CTC Network Connectivity

This chapter provides eight scenarios showing Cisco ONS 15327s in common IP network configurations. The chapter does not provide a comprehensive explanation of IP networking concepts and procedures. For IP set up instructions, refer to the *Cisco ONS 15327 Procedure Guide*.

Chapter topics include:

Note To connect ONS 15327s to an IP network, you must work with a LAN administrator or other individual at your site who has IP networking training and experience.

8.1 IP Networking Overview

ONS 15327s 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 ONS 15327 login node groups, which allow you to provision non-data communications channel (DCC) connected nodes in a 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 15327 to serve as a gateway for ONS 15327s that are not connected to the LAN.
- You can create static routes to enable connections among multiple Cisco Transport Controller (CTC) sessions with ONS 15327s that reside on the same subnet with multiple CTC sessions.
- If ONS 15327s are connected to Open Shortest Path First (OSPF) networks, ONS 15327 network information is automatically communicated across multiple LANs and WANs.
- The ONS 15327 proxy server controls the visibility and accessibility between CTC computers and ONS 15327 element nodes.

8.2 IP Addressing Scenarios

ONS 15327 IP addressing generally has eight common scenarios or configurations. Use the scenarios as building blocks for more complex network configurations. Table 8-1 provides a general list of items to check when setting up ONS 15327s in IP networks.

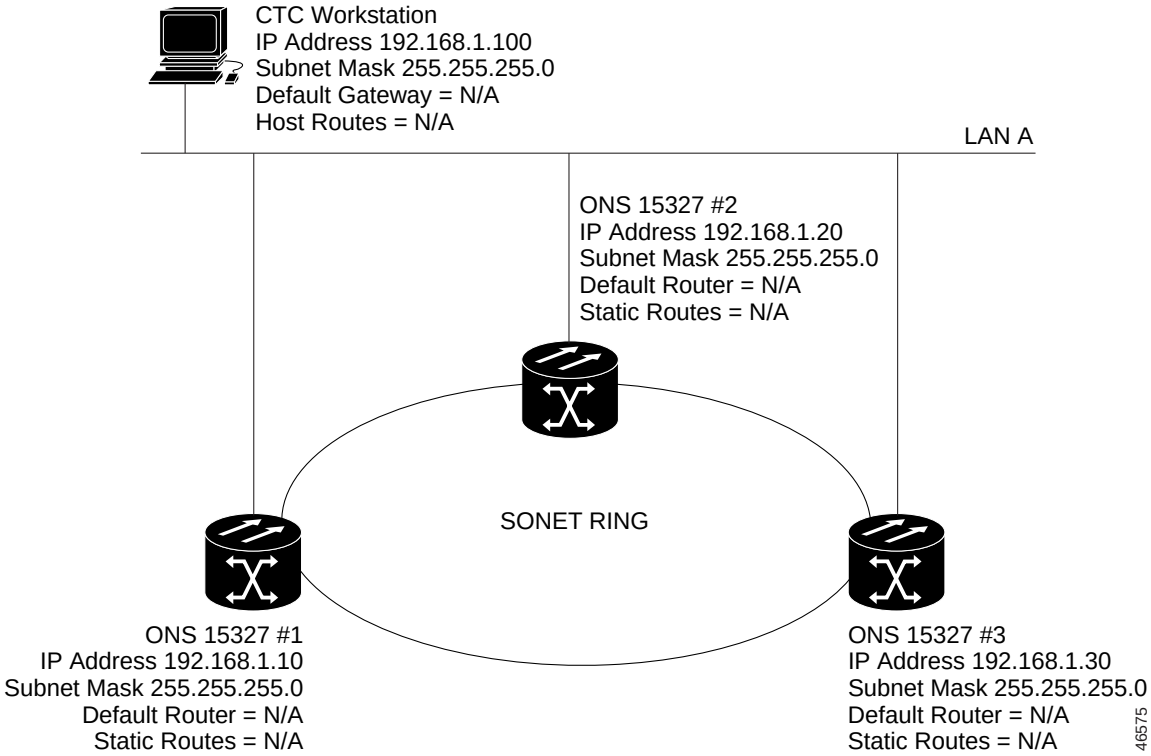
Table 8-1 General ONS 15327 IP Troubleshooting Checklist

Item	What to Check
Link integrity	Verify that link integrity exists between: • The CTC computer and network hub/switch. • ONS 15327s (wire-wrap pins or RJ-45 port) and network hub/switch. • Router ports and hub/switch ports.
ONS 15327 hub/switch ports	Verify connectivity. If connectivity problems occur, set the hub or switch port that is connected to the ONS 15327 to 10 Mbps half-duplex.
Ping	Ping the node to test connections between computers and ONS 15327s.
IP addresses/subnet masks	Verify that ONS 15327 IP addresses and subnet masks are set up correctly.
Optical connectivity	Verify that ONS 15327 optical trunk ports are in service and that a DCC is enabled on each trunk port.

8.2.1 Scenario 1: CTC and ONS 15327s on the Same Subnet

Scenario 1 shows a basic ONS 15327 LAN configuration (Figure 8-1). The ONS 15327s and CTC computer reside on the same subnet. All ONS 15327s connect to LAN A, and all ONS 15327s have DCC connections.

Figure 8-1 Scenario 1: CTC and ONS 15327s on the Same Subnet

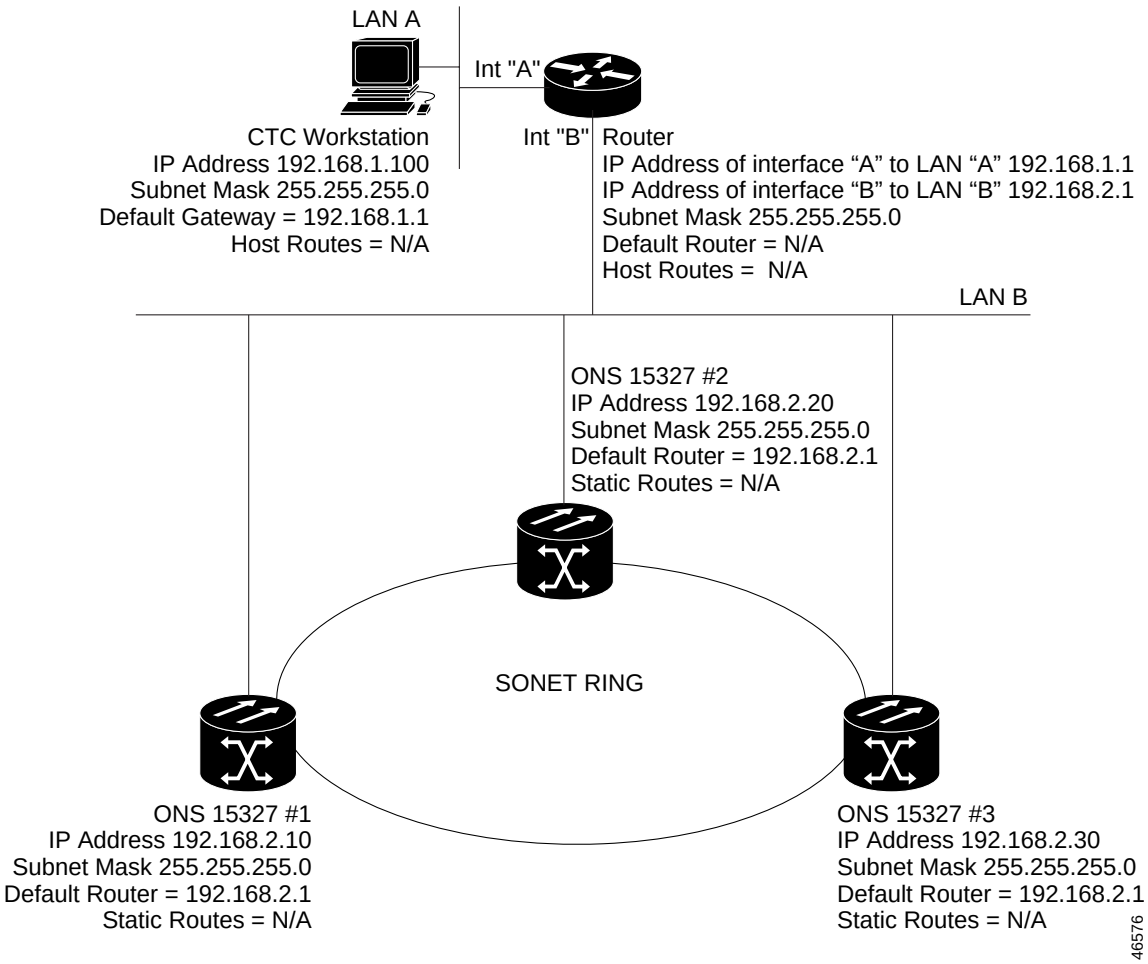


8.2.2 Scenario 2: CTC and ONS 15327s Connected to a Router

In Scenario 2 the CTC computer resides on a subnet (192.168.1.0) and attaches to LAN A (Figure 8-2). The ONS 15327s 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 Figure 8-2, a DHCP server is not available.

