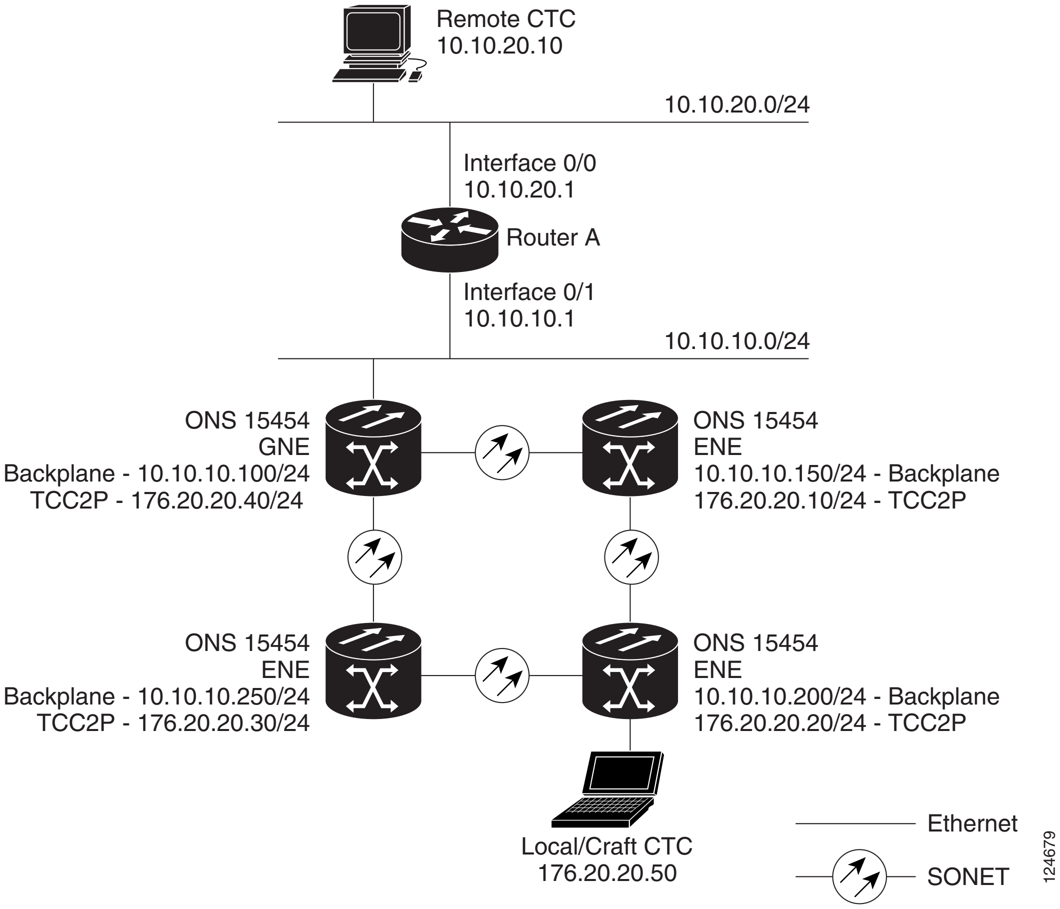
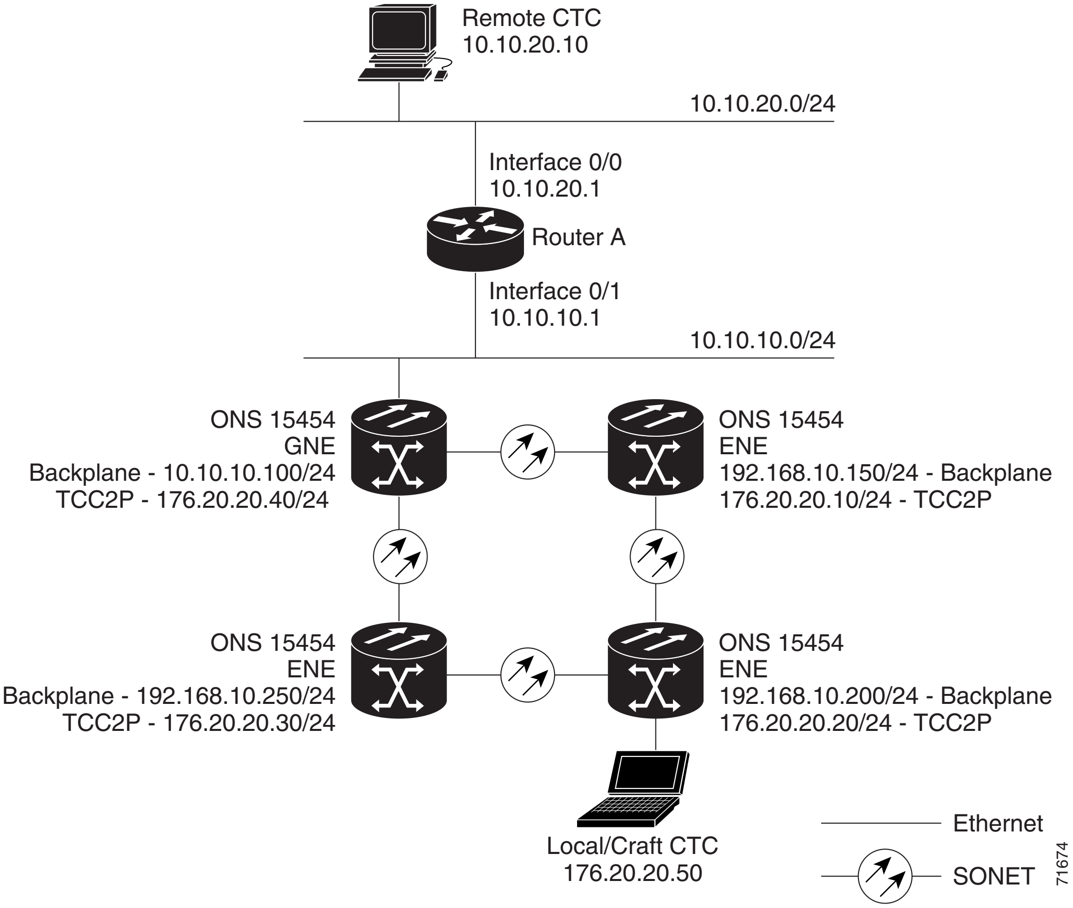


Figure 13-17 shows an example of ONS 15454 nodes connected to a router with secure mode enabled. In each example, the node’s TCC2P port address (node address) resides on a different subnet from the node backplane addresses.

Figure 13-17 IP Scenario 9: ONS 15454 GNE and ENEs on Different Subnets with Secure Mode Enabled



13.2.9.2 Secure Node Locked and Unlocked Behavior

Secure mode can operate on a node in either locked or unlocked mode. By default, secure mode's status is unlocked; only a superuser can convert it to locked mode. Doing so permanently changes the hardware configuration on the active and standby TCC2P cards as well as the chassis.

Locked mode must be used carefully because the cards and shelf retain their locked status even if separated from each other. For example, if a node is in secure, locked mode and you perform a card pull on its standby TCC2P, then insert that as the active card into another node, the secure, locked mode is written to the new node's chassis and standby TCC2P. If you perform a card pull on a secure, locked node's active and standby TCC2Ps and insert both of them into a chassis that previously was in unlocked mode, the node becomes locked.

When it is secure and locked, a node's configuration, Ethernet port status, its secure mode, and the locked status cannot be changed by any network user— including a superuser. To have a secure node's lock removed, contact Cisco Technical Support to arrange a Return Material Authorization (RMA) for the chassis and for the TCC2Ps. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii as needed.

13.3 Routing Table

ONS 15454 routing information appears on the Maintenance > Routing Table tab. The routing table provides the following information:

- Destination—Displays the IP address of the destination network or host.
- Mask—Displays the subnet mask used to reach the destination host or network.
- Gateway—Displays the IP address of the gateway used to reach the destination network or host.
- Usage—Shows the number of times the listed route has been used.
- Interface—Shows the ONS 15454 interface used to access the destination. Values are:
  - motfcc0—The ONS 15454 Ethernet interface, that is, the RJ-45 jack on the TCC2/TCC2P and the LAN 1 pins on the backplane
  - pdcc0—A DCC/OSC/GCC interface
  - lo0—A loopback interface

Table 13-5 shows sample routing table entries for an ONS 15454.

Table 13-5 Sample Routing Table Entries

Entry	Destination	Mask	Gateway	Usage	Interface
1	0.0.0.0	0.0.0.0	172.20.214.1	265103	motfcc0
2	172.20.214.0	255.255.255.0	172.20.214.92	0	motfcc0
3	172.20.214.92	255.255.255.255	127.0.0.1	54	lo0
4	172.20.214.93	255.255.255.255	0.0.0.0	16853	pdcc0
5	172.20.214.94	255.255.255.255	172.20.214.93	16853	pdcc0

Entry 1 shows the following:

- Destination (0.0.0.0) is the default route entry. All undefined destination network or host entries on this routing table are mapped to the default route entry.
- Mask (0.0.0.0) is always 0 for the default route.
- Gateway (172.20.214.1) is the default gateway address. All outbound traffic that cannot be found in this routing table or is not on the node’s local subnet is sent to this gateway.
- Interface (motfcc0) indicates that the ONS 15454 Ethernet interface is used to reach the gateway.

Entry 2 shows the following:

- Destination (172.20.214.0) is the destination network IP address.
- Mask (255.255.255.0) is a 24-bit mask, meaning all addresses within the 172.20.214.0 subnet can be destinations.
- Gateway (172.20.214.92) is the gateway address. All outbound traffic belonging to this network is sent to this gateway.
- Interface (motfcc0) indicates that the ONS 15454 Ethernet interface is used to reach the gateway.

Entry 3 shows the following:

- Destination (172.20.214.92) is the destination host IP address.

- Mask (255.255.255.255) is a 32 bit mask, meaning that only the 172.20.214.92 address is a destination.
- Gateway (127.0.0.1) is a loopback address. The host directs network traffic to itself using this address.
- Interface (lo0) indicates that the local loopback interface is used to reach the gateway.

Entry 4 shows the following:

- Destination (172.20.214.93) is the destination host IP address.
- Mask (255.255.255.255) is a 32 bit mask, meaning that only the 172.20.214.93 address is a destination.
- Gateway (0.0.0.0) means the destination host is directly attached to the node.
- Interface (pdcc0) indicates that a DCC interface is used to reach the destination host.

Entry 5 shows a DCC-connected node that is accessible through a node that is not directly connected:

- Destination (172.20.214.94) is the destination host IP address.
- Mask (255.255.255.255) is a 32-bit mask, meaning that only the 172.20.214.94 address is a destination.
- Gateway (172.20.214.93) indicates that the destination host is accessed through a node with IP address 172.20.214.93.
- Interface (pdcc0) indicates that a DCC interface is used to reach the gateway.

13.4 External Firewalls

This section provides sample access control lists (ACLs) for external firewalls. Table 13-6 lists the ports that are used by the TCC2/TCC2P card.

Table 13-6 Ports Used by the TCC2/TCC2P

Port	Function	Action[1]
0	Never used	D
20	FTP	D
21	FTP control	D
22	SSH (Secure Shell)	D
23	Telnet	D
80	HTTP	D
111	SUNRPC (Sun Remote Procedure Call)	NA
161	SNMP traps destinations	D
162	SNMP traps destinations	D
513	rlogin	D
683	CORBA IIOP[2]	OK
1080	Proxy server (socks)	D
2001-2017	I/O card Telnet	D
2018	DCC processor on active TCC2/TCC2P	D

Table 13-6 Ports Used by the TCC2/TCC2P (continued)

Port	Function	Action[1]
2361	TL1	D
3082	Raw TL1	D
3083	TL1	D
5001	BLSR[3] server port	D
5002	BLSR client port	D
7200	SNMP alarm input port	D
9100	EQM port	D
9401	TCC boot port	D
9999	Flash manager	D
10240-12287	Proxy client	D
57790	Default TCC listener port	OK

[1] D = deny, NA = not applicable, OK = do not deny

[2] CORBA IIOP = Common Object Request Broker Architecture Internet Inter-ORB Protocol

[3] BLSR = bidirectional line switched ring

The following ACL example shows a firewall configuration when the SOCKS proxy server gateway setting is not enabled. In the example, the CTC workstation's address is 192.168.10.10. and the ONS 15454 address is 10.10.10.100. The firewall is attached to the GNE, so inbound is CTC to the GNE and outbound is from the GNE to CTC. The CTC CORBA Standard constant is 683 and the TCC CORBA Default is TCC Fixed (57790).

```
access-list 100 remark *** Inbound ACL, CTC -> NE ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 host 10.10.10.100 eq www
access-list 100 remark *** allows initial contact with ONS 15454 using http (port 80) ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 host 10.10.10.100 eq 57790
access-list 100 remark *** allows CTC communication with ONS 15454 GNE (port 57790) ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 host 10.10.10.100 established
access-list 100 remark *** allows ACKs back from CTC to ONS 15454 GNE ***

access-list 101 remark *** Outbound ACL, NE -> CTC ***
access-list 101 remark
access-list 101 permit tcp host 10.10.10.100 host 192.168.10.10 eq 683
access-list 101 remark *** allows alarms etc., from the 15454 (random port) to the CTC
workstation (port 683) ***
access-list 100 remark
access-list 101 permit tcp host 10.10.10.100 host 192.168.10.10 established
access-list 101 remark *** allows ACKs from the 15454 GNE to CTC ***
```

The following ACL example shows a firewall configuration when the SOCKS proxy server gateway setting is enabled. As with the first example, the CTC workstation address is 192.168.10.10 and the ONS 15454 address is 10.10.10.100. The firewall is attached to the GNE, so inbound is CTC to the GNE and outbound is from the GNE to CTC. CTC CORBA Standard constant is 683 and the TCC CORBA Default is TCC Fixed (57790).

```
access-list 100 remark *** Inbound ACL, CTC -> NE ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 host 10.10.10.100 eq www
```

```
access-list 100 remark *** allows initial contact with the 15454 using http (port 80) ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 host 10.10.10.100 eq 1080
access-list 100 remark *** allows CTC communication with the 15454 GNE (port 1080) ***
access-list 100 remark

access-list 101 remark *** Outbound ACL, NE -> CTC ***
access-list 101 remark
access-list 101 permit tcp host 10.10.10.100 host 192.168.10.10 established
access-list 101 remark *** allows ACKs from the 15454 GNE to CTC ***
```

13.5 Open GNE

The ONS 15454 can communicate with non-ONS nodes that do not support Point-to-Point Protocol (PPP) vendor extensions or OSPF type 10 opaque link-state advertisements (LSA), both of which are necessary for automatic node and link discovery. An open GNE configuration allows the DCC-based network to function as an IP network for non-ONS nodes.

