



## IP Networking

---

This chapter provides eight scenarios showing Cisco ONS 15454 SDH nodes 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 SDH Procedure Guide*.

Chapter topics include:

- [13.1 IP Networking Overview, page 13-1](#)
- [13.2 IP Addressing Scenarios, page 13-2](#)
- [13.3 Routing Table, page 13-18](#)



**Note**

---

To connect ONS 15454 SDH nodes 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 15454 SDH nodes 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 SDH login node groups that allow you to provision non-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 SDH to serve as a gateway for ONS 15454 SDH nodes that are not connected to the LAN.
- Static routes can be created to enable connections among multiple CTC sessions with ONS 15454 SDH nodes that reside on the same subnet but have different destination IP addresses.
- ONS 15454 SDH nodes can be connected to OSPF networks so ONS 15454 SDH network information is automatically communicated across multiple LANs and WANs.
- The ONS 15454 SDH proxy server can control the visibility and accessibility between CTC computers and ONS 15454 SDH element nodes.

## 13.2 IP Addressing Scenarios

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

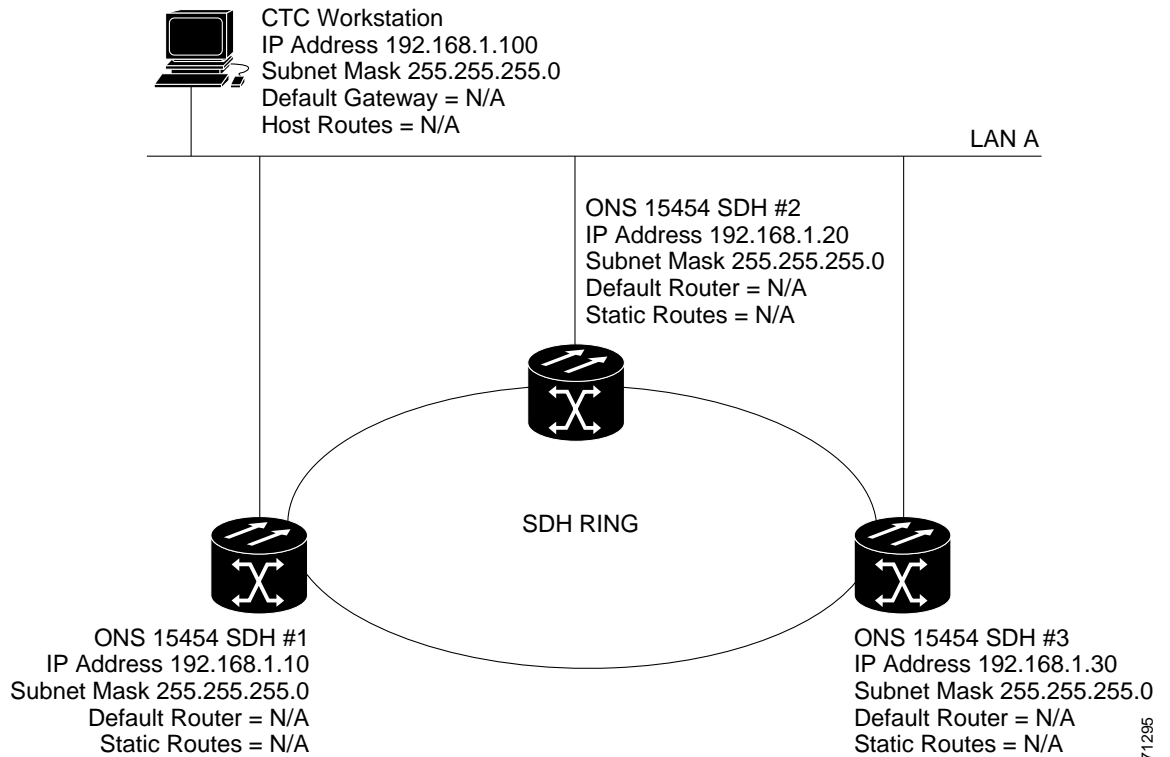
**Table 13-1 General ONS 15454 SDH IP Troubleshooting Checklist**

Item	What to check
Link integrity	Verify that link integrity exists between: <ul style="list-style-type: none"> <li>• CTC computer and network hub/switch</li> <li>• ONS 15454 SDH nodes (backplane wire-wrap pins or RJ-45 port) and network hub/switch</li> <li>• Router ports and hub/switch ports</li> </ul>
ONS 15454 SDH hub/switch ports	If connectivity problems occur, set the hub or switch port that is connected to the ONS 15454 SDH to 10 Mbps half-duplex.
Ping	Ping the node to test connections between computers and ONS 15454 SDH nodes.
IP addresses/subnet masks	Verify that ONS 15454 SDH IP addresses and subnet masks are set up correctly.
Optical connectivity	Verify that ONS 15454 SDH optical trunk (span) ports are in service; DCC is enabled on each trunk port.

### 13.2.1 Scenario 1: CTC and ONS 15454 SDH Nodes on Same Subnet

Scenario 1 shows a basic ONS 15454 SDH LAN configuration ([Figure 13-1 on page 13-3](#)). The ONS 15454 SDH nodes and CTC computer reside on the same subnet. All ONS 15454 SDH nodes connect to LAN A and all ONS 15454 SDH nodes have DCC connections.