Figure 8-2 Scenario 2: CTC and ONS 15327s Connected to Router



8.2.3 Scenario 3: Using Proxy ARP to Enable an ONS 15327 Gateway

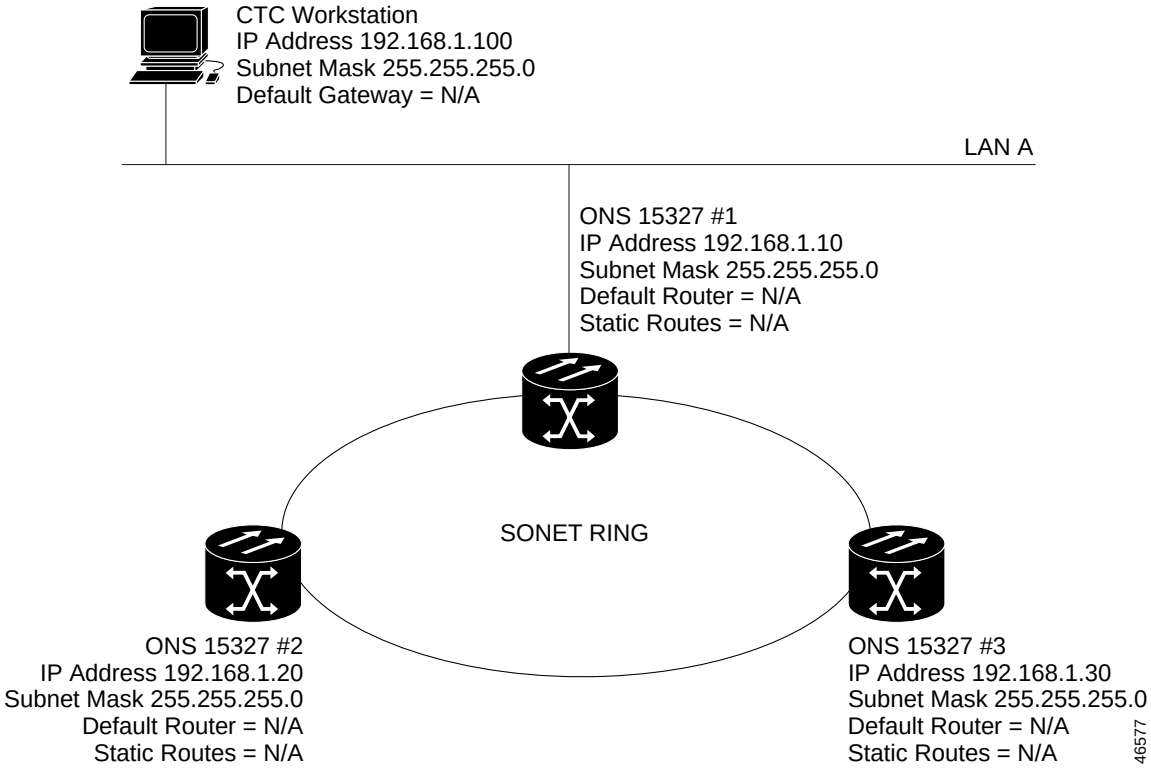
ARP matches higher-level IP addresses to the physical addresses of the destination host. It uses a lookup table (called ARP cache) to perform the translation. When the address is not found in the ARP cache, a broadcast is sent out on the network with a special format called the ARP request. If one of 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 15327 to respond to the ARP request for ONS 15327s not connected to the LAN. (ONS 15327 proxy ARP requires no user configuration.) For this to occur, The DCC-connected ONS 15327s must reside on the same subnet. When a LAN device sends an ARP request to an ONS 15327 that is not connected to the LAN, the gateway ONS 15327 returns its MAC address to the LAN device. The LAN device then sends the datagram for the remote ONS 15327 to the MAC address of the proxy ONS 15327. The proxy ONS 15327 uses its routing table to forward the datagram to the non-LAN ONS 15327.

Scenario 3 is similar to Scenario 1, but only one ONS 15327 (#1) connects to the LAN (Figure 8-3). Two ONS 15327s (#2 and #3) connect to ONS 15327 #1 through the SONET DCC. Because all three ONS 15327s are on the same subnet, Proxy ARP enables ONS 15327 #1 to serve as a gateway for ONS 15327 #2 and #3.

Note This scenario assumes all CTC connections are to ONS 15327 #1. If you connect a laptop to either #2 or #3, network partitioning occurs, and neither the laptop or the CTC computer is able to see all nodes. If you want laptops to connect directly to external network elements, you need to create static routes (see Scenario 5) or enable the ONS 15327 proxy server (see Scenario 7).

Figure 8-3 Scenario 3: Using Proxy ARP

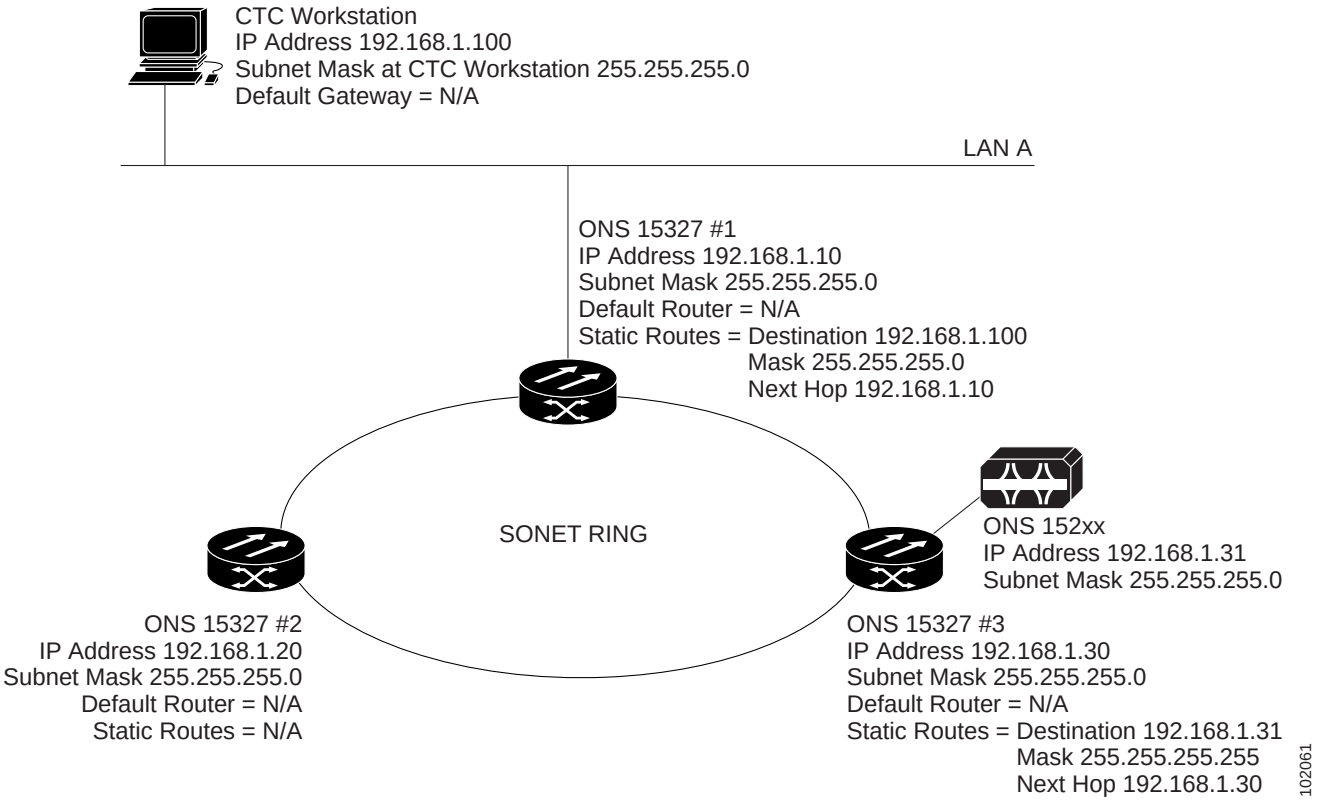


You can also use proxy ARP to communicate with hosts attached to the craft Ethernet ports of DCC-connected nodes (Figure 8-4). The node with an attached host must have a static route to the host. Static routes are propagated to all DCC peers using OSPF. The existing proxy ARP node is the gateway for 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 8-4, 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 can be set up as an additional host.

