IP Networking

This chapter provides seven 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 set up 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.

11.1 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, 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 15454 to serve as a gateway for ONS 15454s that are not connected to the LAN.
- You can create static routes to enable connections among multiple Cisco Transport Controller (CTC) sessions with ONS 15454s that reside on the same subnet but have different destination IP addresses.
- If ONS 15454s are connected to Open Shortest Path First (OSPF) networks, ONS 15454 network information is automatically communicated across multiple LANs and WANs.
- The ONS 15454 proxy server controls the visibility and accessibility between CTC computers and ONS 15454 element nodes.

11.2 IP Addressing Scenarios

ONS 15454 IP addressing generally has seven common scenarios or configurations. Use the scenarios as building blocks for more complex network configurations. Table 11-1 provides a general list of items to check when setting up ONS 15454s in IP networks.

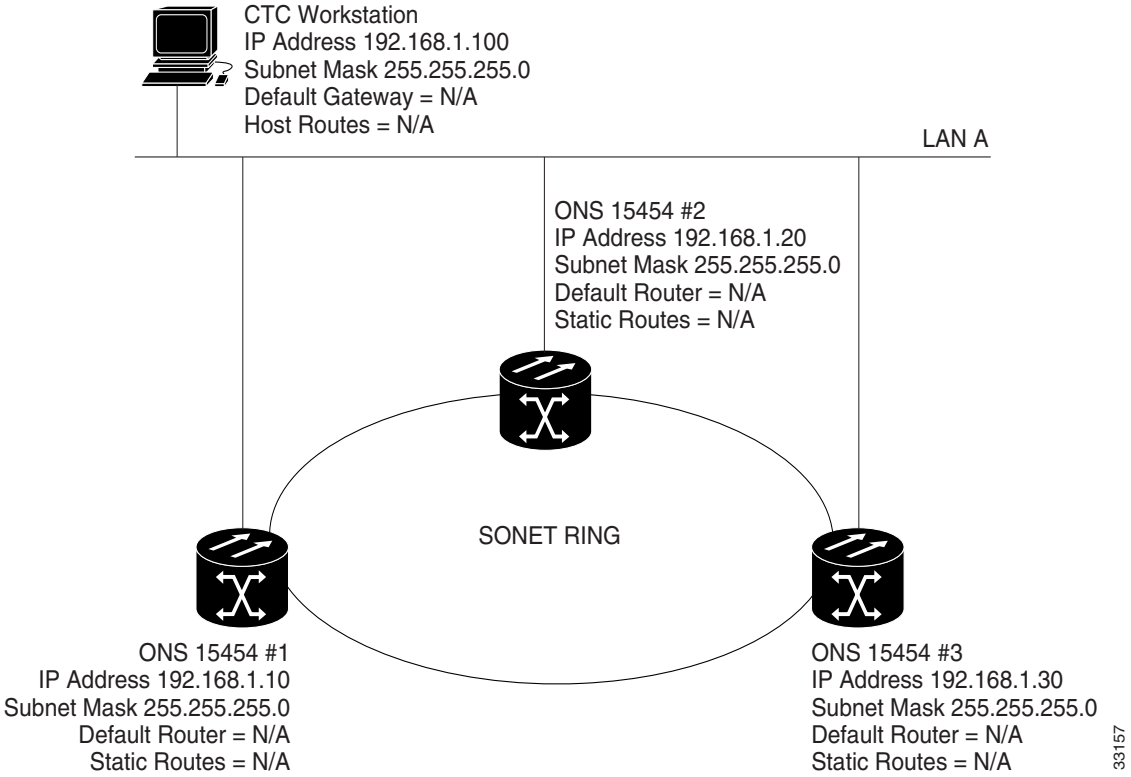
Table 11-1 General ONS 15454 IP Troubleshooting Checklist

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; DCC is enabled on each trunk port

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

Scenario 1 shows a basic ONS 15454 LAN configuration (Figure 11-1 on page 11-3). 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 11-1 Scenario 1: CTC and ONS 15454s on Same Subnet