Figure 13-1 Scenario 1: CTC and ONS 15454 SDH Nodes on the Same Subnet

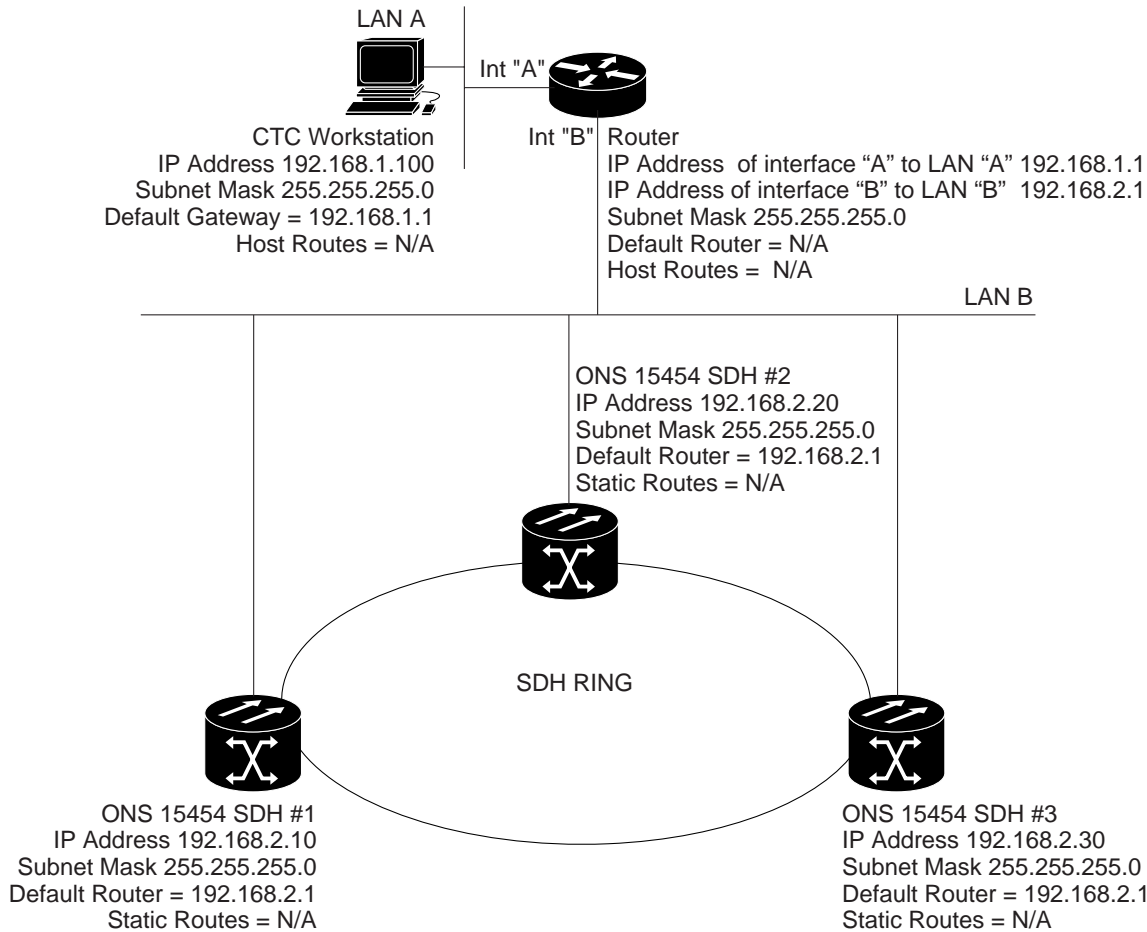


## 13.2.2 Scenario 2: CTC and ONS 15454 SDH Nodes Connected to a Router

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

On the CTC computer, the default gateway is set to router interface A. If the LAN uses Dynamic Host Configuration Protocol (DHCP), the default gateway and IP address are assigned automatically. In the example shown in Figure 13-2 on page 13-4, a DHCP server is not available.