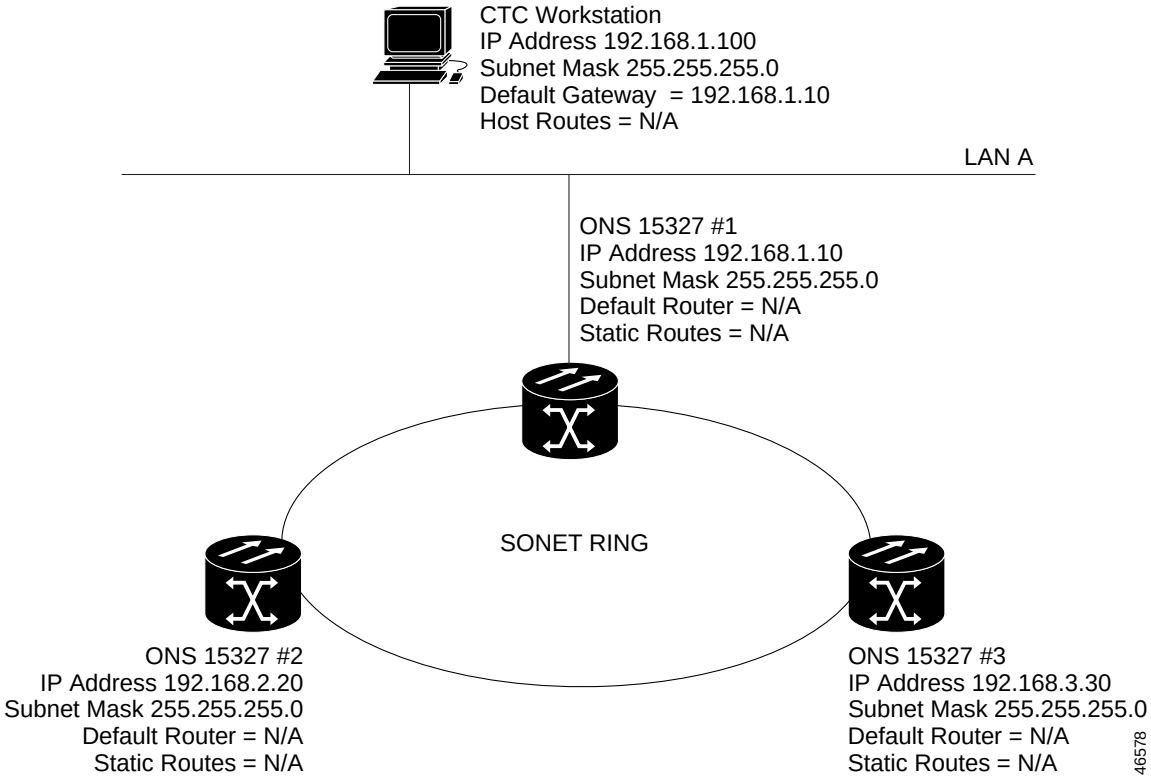
Figure 8-4 Scenario 3: Using Proxy ARP with Static Routing



8.2.4 Scenario 4: Default Gateway on CTC Computer

Scenario 4 is similar to Scenario 3, but ONS 15327 #2 and #3 reside on different subnets, 192.168.2.0 and 192.168.3.0, respectively (Figure 8-5). Node #1 and the CTC computer are on subnet 192.168.1.0. Proxy ARP is not used because the network includes different subnets. In order for the CTC computer to communicate with Nodes #2 and #3, Node #1 is entered as the default gateway on the CTC computer.

Figure 8-5 Scenario 4: Default Gateway on a CTC Computer



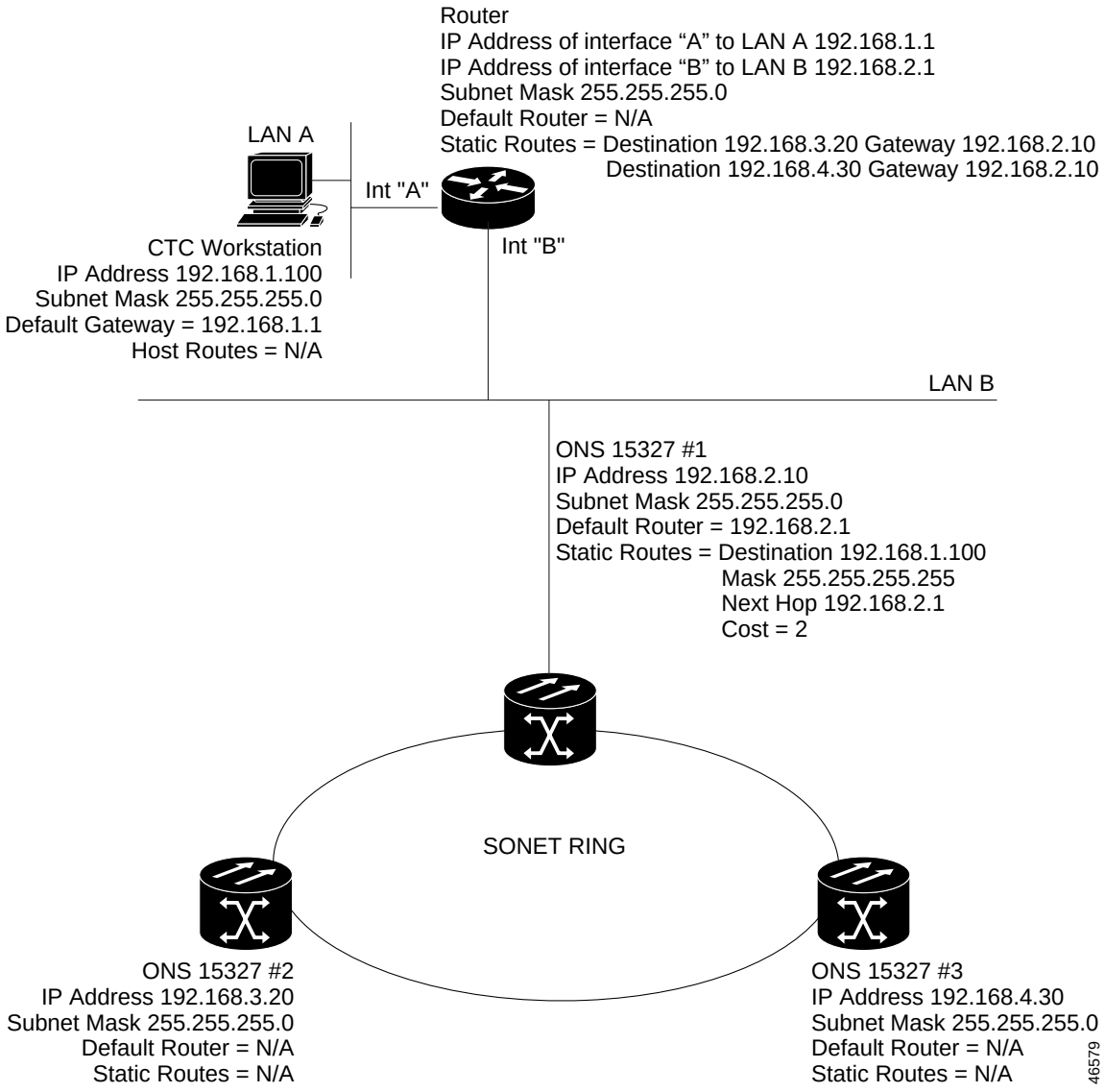
8.2.5 Scenario 5: Using Static Routes to Connect to LANs

Static routes are used for two purposes:

- To connect ONS 15327s to CTC sessions on one subnet that are connected by a router to ONS 15327s residing on another subnet. (These static routes are not needed if OSPF is enabled. Scenario 6 shows an OSPF example.)
- To enable multiple CTC sessions among ONS 15327s residing on the same subnet.

