CHAPTER 13

IP Networking

This chapter provides eight scenarios showing Cisco ONS 15454s in common IP network configurations. The chapter does not provide a comprehensive explanation of IP networking concepts and procedures. For IP setup instructions, refer to 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 ONS 15454 node groups that allow you to provision non-data communication 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 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 Cisco Transport Controller (CTC) sessions with ONS 15454s that reside on the same subnet with multiple CTC sessions.
- ONS 15454s can be connected to Open Shortest Path First (OSPF) networks so ONS 15454 network information is automatically communicated across multiple LANs and WANs.
- The ONS 15454 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 15454s in IP networks.

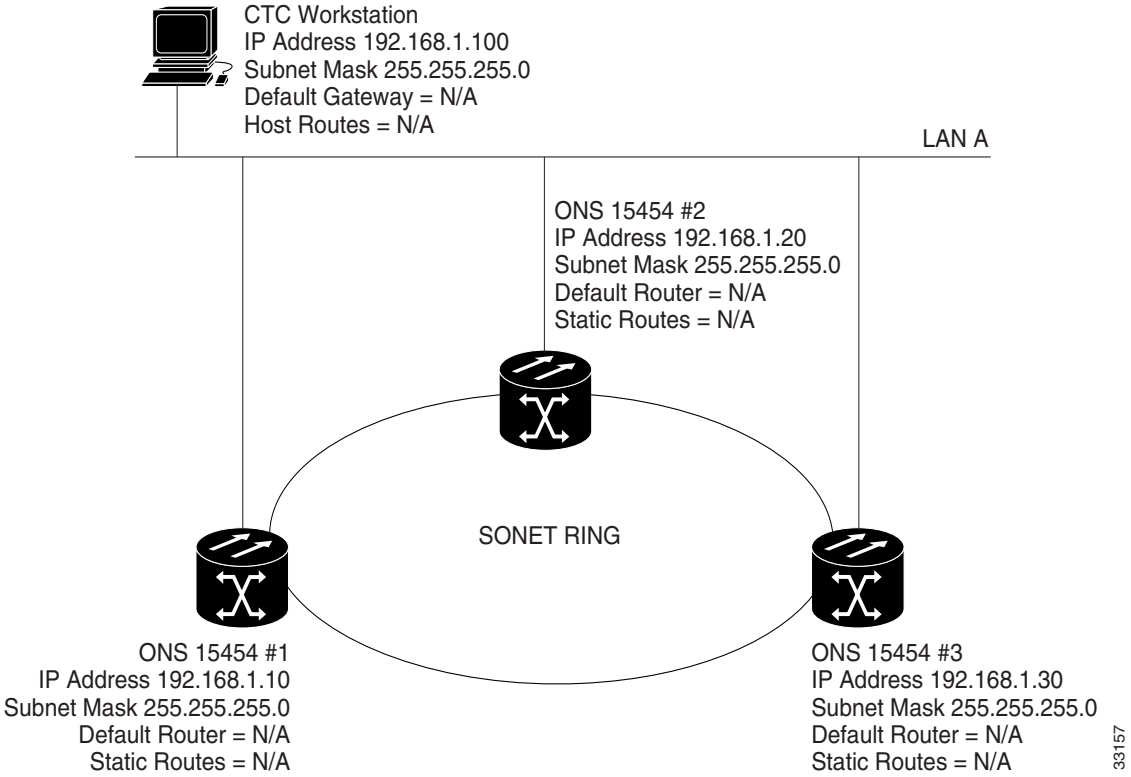
Table 13-1 General ONS 15454 IP Troubleshooting Checklist

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 ports are in service and that a DCC is enabled on each trunk port.

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

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 Scenario 1: CTC and ONS 15454s on Same Subnet

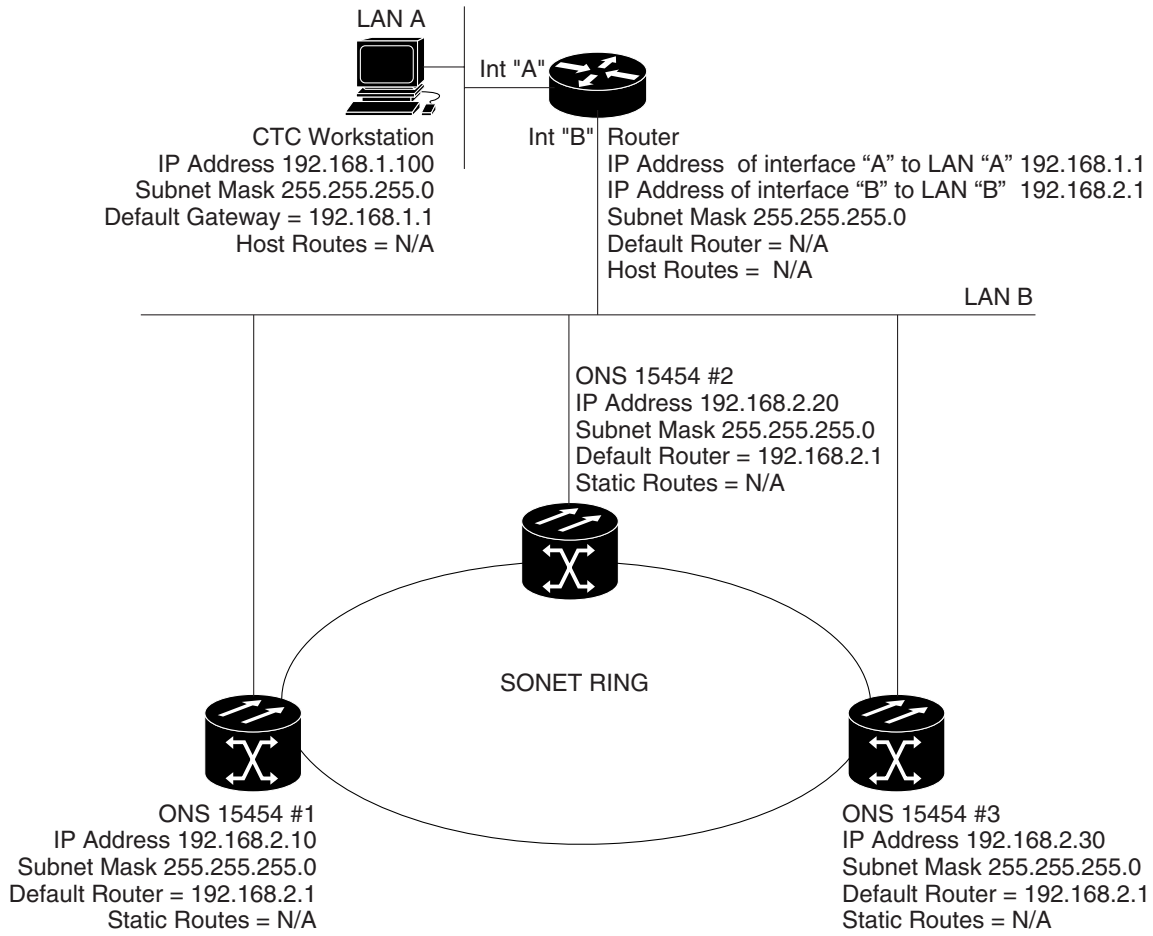


13.2.2 Scenario 2: CTC and ONS 15454s Connected to a Router

In 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 DHCP (Dynamic Host Configuration Protocol), the default gateway and IP address are assigned automatically. In the Figure 13-2 example, a DHCP server is not available.