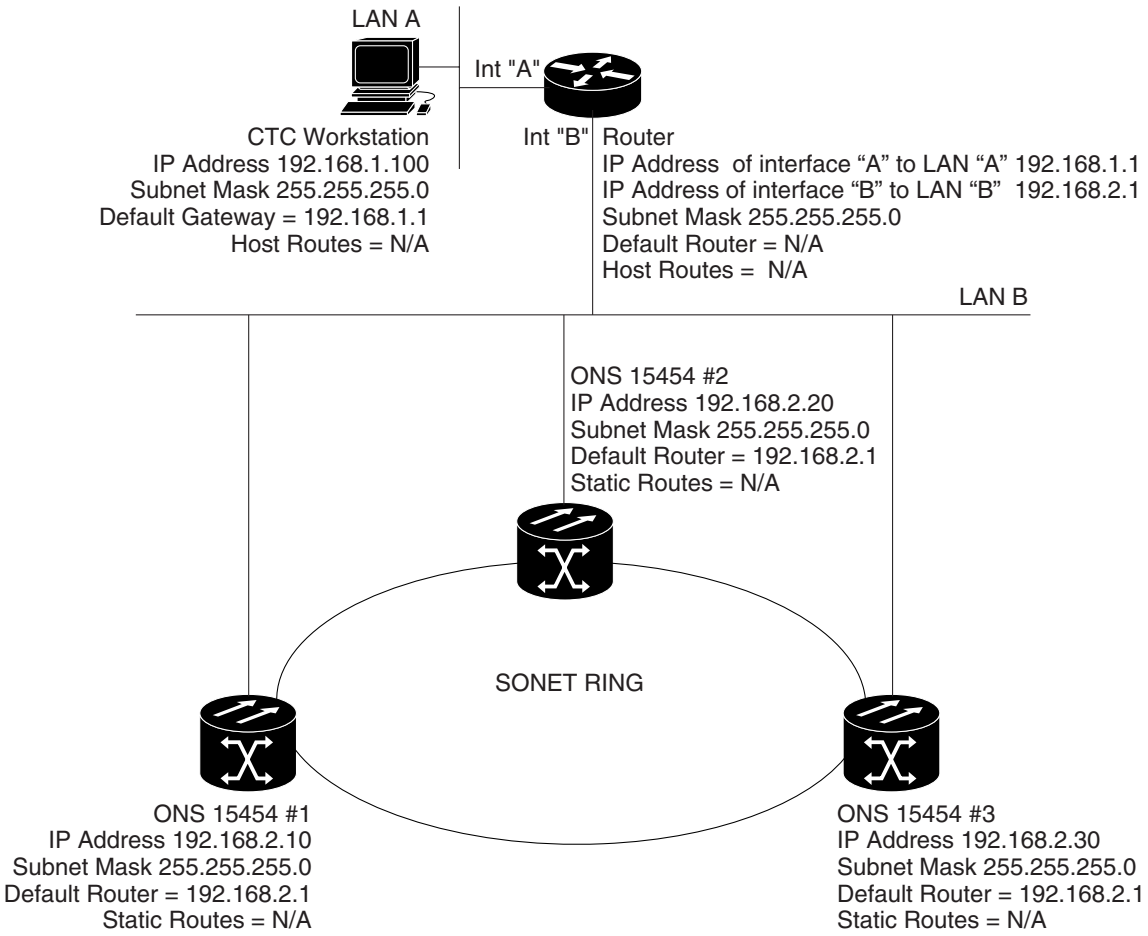


11.2.2 Scenario 2: CTC and ONS 15454s Connected to a Router

In Scenario 2 the CTC computer resides on a subnet (192.168.1.0) and attaches to LAN A (Figure 11-2 on page 11-4). 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 11-2 example, a DHCP server is not available.

Figure 11-2 Scenario 2: CTC and ONS 15454s Connected to Router

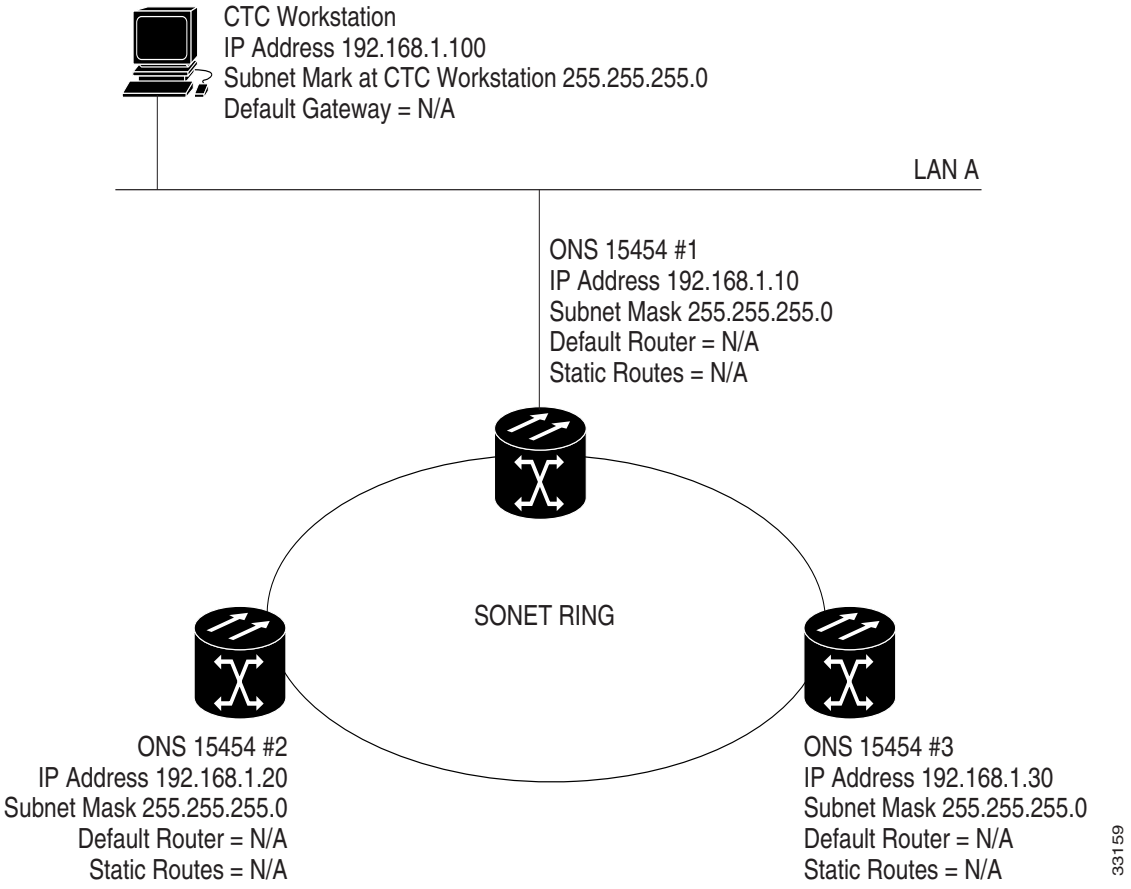


11.2.3 Scenario 3: Using Proxy ARP to Enable an ONS 15454 Gateway

Scenario 3 is similar to Scenario 1, but only one ONS 15454 (node #1) connects to the LAN (Figure 11-3 on page 11-5). 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 15454s #2 and #3.

Note This scenario assumes all CTC connections are to ONS 15454 #1. If you connect a laptop to either ONS 15454 #2 or #3, network partitioning will occur; neither the laptop or the CTC computer will be able to see all nodes. If you want laptops to connect directly to end network elements, you will need to create static routes (see Scenario #5) or enable the ONS 15454 proxy server (see Scenario #7).