To configure an open GNE network, you can provision SDCC, LDCC, and GCC terminations to include a far-end, non-ONS node using either the default IP address of 0.0.0.0 or a specified IP address. You provision a far-end, non-ONS node by checking the Far End is Foreign check box during SDCC, LDCC, and GCC creation. The default 0.0.0.0 IP address allows the far-end, non-ONS node to provide the IP address; if you set an IP address other than 0.0.0.0, a link is established only if the far-end node identifies itself with that IP address, providing an extra level of security.

By default, the SOCKS proxy server only allows connections to discovered ONS peers and the firewall blocks all IP traffic between the DCC network and LAN. You can, however, provision proxy tunnels to allow up to 12 additional destinations for SOCKS version 5 connections to non-ONS nodes. You can also provision firewall tunnels to allow up to 12 additional destinations for direct IP connectivity between the DCC network and the LAN. Proxy and firewall tunnels include both a source and destination subnet. The connection must originate within the source subnet and terminate within the destination subnet before either the SOCKS connection or IP packet flow is allowed.

To set up proxy and firewall subnets in CTC, use the Provisioning > Network > Proxy and Firewalls subtabs. The availability of proxy and/or firewall tunnels depends on the network access settings of the node:

- If the node is configured with the SOCKS proxy server enabled in GNE or ENE mode, you must set up a proxy tunnel and/or a firewall tunnel.
- If the node is configured with the SOCKS proxy server enabled in proxy-only mode, you can set up proxy tunnels. Firewall tunnels are not allowed.
- If the node is configured with the SOCKS proxy server disabled, neither proxy tunnels nor firewall tunnels are allowed.

Figure 13-18 shows an example of a foreign node connected to the DCC network. Proxy and firewall tunnels are useful in this example because the GNE would otherwise block IP access between the PC and the foreign node.

Figure 13-18 Proxy and Firewall Tunnels for Foreign Terminations

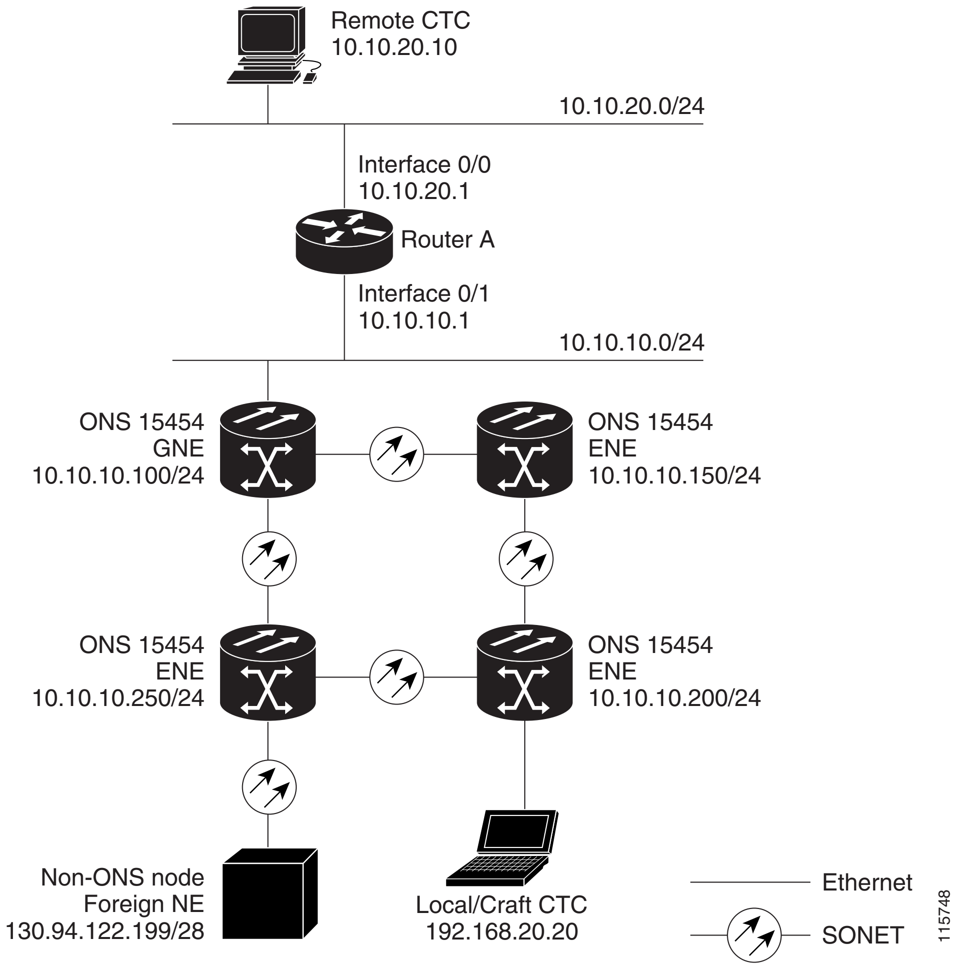
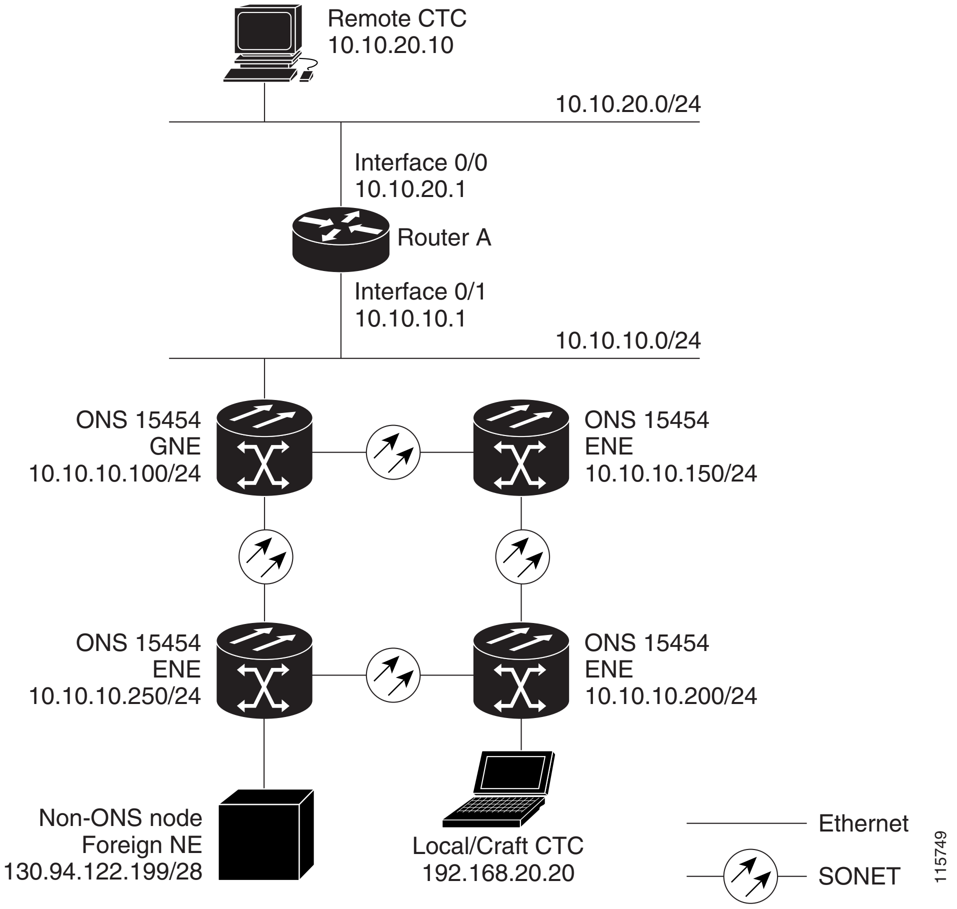


Figure 13-19 shows a remote node connected to an ENE Ethernet port. Proxy and firewall tunnels are useful in this example because the GNE would otherwise block IP access between the PC and foreign node. This configuration also requires a firewall tunnel on the ENE.

Figure 13-19 Foreign Node Connection to an ENE Ethernet Port



13.6 TCP/IP and OSI Networking

ONS 15454 DCN communication is based on the TCP/IP protocol suite. However, ONS 15454s can also be networked with equipment that uses the OSI protocol suite. While TCP/IP and OSI protocols are not directly compatible, they do have the same objectives and occupy similar layers of the OSI reference model. Table 13-7 shows the protocols and mediation processes that are involved when TCP/IP-based NEs are networked with OSI-based NEs.

Table 13-7 TCP/IP and OSI Protocols

OSI Model	IP Protocols	OSI Protocols		IP-OSI Mediation
Layer 7 Application	• TL1 • FTP • HTTP • Telnet • IIOP	• TARP[1]	• TL1 (over OSI) • FTAM[2] • ACSE[3]	• T–TD[4] • FT–TD[5]
Layer 6 Presentation			• PST[6]	
Layer 5 Session			• Session	
Layer 4 Transport	• TCP • UDP		• TP (Transport) Class 4	• IP-over-CLNS[7] tunnels
Layer 3 Network	• IP • OSPF	• CLNP[8] • ES-IS[9] • IS-IS[10]		
Layer 2 Data link	• PPP	• PPP • LAP-D[11]		
Layer 1 Physical	DCC, LAN, fiber, electrical	DCC, LAN, fiber, electrical		

[1] TARP = TID Address Resolution Protocol

[2] FTAM = File Transfer and Access Management

[3] ACSE = association-control service element

[4] T–TD = TL1–Translation Device

[5] FT–TD = File Transfer—Translation Device

[6] PST = Presentation layer

[7] CLNS = Connectionless Network Layer Service

[8] CLNP = Connectionless Network Layer Protocol

[9] ES-IS = End System-to-Intermediate System

[10] IS-IS = Intermediate System-to-Intermediate System

[11] LAP-D = Link Access Protocol on the D Channel

13.6.1 Point-to-Point Protocol

PPP is a data link (Layer 2) encapsulation protocol that transports datagrams over point-to-point links. Although PPP was developed to transport IP traffic, it can carry other protocols including the OSI CLNP. PPP components used in the transport of OSI include:

- High-level data link control (HDLC)—Performs the datagram encapsulation for transport across point-to-point links.
- Link control protocol (LCP)—Establishes, configures, and tests the point-to-point connections.

CTC automatically enables IP over PPP whenever you create an SDCC or LDCC. The SDCC or LDCC can be provisioned to support OSI over PPP.

13.6.2 Link Access Protocol on the D Channel

LAP-D is a data link protocol used in the OSI protocol stack. LAP-D is assigned when you provision an ONS 15454 SDCC as OSI-only. Provisionable LAP-D parameters include:

- Transfer Service—One of the following transfer services must be assigned:
  - Acknowledged Information Transfer Service (AITS)—(Default) Does not exchange data until a logical connection between two LAP-D users is established. This service provides reliable data transfer, flow control, and error control mechanisms.
  - Unacknowledged Information Transfer Service (UITS)—Transfers frames containing user data with no acknowledgement. The service does not guarantee that the data presented by one user will be delivered to another user, nor does it inform the user if the delivery attempt fails. It does not provide any flow control or error control mechanisms.
- Mode—LAP-D is set to either Network or User mode. This parameter sets the LAP-D frame command/response (C/R) value, which indicates whether the frame is a command or a response.
- Maximum transmission unit (MTU)—The LAP-D N201 parameter sets the maximum number of octets in a LAP-D information frame. The range is 512 to 1500 octets.

Note The MTU must be the same size for all NEs on the network.

- Transmission Timers—The following LAP-D timers can be provisioned:
  - The T200 timer sets the timeout period for initiating retries or declaring failures.
  - The T203 timer provisions the maximum time between frame exchanges, that is, the trigger for transmission of the LAP-D “keep-alive” Receive Ready (RR) frames.

Fixed values are assigned to the following LAP-D parameters:

- Terminal Endpoint Identifier (TEI)—A fixed value of 0 is assigned.
- Service Access Point Identifier (SAPI)—A fixed value of 62 is assigned.
- N200 supervisory frame retransmissions—A fixed value of 3 is assigned.

13.6.3 OSI Connectionless Network Service

OSI connectionless network service is implemented by using the Connectionless Network Protocol (CLNP) and Connectionless Network Service (CLNS). CLNP and CLNS are described in the ISO 8473 standard. CLNS provides network layer services to the transport layer through CLNP. CLNS does not perform connection setup or termination because paths are determined independently for each packet that is transmitted through a network. CLNS relies on transport layer protocols to perform error detection and correction.

CLNP is an OSI network layer protocol that carries upper-layer data and error indications over connectionless links. CLNP provides the interface between the CLNS and upper layers. CLNP performs many of the same services for the transport layer as IP. The CLNP datagram is very similar to the IP datagram. It provides mechanisms for fragmentation (data unit identification, fragment/total length, and offset). Like IP, a checksum computed on the CLNP header verifies that the information used to process the CLNP datagram is transmitted correctly, and a lifetime control mechanism (Time to Live) limits the amount of time a datagram is allowed to remain in the system.

CLNP uses network service access points (NSAPs) to identify network devices. The CLNP source and destination addresses are NSAPs. In addition, CLNP uses a network element title (NET) to identify a network-entity in an end system (ES) or intermediate system (IS). NETs are allocated from the same name space as NSAP addresses. Whether an address is an NSAP address or a NET depends on the network selector value in the NSAP.

The ONS 15454 supports the ISO Data Country Code (ISO-DCC) NSAP address format as specified in ISO 8348. The NSAP address is divided into an initial domain part (IDP) and a domain-specific part (DSP). NSAP fields are shown in Table 13-8. NSAP field values are in hexadecimal format. All NSAPs are editable. Shorter NSAPs can be used. However NSAPs for all NEs residing within the same OSI network area usually have the same NSAP format.

Table 13-8 NSAP Fields

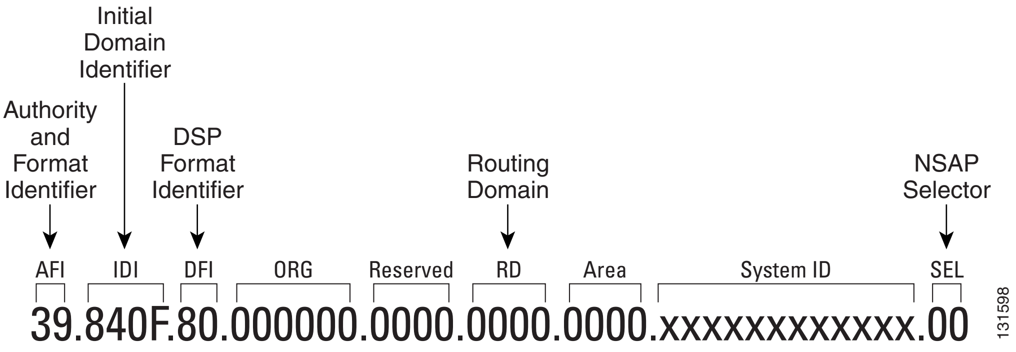
Field	Definition	Description
IDP		
AFI	Authority and format identifier	Specifies the NSAP address format. The initial value is 39 for the ISO-DCC address format.
IDI	Initial domain identifier	Specifies the country code. The initial value is 840F, the United States country code padded with an F.
DSP		
DFI	DSP format identifier	Specifies the DSP format. The initial value is 80, indicating the DSP format follows American National Standards Institute (ANSI) standards.
ORG	Organization	Organization identifier. The initial value is 000000.
Reserved	Reserved	Reserved NSAP field. The Reserved field is normally all zeros (0000).
RD	Routing domain	Defines the routing domain. The initial value is 0000.
AREA	Area	Identifies the OSI routing area to which the node belongs. The initial value is 0000.