In Figure 8-6, 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 15327s 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 CTC computers on LAN A, a static route is created on Node 1.

Figure 8-6 Scenario 5: Static Route with One CTC Computer Used as a Destination

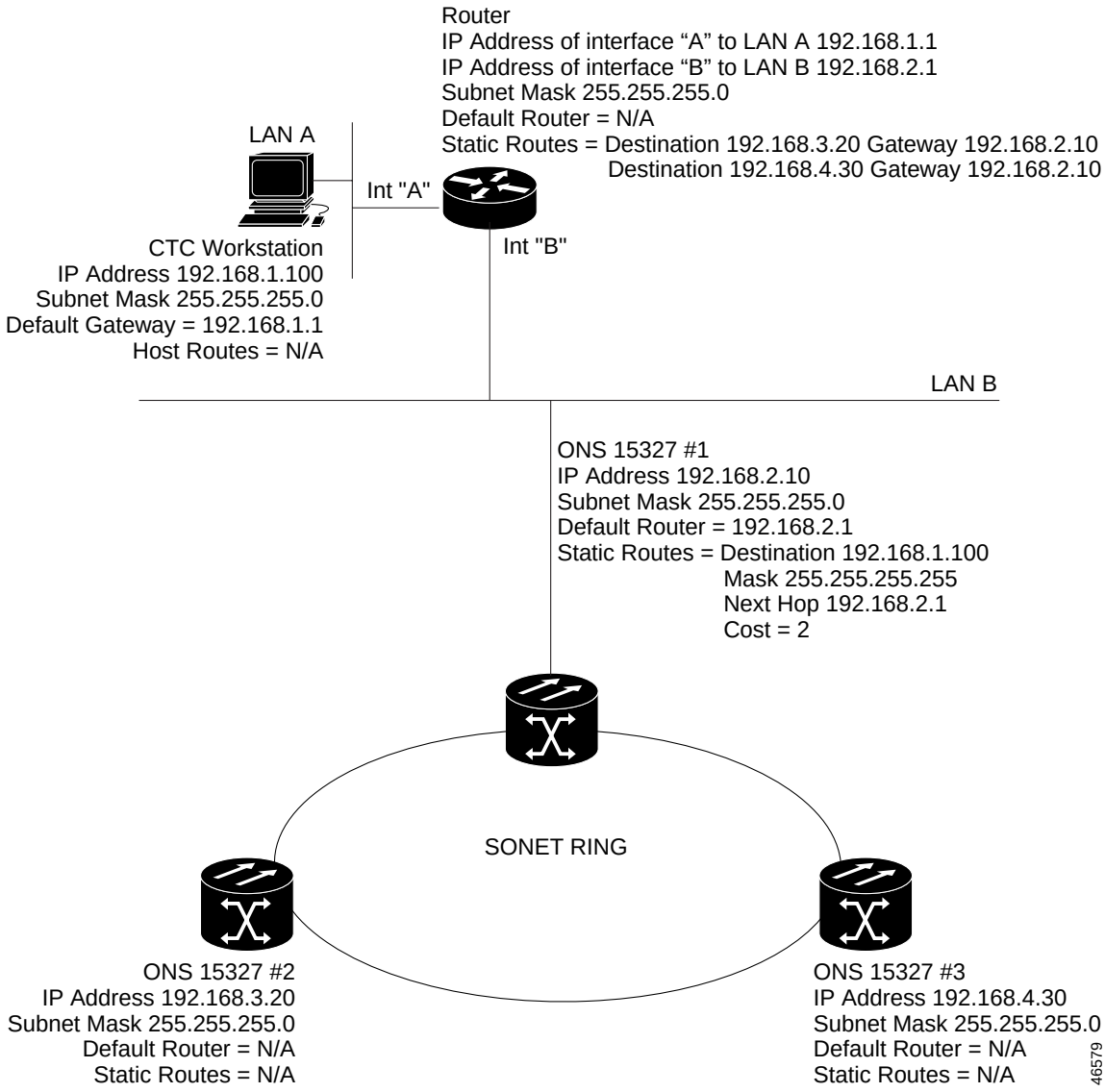


The destination and subnet mask entries control access to the ONS 15327s:

- 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 8-7 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.

Figure 8-7 Scenario 5: Static Route with Multiple LAN Destinations



8.2.6 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.

The ONS 15327 uses OSPF protocol in internal ONS 15327 networks for node discovery, circuit routing, and node management. You can enable OSPF on the ONS 15327 so that the ONS 15327 topology is sent to OSPF routers on a LAN. Advertising the ONS 15327 network topology to LAN routers eliminates the need to enter static routes for ONS 15327 subnetworks manually.

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 15327 OSPF topology for advertising to an OSPF network, you must assign an OSPF area ID in decimal format to the ONS 15327 network. Coordinate the area ID number assignment with your LAN administrator. All DCC-connected ONS 15327s should be assigned the same OSPF area ID.

Figure 8-8 shows a network enabled for OSPF.