Figure 11-3 Scenario 3: Using Proxy ARP



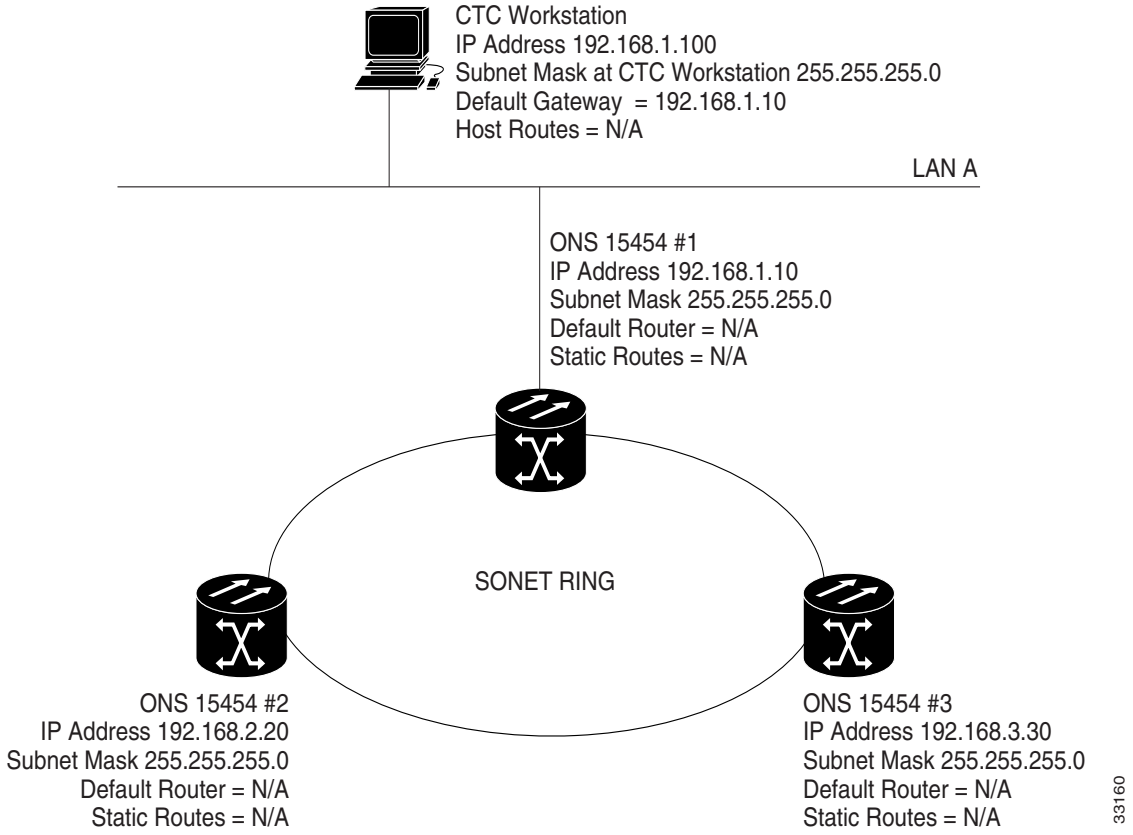
ARP matches higher-level IP addresses to the physical addresses of the destination host. It uses a lookup table (called ARP cache) to perform the translation. When the address is not found in the ARP cache, a broadcast is sent out on the network with a special format called the ARP request. If one of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

11.2.4 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 11-4). 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 ONS 15454s #2 and #3, ONS 15454 #1 is entered as the default gateway on the CTC computer.

Figure 11-4 Scenario 4: Default Gateway on a CTC Computer



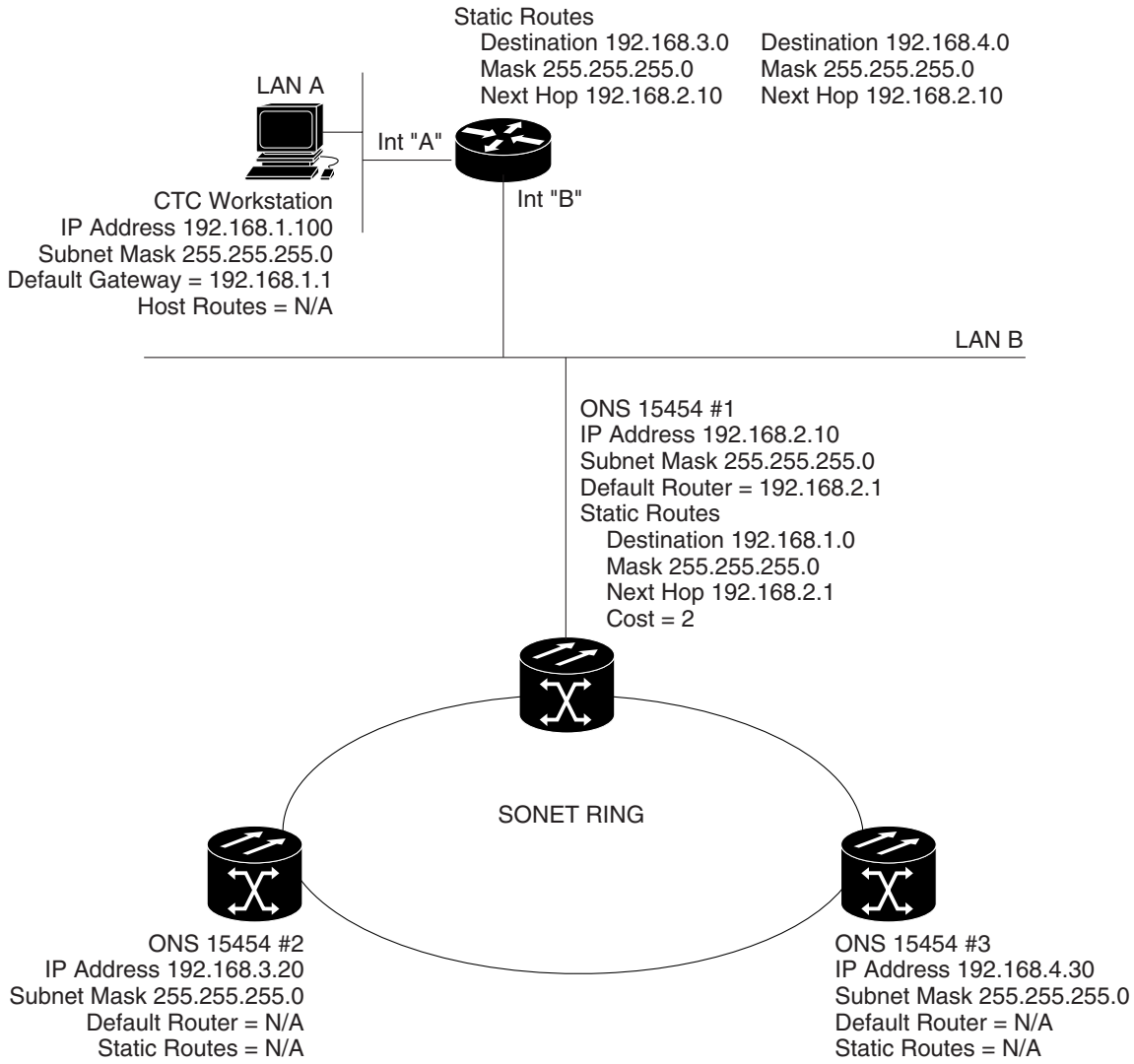
11.2.5 Scenario 5: Using Static Routes to Connect to LANs

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 11-5 on page 11-7, 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 ONS 15454 #1 to the router through interface B. Because ONS 15454s #2 and #3 are on different subnets, proxy ARP does not enable ONS 15454 #1 as a gateway. To connect to CTC computers on LAN A, a static route is created on ONS 15454 #1.