Figure 13-2 Scenario 2: CTC and ONS 15454s Connected to Router



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

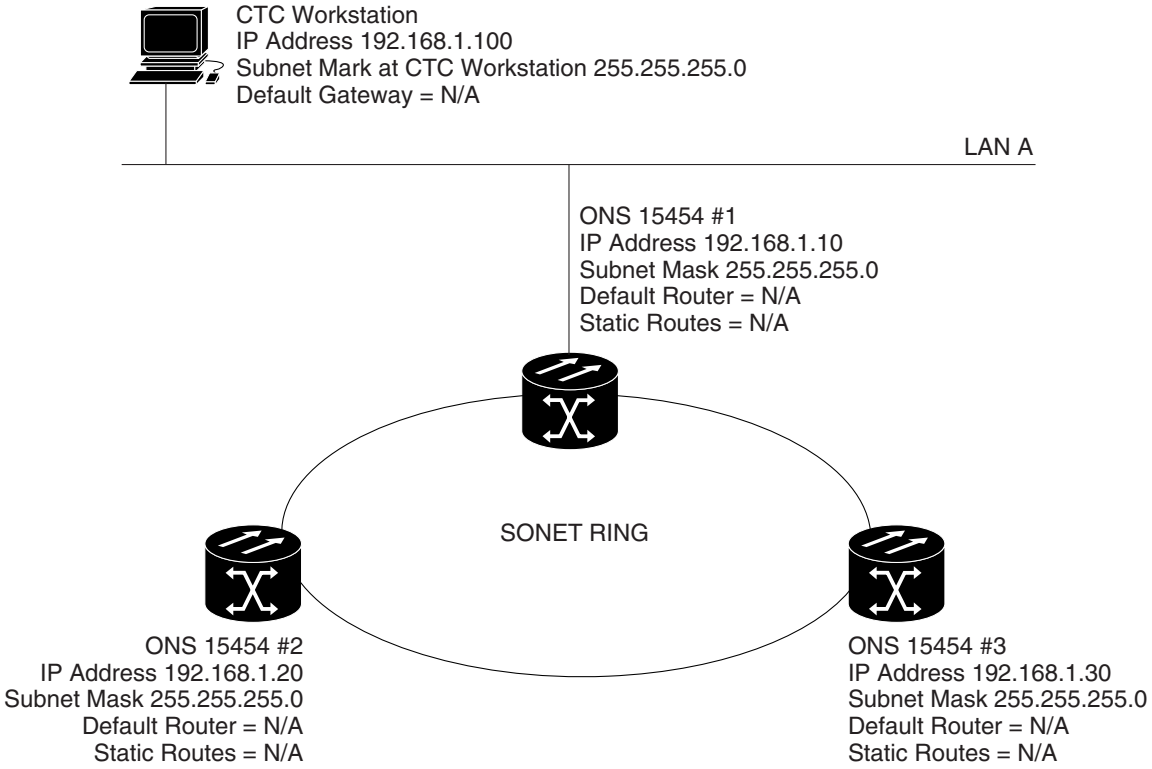
ARP matches higher-level IP addresses to the physical addresses of the destination host. It uses a lookup table (called ARP cache) to perform the translation. When the address is not found in the ARP cache, a broadcast is sent out on the network with a special format called the ARP request. If one of 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.

Scenario 3 is similar to 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 15345 #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 or the CTC computer can see all nodes. If you want laptops to connect directly to external network elements, you must create static routes (see Scenario 5) or enable the ONS 15454 proxy server (see Scenario 7).