Figure 8-8 Scenario 6: OSPF Enabled

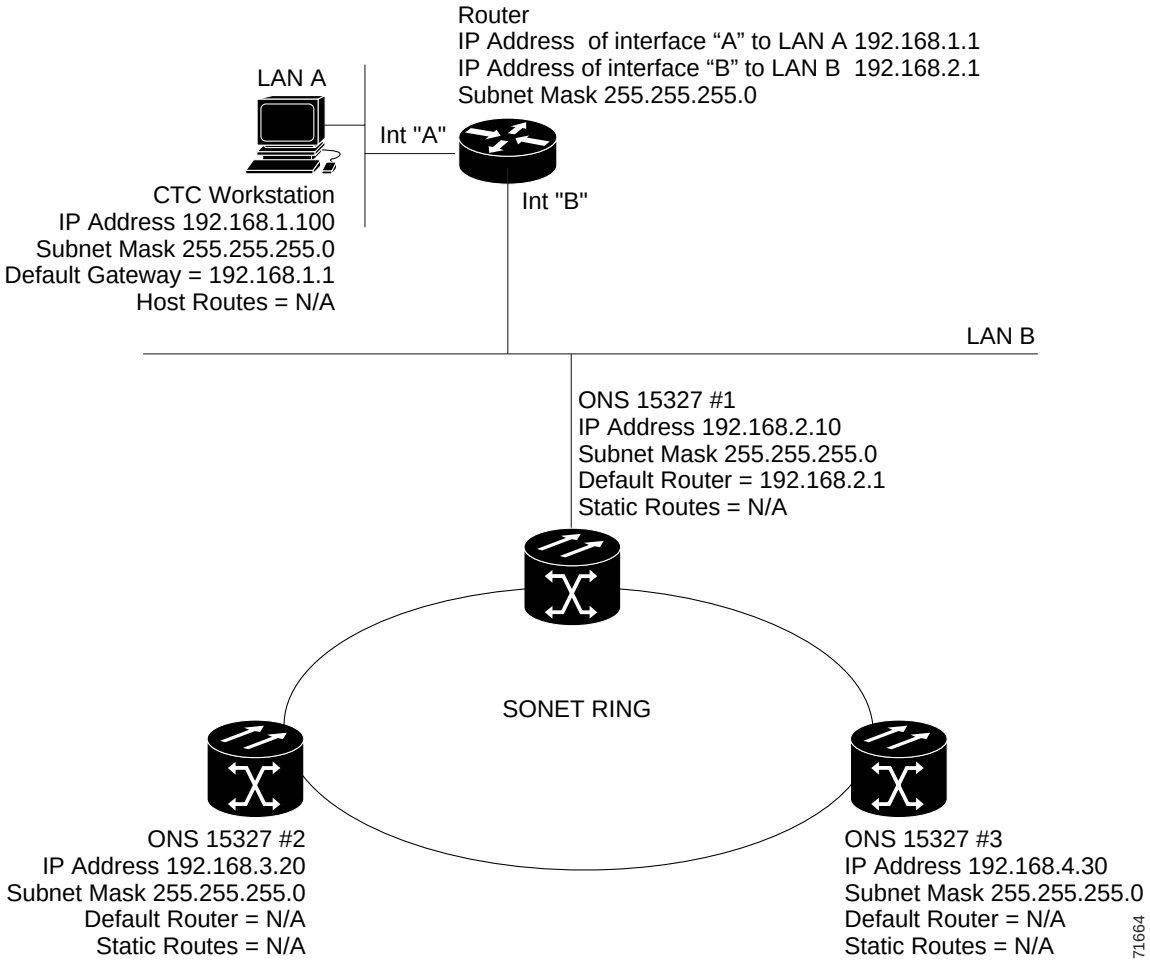
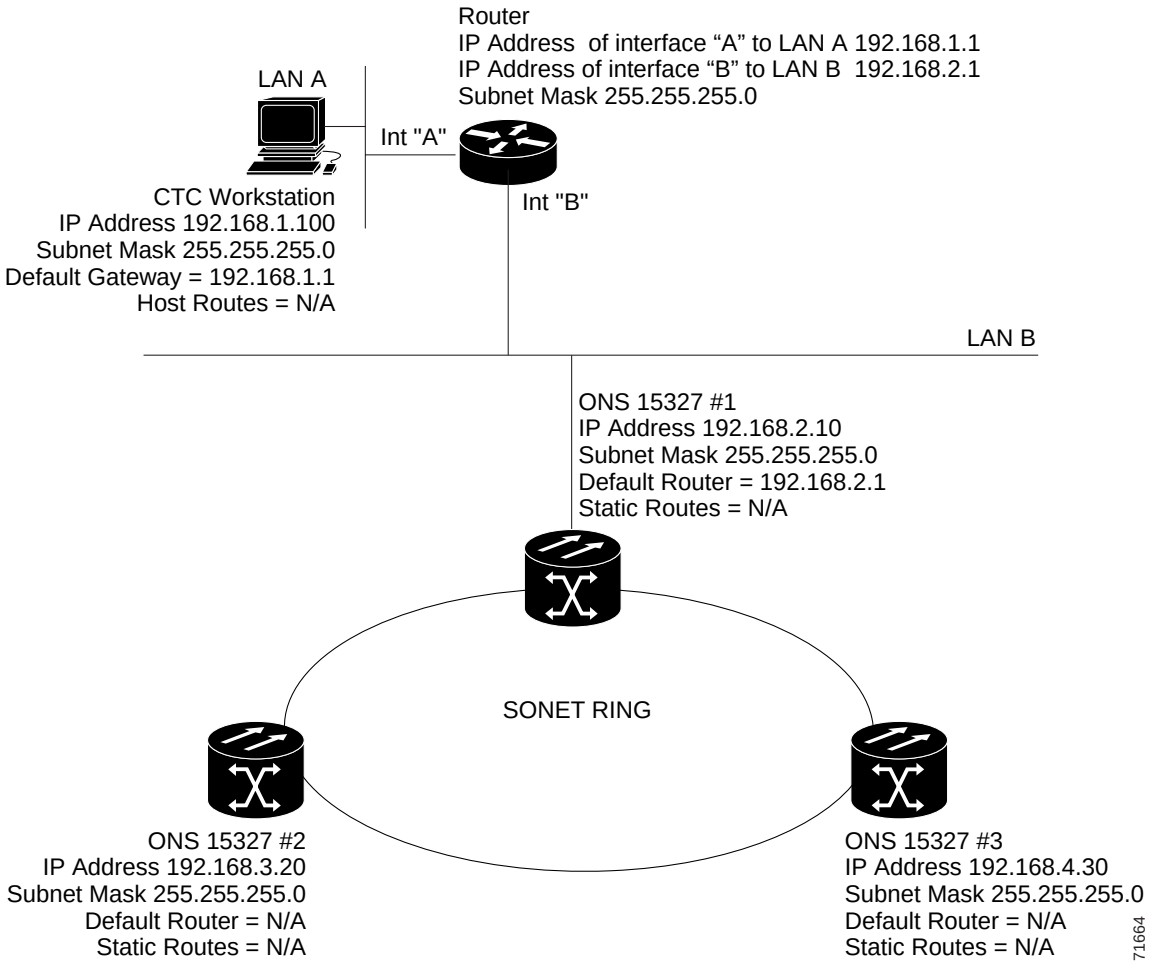


Figure 8-9 shows the same network without OSPF. Static routes must be manually added to the router for CTC computers on LAN A to communicate with Nodes 2 and 3 because these nodes reside on different subnets.

Figure 8-9 Scenario 6: OSPF Not Enabled



8.2.7 Scenario 7: Provisioning the ONS 15327 Proxy Server

The ONS 15327 proxy server is a set of functions that allows you to network ONS 15327s in environments where visibility and accessibility between ONS 15327s and CTC computers must be restricted. For example, you can set up a network so that field technicians and network operating center (NOC) personnel can both access the same ONS 15327s while preventing the field technicians from accessing the NOC LAN. To do this, one ONS 15327 is provisioned as a gateway network element (GNE) and the other ONS 15327s are provisioned as external network elements (ENEs). The GNE tunnels connections between CTC computers and ENEs, which provides management capability while preventing access for non-ONS 15327 management purposes.

The ONS 15327 proxy server 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 8-3 on page 8-15 and Table 8-4 on page 8-16) depend on whether the packet arrives at the ONS 15327 DCC or XTC Ethernet interface.

- Processes SNTP (Simple Network Timing Protocol) and NTP (Network Timing Protocol) requests. Element ONS 15327 NEs can derive time-of-day from an SNTP/NTP LAN server through the GNE.
- Process SNMPv1 traps. The GNE receives SNMPv1 traps from the ENE and forwards them to all provisioned SNMPv1 trap destinations.

The ONS 15327 proxy server is provisioned using the Enable proxy server on port check box on the Provisioning > Network > General tab. If checked, the ONS 15327 serves as a proxy for connections between CTC clients and ONS 15327s that are DCC-connected to the proxy ONS 15327. 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 proxy server as an ENE or a GNE:

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.

- External Network Element (ENE)—If set as an ENE, the ONS 15327 neither installs nor advertises default or static routes. CTC computers can communicate with the ONS 15327 using the TCC2 craft port, but they cannot communicate directly with any other DCC-connected ONS 15327.

  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 15327 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, CTC cannot communicate with any other DCC-connected ONS 15327s and firewall is not enabled.

Figure 8-10 shows an ONS 15327 proxy server implementation. A GNE is connected to a central office LAN and to ENEs. The central office LAN is connected to a NOC LAN, which has CTC computers. The NOC CTC computer and craft technicians must both be able to access the ENEs. However, the craft technicians must be prevented from accessing or seeing the NOC or central office LANs.

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

Figure 8-10 ONS 15327 Proxy Server with GNE and ENEs on the Same Subnet

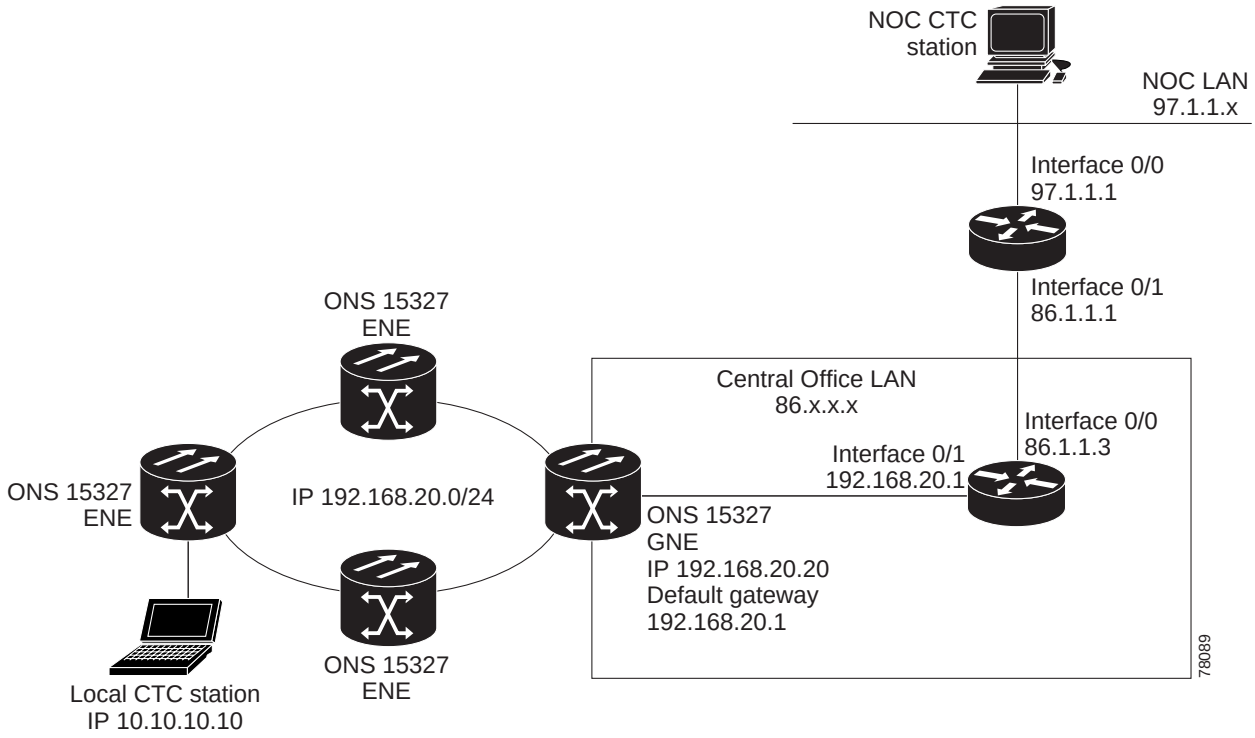


Table 8-2 shows recommended settings for ONS 15327 GNEs and ENEs in the configuration shown in Figure 8-10.