Figure 11-5 Scenario 5: Static Route With One CTC Computer Used as a Destination

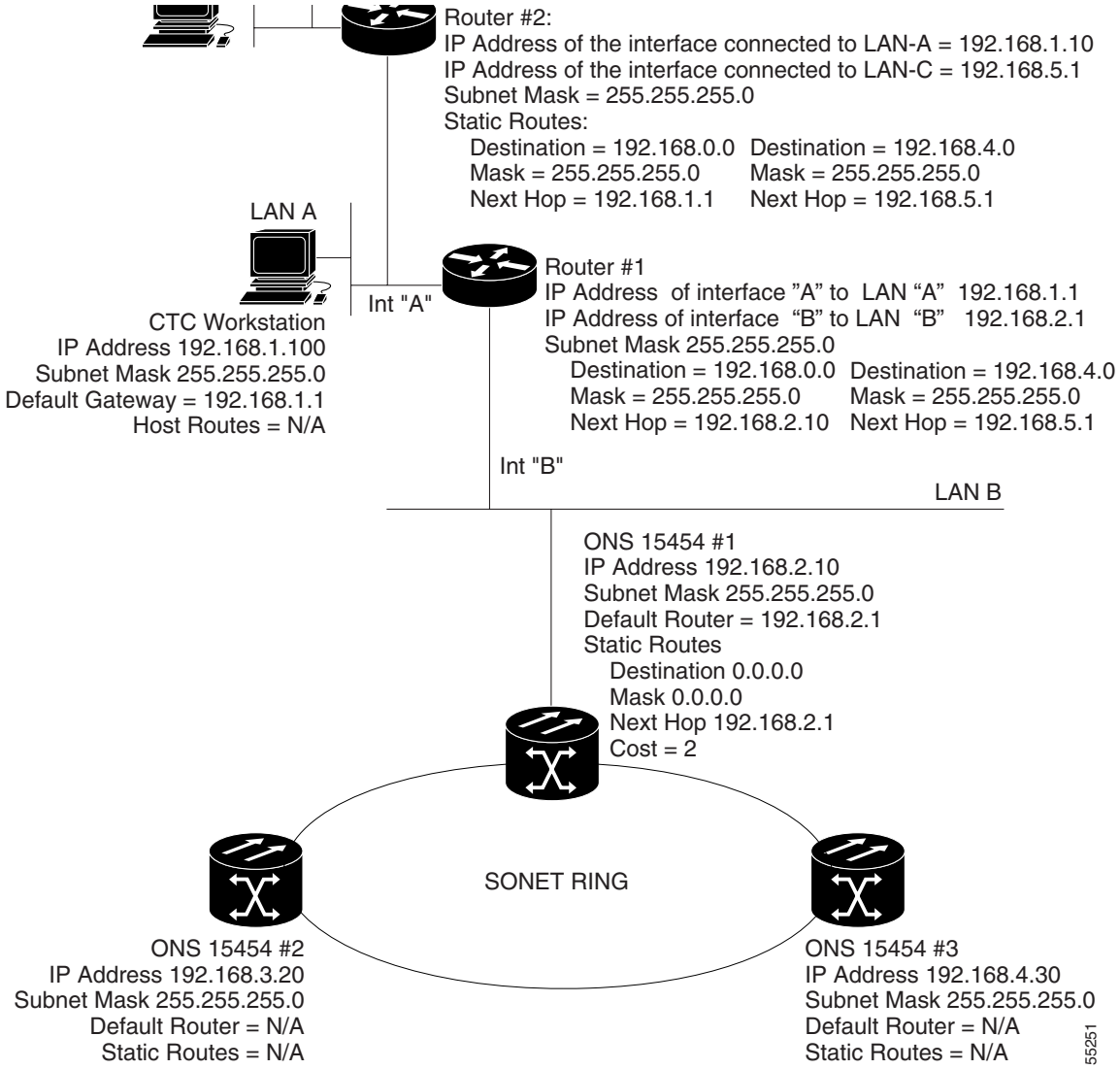


The destination and subnet mask entries control access to the ONS 15454s:

- 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 toa router, enter a destination of 0.0.0.0 and a subnet mask of 0.0.0.0. Figure 11-6 on page 11-8 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 11-6 Scenario 5: Static Route With Multiple LAN Destinations



11.2.6 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 11-7 shows a network enabled for OSPF. Figure 11-8 on page 11-10 shows the same network without OSPF. Static routes must be manually added to the router in order for CTC computers on LAN A to communicate with ONS 15454 #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, that can range from 0 to 4,294,967,295. 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 11-7 Scenario 6: OSPF enabled