Table 13-8 NSAP Fields (continued)

Field	Definition	Description
System	System identifier	The ONS 15454 system identifier is set to its IEEE 802.3 MAC address. Each ONS 15454 supports three OSI virtual routers. Each router NSAP system identifier is the ONS 15454 IEEE 802.3 MAC address + *n*, where *n* = 0 to 2. For the primary virtual router, *n* = 0.
SEL	Selector	The selector field directs the protocol data units (PDUs) to the correct destination using the CLNP network layer service. Selector values supported by the ONS 15454 include: • 00—Network Entity Title (NET). Used to exchange PDUs in the ES-IS and IS-IS routing exchange protocols. (See the "13.6.4.1 End System-to-Intermediate System Protocol" section on page 13-36 and the "13.6.4.2 Intermediate System-to-Intermediate System Protocol" section on page 13-36.) • 1D—Selector for Transport Class 4 (and for FTAM and TL1 applications (Telcordia GR-253-CORE standard) • AF—Selector for the TARP protocol (Telcordia GR-253-CORE standard) • 2F—Selector for the GRE IP-over-CLNS tunnel (ITU/RFC standard) • CC—Selector for the Cisco IP-over-CLNS tunnels (Cisco specific) • E0—Selector for the OSI ping application (Cisco specific) NSELs are only advertised when the node is configured as an ES. They are not advertised when a node is configured as an IS. Tunnel NSELs are not advertised until a tunnel is created.

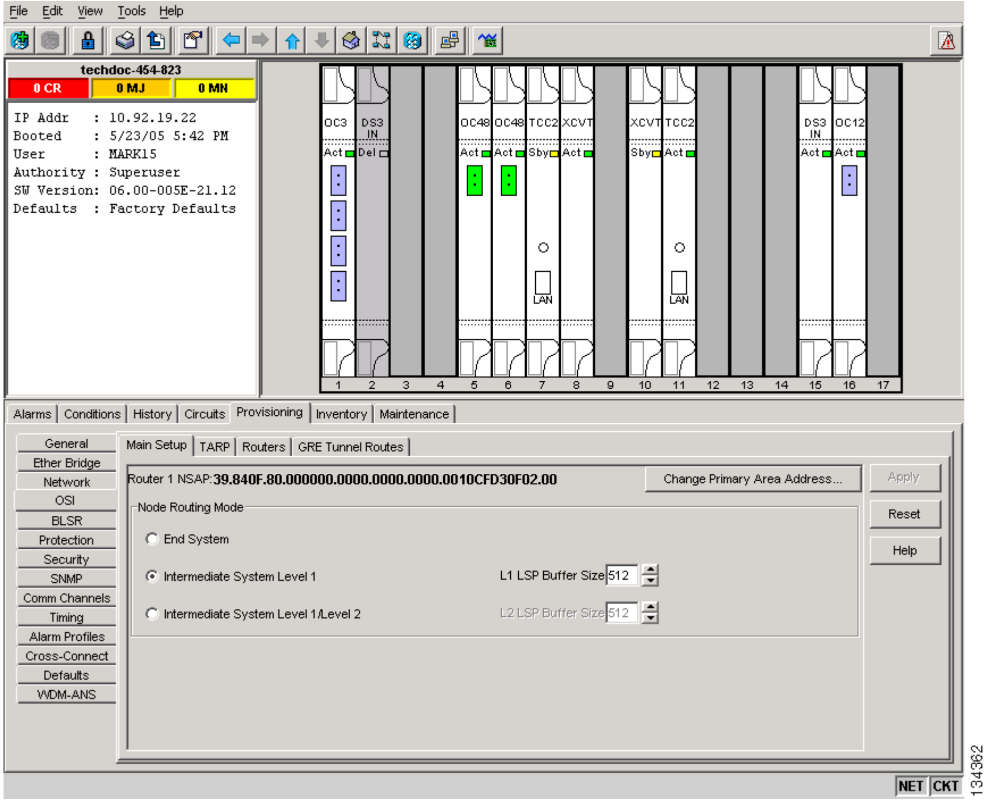
Figure 13-20 shows the ISO-DCC NSAP address with the default values delivered with the ONS 15454. The System ID is automatically populated with the node MAC address.

Figure 13-20 ISO-DCC NSAP Address


Initial Domain Identifier
Authority and Format Identifier
DSP Format Identifier
Routing Domain
NSAP Selector
AFI
IDI
DFI
ORG
Reserved
RD
Area
System ID
SEL
39.840F.80.000000.0000.0000.0000.xxxxxxxxxxxx.00
131598

The ONS 15454 main NSAP address is shown on the node view Provisioning > OSI > Main Setup subtab (Figure 13-21).

Figure 13-21 OSI Main Setup



```
IP Addr   : 10.92.19.22
Booted    : 5/23/05 5:42 PM
User      : MARK15
Authority : Superuser
SW Version: 06.00-005E-21.12
Defaults  : Factory Defaults
```

Router 1 NSAP: **39.840F.80.000000.0000.0000.0000.0010CFD30F02.00**

Node Routing Mode

○ End System

● Intermediate System Level 1 — L1 LSP Buffer Size 512

○ Intermediate System Level 1/Level 2 — L2 LSP Buffer Size 512

This address is also the Router 1 primary manual area address, which is viewed and edited on the Provisioning > OSI > Routers subtab. See the "13.6.7 OSI Virtual Routers" section on page 13-41 for information about the OSI router and manual area addresses in CTC.

13.6.4 OSI Routing

OSI architecture includes ESs and ISs. The OSI routing scheme includes:

- A set of routing protocols that allow ESs and ISs to collect and distribute the information necessary to determine routes. Protocols include the ES-IS and IS-IS protocols. ES-IS routing establishes connectivity and reach ability among ESs and ISs attached to the same (single) subnetwork.
- A routing information base (RIB) (see containing this information, from which routes between ESs can be computed. The RIB consists of a table of entries that identify a destination (for example, an NSAP), the subnetwork over which packets should be forwarded to reach that destination, and a routing metric. The routing metric communicates characteristics of the route (such as delay properties or expected error rate) that are used to evaluate the suitability of a route compared to another route with different properties, for transporting a particular packet or class of packets.
- A routing algorithm, Shortest Path First (SPF), that uses information contained in the RIB to derive routes between ESs.

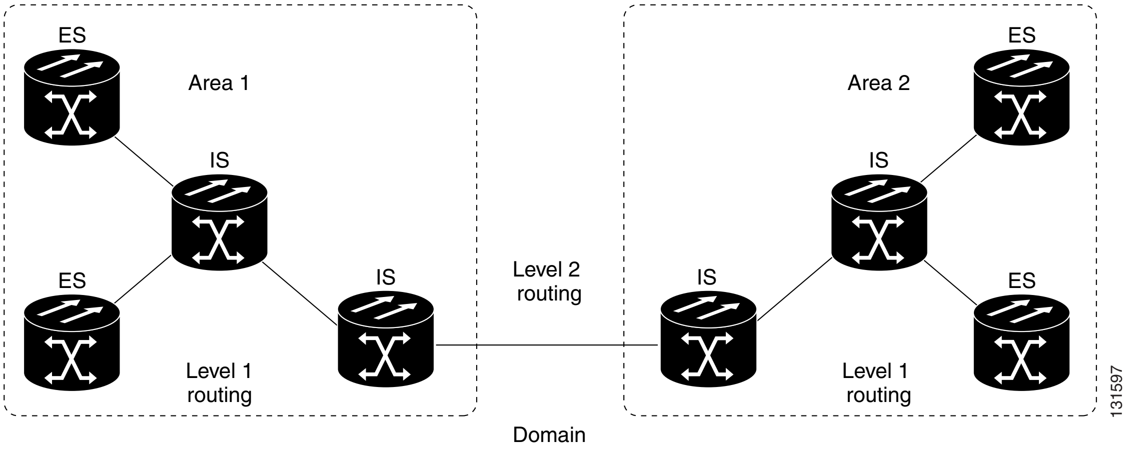
In OSI networking, discovery is based on announcements. An ES uses the ES-IS protocol end system hello (ESH) message to announce its presence to ISs and ESs connected to the same network. Any ES or IS that is listening for ESHs gets a copy. ISs store the NSAP address and the corresponding subnetwork address pair in routing tables. ESs might store the address, or they might wait to be informed by ISs when they need such information.

An IS composes intermediate system hello (ISH) messages to announce its configuration information to ISs and ESs that are connected to the same broadcast subnetwork. Like the ESHs, the ISH contains the addressing information for the IS (the NET and the subnetwork point-of-attachment address [SNPA]) and a holding time. ISHs might also communicate a suggested ES configuration time recommending a configuration timer to ESs.

The exchange of ISHs is called neighbor greeting or initialization. Each router learns about the other routers with which they share direct connectivity. After the initialization, each router constructs a link-state packet (LSP). The LSP contains a list of the names of the IS's neighbors and the cost to reach each of the neighbors. Routers then distribute the LSPs to all of the other routers. When all LSPs are propagated to all routers, each router has a complete map of the network topology (in the form of LSPs). Routers use the LSPs and the SPF algorithm to compute routes to every destination in the network.

OSI networks are divided into areas and domains. An area is a group of contiguous networks and attached hosts that is designated as an area by a network administrator. A domain is a collection of connected areas. Routing domains provide full connectivity to all ESs within them. Routing within the same area is known as Level 1 routing. Routing between two areas is known as Level 2 routing. LSPs that are exchanged within a Level 1 area are called L1 LSPs. LSPs that are exchanged across Level 2 areas are called L2 LSPs. Figure 13-22 shows an example of Level 1 and Level 2 routing.

Figure 13-22 Level 1 and Level 2 OSI Routing



When you provision an ONS 15454 for a network with NEs that use both the TCP/IP and OSI protocol stacks, you will provision it as one of the following:

- End System—The ONS 15454 performs OSI ES functions and relies upon an IS for communication with nodes that reside within its OSI area.
- Intermediate System Level 1—The ONS 15454 performs OSI IS functions. It communicates with IS and ES nodes that reside within its OSI area. It depends upon an IS L1/L2 node to communicate with IS and ES nodes that reside outside its OSI area.

- Intermediate System Level 1/Level 2—The ONS 15454 performs IS functions. It communicates with IS and ES nodes that reside within its OSI area. It also communicates with IS L1/L2 nodes that reside in other OSI areas. This option should not be provisioned unless the node is connected to another IS L1/L2 node that resides in a different OSI area. The node must also be connected to all nodes within its area that are provisioned as IS L1/L2.

13.6.4.1 End System-to-Intermediate System Protocol

ES-IS is an OSI protocol that defines how ESs (hosts) and ISs (routers) learn about each other. ES-IS configuration information is transmitted at regular intervals through the ES and IS hello messages. The hello messages contain the subnetwork and network layer addresses of the systems that generate them.

The ES-IS configuration protocol communicates both OSI network layer addresses and OSI subnetwork addresses. OSI network layer addresses identify either the NSAP, which is the interface between OSI Layer 3 and Layer 4, or the NET, which is the network layer entity in an OSI IS. OSI SNPAs are the points at which an ES or IS is physically attached to a subnetwork. The SNPA address uniquely identifies each system attached to the subnetwork. In an Ethernet network, for example, the SNPA is the 48-bit MAC address. Part of the configuration information transmitted by ES-IS is the NSAP-to-SNPA or NET-to-SNPA mapping.

13.6.4.2 Intermediate System-to-Intermediate System Protocol

IS-IS is an OSI link-state hierarchical routing protocol that floods the network with link-state information to build a complete, consistent picture of a network topology. IS-IS distinguishes between Level 1 and Level 2 ISs. Level 1 ISs communicate with other Level 1 ISs in the same area. Level 2 ISs route between Level 1 areas and form an intradomain routing backbone. Level 1 ISs need to know only how to get to the nearest Level 2 IS. The backbone routing protocol can change without impacting the intra-area routing protocol.

OSI routing begins when the ESs discover the nearest IS by listening to ISH packets. When an ES wants to send a packet to another ES, it sends the packet to one of the ISs on its directly attached network. The router then looks up the destination address and forwards the packet along the best route. If the destination ES is on the same subnetwork, the local IS knows this from listening to ESHs and forwards the packet appropriately. The IS also might provide a redirect (RD) message back to the source to tell it that a more direct route is available. If the destination address is an ES on another subnetwork in the same area, the IS knows the correct route and forwards the packet appropriately. If the destination address is an ES in another area, the Level 1 IS sends the packet to the nearest Level 2 IS. Forwarding through Level 2 ISs continues until the packet reaches a Level 2 IS in the destination area. Within the destination area, the ISs forward the packet along the best path until the destination ES is reached.

Link-state update messages help ISs learn about the network topology. Each IS generates an update specifying the ESs and ISs to which it is connected, as well as the associated metrics. The update is then sent to all neighboring ISs, which forward (flood) it to their neighbors, and so on. (Sequence numbers terminate the flood and distinguish old updates from new ones.) Using these updates, each IS can build a complete topology of the network. When the topology changes, new updates are sent.

IS-IS uses a single required default metric with a maximum path value of 1024. The metric is arbitrary and typically is assigned by a network administrator. Any single link can have a maximum value of 64, and path links are calculated by summing link values. Maximum metric values were set at these levels to provide the granularity to support various link types while at the same time ensuring that the shortest-path algorithm used for route computation is reasonably efficient. Three optional IS-IS metrics (costs)—delay, expense, and error—are not supported by the ONS 15454. IS-IS maintains a mapping of the metrics to the quality of service (QoS) option in the CLNP packet header. IS-IS uses the mappings to compute routes through the internetwork.

13.6.5 TARP

TARP is used when TL1 target identifiers (TIDs) must be translated to NSAP addresses. The TID-to-NSAP translation occurs by mapping TIDs to the NETs, then deriving NSAPs from the NETs by using the NSAP selector values (Table 13-8 on page 13-32).

TARP uses a selective PDU propagation methodology in conjunction with a distributed database (that resides within the NEs) of TID-to-NET mappings. TARP allows NEs to translate between TID and NET by automatically exchanging mapping information with other NEs. The TARP PDU is carried by the standard CLNP Data PDU. TARP PDU fields are shown in Table 13-9.