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



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

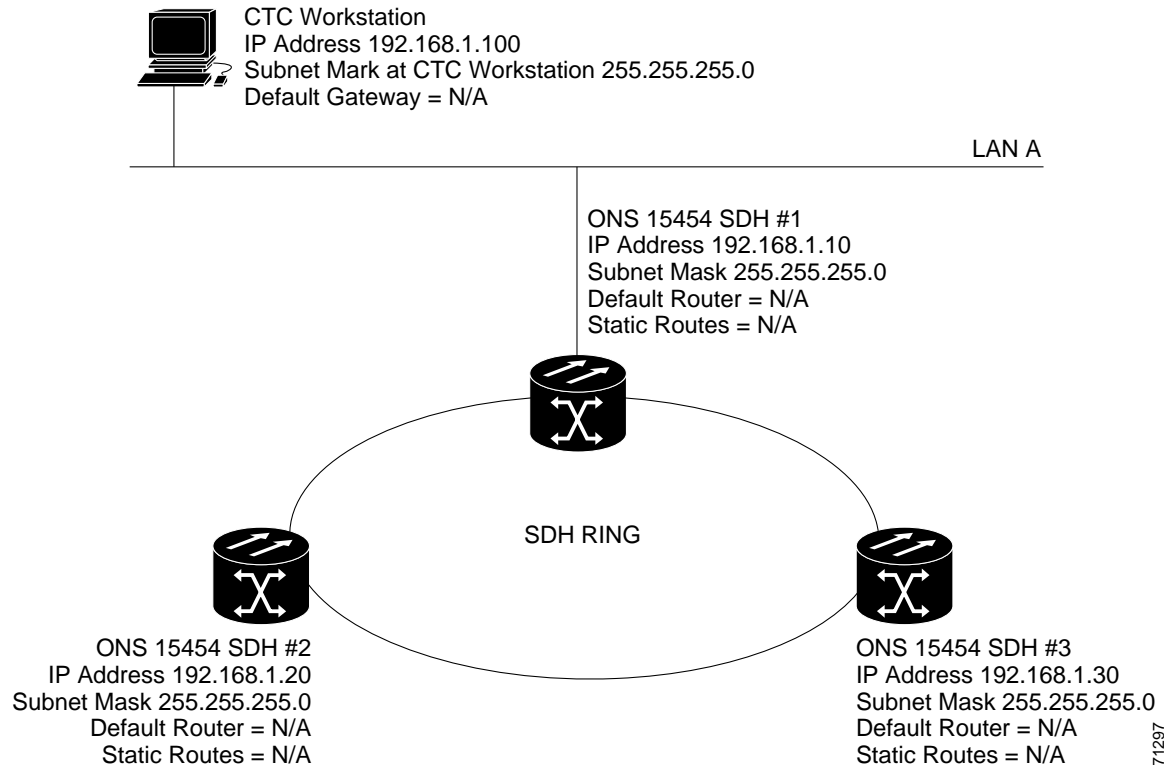
Scenario 3 is similar to Scenario 1, but only one ONS 15454 SDH (Node 1) connects to the LAN (Figure 13-3 on page 13-5). Two nodes (Nodes 2 and 3) connect to Node 1 through the SDH DCC. Because all three nodes are on the same subnet, Proxy ARP enables Node 1 to serve as a gateway for Nodes 2 and 3.



#### Note

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

Figure 13-3 Scenario 3: Using Proxy ARP



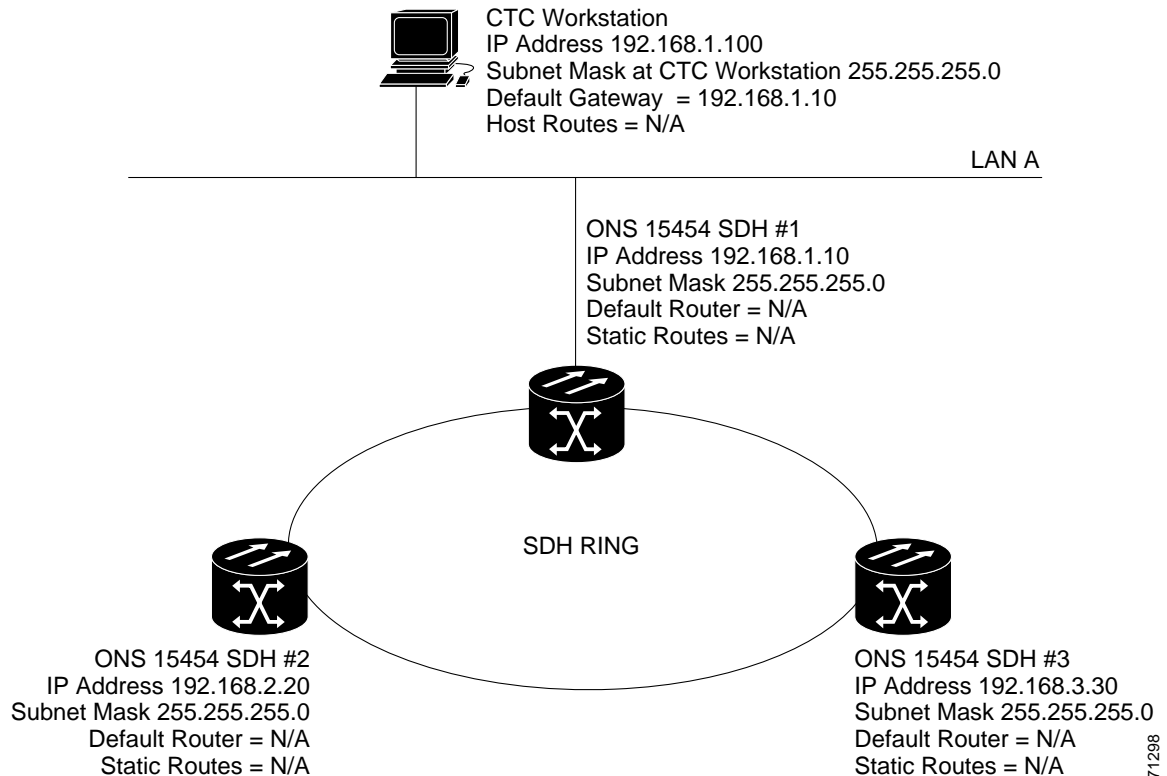
ARP matches higher-level IP addresses to the physical addresses of the destination host. It uses a lookup table (called an ARP cache) to perform the translation. When the address is not found in the ARP cache, a broadcast is sent out on the network with a special format called the ARP request. If one 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 SDH to respond to the ARP request for ONS 15454 SDH nodes that are not connected to the LAN. (ONS 15454 SDH proxy ARP requires no user configuration.) The DCC-connected ONS 15454 SDH nodes must reside on the same subnet. When a LAN device sends an ARP request to an ONS 15454 SDH that is not connected to the LAN, the gateway ONS 15454 SDH returns its MAC address to the LAN device. The LAN device then sends the datagram for the remote ONS 15454 SDH to the MAC address of the proxy ONS 15454 SDH. The proxy ONS 15454 SDH uses its routing table to forward the datagram to the non-LAN ONS 15454 SDH.