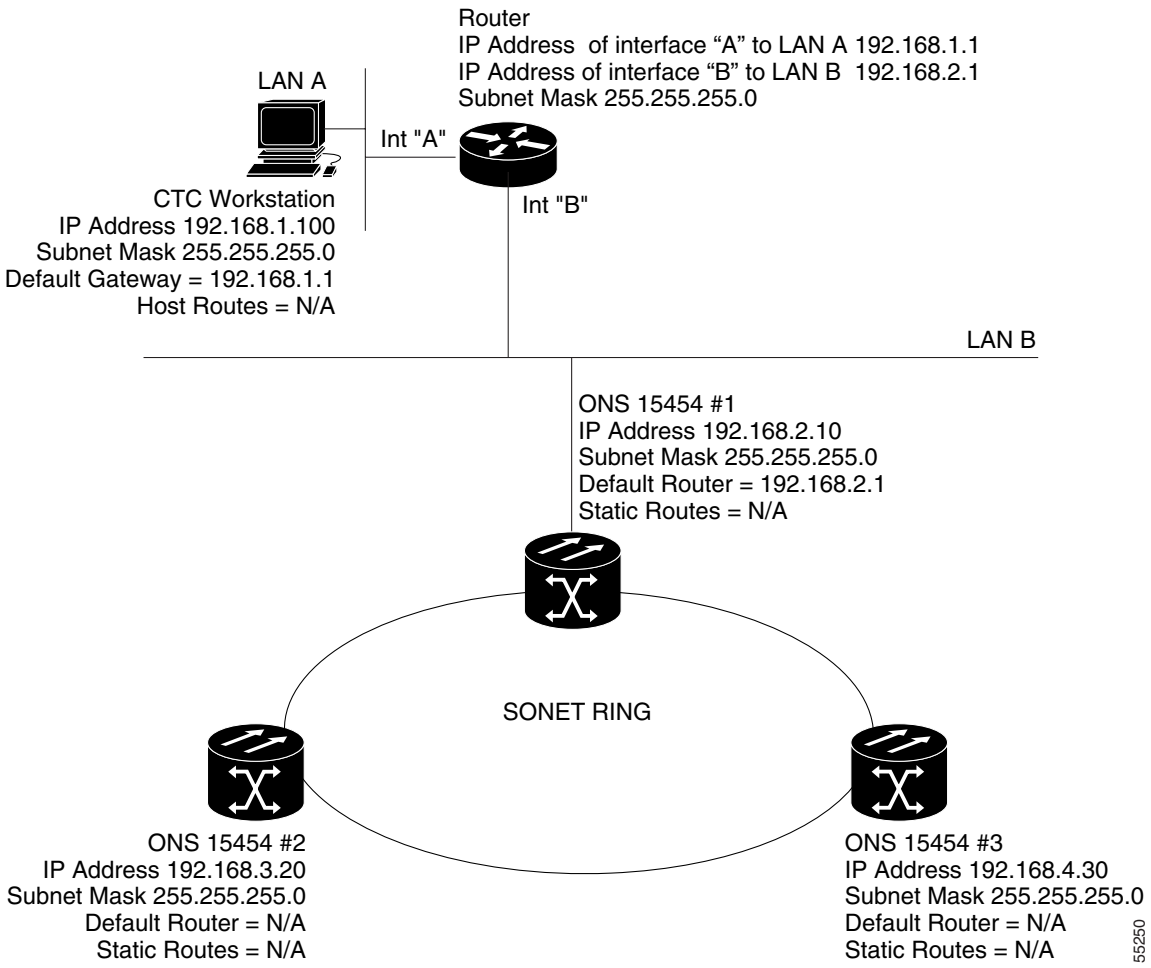
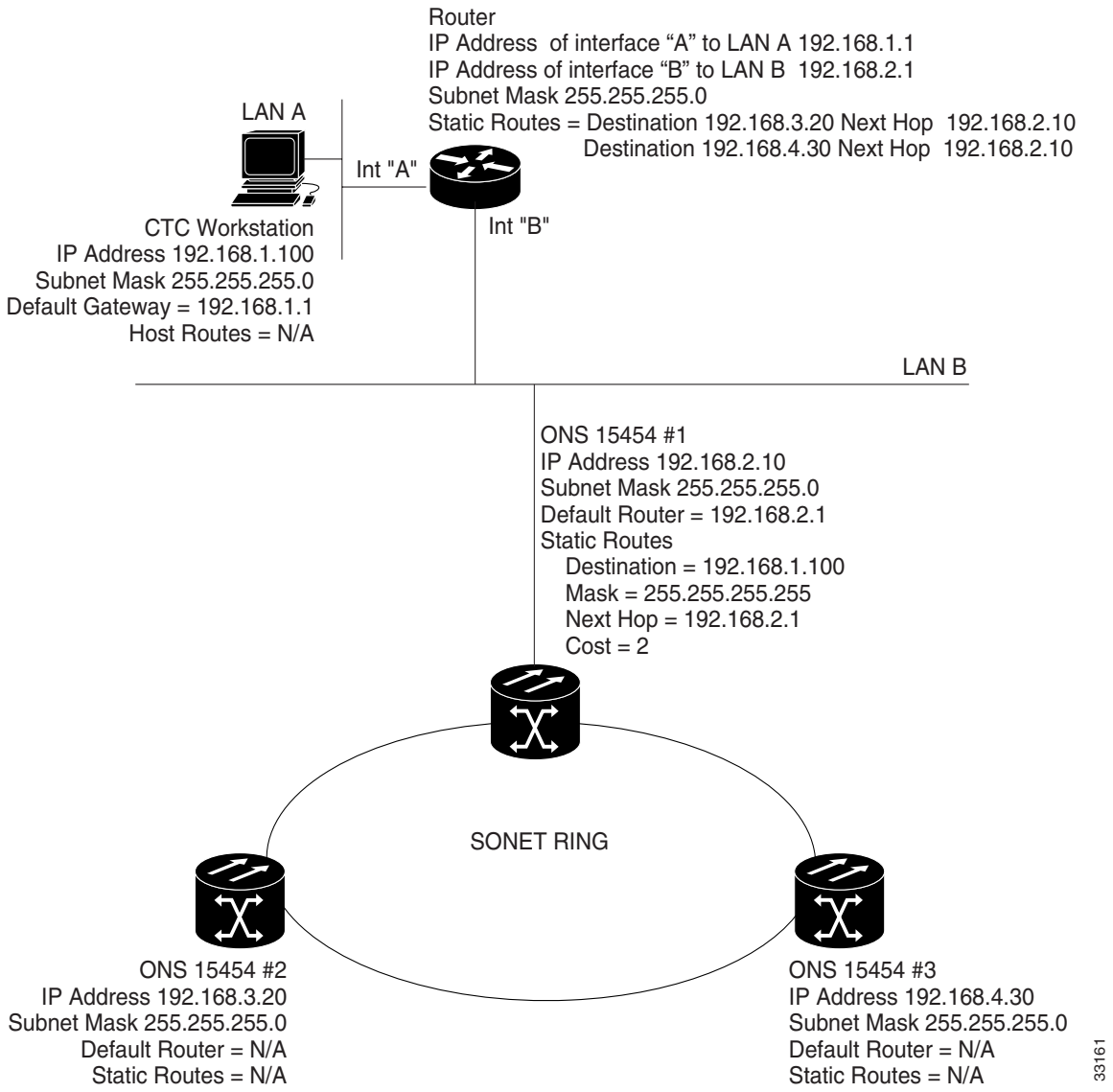


Figure 11-8 Scenario 6: OSPF Not Enabled



11.2.7 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 NE (GNE) and the other ONS 15454s are provisioned as end NEs (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 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 11-3 and Table 11-4) depend on whether the packet arrives at the ONS 15454 DCC or TCC+/TCC2 Ethernet interface.
- Monitors ARP request packets on its Ethernet port. If the ARP request is from an address that is not on the current subnet, the ONS 15454 creates an entry its ARP table. The ARP entry allows the ONS 15454 to reply to an address over the local Ethernet so craft technicians can connect to ONS 15454s without changing the IP addresses of their computers.
- Processes SNTP/NTP requests. Element ONS 15454 NEs can derive time-of-day from an SNTP/NTP LAN server through the GNE ONS 15454.
- Process SNMPv1 traps. The GNE ONS 15454 receives SNMPv1 traps from the ENE ONS 15454s and forwards them to all provisioned SNMPv1 trap destinations.