Figure 13-3 Scenario 3: Using Proxy ARP

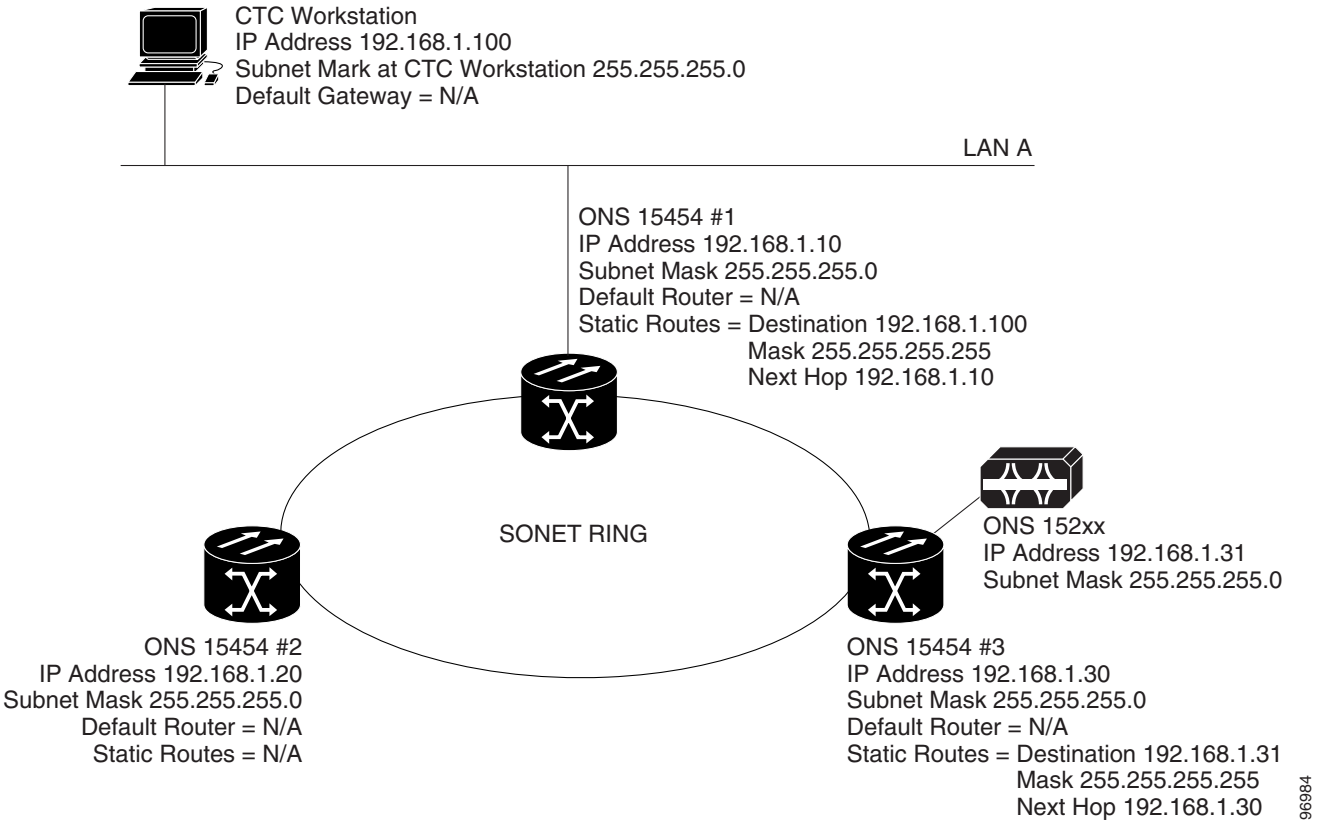


You can also use proxy ARP to communicate with hosts attached to the craft Ethernet ports of DCC-connected nodes (Figure 13-4). The node with an attached host must have a static route to the host. Static routes are propagated to all DCC peers using OSPF. The existing proxy ARP node is the gateway for 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 can be set up as an additional host.

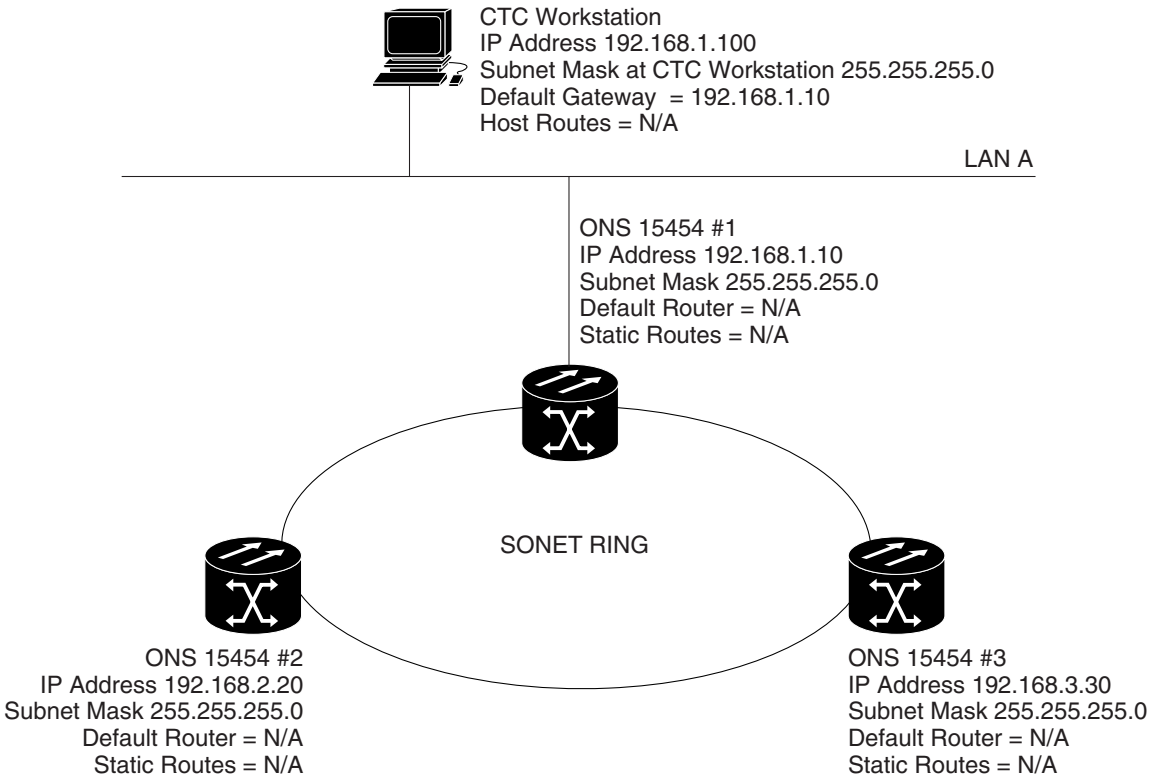
Figure 13-4 Scenario 3: Using Proxy ARP with Static Routing



13.2.4 Scenario 4: Default Gateway on CTC Computer

Scenario 4 is similar to 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 Scenario 4: Default Gateway on a CTC Computer



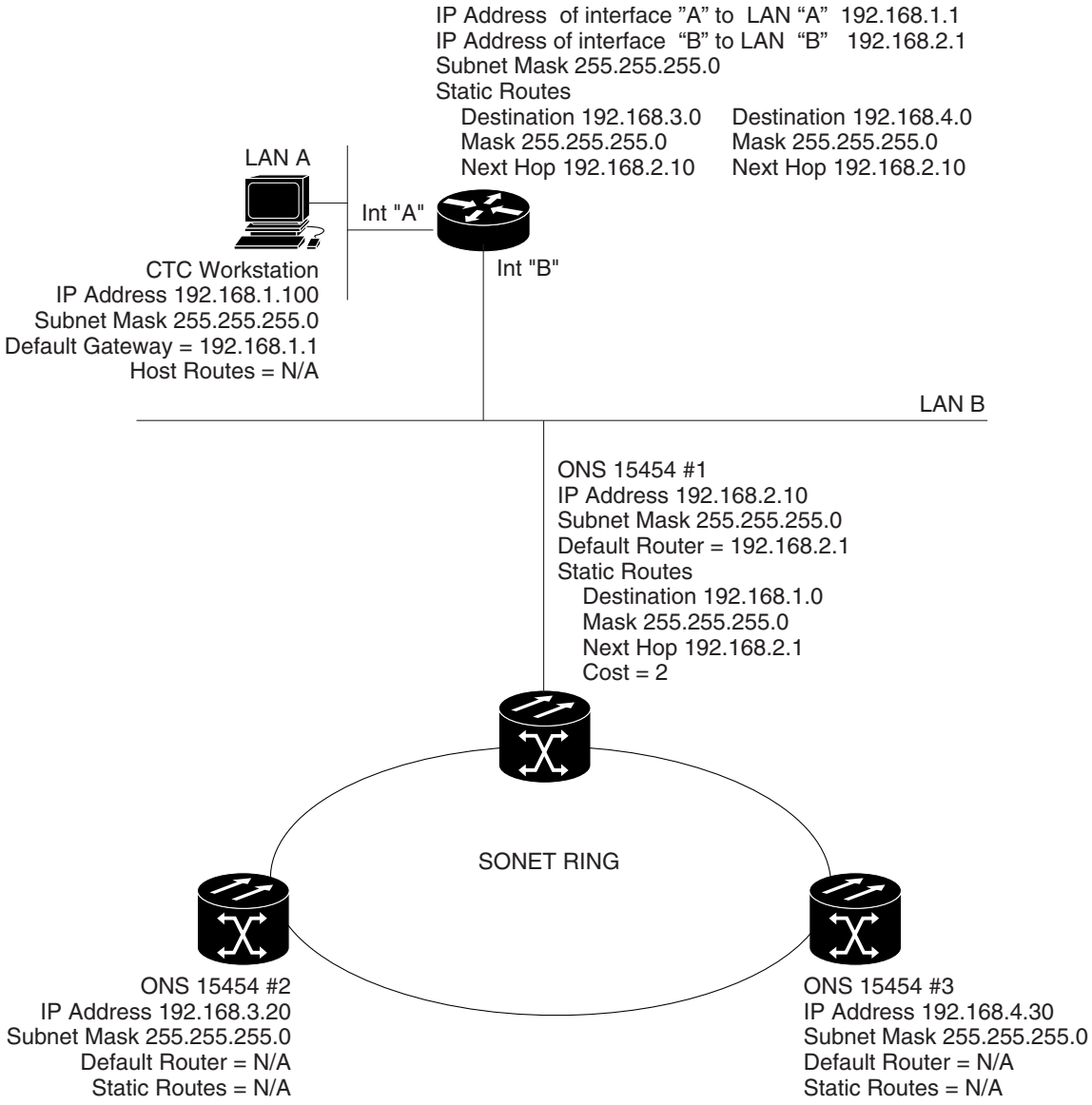
13.2.5 Scenario 5: Using Static Routes to Connect to LANs