## 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 13-4). 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 Nodes 2 and 3, Node 1 is entered as the default gateway on the CTC computer.

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



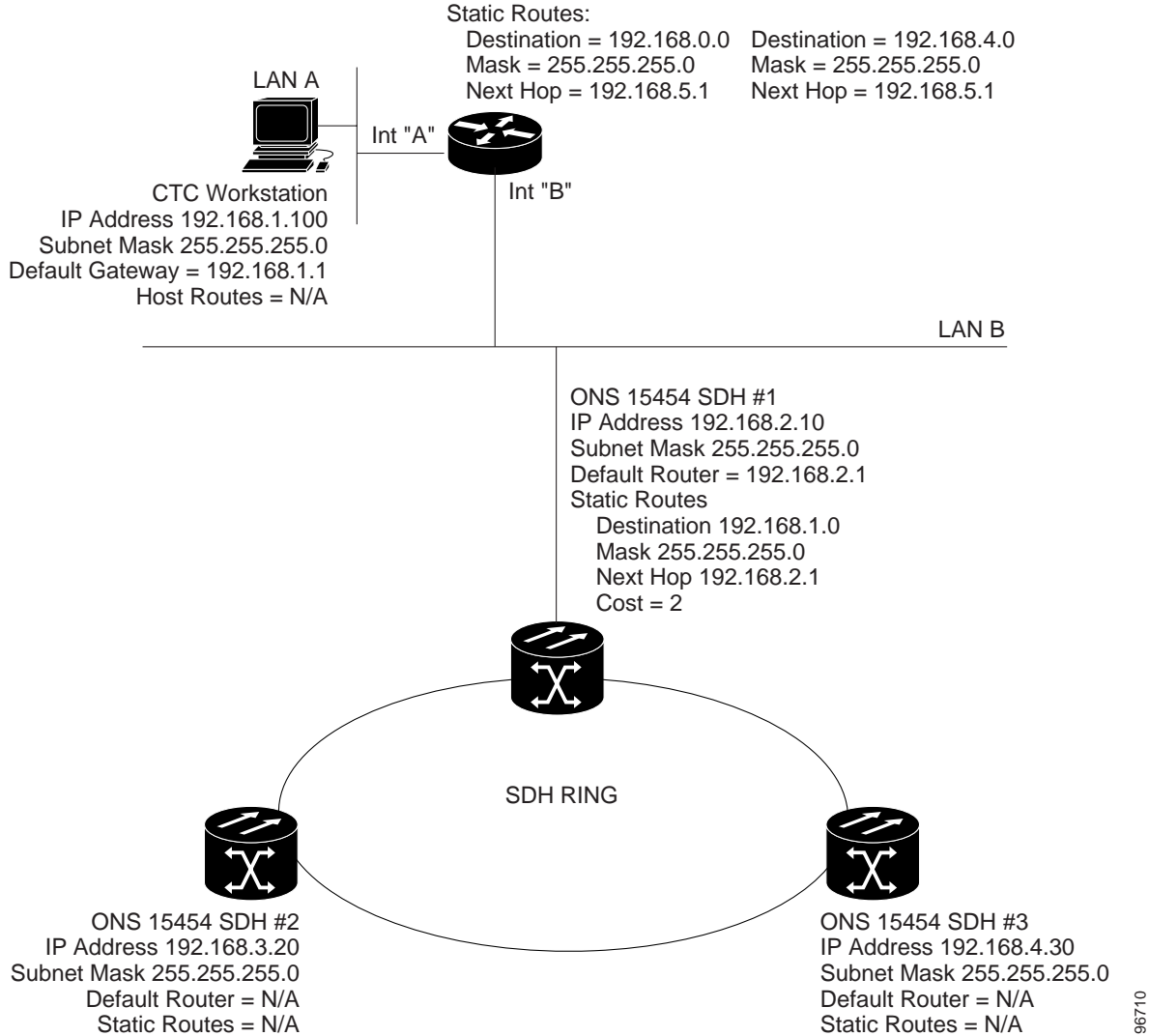
## 13.2.5 Scenario 5: Using Static Routes to Connect to LANs

Static routes are used for two purposes:

- To connect ONS 15454 SDH nodes to CTC sessions on one subnet that are connected by a router to ONS 15454 SDH nodes 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 15454 SDH nodes residing on the same subnet.