The ONS 15454 proxy server is provisioned using three check boxes on the Provisioning > Network > General tab (see Figure 11-9 on page 11-12):

- Enable Proxy—When enabled, 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 Enable Proxy is off, the node does not proxy for any CTC clients, although any established proxy connections will continue until the CTC client exits.

Note If you launch CTC against a node through a NAT/PAT router and that node does not have proxy enabled, your CTC session will start and initially appear to be fine. However CTC will never receive alarm updates and will disconnect and reconnect 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.

- Craft Access Only—When enabled, the ONS 15454 neither installs nor advertises default or static routes. CTC computers can communicate with the ONS 15454 using the TCC+/TCC2 craft port, but they cannot communicate directly with any other DCC-connected ONS 15454.
- Enable Firewall—If selected, 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.

Figure 11-9 Proxy Server Gateway Settings

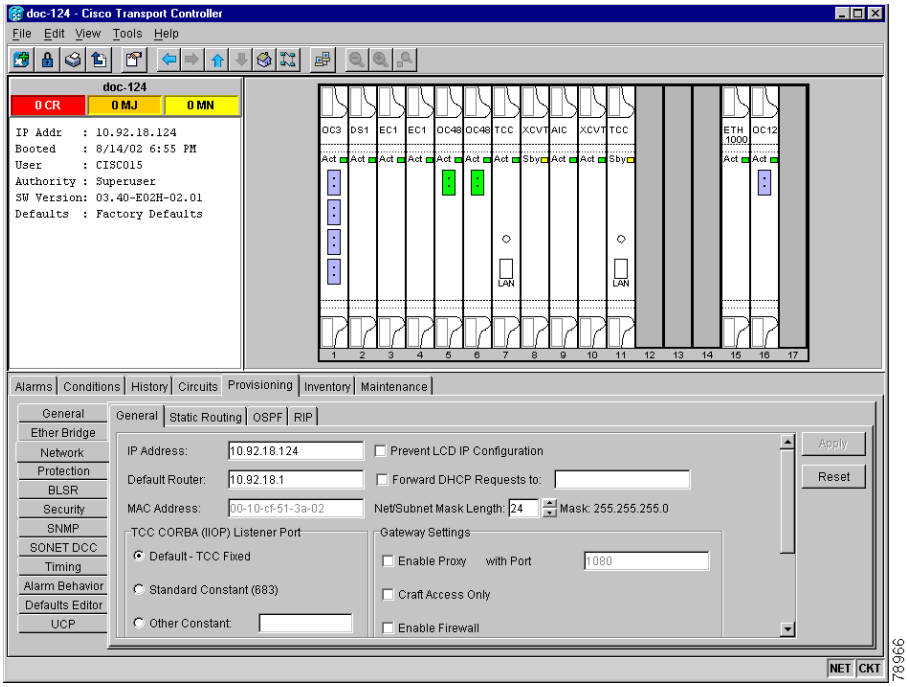


Figure 11-10 on page 11-13 shows an ONS 15454 proxy server implementation. A GNE ONS 15454 is connected to a central office LAN and to ENE ONS 15454s. The central office LAN is connected to a NOC LAN, which has CTC computers. The NOC CTC computer and craft technicians must both be able to access the 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 co-located, the craft LAN ports could be connected to a hub. However, the hub should have no other network connections.

Figure 11-10 ONS 15454 Proxy Server with GNE and ENEs on the Same Subnet

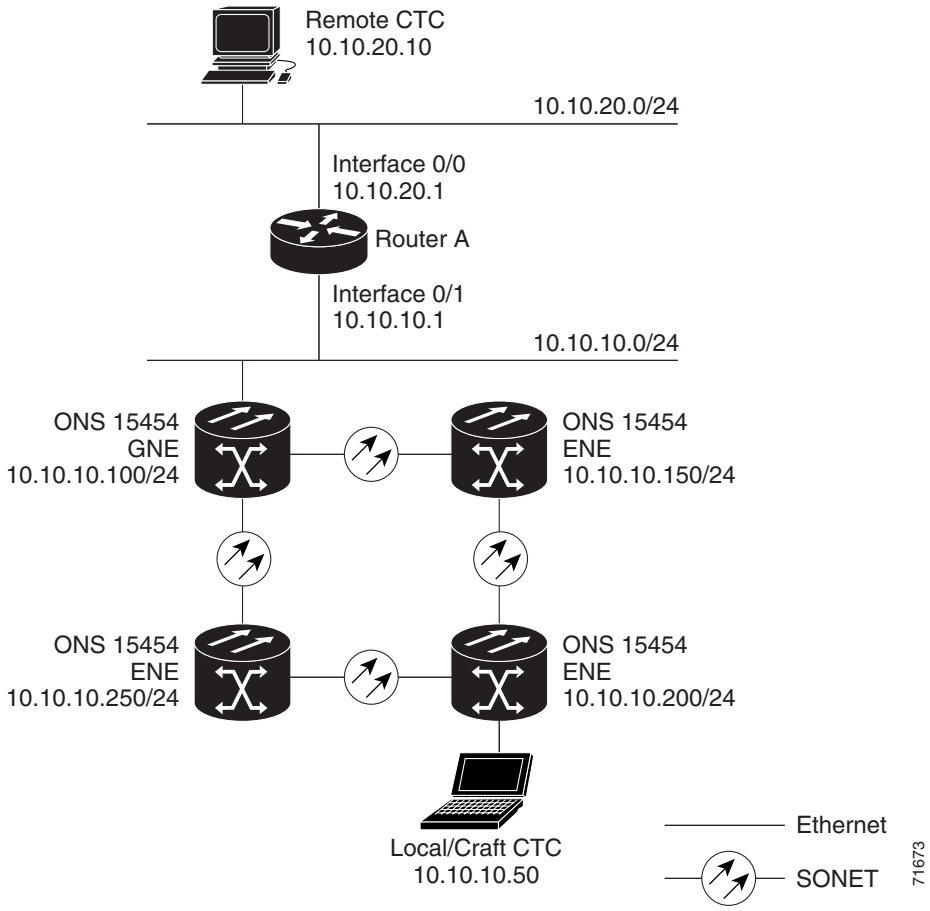


Table 11-2 shows recommended settings for ONS 15454 GNEs and ENEs in the configuration shown in Figure 11-10.