Table 13-9 TARP PDU Fields

Field	Abbreviation	Size (bytes)	Description
TARP Lifetime	tar-lif	2	The TARP time-to-live in hops.
TARP Sequence Number	tar-seq	2	The TARP sequence number used for loop detection.
Protocol Address Type	tar-pro	1	Used to identify the type of protocol address that the TID must be mapped to. The value FE is used to identify the CLNP address type.
TARP Type Code	tar-tcd	1	The TARP Type Code identifies the TARP type of PDU. Five TARP types, shown in Table 13-10, are defined.
TID Target Length	tar-tln	1	The number of octets that are in the tar-ttg field.
TID Originator Length	tar-oln	1	The number of octets that are in the tar-tor field.
Protocol Address Length	tar-pln	1	The number of octets that are in the tar-por field.
TID of Target	tar-ttg	n = 0, 1, 2...	TID value for the target NE.
TID of Originator	tar-tor	n = 0, 1, 2...	TID value of the TARP PDU originator.
Protocol Address of Originator	tar-por	n = 0, 1, 2...	Protocol address (for the protocol type identified in the tar-pro field) of the TARP PDU originator. When the tar-pro field is set to FE (hex), tar-por will contain a CLNP address (that is, the NET).

Table 13-10 shows the TARP PDUs types that govern TARP interaction and routing.

Table 13-10 TARP PDU Types

Type	Description	Actions
1	Sent when a device has a TID for which it has no matching NSAP.	After an NE originates a TARP Type 1 PDU, the PDU is sent to all adjacent NEs within the NE routing area.
2	Sent when a device has a TID for which it has no matching NSAP and no response was received from the Type 1 PDU.	After an NE originates a TARP Type 2 PDU, the PDU is sent to all Level 1 and Level 2 neighbors.

Table 13-10 TARP PDU Types (continued)

Type	Description	Actions
3	Sent as a response to Type 1, Type 2, or Type 5 PDUs.	After a TARP Request (Type 1 or 2) PDU is received, a TARP Type 3 PDU is sent to the request originator. Type 3 PDUs do not use the TARP propagation procedures.
4	Sent as a notification when a change occurs locally, for example, a TID or NSAP change. It might also be sent when an NE initializes.	A Type 4 PDU is a notification of a TID or Protocol Address change at the NE that originates the notification. The PDU is sent to all adjacencies inside and outside the NE's routing area.
5	Sent when a device needs a TID that corresponds to a specific NSAP.	When a Type 5 PDU is sent, the CLNP destination address is known, so the PDU is sent to only that address. Type 5 PDUs do not use the TARP propagation procedures.

13.6.5.1 TARP Processing

A TARP data cache (TDC) is created at each NE to facilitate TARP processing. In CTC, the TDC is displayed and managed on the node view Maintenance > OSI > TDC subtab. The TDC subtab contains the following TARP PDU fields:

- TID—TID of the originating NE (tar-tor).
- NSAP—NSAP of the originating NE.
- Type— Indicates whether the TARP PDU was created through the TARP propagation process (dynamic) or manually created (static).

Provisionable timers, shown in Table 13-11, control TARP processing.

Table 13-11 TARP Timers

Timer	Description	Default (seconds)	Range (seconds)
T1	Waiting for response to TARP Type 1 Request PDU	15	0–3600
T2	Waiting for response to TARP Type 2 Request PDU	25	0–3600
T3	Waiting for response to address resolution request	40	0–3600
T4	Timer starts when T2 expires (used during error recovery)	20	0–3600

Table 13-12 shows the main TARP processes and the general sequence of events that occurs in each process.

Table 13-12 TARP Processing Flow

Process	General TARP Flow
Find a NET that matches a TID	1. TARP checks its TDC for a match. If a match is found, TARP returns the result to the requesting application. 2. If no match is found, a TARP Type 1 PDU is generated and Timer T1 is started. 3. If Timer T1 expires before a match if found, a Type 2 PDU is generated and Timer T2 is started. 4. If Timer T2 expires before a match is found, Timer T4 is started. 5. If Timer T4 expires before a match is found, a Type 2 PDU is generated and Timer T2 is started.
Find a TID that matches a NET	A Type 5 PDU is generated. Timer T3 is used. However, if the timer expires, no error recovery procedure occurs, and a status message is provided to indicate that the TID cannot be found.
Send a notification of TID or protocol address change	TARP generates a Type 4 PDU in which the tar-ttg field contains the NE TID value that existed prior to the change of TID or protocol address. Confirmation that other NEs successfully received the address change is not sent.

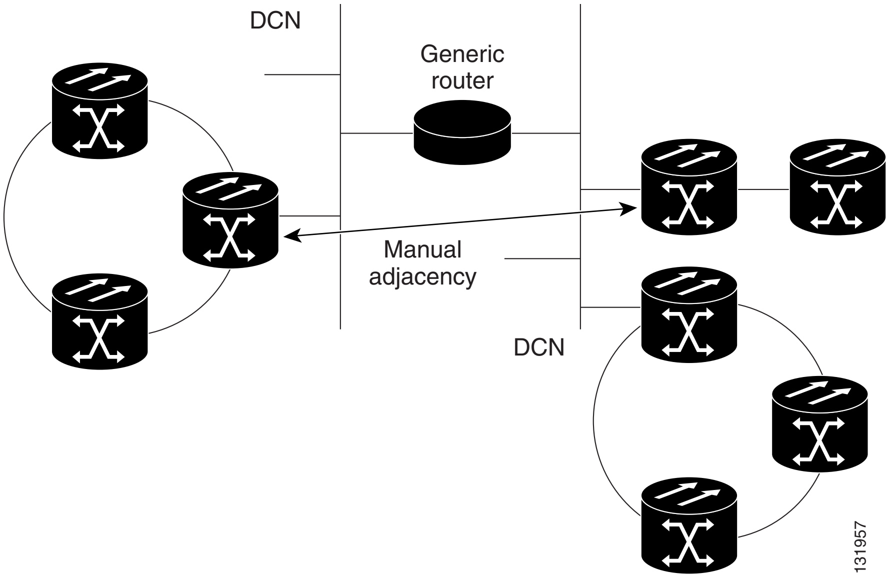
13.6.5.2 TARP Loop Detection Buffer

The TARP loop detection buffer (LDB) can be enabled to prevent duplicate TARP PDUs from entering the TDC. When a TARP Type 1, 2, or 4 PDU arrives, TARP checks its LDB for a NET address (tar-por) of the PDU originator match. If no match is found, TARP processes the PDU and assigns a tar-por, tar-seq (sequence) entry for the PDU to the LDB. If the tar-seq is zero, a timer associated with the LDB entry is started using the provisionable LDB entry timer on the node view OSI > TARP > Config tab. If a match exists, the tar-seq is compared to the LDB entry. If the tar-seq is not zero and is less than or equal to the LDB entry, the PDU is discarded. If the tar-seq is greater than the LDB entry, the PDU is processed and the tar-seq field in the LDB entry is updated with the new value. The Cisco ONS 15454 LDB holds approximately 500 entries. The LDB is flushed periodically based on the time set in the LDB Flush timer on the node view OSI > TARP > Config tab.

13.6.5.3 Manual TARP Adjacencies

TARP adjacencies can be manually provisioned in networks where ONS 15454s must communicate across routers or non-SONET NEs that lack TARP capability. In CTC, manual TARP adjacencies are provisioned on the node view Provisioning > OSI > TARP > MAT (Manual Area Table) subtab. The manual adjacency causes a TARP request to hop through the general router or non-SONET NE, as shown in Figure 13-23.

Figure 13-23 Manual TARP Adjacencies



13.6.5.4 Manual TID to NSAP Provisioning

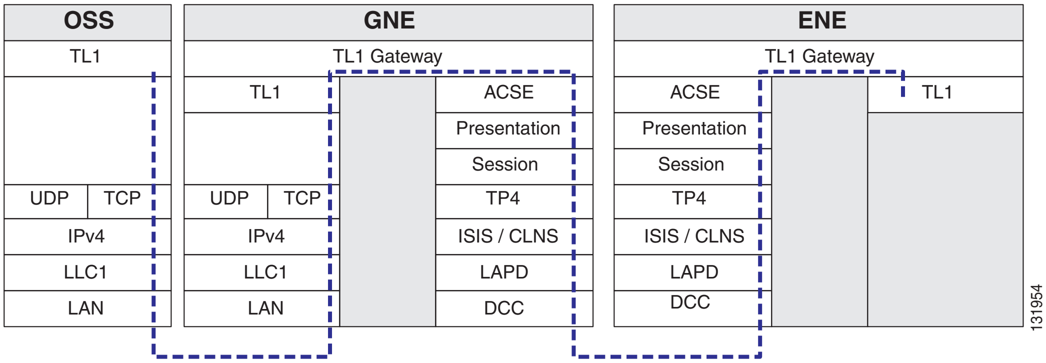
TIDs can be manually linked to NSAPs and added to the TDC. Static TDC entries are similar to static routes. For a specific TID, you force a specific NSAP. Resolution requests for that TID always return that NSAP. No TARP network propagation or instantaneous replies are involved. Static entries allow you to forward TL1 commands to NEs that do not support TARP. However, static TDC entries are not dynamically updated, so outdated entries are not removed after the TID or the NSAP changes on the target node.

13.6.6 TCP/IP and OSI Mediation

Two mediation processes facilitate TL1 networking and file transfers between NEs and ONS client computers running TCP/IP and OSI protocol suites:

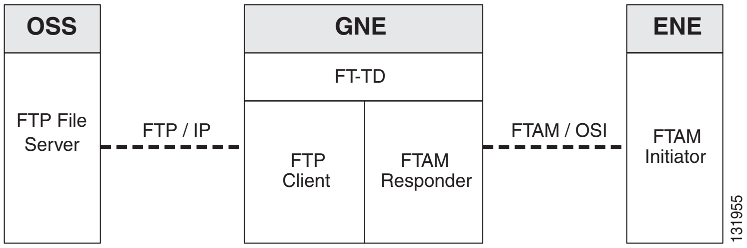
- T–TD—Performs a TL1-over-IP to TL1-over-OSI gateway mediation to enable an IP-based OSS to manage OSI-only NEs subtended from a GNE. Figure 13-24 shows the T–TD protocol flow.

Figure 13-24 T–TD Protocol Flow



- FT–TD—Performs an FTP conversion between FTAM and FTP. The FT–TD gateway entity includes an FTAM responder (server) and an FTP client, allowing FTAM initiators (clients) to store, retrieve, or delete files from an FTP server. The FT–TD gateway is unidirectional and is driven by the FTAM initiator. The FT–TD FTAM responder exchanges messages with the FTAM initiator over the full OSI stack. Figure 13-25 shows the FT–TD protocol flow.

Figure 13-25 FT–TD Protocol Flow



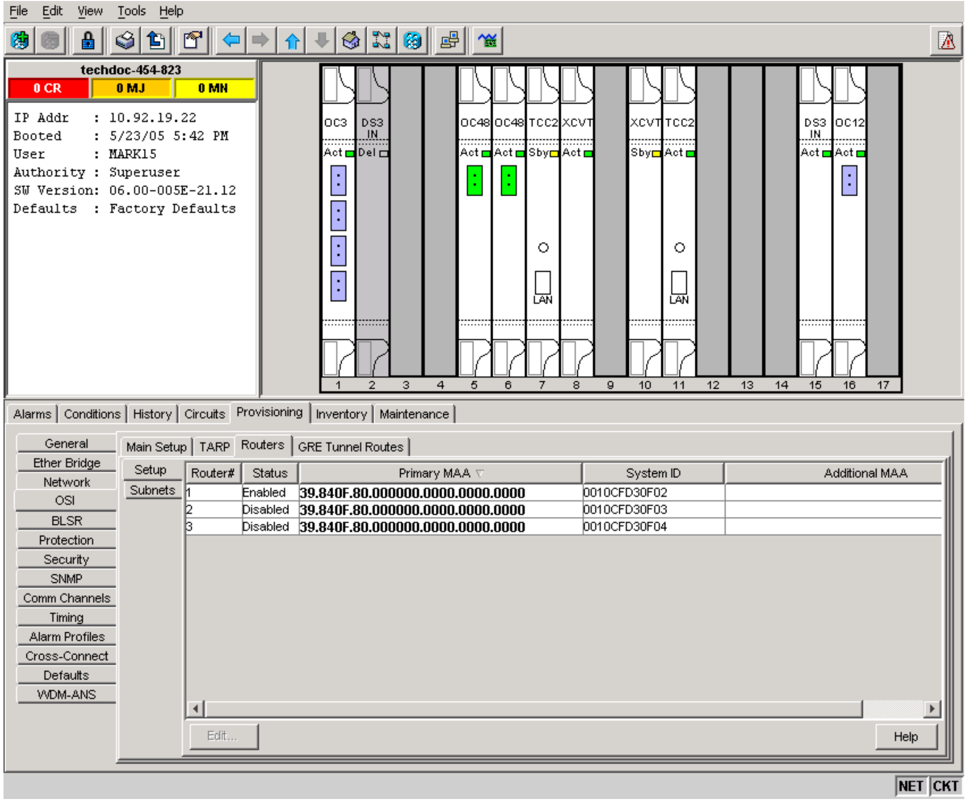
The ONS 15454 uses FT–TD for the following file transfer processes:

- Software downloads
- Database backups and restores
- Cisco IOS configuration backups and restores for ML and ML2 Series cards.

13.6.7 OSI Virtual Routers

The ONS 15454 supports three OSI virtual routers. The routers are provisioned on the Provisioning > OSI > Routers tab, shown in Figure 13-26.

Figure 13-26 Provisioning OSI Routers



techdoc-454-823

0 CR | 0 MJ | 0 MN

```
IP Addr   : 10.92.19.22
Booted    : 5/23/05 5:42 PM
User      : MARK15
Authority : Superuser
SW Version: 06.00-005E-21.12
Defaults  : Factory Defaults
```

Router#	Status	Primary MAA	System ID	Additional MAA
1	Enabled	39.840F.80.000000.0000.0000.0000	0010CFD30F02	
2	Disabled	39.840F.80.000000.0000.0000.0000	0010CFD30F03	
3	Disabled	39.840F.80.000000.0000.0000.0000	0010CFD30F04	

Each router has an editable manual area address and a unique NSAP System ID that is set to the node MAC address + *n*. For Router 1, *n* = 0. For Router 2, *n* = 1. For Router 3, *n* = 2. Each router can be enabled and connected to different OSI routing areas. However, Router 1 is the primary router, and it must be enabled before Router 2 and Router 3 can be enabled. The Router 1 manual area address and System ID create the NSAP address assigned to the node's TID. In addition, Router 1 supports OSI TARP, mediation, and tunneling functions that are not supported by Router 2 and Router 3. These include:

- TID-to-NSAP resolution
- TARP data cache
- IP-over-CLNS tunnels
- FTAM
- FT-TD
- T-TD
- LAN subnet

OSI virtual router constraints depend on the routing mode provisioned for the node. Table 13-13 shows the number of IS L1s, IS L1/L2s, and DCCs that are supported by each router. An IS Level1 and IS Level1/Level2 support one ES per DCC subnet and up to 100 ESs per LAN subnet.