In [Figure 13-5 on page 13-7](#), 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 15454 SDH nodes residing on different subnets are connected through Node1 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 13-5 Scenario 5: Static Route With One CTC Computer Used as a Destination

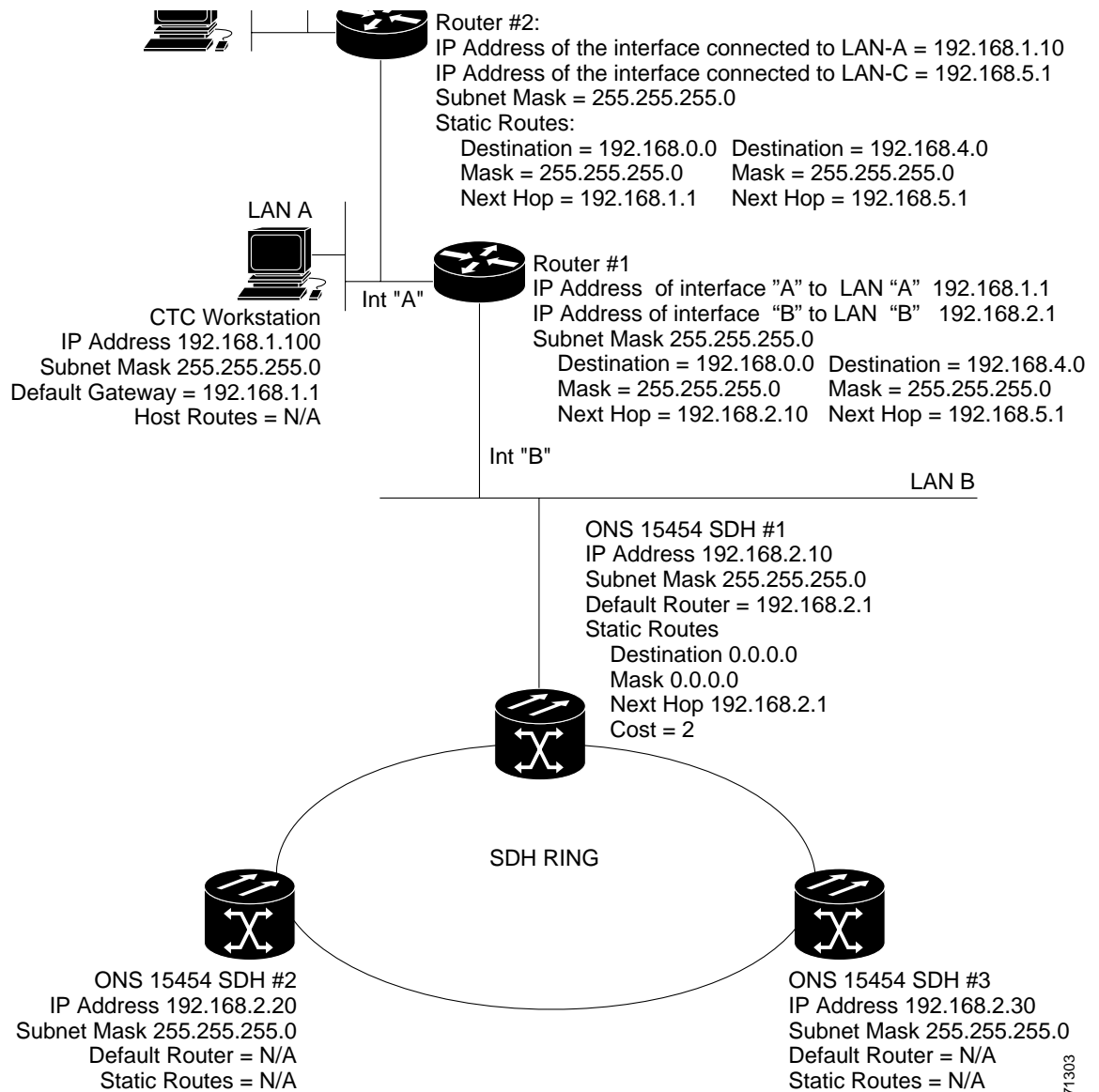


The destination and subnet mask entries control access to the ONS 15454 SDH nodes:

- 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 13-6 on page 13-8](#) 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 13-6 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 continuously recalculated to capture ongoing topology changes.