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. Scenario 6 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 Scenario 5: Static Route With One CTC Computer Used as a Destination

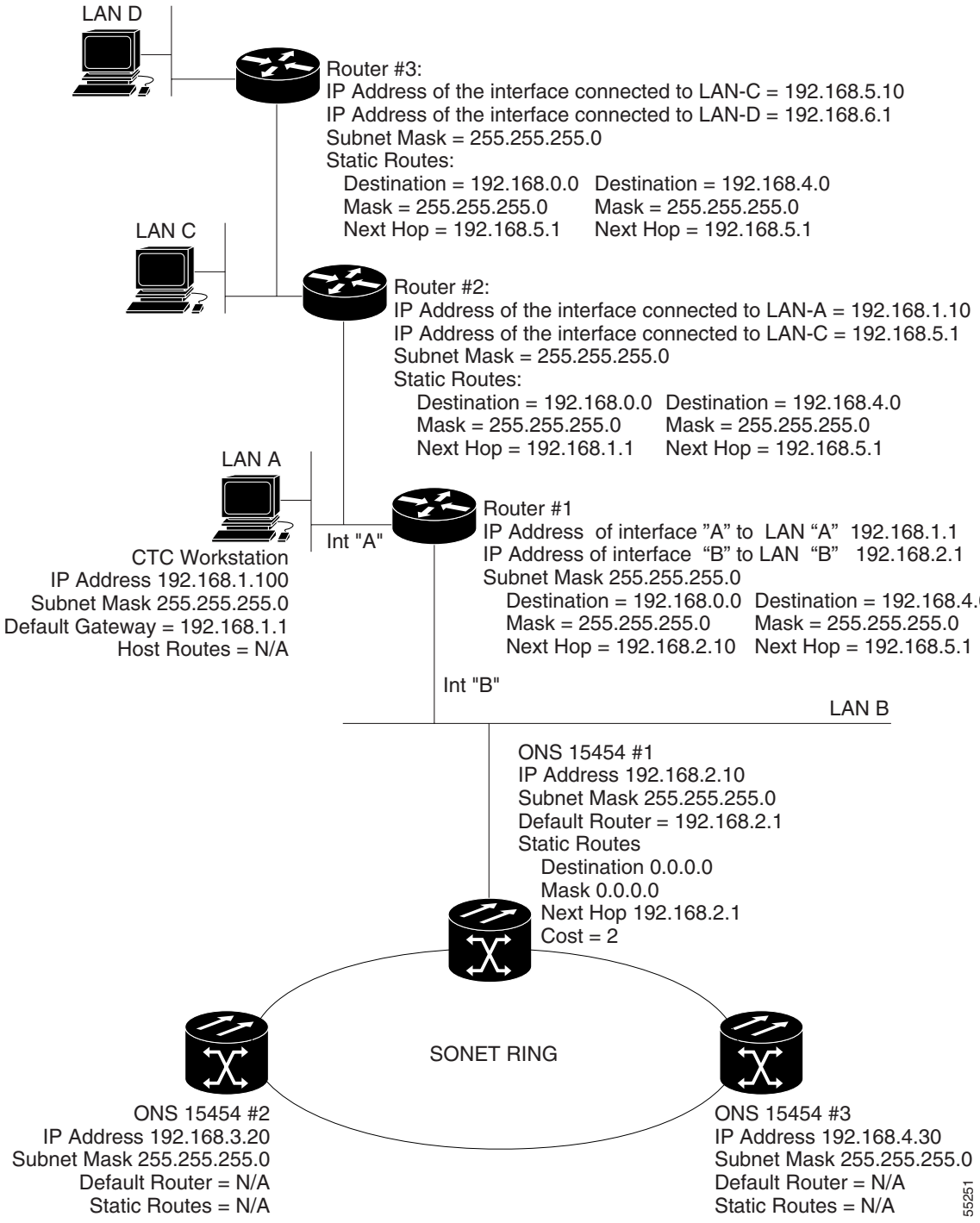


The destination and subnet mask entries control access to the ONS 15454s:

- 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 Scenario 5: Static Route With Multiple LAN Destinations



13.2.6 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.