Table 8-2 ONS 15327 Gateway and Element NE Settings

Setting	ONS 15327 Gateway NE	ONS 15327 Element NE
Craft Access Only	Off	On
Enable Proxy	On	On
Enable Firewall	On	On
Ospf	Off	Off
Sntp Server (if used)	SNTP server IP address	Set to ONS 15327 GNE IP address
SNMP (if used)	SNMPv1 trap destinations	Set SNMPv1 trap destinations to ONS 15327 GNE

Figure 8-11 shows the same proxy server implementation with ONS 15327 ENEs on different subnets. In this example, ONS 15327 GNEs and ENEs are provisioned with the settings shown in Table 8-2.

Figure 8-11 Scenario 7: ONS 15327 Proxy Server with GNE and ENEs on Different Subnets

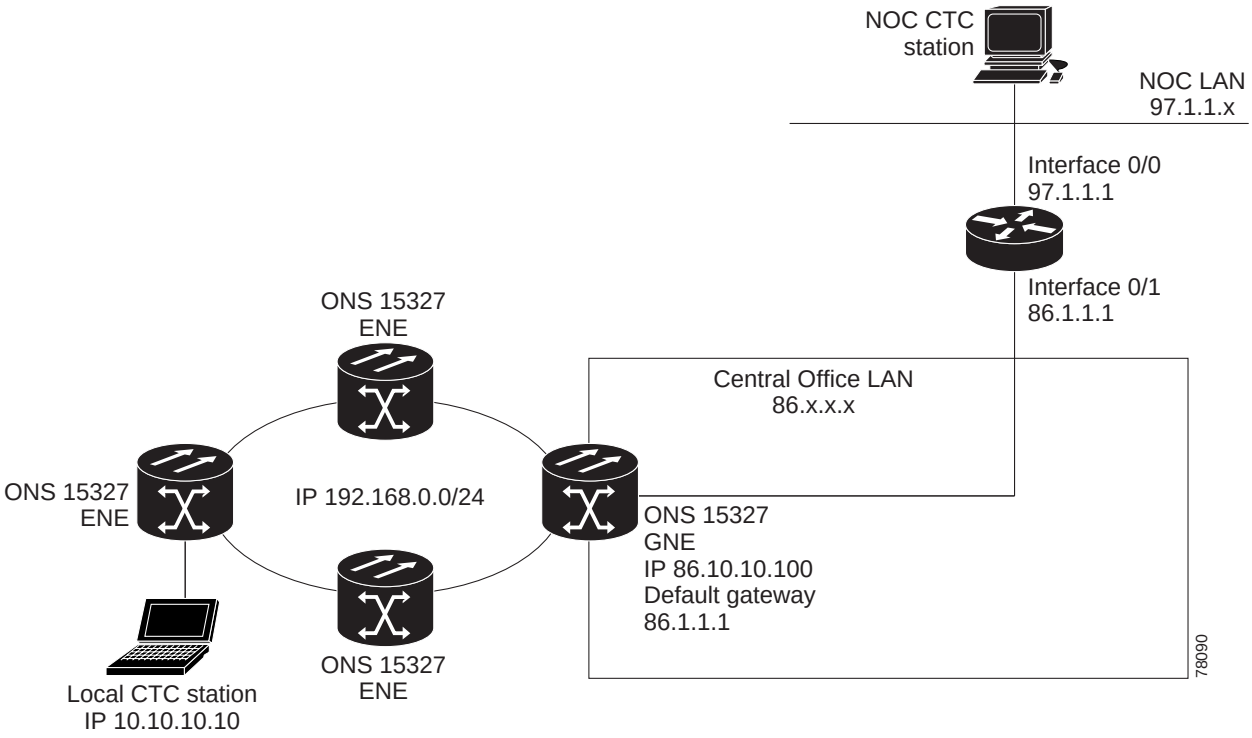


Figure 8-12 shows the implementation with ONS 15327 ENEs in multiple rings. In this example, ONS 15327 GNEs and ENEs are provisioned with the settings shown in Table 8-2.

Figure 8-12 Scenario 7: ONS 15327 Proxy Server with ENEs on Multiple Rings

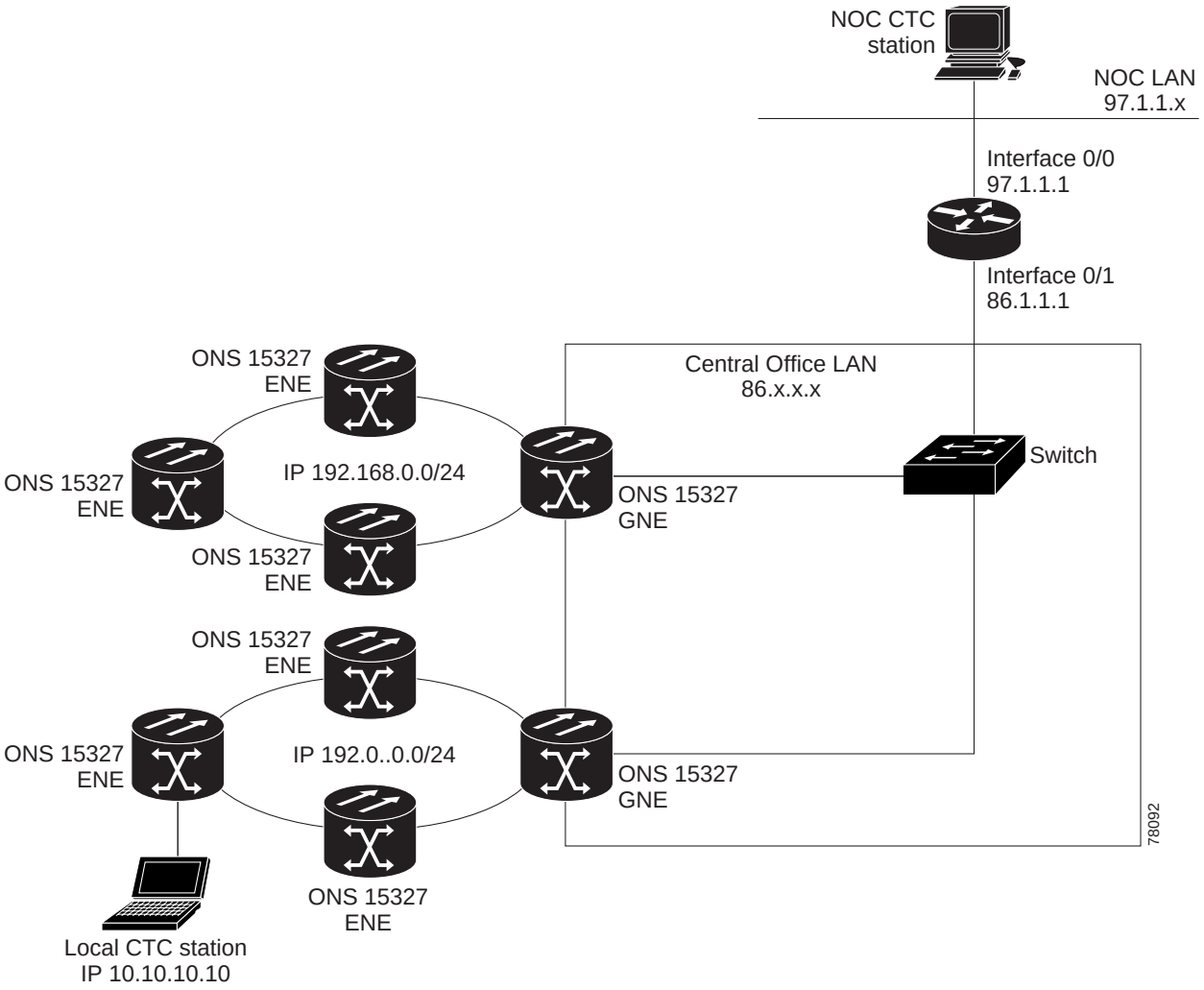


Table 8-3 shows the rules the ONS 15327 follows to filter packets when * is enabled.