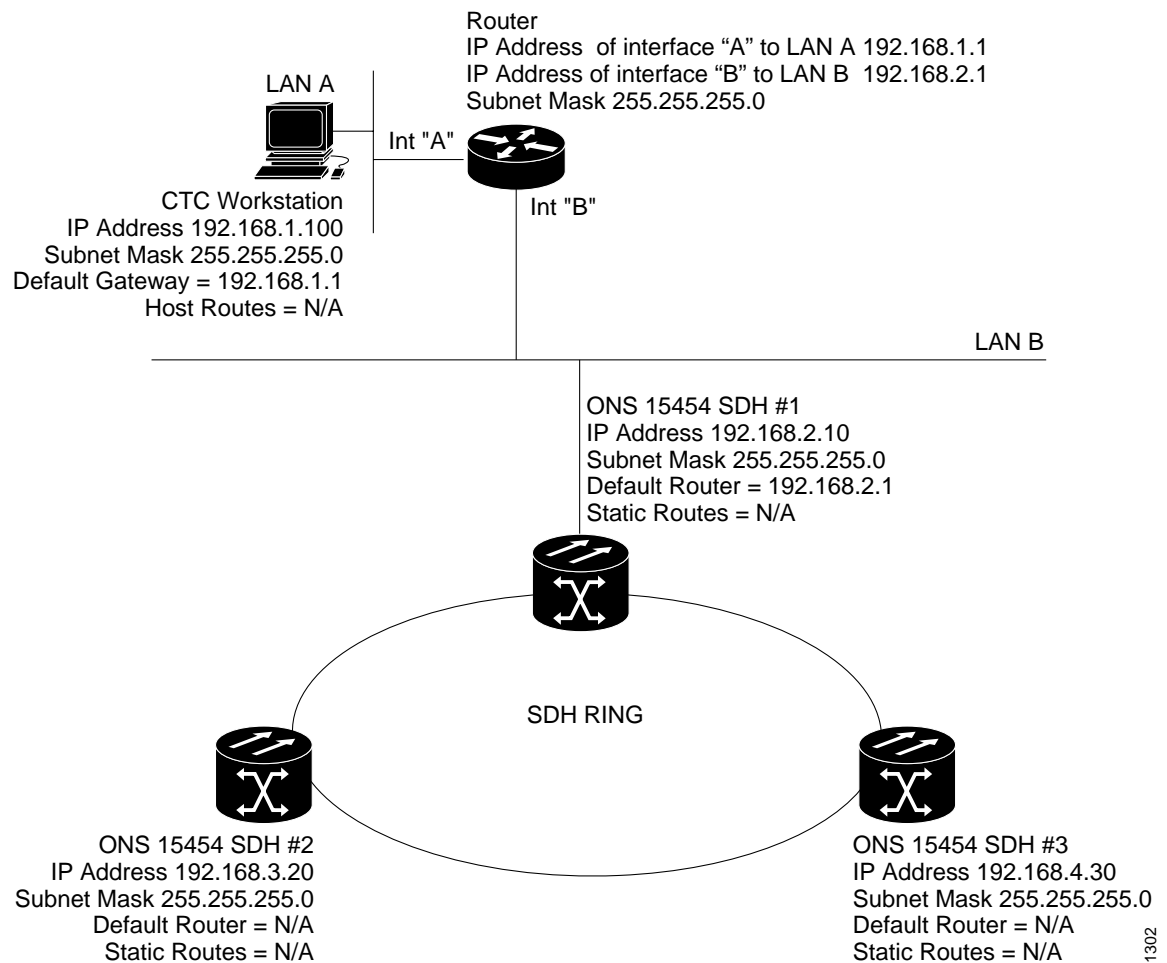
ONS 15454 SDH nodes use the OSPF protocol in internal ONS 15454 SDH networks for node discovery, circuit routing, and node management. You can enable OSPF on the ONS 15454 SDH nodes so that the ONS 15454 SDH topology is sent to OSPF routers on a LAN. Advertising the ONS 15454 SDH network topology to LAN routers eliminates the need to enter static routes for ONS 15454 SDH 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, 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 SDH OSPF topology for advertising to an OSPF network, you must assign an OSPF area ID to the ONS 15454 SDH network. Coordinate the area ID number assignment with your LAN administrator. All DCC-connected ONS 15454 SDH nodes should be assigned the same OSPF area ID.

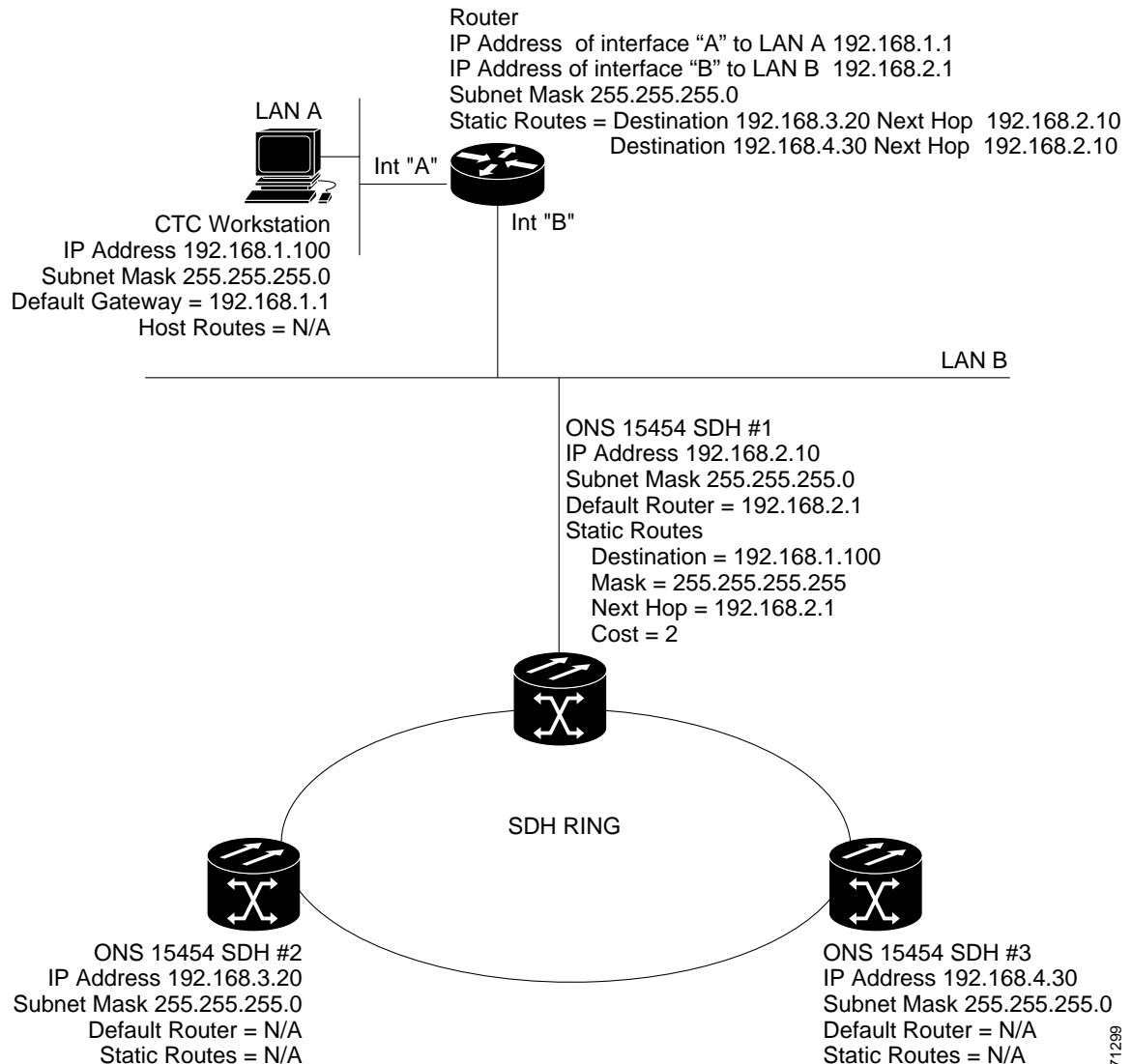
Figure 13-7 shows a network enabled for OSPF. Figure 13-8 on page 13-10 shows the same network without OSPF. Static routes must be manually added to the router for CTC computers on LAN A to communicate with Nodes 2 and 3 because these nodes reside on different subnets.