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 Scenario 6: OSPF Enabled

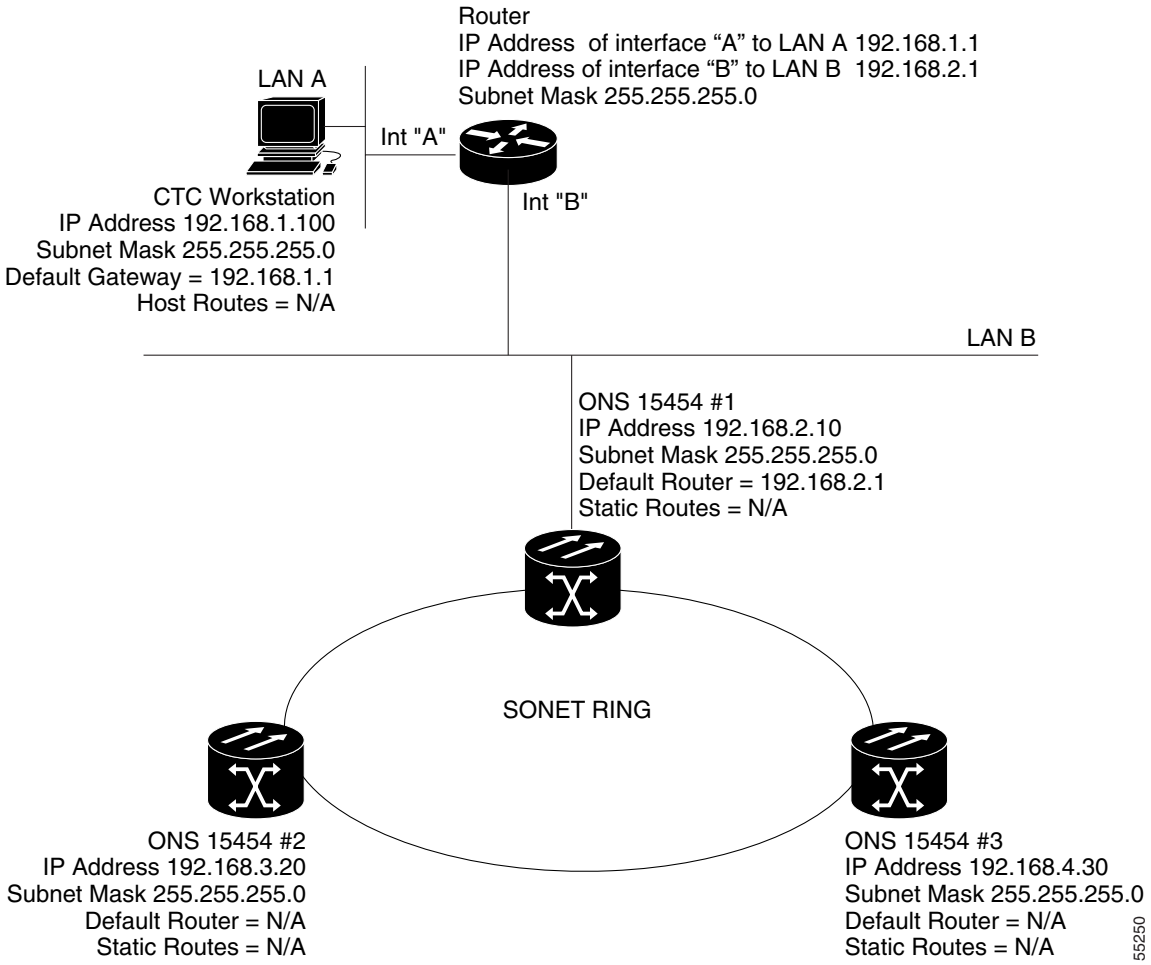
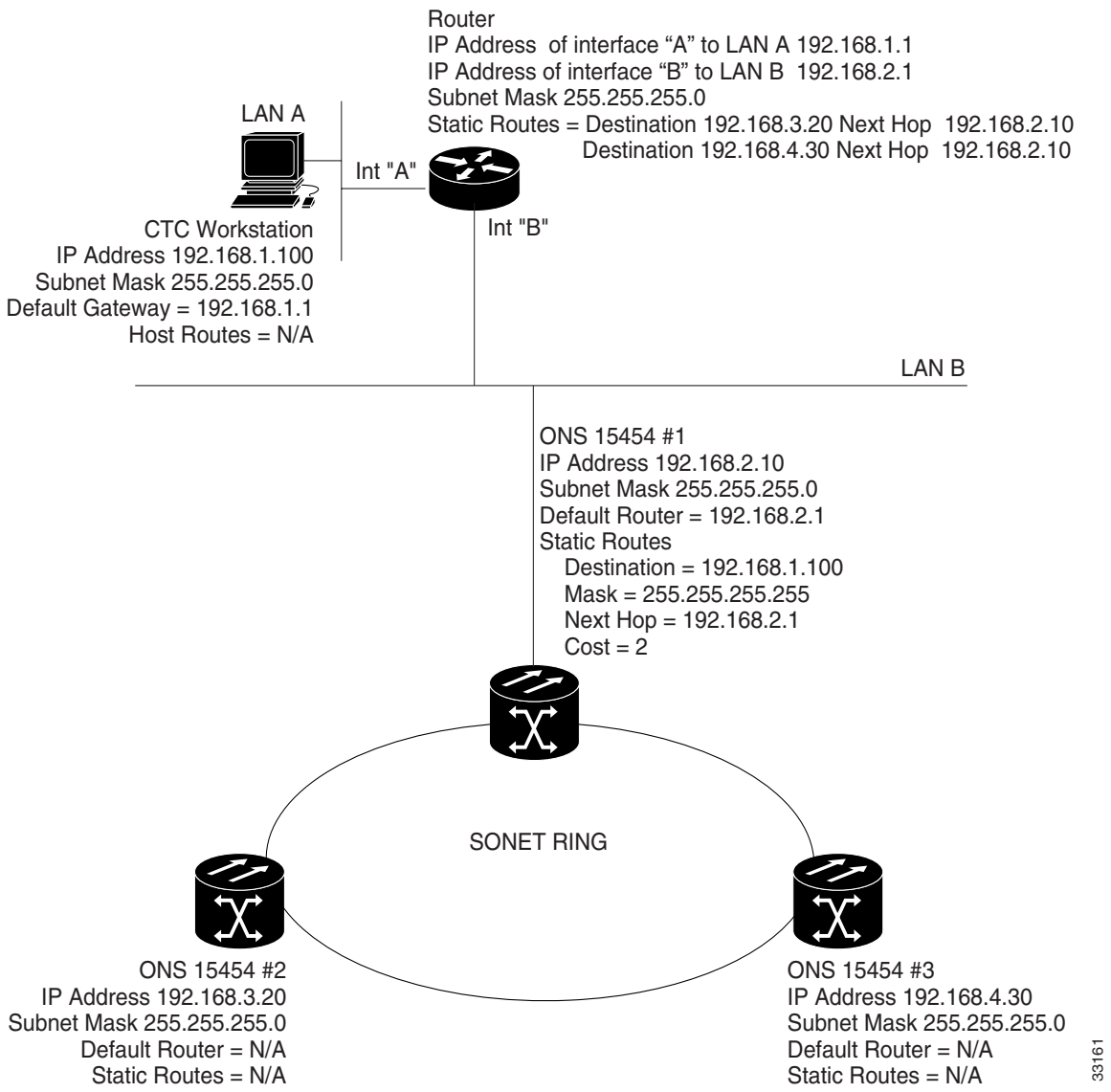


Figure 13-9 Scenario 6: OSPF Not Enabled



13.2.7 Scenario 7: Provisioning the ONS 15454 Proxy Server

The ONS 15454 proxy server is a set of functions that allows you to network ONS 15454s in environments where visibility and accessibility between ONS 15454s 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 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 external 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 TCC2 Ethernet interface.
- Processes SNTP (Simple Network Time Protocol) and NTP (Network Time Protocol) requests. ONS 15454 ENEs can derive time-of-day from an SNTP/NTP LAN server through the GNE ONS 15454.
- Processes 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 proxy server is provisioned using the Enable proxy server on port check box on the Provisioning > Network > General tab (see Figure 13-10). 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 proxy server as an ENE or a GNE:

Note If you launch CTC against a node through a NAT (Network Address Translation) or PAT (Port Address Translation) 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 15454 neither installs nor advertises default or static routes. CTC computers can communicate with the ONS 15454 using the TCC2 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.