Table 13-13 OSI Virtual Router Constraints

Routing Mode	Router 1	Router 2	Router 3	IS L1 per area	IS L1/L2 per area	DCC per IS
End System	Yes	No	No	—	—	—
IS L1	Yes	Yes	Yes	250	—	40
IS L1/L2	Yes	Yes	Yes	250	50	40

Each OSI virtual router has a primary manual area address. You can also create two additional manual area addresses. These manual area addresses can be used to:

- Split up an area—Nodes within a given area can accumulate to a point that they are difficult to manage, cause excessive traffic, or threaten to exceed the usable address space for an area. Additional manual area addresses can be assigned so that you can smoothly partition a network into separate areas without disrupting service.
- Merge areas—Use transitional area addresses to merge as many as three separate areas into a single area that shares a common area address.
- Change to a different address—You might need to change an area address for a particular group of nodes. Use multiple manual area addresses to allow incoming traffic intended for an old area address to continue being routed to associated nodes.

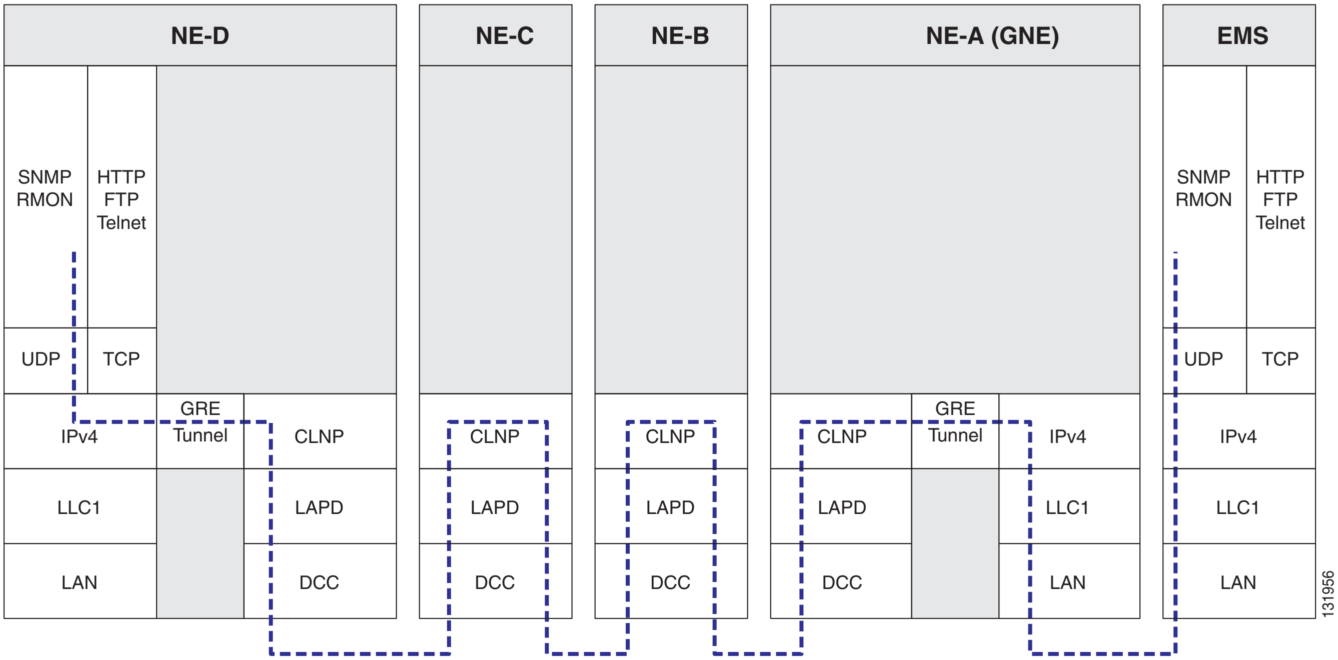
13.6.8 IP-over-CLNS Tunnels

IP-over-CLNS tunnels are used to encapsulate IP for transport across OSI NEs. The ONS 15454 supports two tunnel types:

- GRE—Generic Routing Encapsulation is a tunneling protocol that encapsulates one network layer for transport across another. GRE tunnels add both a CLNS header and a GRE header to the tunnel frames. GRE tunnels are supported by Cisco routers and some other vendor NEs.
- Cisco IP—The Cisco IP tunnel directly encapsulates the IP packet with no intermediate header. Cisco IP is supported by most Cisco routers.

Figure 13-24 shows the protocol flow when an IP-over-CLNS tunnel is created through four NEs (A, B, C, and D). The tunnel ends are configured on NEs A and D, which support both IP and OSI. NEs B and C only support OSI, so they only route the OSI packets.

Figure 13-27 IP-over-CLNS Tunnel Flow



13.6.8.1 Provisioning IP-over-CLNS Tunnels

IP-over-CLNS tunnels must be carefully planned to prevent nodes from losing visibility or connectivity. Before you begin a tunnel, verify that the tunnel type, either Cisco IP or GRE, is supported by the equipment at the other end. Always verify IP and NSAP addresses. Provisioning of IP-over-CLNS tunnels in CTC is performed on the node view Provisioning > OSI > IP over CLNS Tunnels tab. For procedures, refer to the “Turn Up a Node” chapter in the *Cisco ONS 15454 Procedure Guide*.

Provisioning IP-over-CLNS tunnels on Cisco routers requires the following prerequisite tasks, as well as other OSI provisioning:

- (Required) Enable IS-IS
- (Optional) Enable routing for an area on an interface
- (Optional) Assign multiple area addresses
- (Optional) Configure IS-IS interface parameters
- (Optional) Configure miscellaneous IS-IS parameters

The Cisco IOS commands used to create IP-over-CLNS tunnels (CTunnels) are shown in Table 13-14.

Table 13-14 IP-over-CLNS Tunnel IOS Commands

Step	Step	Purpose
1	Router (config) # **interface ctunnel** *interface-number*	Creates a virtual interface to transport IP over a CLNS tunnel and enters interface configuration mode. The interface number must be unique for each CTunnel interface.
2	Router (config-if # **ctunnel destination** *remote-nsap-address*	Configures the destination parameter for the CTunnel. Specifies the destination NSAP1 address of the CTunnel, where the IP packets are extracted.
3	Router (config-if) # **ip address** *ip-address mask*	Sets the primary or secondary IP address for an interface.

If you are provisioning an IP-over-CLNS tunnel on a Cisco router, always follow procedures provided in the Cisco IOS documentation for the router you are provisioning. For information about ISO CLNS provisioning including IP-over-CLNS tunnels, see the "Configuring ISO CLNS" chapter in the *Cisco IOS Apollo Domain, Banyon VINES, DECnet, ISO CLNS, and XNS Configuration Guide*.

13.6.8.2 IP-over-CLNS Tunnel Scenario 1: ONS Node to Other Vendor GNE

Figure 13-28 shows an IP-over-CLNS tunnel created from an ONS node to another vendor GNE. The other vendor NE has an IP connection to an IP DCN to which a CTC computer is attached. An OSI-only (LAP-D) SDCC and a GRE tunnel are created between the ONS NE 1 to the other vender GNE.

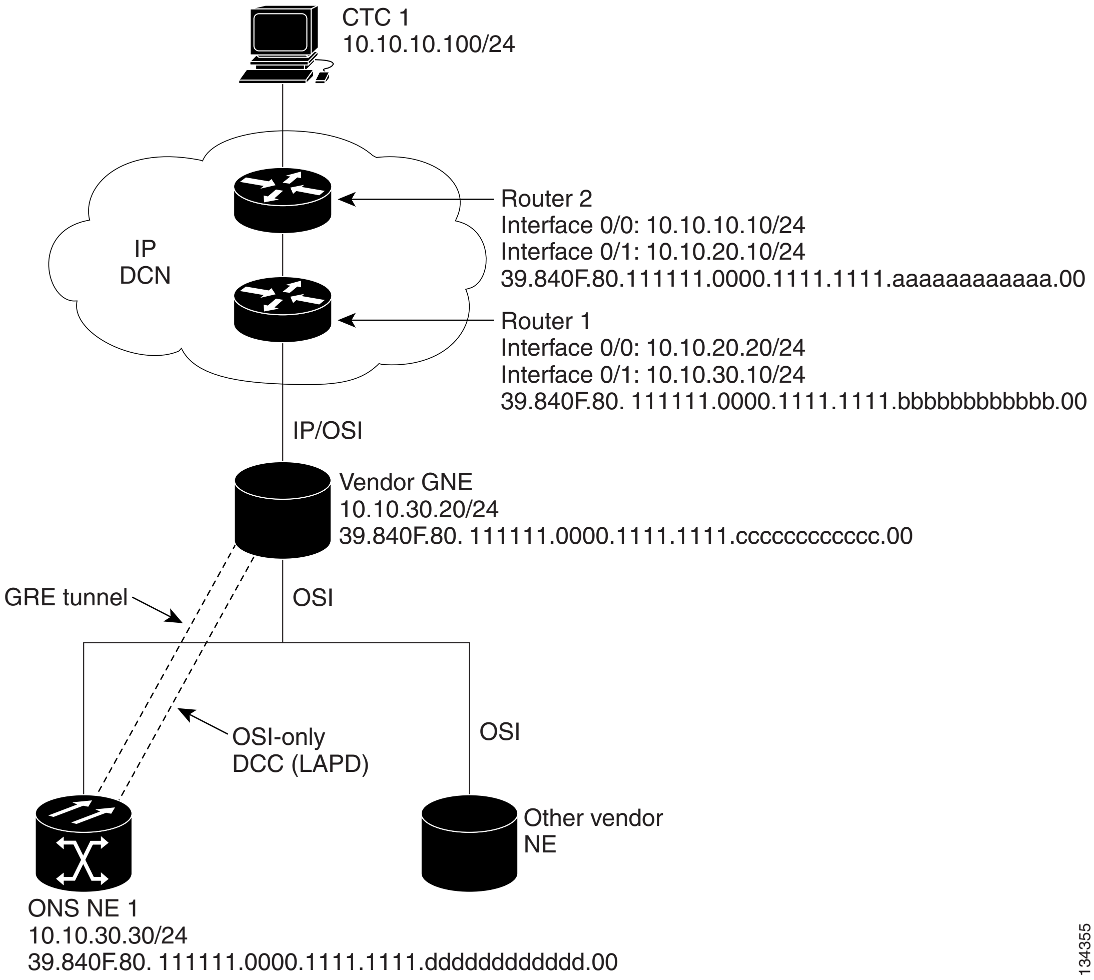
ONS NE 1 IP-over-CLNS tunnel provisioning information:

- Destination: 10.10.10.100 (CTC 1)
- Mask: 255.255.255.255 for host route (CTC 1 only), or 255.255.255.0 for subnet route (all CTC computers residing on the 10.10.10.0 subnet)
- NSAP: 39.840F.80.1111.0000.1111.1111.cccccccccccc.00 (other vendor GNE)
- Metric: 110
- Tunnel Type: GRE

Other vender GNE IP-over-CLNS tunnel provisioning information:

- Destination: 10.20.30.30 (ONS NE 1)
- Mask: 255.255.255.255 for host route (ONS NE 1 only), or 255.255.255.0 for subnet route (all ONS nodes residing on the 10.30.30.0 subnet)
- NSAP: 39.840F.80.1111.0000.1111.1111.dddddddddddd.00 (ONS NE 1)
- Metric: 110
- Tunnel Type: GRE

Figure 13-28 IP-over-CLNS Tunnel Scenario 1: ONS NE to Other Vender GNE


CTC 1
10.10.10.100/24
IP
DCN
Router 2
Interface 0/0: 10.10.10.10/24
Interface 0/1: 10.10.20.10/24
39.840F.80.111111.0000.1111.1111.aaaaaaaaaaaa.00
Router 1
Interface 0/0: 10.10.20.20/24
Interface 0/1: 10.10.30.10/24
39.840F.80. 111111.0000.1111.1111.bbbbbbbbbbbb.00
IP/OSI
Vendor GNE
10.10.30.20/24
39.840F.80. 111111.0000.1111.1111.cccccccccccc.00
GRE tunnel
OSI
OSI-only
DCC (LAPD)
OSI
Other vendor
NE
ONS NE 1
10.10.30.30/24
39.840F.80. 111111.0000.1111.1111.dddddddddddd.00
134355

13.6.8.3 IP-over-CLNS Tunnel Scenario 2: ONS Node to Router

Figure 13-29 shows an IP-over-CLNS tunnel from an ONS node to a router. The other vendor NE has an OSI connection to a router on an IP DCN, to which a CTC computer is attached. An OSI-only (LAP-D) SDCC is created between the ONS NE 1 and the other vender GNE. The OSI over IP tunnel can be either the Cisco IP tunnel or a GRE tunnel, depending on the tunnel types supported by the router.

ONS NE 1 IP-over-CLNS tunnel provisioning:

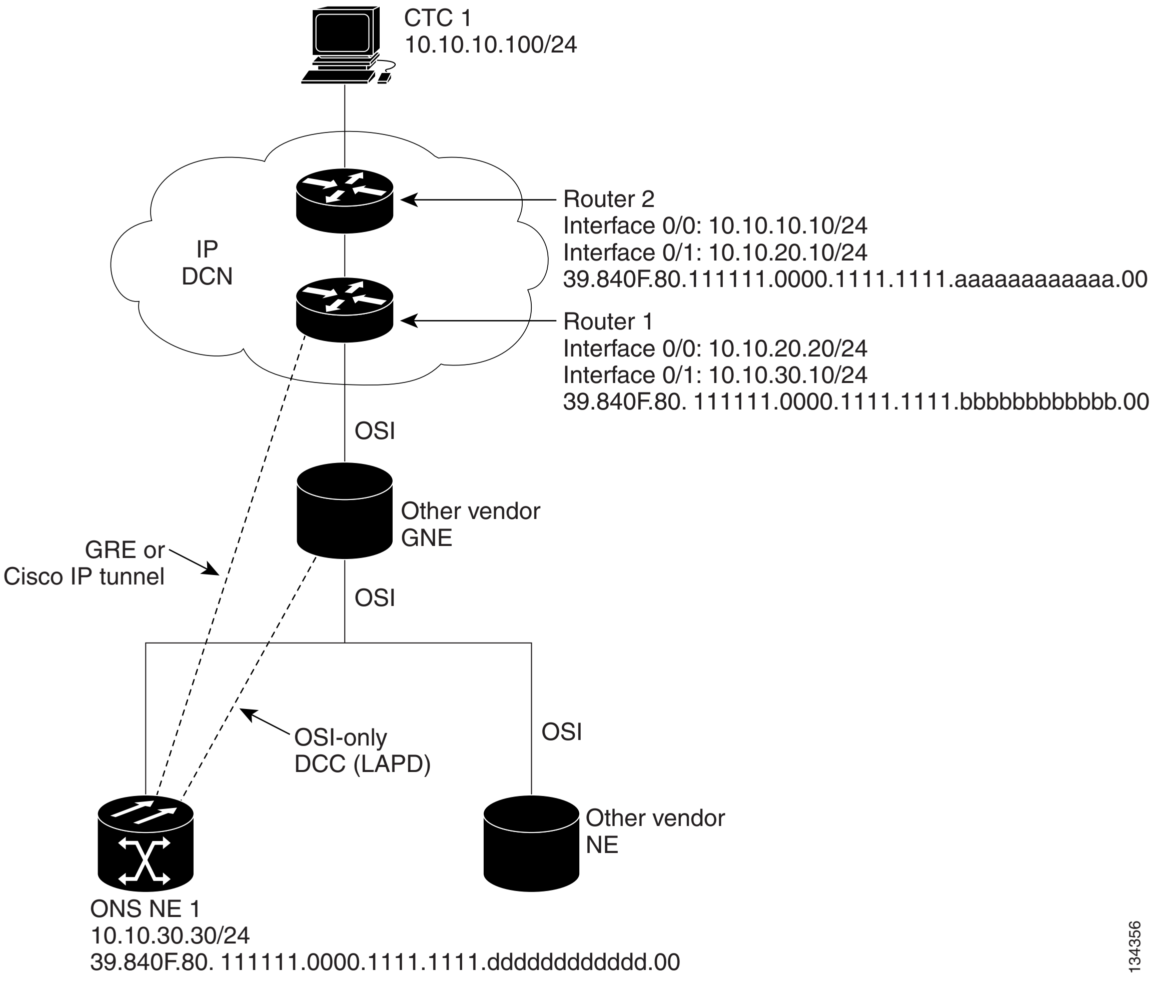
- Destination: 10.10.30.10 (Router 1, Interface 0/1)
- Mask: 255.255.255.255 for host route (Router 1 only), or 255.255.255.0 for subnet route (all routers on the same subnet)
- NSAP: 39.840F.80.1111.0000.1111.1111.bbbbbbbbbbbb.00 (Router 1)
- Metric: 110
- Tunnel Type: Cisco IP