Figure 13-7 Scenario 6: OSPF Enabled



71302

Figure 13-8 Scenario 6: OSPF Not Enabled



71299

## 13.2.7 Scenario 7: Provisioning the ONS 15454 SDH Proxy Server

The ONS 15454 SDH proxy server is a set of functions that allows you to network ONS 15454 SDH nodes in environments where visibility and accessibility between ONS 15454 SDH nodes 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 access the same ONS 15454 SDH nodes while preventing the field technicians from accessing the NOC LAN. To provision the proxy server, one ONS 15454 SDH is provisioned as a gateway NE (GNE) and the other ONS 15454 SDH nodes are provisioned as end NEs (ENEs). The GNE tunnels connections between CTC computers and ENE nodes, which provides management capability while preventing access for non-ONS 15454 SDH management purposes.

The ONS 15454 SDH 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 13-3 on page 13-15](#) and [Table 13-4 on page 13-16](#)) depend on whether the packet arrives at the ONS 15454 SDH DCC or 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 SDH creates an entry in its ARP table. The ARP entry allows the ONS 15454 SDH to reply to an address over the local Ethernet so craft technicians can connect to ONS 15454 SDH nodes without changing the IP addresses of their computers.
- Processes SNTP/NTP requests. ENEs can derive time-of-day from an SNTP/NTP LAN server through the GNE ONS 15454 SDH.
- Processes SNMPv1 traps. The GNE ONS 15454 SDH receives SNMPv1 traps from the ENE ONS 15454 SDH nodes and forwards them to all provisioned SNMPv1 trap destinations.

The ONS 15454 SDH proxy server is provisioned using three check boxes on the Provisioning > Network > General tab ([Figure 13-9 on page 13-12](#)):

- **Enable Proxy**—If enabled, the ONS 15454 SDH serves as a proxy for connections between CTC clients and ONS 15454 SDH nodes that are DCC-connected to the proxy ONS 15454 SDH. The CTC client establishes connections to DCC-connected nodes through the proxy node. The CTC client can connect to nodes that it cannot directly contact 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 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 server enabled, your CTC session starts and initially appears error free. 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.

- **Craft Access Only**—If enabled, the ONS 15454 SDH does not install or advertise default or static routes. CTC computers can communicate with the ONS 15454 SDH using the TCC2 craft port, but they cannot communicate directly with any other DCC-connected ONS 15454 SDH.
- **Enable Firewall**—If selected, the node prevents IP traffic from being routed between the DCC and the LAN port. The ONS 15454 SDH 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 13-9 Proxy Server Gateway Settings