Figure 13-10 Proxy Server Gateway Settings

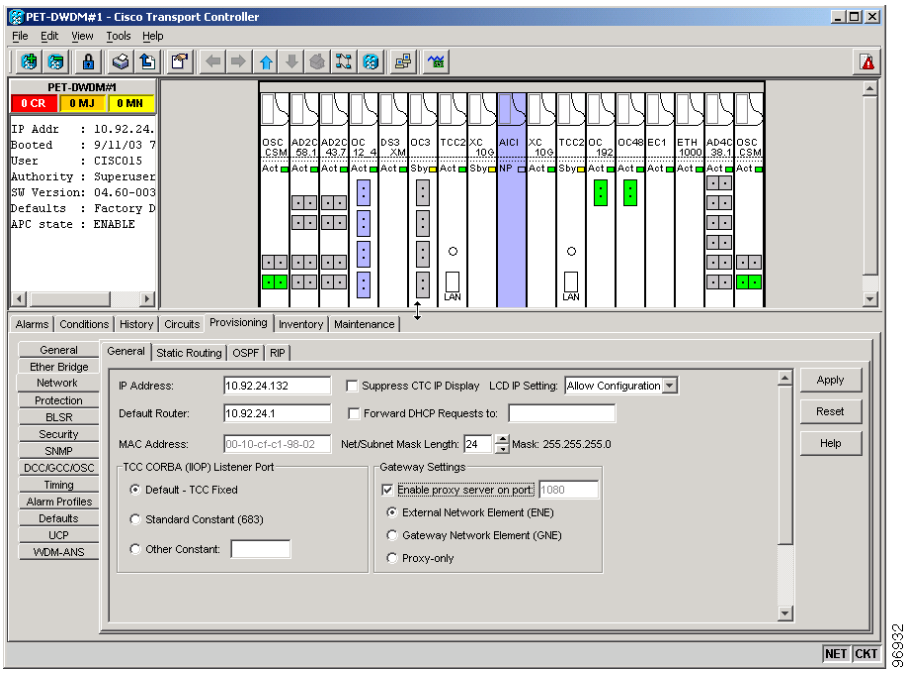


Figure 13-11 shows an ONS 15454 proxy server implementation. A GNE ONS 15454 is connected to a central office LAN and to ENE ONS 15454s. The central office LAN is connected to a NOC LAN, which has CTC computers. The NOC CTC computer and craft technicians must both be able to access the ONS 15454 ENEs. 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 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 ONS 15454 Proxy Server with GNE and ENEs on the Same Subnet

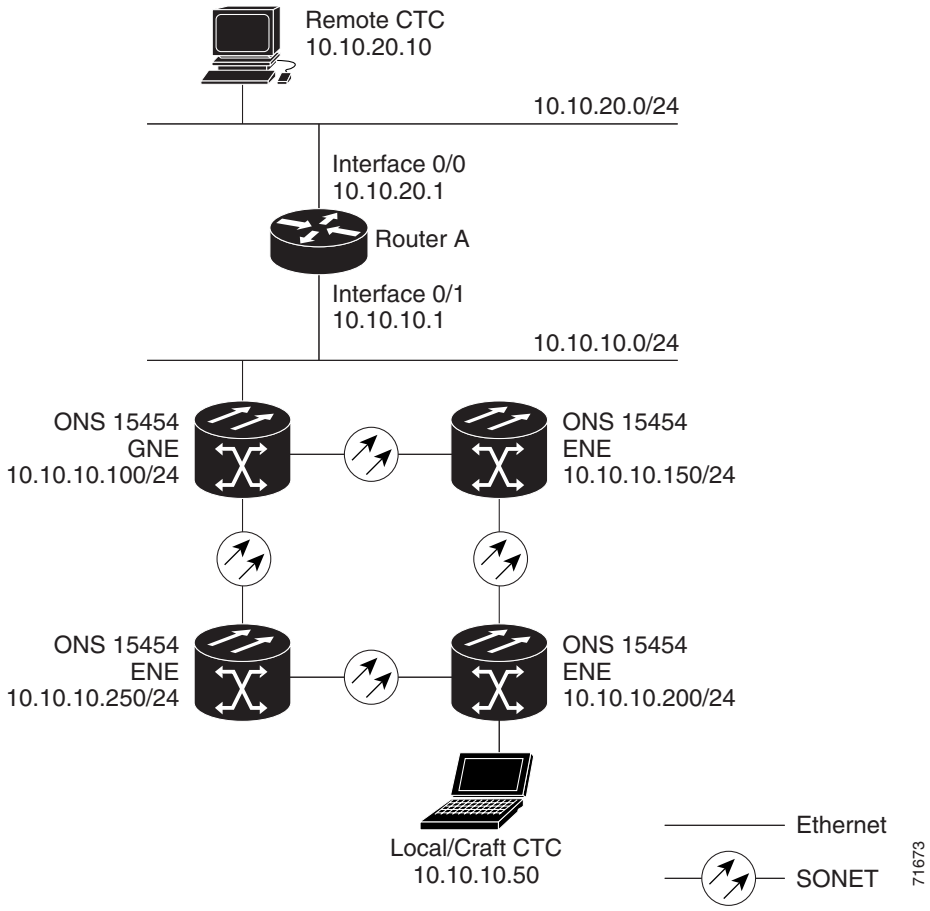


Table 13-2 shows recommended settings for ONS 15454 GNEs and ENEs in the configuration shown in Figure 13-11.