Table 11-2 ONS 15454 Gateway and Element NE Settings

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

Figure 11-11 on page 11-14 shows the same proxy server implementation with ONS 15454 ENEs on different subnets. Figure 11-12 on page 11-15 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 11-2.

Figure 11-11 Scenario 7: ONS 15454 Proxy Server with GNE and ENEs on Different Subnets

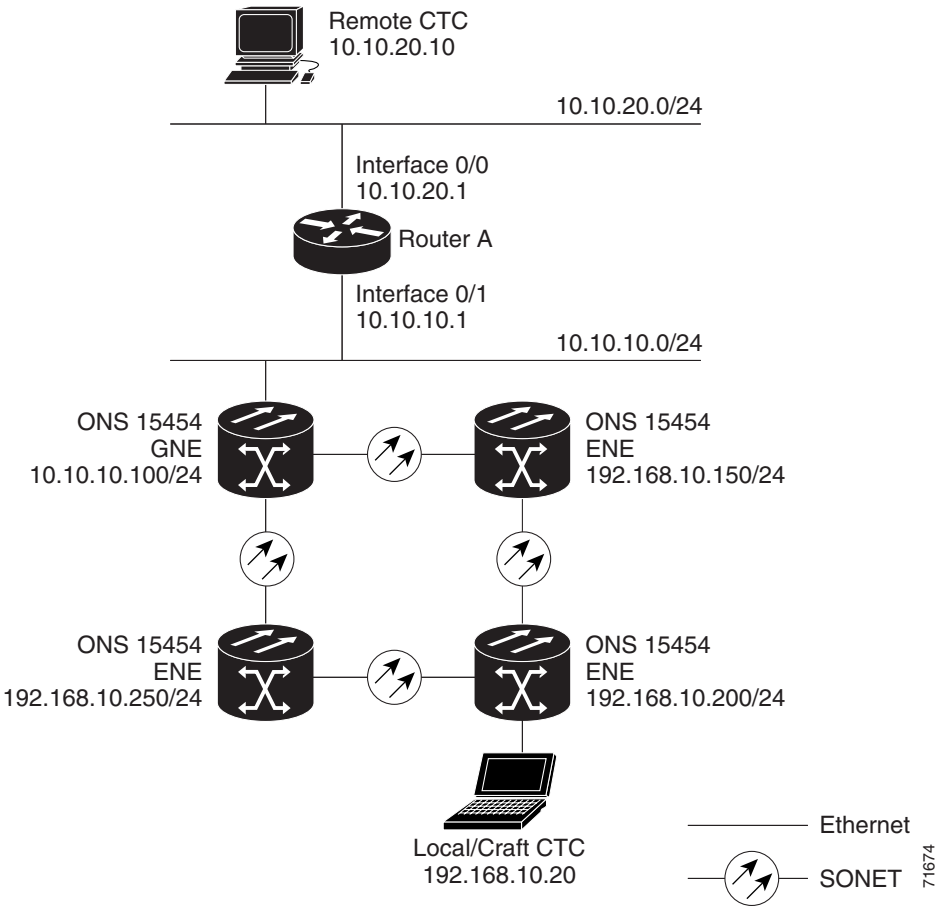


Figure 11-12 Scenario 7: ONS 15454 Proxy Server With ENEs on Multiple Rings

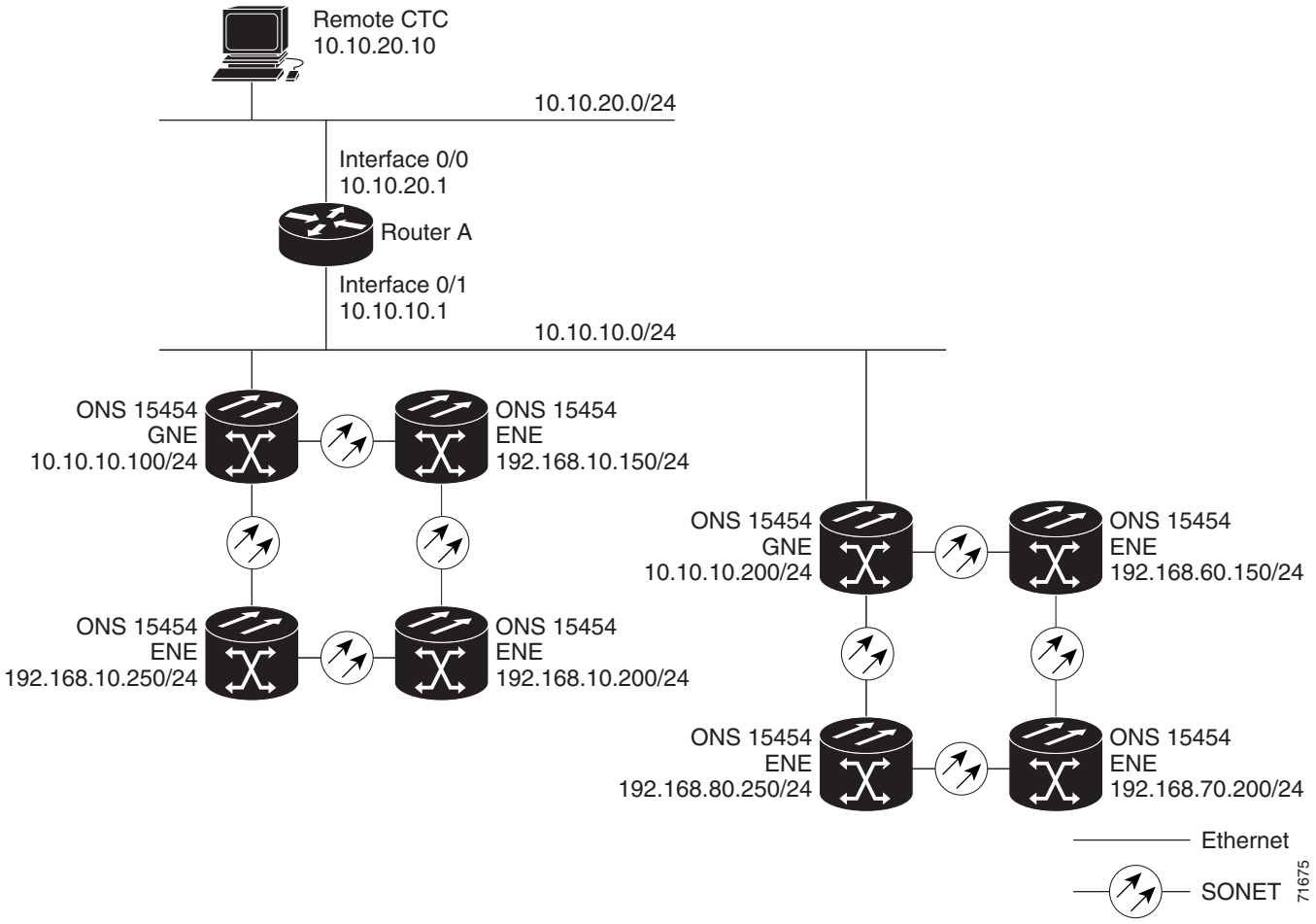


Table 11-3 shows the rules the ONS 15454 follows to filter packets when Enable Firewall is enabled. If the packet is addressed to the ONS 15454, additional rules, shown in Table 11-4 on page 11-16, are applied. Rejected packets are silently discarded.

Table 11-3 Proxy Server Firewall Filtering Rules

Packets arriving at:	Are accepted if the IP destination address is:
TCC+ 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 11-4 Proxy Server Firewall Filtering Rules When Packet Addressed to ONS 15454

Packets Arrive At	Accepted	Rejected
TCC+ Ethernet Interface	• All 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 • 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 15454s on the same Ethernet segment must have the same Craft Access Only setting. Mixed values will produce unpredictable results, and may leave some nodes unreachable through the shared Ethernet segment.
2. All DCC-connected ONS 15454s on the same Ethernet segment must have the same Enable Firewall setting. Mixed values will produce unpredictable results. Some nodes may become unreachable.
3. If you enable Enable Firewall, always check Enable Proxy. If Enable Proxy is not enabled, CTC will not be able to see nodes on the DCC side of the ONS 15454.
4. If Craft Access Only is enabled, check Enable Proxy. If Enable Proxy is not enabled, CTC will not be able to see nodes on the DCC side of the ONS 15454.

If nodes become unreachable in cases 1, 2, and 3, 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 the Ethernet cable from the unreachable ONS 15454. Connect a CTC computer directly to the ONS 15454.