Router 1 CTunnel (IP-over-CLNS) provisioning:

```
ip routing
```

```
clns routing
interface ctunnel 102
    ip address 10.10.30.30 255.255.255.0
    ctunnel destination 39.840F.80.1111.0000.1111.1111.dddddddddddd.00
interface Ethernet0/1
    clns router isis
router isis
    net 39.840F.80.1111.0000.1111.1111.bbbbbbbbbbbb.00
```

Figure 13-29 IP-over-CLNS Tunnel Scenario 2: ONS Node to Router


CTC 1
10.10.10.100/24
IP
DCN
Router 2
Interface 0/0: 10.10.10.10/24
Interface 0/1: 10.10.20.10/24
39.840F.80.111111.0000.1111.1111.aaaaaaaaaaaa.00
Router 1
Interface 0/0: 10.10.20.20/24
Interface 0/1: 10.10.30.10/24
39.840F.80. 111111.0000.1111.1111.bbbbbbbbbbbb.00
OSI
Other vendor
GNE
GRE or
Cisco IP tunnel
OSI
OSI-only
DCC (LAPD)
OSI
Other vendor
NE
ONS NE 1
10.10.30.30/24
39.840F.80. 111111.0000.1111.1111.dddddddddddd.00
134356

13.6.8.4 IP-over-CLNS Tunnel Scenario 3: ONS Node to Router Across an OSI DCN

Figure 13-30 shows an IP-over-CLNS tunnel from an ONS node to a router across an OSI DCN. The other vendor NE has an OSI connection to an IP DCN to which a CTC computer is attached. An OSI-only (LAP-D) SDCC is created between the ONS NE 1 and the other vender GNE. The OSI over IP tunnel can be either the Cisco IP tunnel or a GRE tunnel, depending on the tunnel types supported by the router.

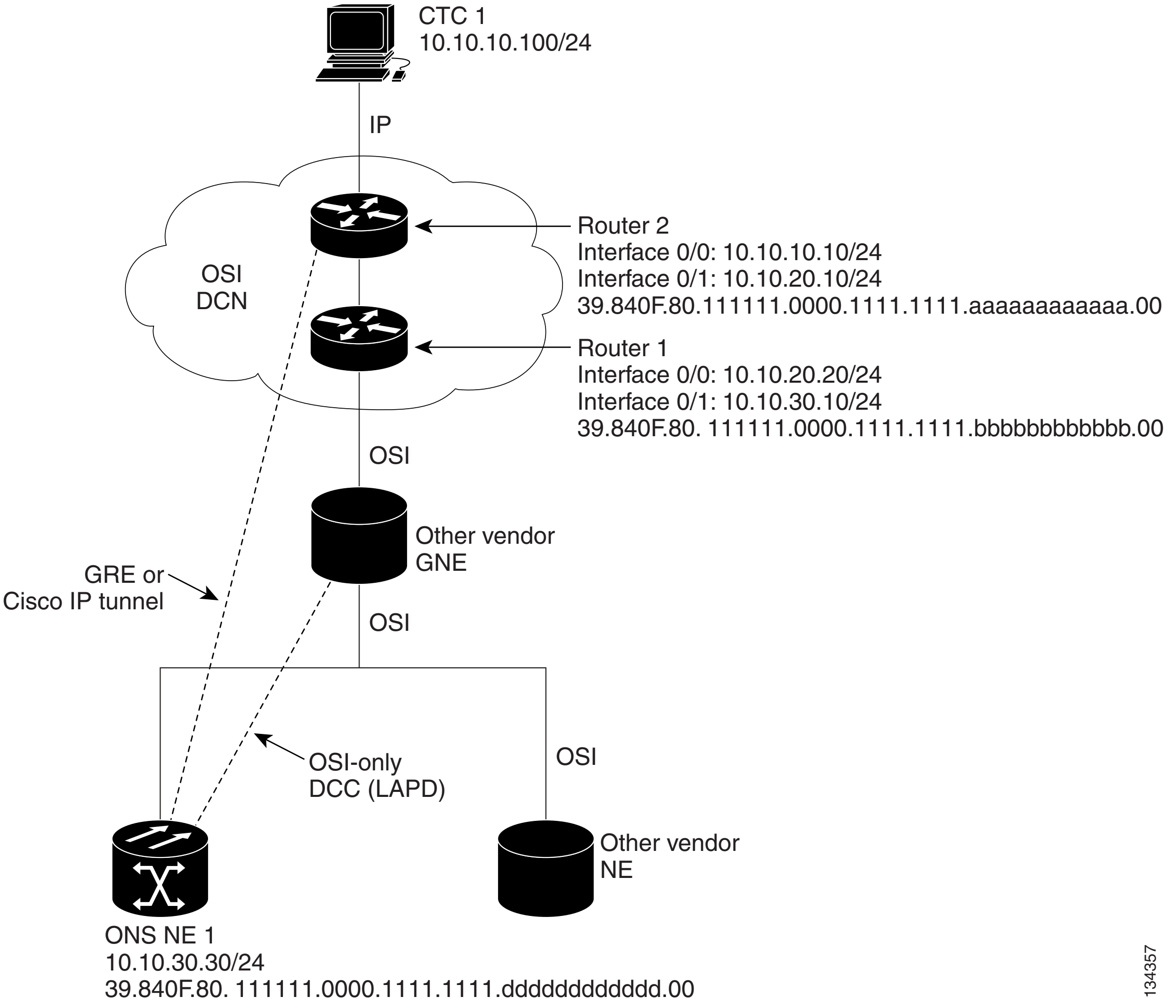
ONS NE 1 IP-over-CLNS tunnel provisioning:

- Destination: Router 2 IP address
- Mask: 255.255.255.255 for host route (CTC 1 only), or 255.255.255.0 for subnet route (all CTC computers on the same subnet)
- NSAP: Other vender GNE NSAP address
- Metric: 110
- Tunnel Type: Cisco IP

Router 2 IP-over-CLNS tunnel provisioning (sample Cisco IOS provisioning):

```
ip routing
clns routing
interface ctunnel 102
    ip address 10.10.30.30 255.255.255.0
    ctunnel destination 39.840F.80.1111.0000.1111.1111.dddddddddddd.00
interface Ethernet0/1
    clns router isis
router isis
    net 39.840F.80.1111.0000.1111.1111.aaaaaaaaaaaa.00
```

Figure 13-30 IP-over-CLNS Tunnel Scenario 3: ONS Node to Router Across an OSI DCN


CTC 1
10.10.10.100/24
IP
OSI
DCN
Router 2
Interface 0/0: 10.10.10.10/24
Interface 0/1: 10.10.20.10/24
39.840F.80.111111.0000.1111.1111.aaaaaaaaaaaa.00
Router 1
Interface 0/0: 10.10.20.20/24
Interface 0/1: 10.10.30.10/24
39.840F.80. 111111.0000.1111.1111.bbbbbbbbbbbb.00
OSI
Other vendor
GNE
GRE or
Cisco IP tunnel
OSI
OSI-only
DCC (LAPD)
OSI
Other vendor
NE
ONS NE 1
10.10.30.30/24
39.840F.80. 111111.0000.1111.1111.dddddddddddd.00
134357

13.6.9 OSI/IP Networking Scenarios

The following eight scenarios show examples of ONS 15454s in networks with OSI-based NEs. The scenarios show ONS 15454 nodes in a variety of roles. The scenarios assume the following:

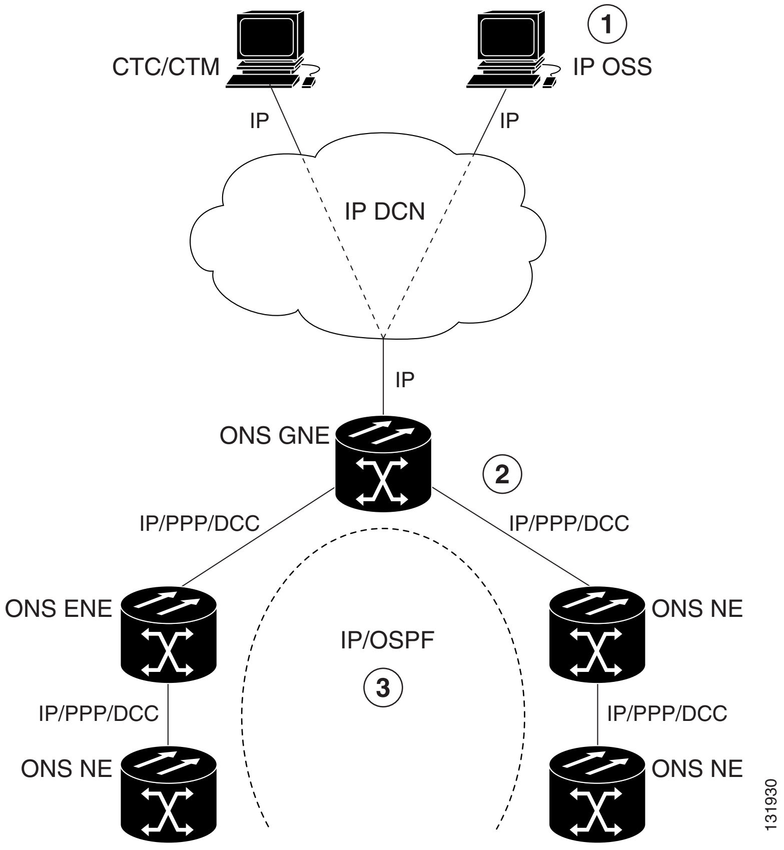
- ONS 15454 NEs are configured as dual OSI and IP nodes with both IP and NSAP addresses. They run both OSPF and OSI (IS-IS or ES-IS) routing protocols as “Ships-In-The-Night,” with no route redistribution.
- ONS 15454 NEs run TARP, which allows them to resolve a TL1 TID to a NSAP address. A TID might resolve to both an IP and an NSAP address when the destination TID is an ONS 15454 NE that has both IP and NSAP address.
- DCC links between ONS 15454 NEs and OSI-only NEs run the full OSI stack over LAP-D, which includes IS-IS, ES-IS, and TARP.
- DCC links between ONS 15454 NEs run the full OSI stack and IP (OSPF) over PPP.

- All ONS 15454 NEs participating in an OSI network run OSI over PPP between themselves. This is needed so that other vendor GNEs can route TL1 commands to all ONS 15454 NEs participating in the OSI network.

13.6.9.1 OSI/IP Scenario 1: IP OSS, IP DCN, ONS GNE, IP DCC, and ONS ENE

Figure 13-31 shows OSI/IP Scenario 1, the current ONS 15454 IP-based implementation, with an IP DCN, IP-over-PPP DCC, and OSPF routing.

Figure 13-31 OSI/IP Scenario 1: IP OSS, IP DCN, ONS GNE, IP DCC, and ONS ENE

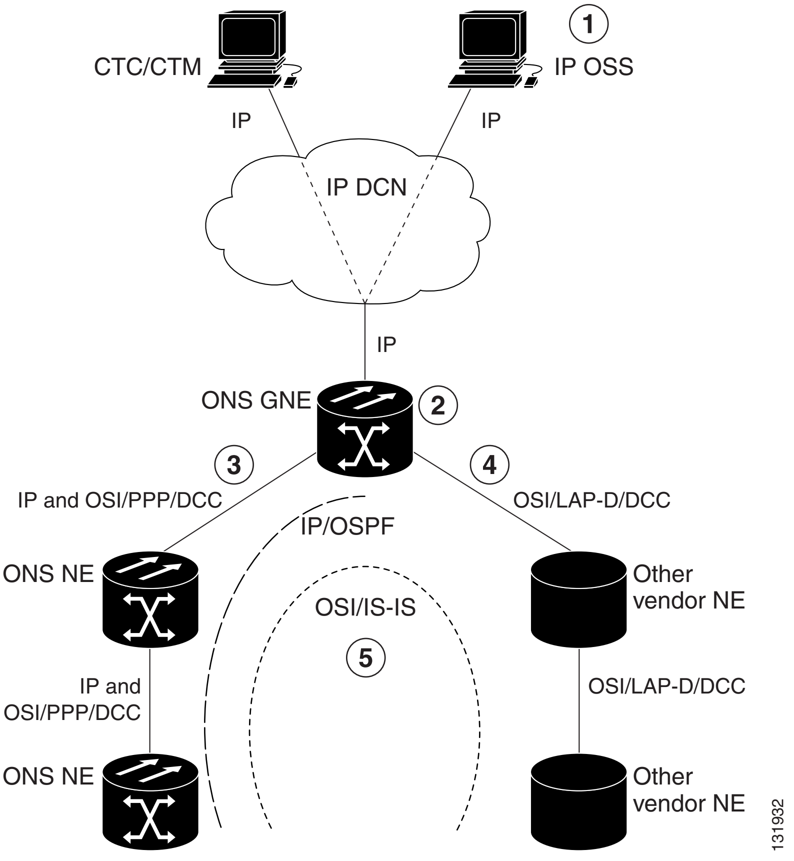


1	IP OSS manages ONS 15454 using TL1 and FTP.
2	DCCs carry IP over the PPP protocol.
3	The ONS 15454 network is managed by IP over OSPF.