Table 13-2 ONS 15454 Gateway and External NE Settings

Setting	ONS 15454 Gateway NE	ONS 15454 External 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 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 Scenario 7: ONS 15454 Proxy Server with GNE and ENEs on Different Subnets

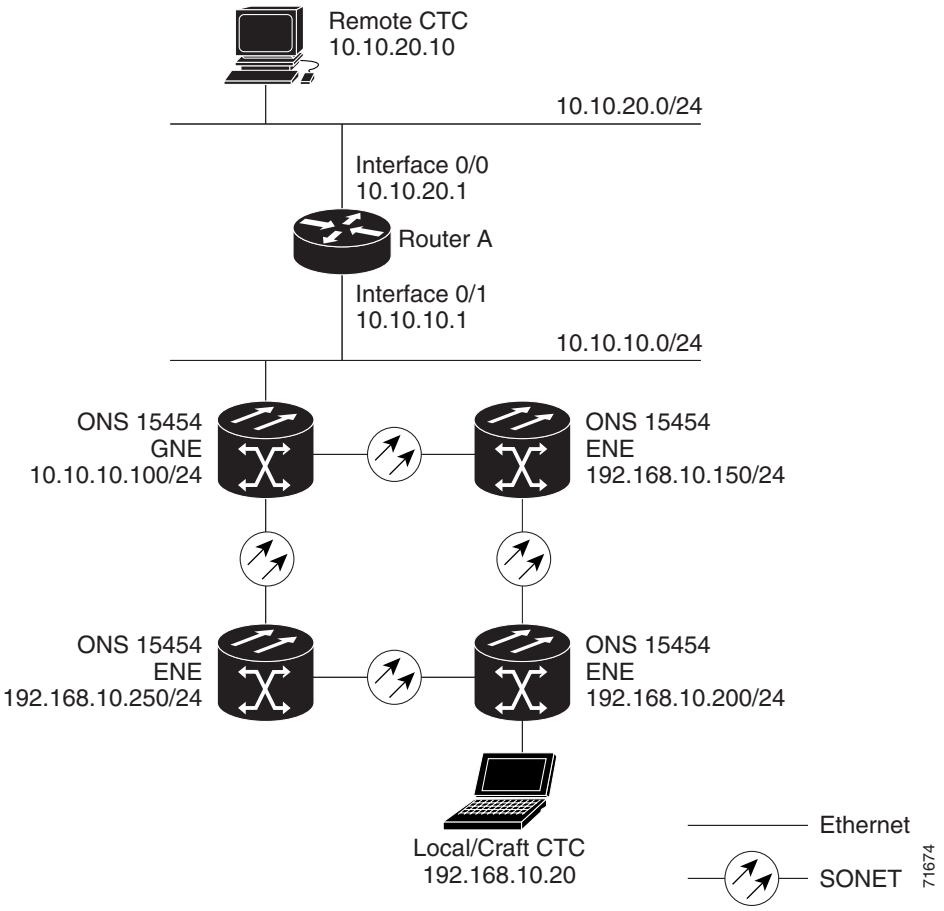


Figure 13-13 Scenario 7: ONS 15454 Proxy Server With ENEs on Multiple Rings

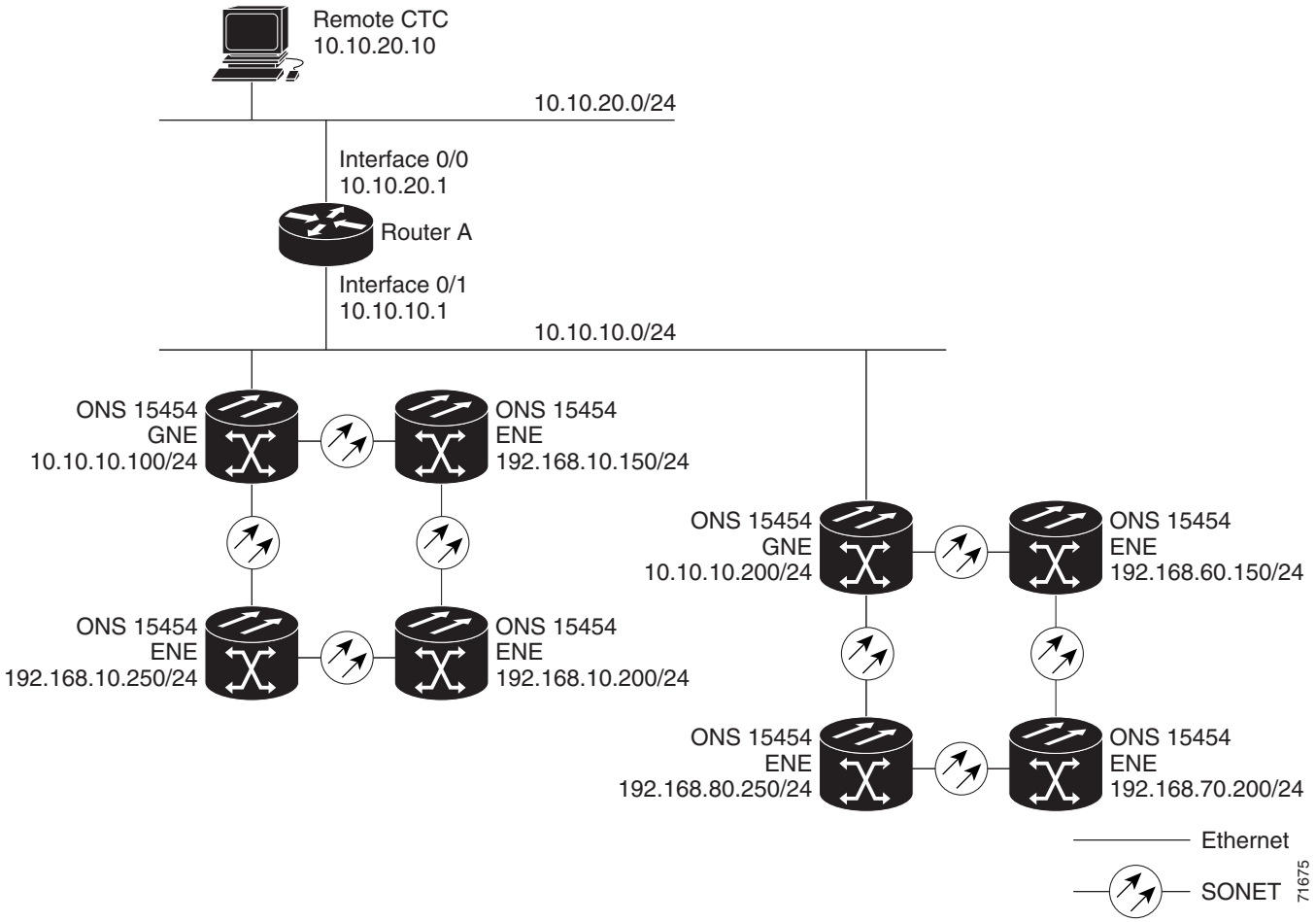


Table 13-3 shows the rules the ONS 15454 follows to filter packets for the firewall when nodes are configured as ENEs and GNEs. If the packet is addressed to the ONS 15454, additional rules, shown in Table 13-4, are applied. Rejected packets are silently discarded.

Table 13-3 Proxy Server Firewall Filtering Rules

Packets Arriving At:	Are Accepted if the Destination IP Address is:
TCC2 Ethernet interface	• The ONS 15454 itself • The ONS 15454'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 itself • Any destination connected through another DCC interface • Within the 224.0.0.0/8 network

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

Packets Arriving At	Accepts	Rejects
TCC2 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 those in the Rejected column • OSPF packets • ICMP[3] packets	• TCP packets addressed to the Telnet port • TCP packets addressed to the 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 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 by performing one of the following:

- 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 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 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. Figure 13-14 shows a network with dual GNEs on the same subnet. Figure 13-15 shows a network with dual GNEs on different subnets.