Table 8-3 Proxy Server Firewall Filtering Rules

Packets arriving at:	Are accepted if the IP destination address is:
XTC Ethernet interface	• The ONS 15327 shelf itself • The ONS 15327'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 15327 itself • Any destination that is connected through another DCC interface • Within the 224.0.0.0/8 network

Table 8-4 shows additional rules that apply if the packet addressed to the ONS 15327 is discarded. Rejected packets are silently discarded.

Table 8-4 Proxy Server Firewall Filtering Rules When Packet Addressed to ONS 15327

Packets Arrive At	Accepted	Rejected
XTC Ethernet interface	• All User Datagram Protocol (UDP) packets except those in the Rejected column	• UDP packets addressed to the SNMP trap relay port (391)
DCC interface	• All UDP packets • All TCP packets except those in the Rejected column • OSPF packets • Internet Control Message Protocol (ICMP) packets	• TCP packets addressed to the Telnet port • TCP packets addressed to the proxy server port • All packets other than UDP, TCP, OSPF, ICMP

If you implement the proxy server, keep the following rules in mind:

1. All DCC-connected ONS 15327s on the same Ethernet segment must have the same Craft Access Only setting. Mixed values produce unpredictable results, and might leave some nodes unreachable through the shared Ethernet segment.
2. All DCC-connected ONS 15327s on the same Ethernet segment must have the same Enable Firewall setting. Mixed values produce unpredictable results. Some nodes might become unreachable.
3. If you check Enable Firewall, always check Enable Proxy. If Enable Proxy is unchecked, CTC is not able to see nodes on the DCC side of the ONS 15327.
4. If Craft Access Only is checked, check Enable Proxy. If Enable Proxy is not checked, CTC is not able to see nodes on the DCC side of the ONS 15327.

If nodes become unreachable in cases 1, 2, and 3, you can correct the setting by performing one of the following actions:

- Disconnect the craft computer from the unreachable ONS 15327. Connect to the ONS 15327 through another ONS 15327 in the network that has a DCC connection to the unreachable ONS 15327.
- Disconnect the Ethernet cable from the unreachable ONS 15327. Connect a CTC computer directly to the ONS 15327.

8.2.8 Scenario 8: Dual GNEs on a Subnet

The ONS 15327 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 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 8-13 shows a network with dual GNEs on the same subnet.

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

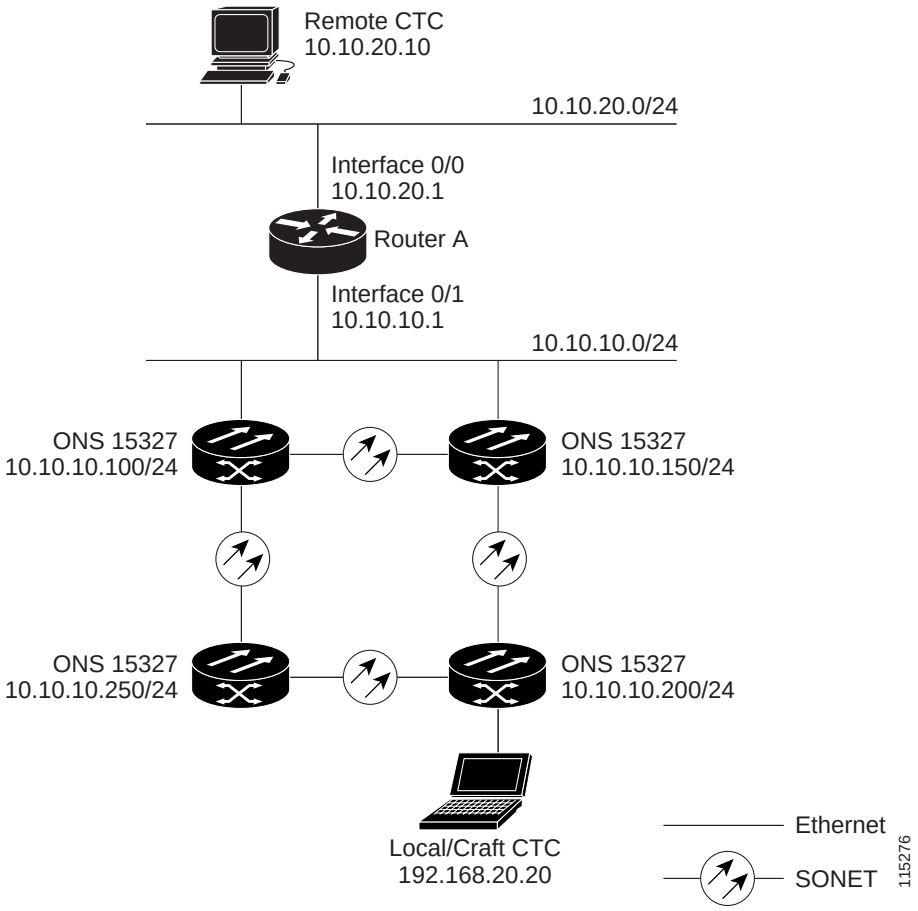
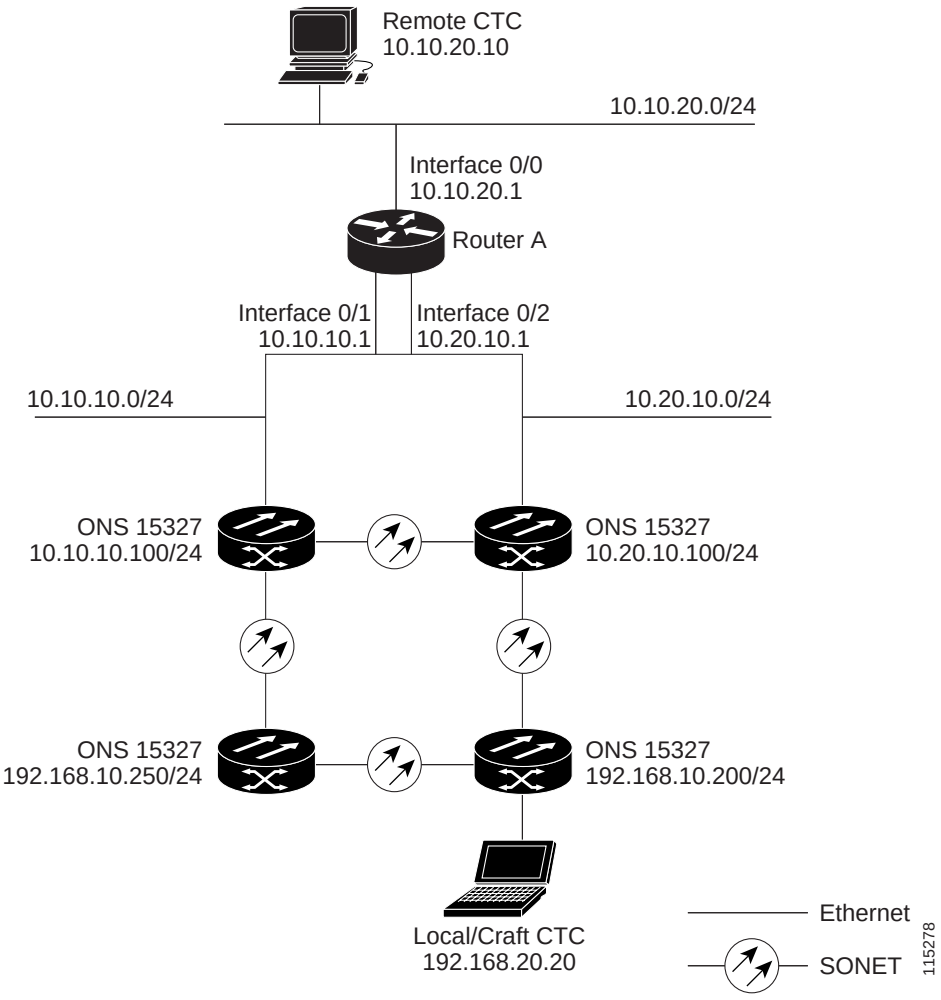


Figure 8-14 shows a network with dual GNEs on different subnets.