13.6.9.2 OSI/IP Scenario 2: IP OSS, IP DCN, ONS GNE, OSI DCC, and Other Vendor ENE

OSI/IP Scenario 2 (Figure 13-32) shows an ONS 15454 GNE in a multivendor OSI network. Both the ONS 15454 GNE and the other vendor NEs are managed by an IP OSS using TL1 and FTP. The ONS 15454 is also managed by CTC and Cisco Transport Manager (CTM). Because the other vendor NE only supports TL1 and FTAM over the full OSI stack, the ONS 15454 GNE provides T–TD and FT–TD mediation to convert TL1/IP to TL1/OSI and FTAM/OSI to FTP/IP.

Figure 13-32 OSI/IP Scenario 2: IP OSS, IP DCN, ONS GNE, OSI DCC, and Other Vendor ENE



1	The IP OSS manages ONS 15454 and other vendor NEs using TL1 and FTP.
2	The ONS 15454 GNE performs mediation for other vendor NEs.
3	DCCs between the ONS 15454 GNE and ONS 15454 NEs are provisioned for IP and OSI over PPP.
4	DCCs between the ONS 15454 GNE and other vendor NEs are provisioned for OSI over LAP-D.
5	The ONS 15454 and the other vendor NE network include IP over OSPF and OSI over the IS-IS protocol.

The ONS 15454 GNE routes TL1 traffic to the correct NE by resolving the TL1 TID to either an IP or NSAP address. For TL1 traffic to other vendor NEs (OSI-only nodes), the TID is resolved to an NSAP address. The ONS 15454 GNE passes the TL1 to the mediation function, which encapsulates it over the full OSI stack and routes it to the destination using the IS-IS protocol.

For TL1 traffic to ONS 15454 NEs, the TID is resolved to both an IP and an NSAP address. The ONS 15454 GNE follows the current TL1 processing model and forwards the request to the destination NE using the TCP/IP stack and OSPF routing.

OSS-initiated software downloads consist of two parts: the OSS to destination NE TL1 download request and the file transfer. The TL1 request is handled the same as described in the previous paragraph. The ONS 15454 NEs use FTP for file transfers. OSI-only NEs use FTAM to perform file transfers. The FTAM protocol is carried over OSI between the OSI NE and the ONS 15454 GNE. The GNE mediation translates between FTAM to FTP.

13.6.9.3 OSI/IP Scenario 3: IP OSS, IP DCN, Other Vendor GNE, OSI DCC, and ONS ENE

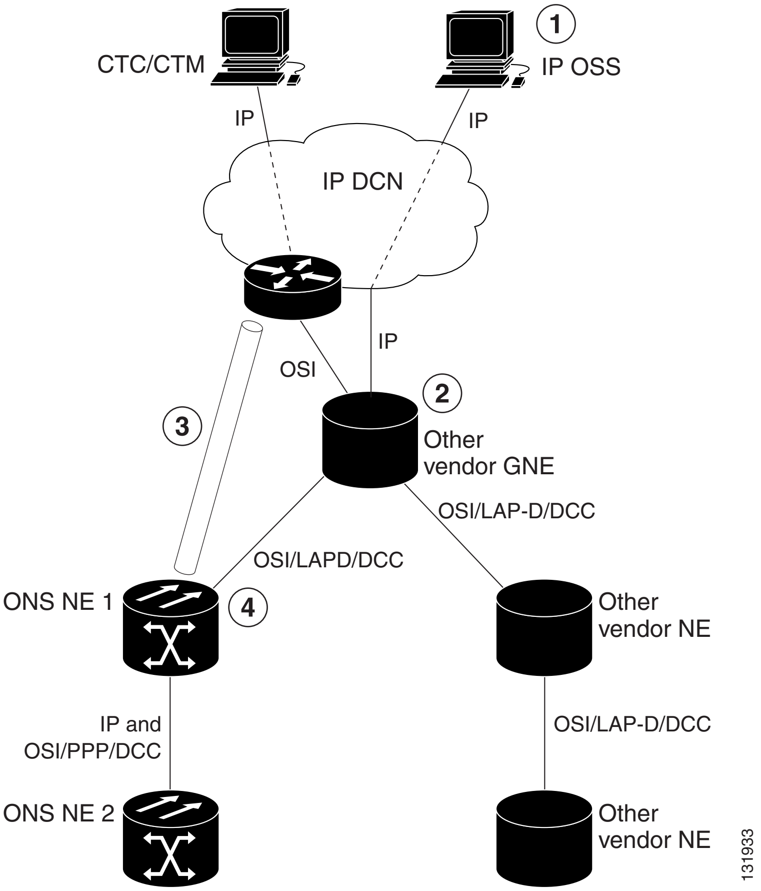
In OSI/IP Scenario 3 (Figure 13-33), all TL1 traffic between the OSS and GNE is exchanged over the IP DCN. TL1 traffic targeted for the GNE is processed locally. All other TL1 traffic is forwarded to the OSI stack, which performs IP-to-OSI TL1 translation. The TL1 is encapsulated in the full OSI stack and sent to the target NE over the DCC. The GNE can route to any node within the IS-IS domain because all NEs, ONS 15454 and non-ONS 15454, have NSAP addresses and support IS-IS routing.

TL1 traffic received by an ONS 15454 NE and not addressed to its NSAP address is forwarded by IS-IS routing to the correct destination. TL1 traffic received by an ONS 15454 NE and addressed to its NSAP is sent up the OSI stack to the mediation function, which extracts the TL1 and passes it to the ONS 15454 TL1 processor.

An OSS initiated software download includes the OSS-to-destination node TL1 download request and the file transfer. The TL1 request is handled as described in the previous paragraph. The target node uses FTAM for file transfers because the GNE does not support IP on the DCC and cannot forward FTP. The ONS 15454 NEs therefore must support an FTAM client and initiate file transfer using FTAM when subtended to an OSI GNE.

In this scenario, the GNE has both IP and OSI DCN connections. The GNE only supports TL1 and FTP over IP. Both are translated and then carried over OSI to the destination ENE (ONS 15454 or OSI-only NE). All other IP traffic is discarded by the GNE. The CTC/CTM IP traffic is carried over an IP-over-OSI tunnel to an ONS 15454 NE. The tunnel is created between an external router and an ONS 15454 NE. The traffic is sent to the ONS 15454 terminating the tunnel. That ONS 15454 then forwards the traffic over the tunnel to CTC/CTM by way of the external router.

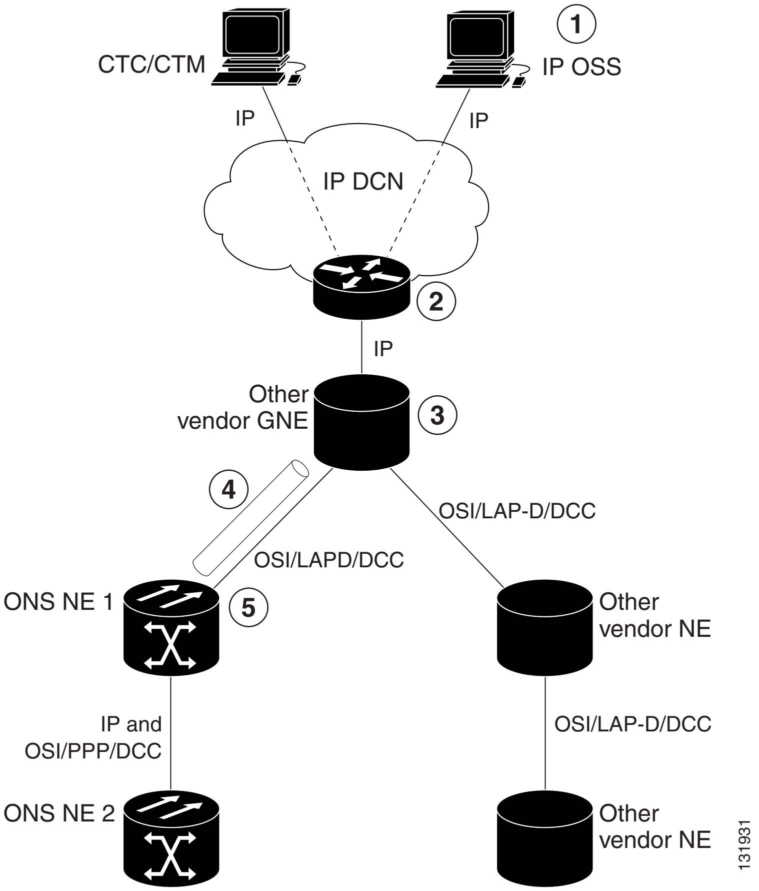
Figure 13-33 OSI/IP Scenario 3: IP OSS, IP DCN, Other Vendor GNE, OSI DCC, and ONS ENE



1	The IP OSS manages the ONS 15454 and other vendor NEs using TL1 and FTP.
2	The other vendor GNE performs mediation for TL1 and FTP, so the DCCs to the ONS 15454 and other vendor NEs are OSI-only.
3	CTC/CTM communicates with ONS 15454 NEs over a IP-over-CLNS tunnel. The tunnel is created from the ONS 15454 node to the external router.
4	The ONS 15454 NE exchanges TL1 over the full OSI stack using FTAM for file transfer.

Figure 13-34 shows the same scenario, except the IP-over-CLNS tunnel endpoint is the GNE rather than the DCN router.

Figure 13-34 OSI/IP Scenario 3 with OSI/IP-over-CLNS Tunnel Endpoint at the GNE

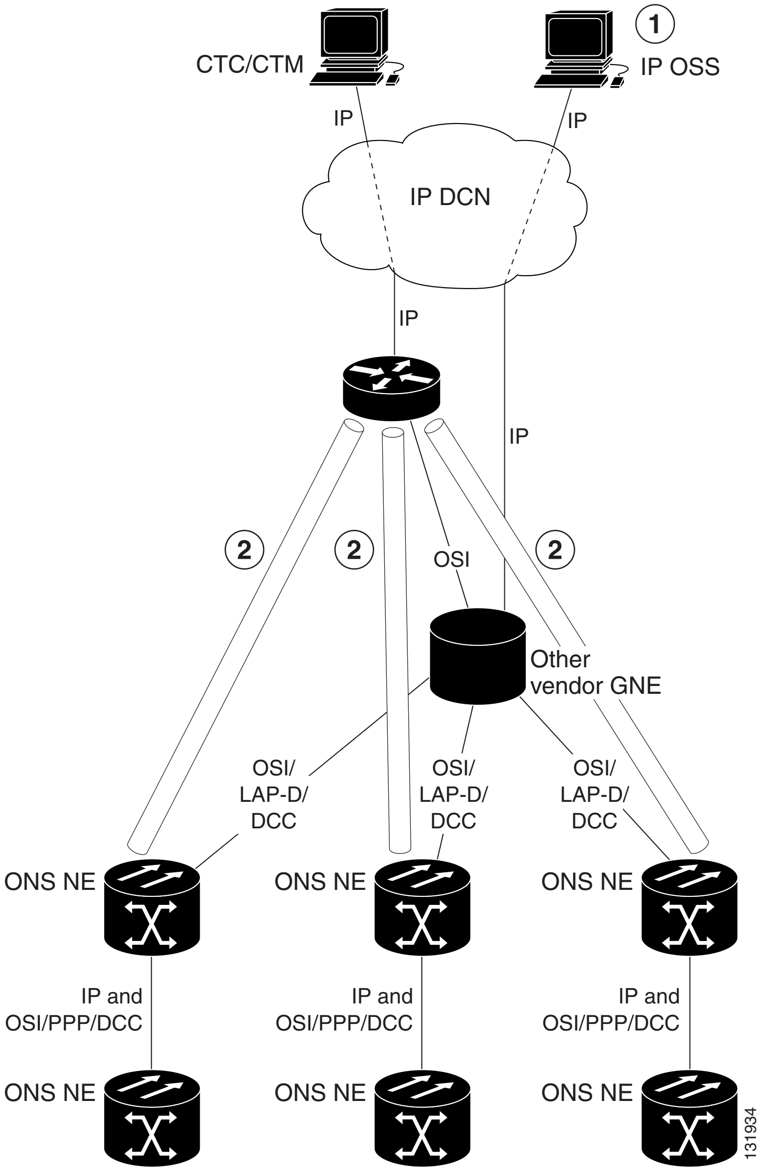


1	The IP OSS manages ONS and other vendor NEs using TL1 and FTP.
2	The router routes requests to the other vender GNE.
3	The other vendor GNE performs mediation for TL1 and FTP, so the DCCs to ONS 15454 and other vendor NEs are OSI-only.
4	CTC/CTM communicates with ONS 15454 NEs over an IP-over-CLNS tunnel between the ONS 15454 and the GNE.
5	ONS 15454 NEs exchange TL1 over the full OSI stack. FTAM is used for file transfer.

13.6.9.4 OSI/IP Scenario 4: Multiple ONS DCC Areas

OSI/IP Scenario 4 (Figure 13-35) is similar to OSI/IP Scenario 3 except that the OSI GNE is subtended by multiple isolated ONS 15454 areas. A separate IP-over-CLNS tunnel is required to each isolated ONS 15454 OSPF area. An alternate approach is to create a single IP-over-CLNS tunnel from CTC/CTM to an ONS 15454 NE, and then to configure a tunnel from that NE to an NE in each isolated OSPF area. This approach requires additional static routes.

Figure 13-35 OSI/IP Scenario 4: Multiple ONS DCC Areas

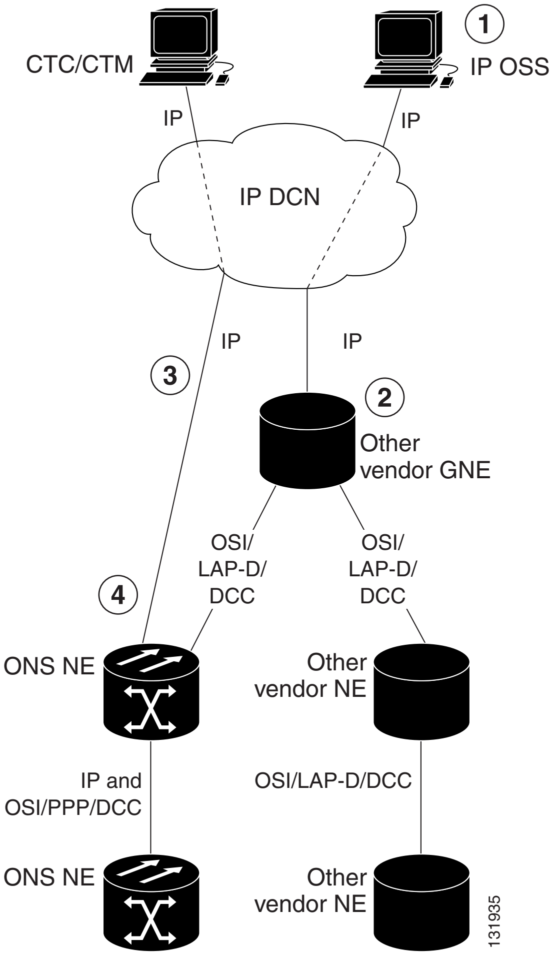


1	The IP OSS manages ONS 15454 and other vendor NEs using TL1 and FTP.
2	A separate tunnel is created for each isolated ONS 15454 DCC area.