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

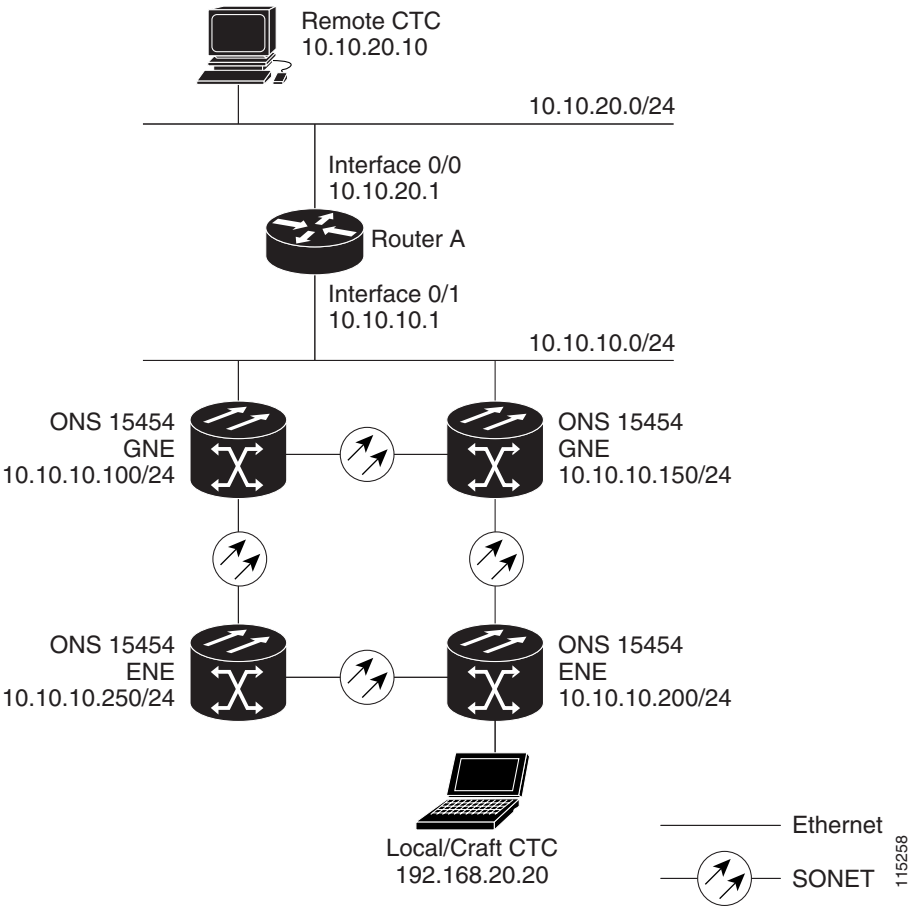
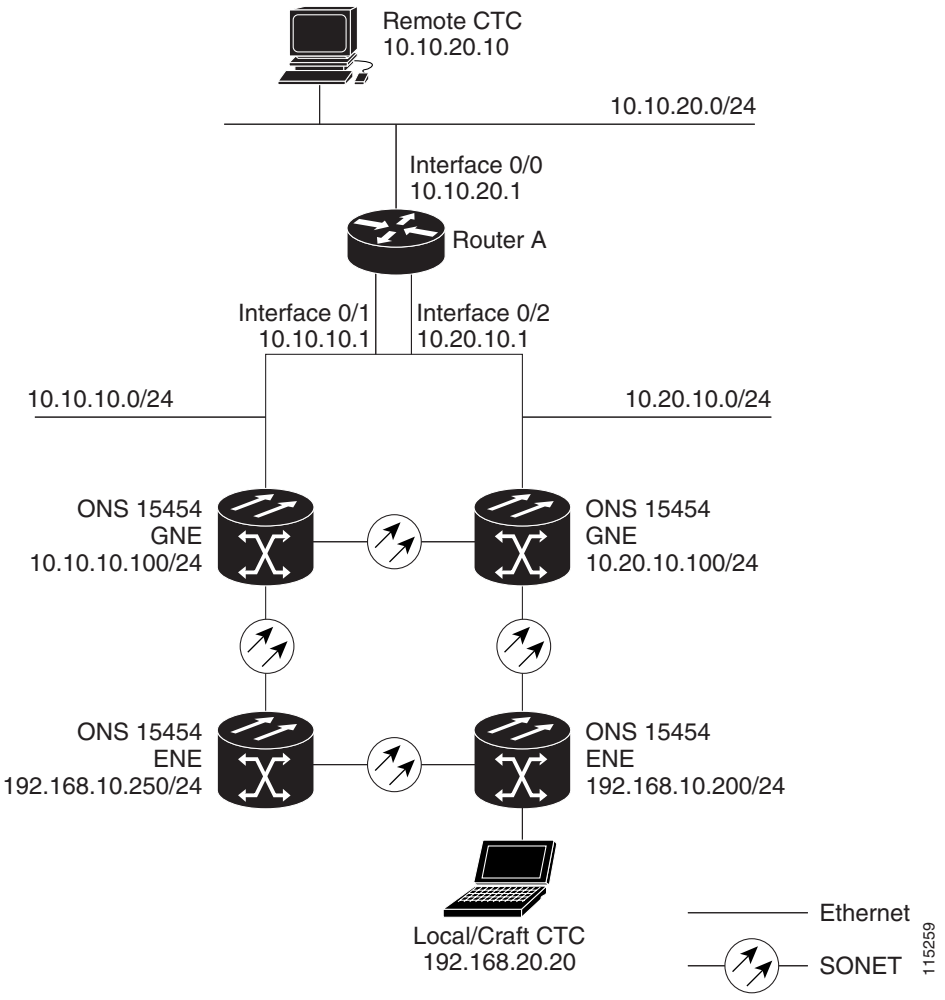


Figure 13-15 Scenario 8: Dual GNEs on Different Subnets



13.3 Routing Table

ONS 15454 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 15454 interface used to access the destination. Values are:
  - motfcc0—The ONS 15454 Ethernet interface, that is, the RJ-45 jack on the TCC2 and the LAN 1 pins on the backplane
  - pdcc0—A SONET data communications channel (SDCC) interface, that is, an OC-N trunk card identified as the SDCC termination

– lo0—A loopback interface

Table 13-5 shows sample routing 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 a destination.
- 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 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 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 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 for external firewalls. Table 13-6 lists the ports that are used by the TCC2.

Table 13-6 Ports Used by the TCC2

Port	Function
0	Reserved
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	Reserved
2361	TL1
3082	TL1
3083	TL1
5001	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
10240-12288	Proxy client
57790	Default TCC listener port

The following ACL (access control list) example shows a firewall configuration when the 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 Common Object Request Broker Architecture (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 (access control list) example shows 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 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 (683) and 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 ***
```