Figure 8-14 Scenario 8: Dual GNEs on Different Subnets



8.3 Provisionable Patchcords

A provisionable patchcord is a user-provisioned link that is advertised by OSPF throughout the network. Provisionable patchcords, also called virtual links, are needed if an ONS 15327 optical port is connected to an ONS 15454 transponder or muxponder client port provisioned in transparent mode.

Provisionable patchcords are required on both ends of a physical link. The provisioning at each end includes a local patchcord ID, slot/port information, remote IP address, and remote patchcord ID. Patchcords appear as dashed lines in CTC network view.

Table 8-5 lists the supported card combinations for ONS 15327 optical cards and the ONS 15454 transponder/muxponder cards used in a provisionable patchcord. For more information about the ONS 15454 transponder and muxponder cards, refer to the *Cisco ONS 15454 Reference Manual*.

Table 8-5 Client and Trunk Card Combinations in Provisionable Patchcords

	ONS 15454 Client Cards		
ONS 15327 Trunk Cards	MXP_2.5G_10G/ TXP_MR_10G	TXP(P)_MR_2.5G	MXP_2.5G_10E/ TXP_MR_10E
OC-3	—		—
OC-12	—	Yes	—
OC-48	Yes	Yes	Yes

Optical ports have the following requirements when used in a provisionable patchcord:

- An optical port connected to an ONS 15454 transponder/muxponder port requires SDCC/LDCC termination.
- If the optical port is the protection port in a 1+1 group, the working port must have SDCC/LDCC termination provisioned.
- If the remote end of a patchcord is Y-cable protected, an optical port requires two patchcords.

8.4 Routing Table

ONS 15327 routing information is displayed on the Maintenance > Routing Table tabs. 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 15327 interface used to access the destination:
  - cpm0—The ONS 15327 Ethernet interface, that is, the RJ-45 jack and the LAN pin on the XTC card
  - pdcc0—An SDCC interface, that is, an OC-N trunk card identified as the SDCC termination
  - lo0—A loopback interface

Table 8-6 shows sample routing entries for an ONS 15327.

Table 8-6 Sample Routing Table Entries

Entry	Destination	Mask	Gateway	Interface
1	0.0.0.0	0.0.0.0	172.20.214.1	cpm0
2	172.20.214.0	255.255.255.0	172.20.214.92	cpm0
3	172.20.214.92	255.255.255.255	127.0.0.1	lo0
4	172.20.214.93	255.255.255.255	0.0.0.0	pdcc0
5	172.20.214.94	255.255.255.255	172.20.214.93	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 is 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 (cpm0) indicates that the ONS 15327 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 a destination.
- Gateway (172.20.214.92) is the gateway address. All outbound traffic belonging to this network is sent to this gateway.
- Interface (cpm0) indicates that the ONS 15327 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 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 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 SONET SDCC 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 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 SONET SDCC interface is used to reach the gateway.

8.5 External Firewalls

Table 8-7 shows the ports that are used by the XTC.

Table 8-7 Ports Used by the XTC

Port	Function
0	Never used
21	FTP control
23	Telnet
80	HTTP
111	rpc (not used; but port is in use)
513	rlogin (not used; but port is in use)
=<1023	Default CTC listener ports
1080	Proxy server
2001-2017	I/O card Telnet
2018	DCC processor on active XTC
2361	TL1
3082	TL1
3083	TL1
5001	Bidirectional line switch ring (BLSR) server port
5002	BLSR client port
7200	SNMP input port
9100	EQM port
9101	EQM port 2
9401	TCC boot port
9999	Flash manager
57790	Default TCC listener port

The following access control list (ACL) examples show a firewall configuration when the proxy server gateway setting is not enabled. In the example, the CTC workstation address is 192.168.10.10 and the ONS 15327 address is 10.10.10.100. The firewall is attached to the GNE, so the inbound path is CTC to the GNE and the outbound path 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 the 15327 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 the 15327 GNE (port 57790) ***
access-list 100 remark

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 15327 (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 15327 GNE to CTC ***
```

The following ACL examples show a firewall configuration when the proxy server gateway setting is enabled. As with the first example, the CTC workstation address is 192.168.10.10 and the ONS 15327 address is 10.10.10.100. The firewall is attached to the GNE, so the inbound path is CTC to the GNE and the outbound path 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 the 15327 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 15327 GNE proxy server (port
1080) ***
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 from CTC to the 15327 GNE ***
access-list 101 remark *** Outbound ACL, NE -> CTC ***
access-list 101 remark
access-list 101 permit tcp host 10.10.10.100 eq 1080 host 192.168.10.10
access-list 101 remark *** allows alarms and other communications from the 15327 (proxy
server) 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 15327 GNE to CTC ***
```

8.6 Open GNE

The ONS 15327 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 and LDCC 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 and LDCC 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 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 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 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 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 proxy server disabled, neither proxy tunnels or firewall tunnels are allowed.

Figure 8-15 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 8-15 Proxy and Firewall Tunnels for Foreign Terminations

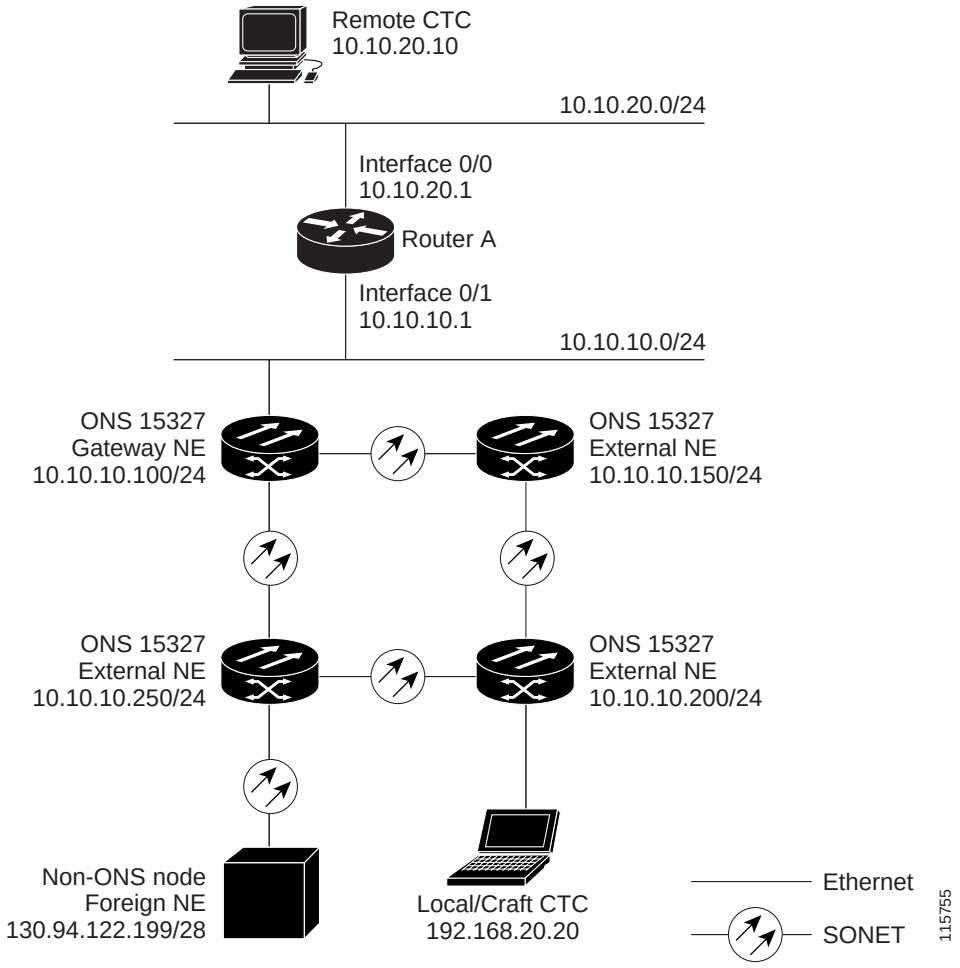


Figure 8-16 shows a remote node connected to an ENE Ethernet port. Proxy and firewall tunnels are useful in this example because the GNE would otherwise block IP access between the PC and foreign node. This configuration also requires a firewall tunnel on the ENE.

Figure 8-16 Foreign Node Connection to an ENE Ethernet Port