11.3 Routing Table

ONS 15454 routing information is displayed on the Maintenance > Routing Table tabs (Figure 11-13 on page 11-17). 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:
  - cpm0—The ONS 15454 Ethernet interface, that is, the RJ-45 jack on the TCC+/TCC2and 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

Figure 11-13 Viewing the ONS 15454 routing table

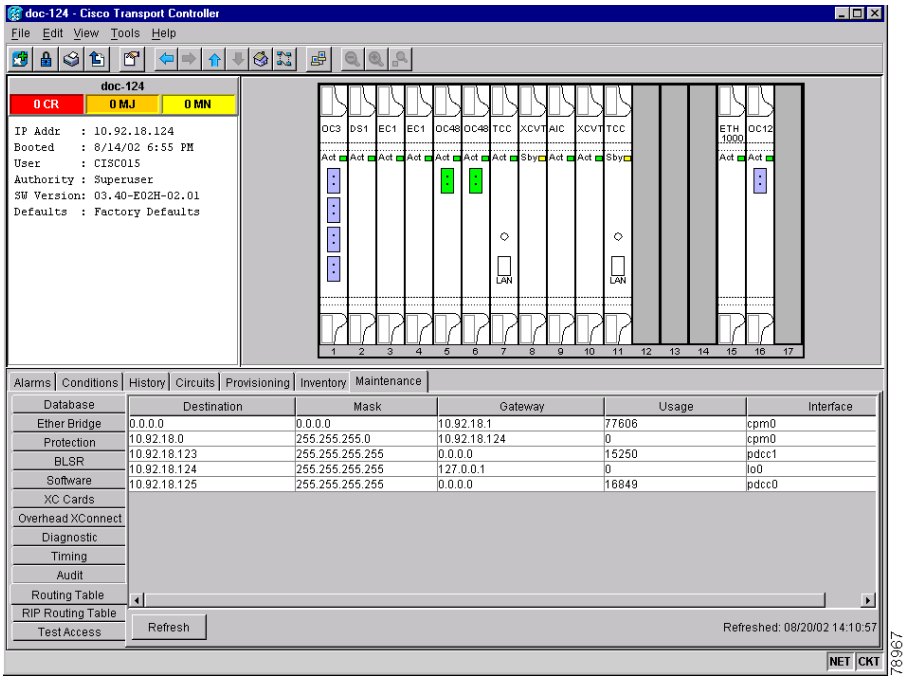


Table 11-5 shows sample routing entries for an ONS 15454.

Table 11-5 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 will be 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 will be sent to this gateway.
- Interface (cpm0) 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 (cpm0) 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 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.

11.4 Provisioning an External Firewall

Table 11-6 shows the ports that are used by the TCC+/TCC2.

Table 11-6 Ports Used by the TCC+/TCC2

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 TCC+/TCC2
2361	TL1
3082	TL1

Table 11-6 Ports Used by the TCC+/TCC2 (continued)

Port	Function
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

11.4.1 Access Control List Example With Proxy Server Not Enabled

The following ACL (access control list) examples shows a firewall configuration when the Proxy Server feature 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 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 57790
access-list 100 remark *** allows CTC communication with the 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 the 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 ***
```

11.4.2 Access Control List Example With Proxy Server Enabled

The following ACL (access control list) examples shows a firewall configuration when the Proxy Server feature 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 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 15454 GNE  ***

access-list 101 remark *** Outbound ACL, NE -> CTC ***
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 ***
```