13.6.9.5 OSI/IP Scenario 5: GNE Without an OSI DCC Connection

OSI/IP Scenario 5 (Figure 13-36) is similar to OSI/IP Scenario 3 except that the OSI GNE only has an IP connection to the DCN. It does not have an OSI DCN connection to carry CTC/CTM IP traffic through an IP-over-OSI tunnel. A separate DCN to ONS 15454 NE connection is created to provide CTC/CTM access.

Figure 13-36 OSI/IP Scenario 5: GNE Without an OSI DCC Connection

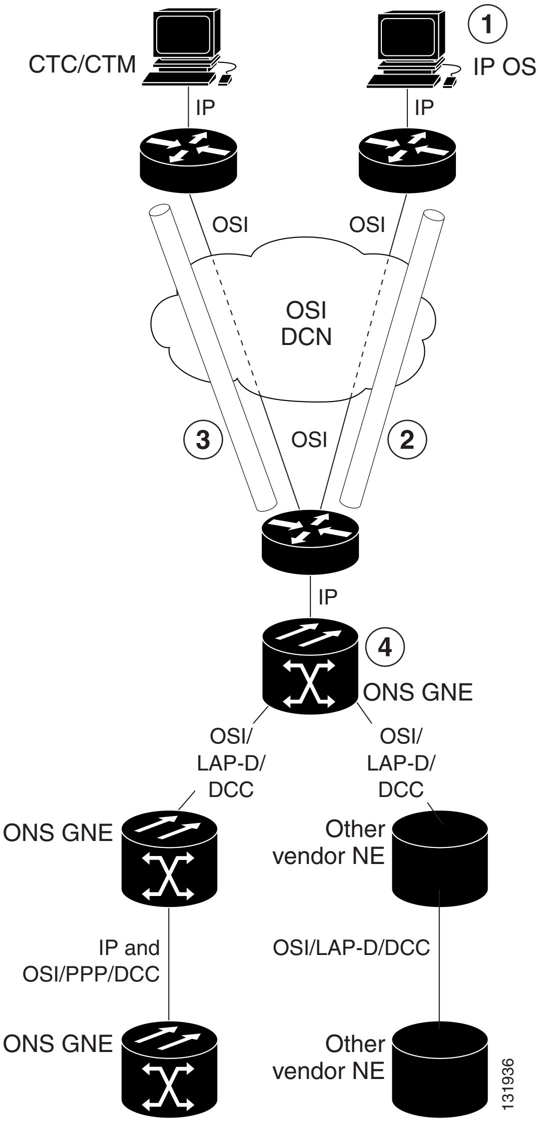


1	The IP OSS manages ONS 15454 and other vendor NEs using TL1 and FTP.
2	The other vendor GNE performs mediation on TL1 and FTP, so DCCs are OSI-only.
3	CTC/CTM communicates with ONS 15454 NEs over a separate IP DCN connection.
4	ONS 15454 NE exchanges TL1 over the full OSI stack. FTAM is used for file transfers.

13.6.9.6 OSI/IP Scenario 6: IP OSS, OSI DCN, ONS GNE, OSI DCC, and Other Vendor ENE

OSI/IP Scenario 6 (Figure 13-37) shows how the ONS 15454 supports OSI DCNs. The OSI DCN has no impact on the ONS 15454 because all IP traffic (CTC/CTM, FTP, and TL1) is tunneled through the OSI DCN.

Figure 13-37 OSI/IP Scenario 6: IP OSS, OSI DCN, ONS GNE, OSI DCC, and Other Vendor ENE

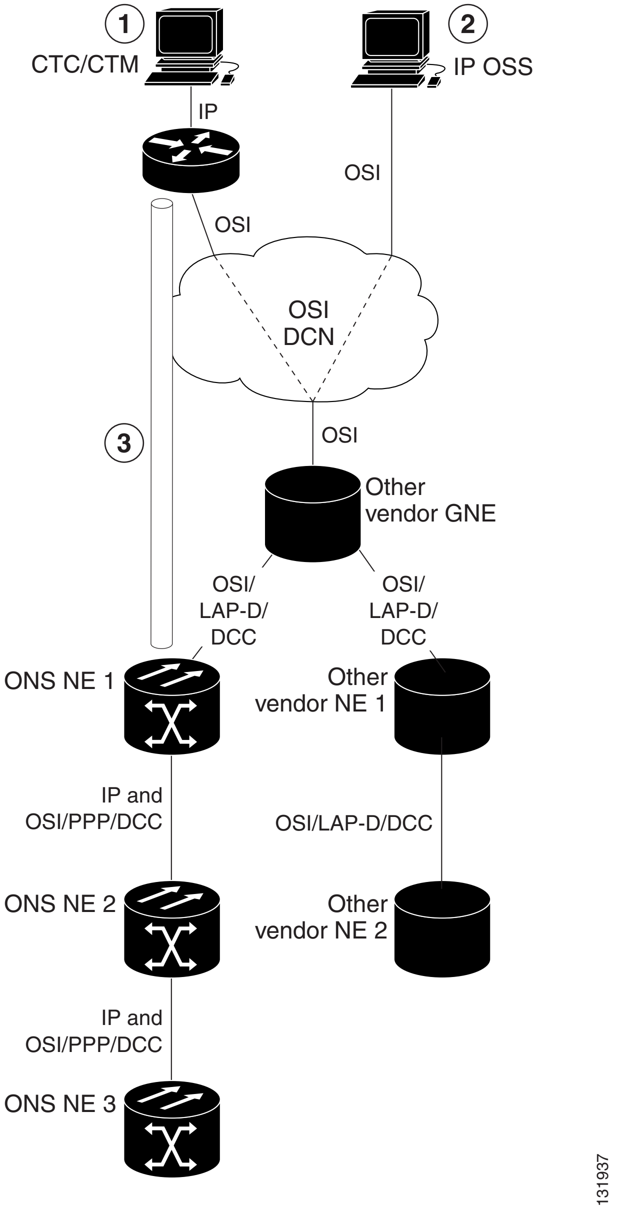


1	The IP OSS manages ONS 15454 and other vendor NEs using TL1 and FTP.
2	OSS IP traffic is tunneled through the DCN to the ONS 15454 GNE.
3	CTC/CTM IP traffic is tunneled through the DCN to the ONS 15454 GNE.
4	The GNE performs mediation for other vendor NEs.

13.6.9.7 OSI/IP Scenario 7: OSI OSS, OSI DCN, Other Vender GNE, OSI DCC, and ONS NEs

OSI/IP Scenario 7 (Figure 13-38) shows an example of a European network.

Figure 13-38 OSI/IP Scenario 7: OSI OSS, OSI DCN, Other Vender GNE, OSI DCC, and ONS NEs



1	ONS 15454 NEs are managed by CTC/CTM only (TL1/FTP is not used).
2	The OSI OSS manages other vendor NEs only.
3	CTC/CTM communicates with the ONS 15454 over a IP-over-CLNS tunnel between the ONS 15454 NE and external router.

In European networks:

- CTC and CTM are used for management only.
- IP-over-CLNS tunnels are widely accepted and deployed.

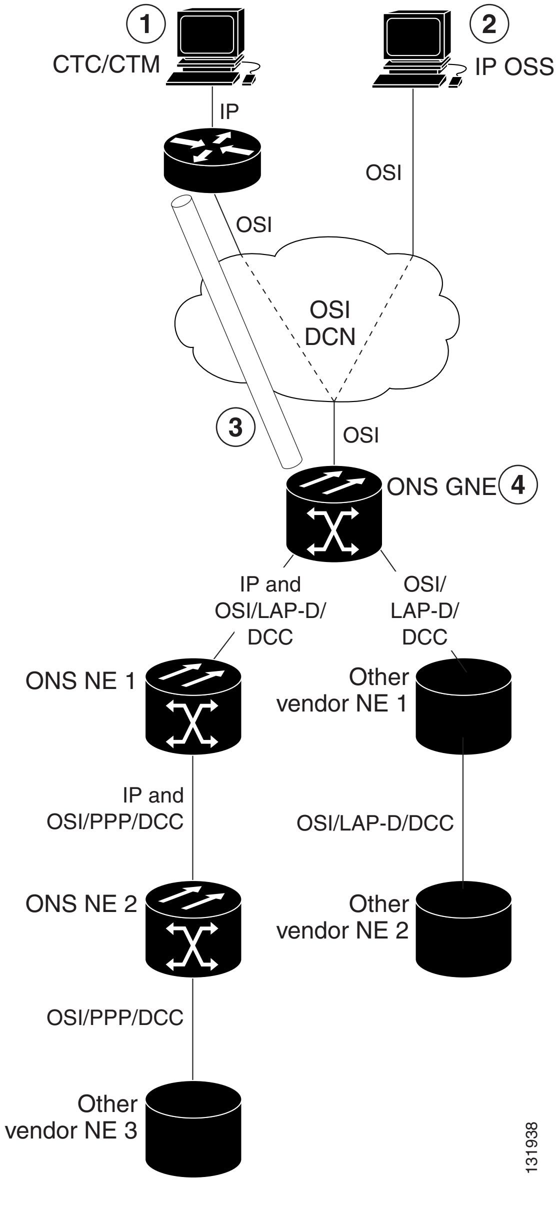
- TL1 management is not required.
- FTP file transfer is not required.
- TL1 and FTAM to FTP mediation is not required.

Management traffic between CTC/CTM and ONS 15454 NEs is carried over an IP-over-CLNS tunnel. A static route is configured on the ONS 15454 that terminates the tunnel (ONS 15454 NE 1) so that downstream ONS 15454 NEs (ONS 15454 NE 2 and 3) know how to reach CTC/CTM.

13.6.9.8 OSI/IP Scenario 8: OSI OSS, OSI DCN, ONS GNE, OSI DCC, and Other Vender NEs

OSI/IP Scenario 8 (Figure 13-39) is another example of a European network. Similar to OSI/IP Scenario 7, the ONS 15454 NEs are solely managed by CTC/CTM. The CTC/CTM IP traffic is carried over a IP-over-OSI tunnel between an external router and the ONS 15454 GNE. The GNE extracts the IP from the tunnel and forwards it to the destination ONS 15454. Management traffic between the OSS and other vendor NEs is routed by the ONS 15454 GNE and NEs. This is possible because all ONS 15454 NEs run dual stacks (OSI and IP).

Figure 13-39 OSI/IP Scenario 8: OSI OSS, OSI DCN, ONS GNE, OSI DCC, and Other Vender NEs



1	The ONS NEs are managed by CTC/CTM only (TL1/FTP is not used).
2	The OSI OSS manages other vendor NEs only.
3	CTC/CTM communicates with the ONS 15454 over an IP-over-CLNS tunnel between the ONS 15454 NE and the external router. A static route is needed on the GNE.
4	The ONS 15454 GNE routes OSI traffic to other vendor NEs. No IP-over-CLNS tunnel is needed.

13.6.10 Provisioning OSI in CTC

Table 13-15 shows the OSI actions that are performed from the node view Provisioning tab. Refer to the *Cisco ONS 15454 Procedure Guide* for OSI procedures and tasks.

Table 13-15 OSI Actions from the CTC Provisioning Tab

Tab	Actions
OSI > Main Setup	• View and edit Primary Area Address. • Change OSI routing mode. • Change LSP buffers.
OSI > TARP > Config	Configure the TARP parameters: • PDU L1/L2 propagation and origination. • TARP data cache and loop detection buffer. • LAN storm suppression. • Type 4 PDU on startup. • TARP timers: LDB, T1, T2, T3, T4.
OSI > TARP > Static TDC	Add and delete static TARP data cache entries.
OSI > TARP > MAT	Add and delete static manual area table entries.
OSI > Routers > Setup	• Enable and disable routers. • Add, delete, and edit manual area addresses.
OSI > Routers > Subnets	Edit SDCC, LDCC, and LAN subnets that are provisioned for OSI.
OSI > Tunnels	Add, delete, and edit Cisco and IP-over-CLNS tunnels.
Comm Channels > SDCC	• Add OSI configuration to an SDCC. • Choose the data link layer protocol, PPP or LAP-D.
Comm Channels > LDCC	• Add OSI configuration to an SDCC.

Table 13-16 shows the OSI actions that are performed from the node view Maintenance tab.

Table 13-16 OSI Actions from the CTC Maintenance Tab

Tab	Actions
OSI > ISIS RIB	View the IS-IS routing table.
OSI > ESIS RIB	View ESs that are attached to ISs.
OSI > TDC	• View the TARP data cache and identify static and dynamic entries. • Perform TID to NSAP resolutions. • Flush the TDC.

13.7 IPv6 Network Compatibility

Cisco ONS 15xxx products can function in an IPv6 network when an internet router that supports Network Address Translation - Protocol Translation (NAT-PT) is positioned between the GNE, such as an ONS 15454, and the client workstation. NAT-PT is defined in RFC-2766. IPv4 and IPv6 nodes communicate with each other using NAT-PT by allowing both IPv6 and IPv4 stacks to interface between the IPv6 DCN and the IPv4 DCC networks.

NAT-PT binds addresses in IPv6 networks with addresses in IPv4 networks and vice versa to provide transparent routing for the packets traveling between address types. This requires no changes to end nodes and IP packet routing is completely transparent to end nodes. It does, however, require NAT-PT to track the sessions it supports and mandates that inbound and outbound datagrams pertaining to a session traverse the same NAT-PT router. Protocol translation is used to extend address translation with protocol syntax/semantics translation.

Note Only Mozilla 1.7 is supported on clients interfacing with IPv6 networks.

13.8 FTP Support for ENE Database Backup

The Cisco ONS 15454 provides FTP database backup and restore download to ENEs when proxy/firewall is enabled. This feature allows you to provision a list of legal FTP hosts in CTC, that can be used with TL1 commands to perform database backup/restore or software download. The FTP hosts can be provisioned to elapse after a specified time interval with the enable FTP relay function.

Once FTP host are provisioned, and FTP Relay is enabled, TL1 users can then use the COPY-RFILE command to perform database backup/restore or software download to and from this list of legal FTP hosts that are provisioned to ENEs. Also, TL1 supports TID to IP address translation for the GNE TID that is specified in the FTP URL of COPY-RFILE and COPY-IOSCFG commands.

Using the FTP Host provisioning feature in CTC and TL1 you can configure up to 12 valid FTP hosts.

ENEs are allowed access through the firewall according to the time configured in the FTP Relay Timer in CTC or TL1. The time interval is 1 to 60 minutes, and once the timer elapses, all FTP access to the FTP host is blocked again. A time of 0 disallows ENE access to FTP commands through the firewall.

When the firewall is not enabled (Proxy only), all FTP operations to the ENE will be allowed – software download, database backup/restore and IOS config file backup/restore. All FTP operations to the ENEs will be blocked when firewall is enabled.