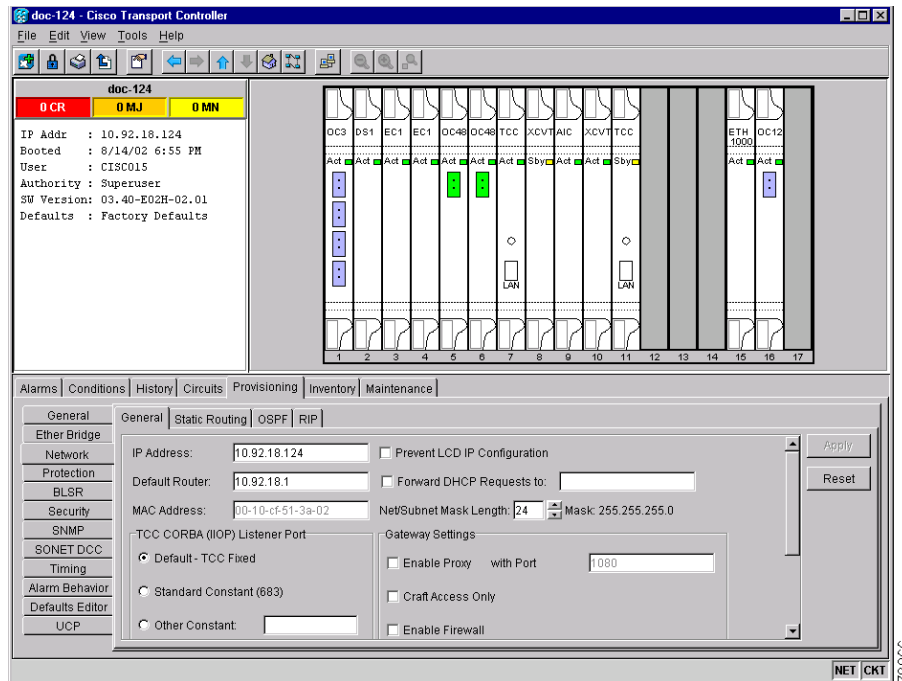


Figure 13-10 on page 13-13 shows an ONS 15454 SDH proxy server implementation. A GNE ONS 15454 SDH is connected to a central office LAN and to ENE ONS 15454 SDH nodes. The central office LAN is connected to a NOC LAN, which has CTC computers. The NOC CTC computer and craft technicians must be able to access the ONS 15454 SDH ENEs. However, the craft technicians must be prevented from accessing or seeing the NOC or central office LANs.

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

Figure 13-10 ONS 15454 SDH Proxy Server with GNE and ENEs on the Same Subnet

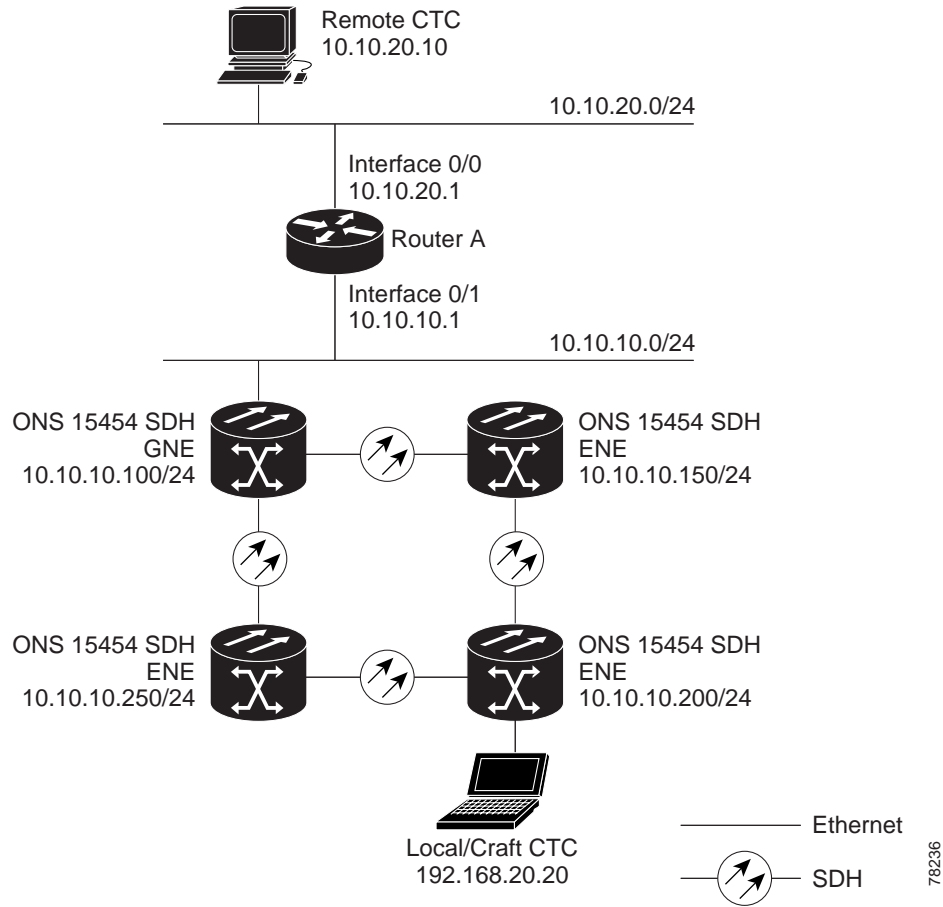


Table 13-2 shows recommended settings for ONS 15454 SDH GNEs and ENEs in the configuration shown in Figure 13-10.

Table 13-2 ONS 15454 SDH Gateway and Element NE Settings

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

Figure 13-11 on page 13-14 shows the same proxy server implementation with ONS 15454 SDH ENEs on different subnets. In the example, ONS 15454 SDH GNEs and ENEs are provisioned with the settings shown in Table 13-2.

Figure 13-11 Scenario 7: ONS 15454 SDH Proxy Server with GNE and ENEs on Different Subnets

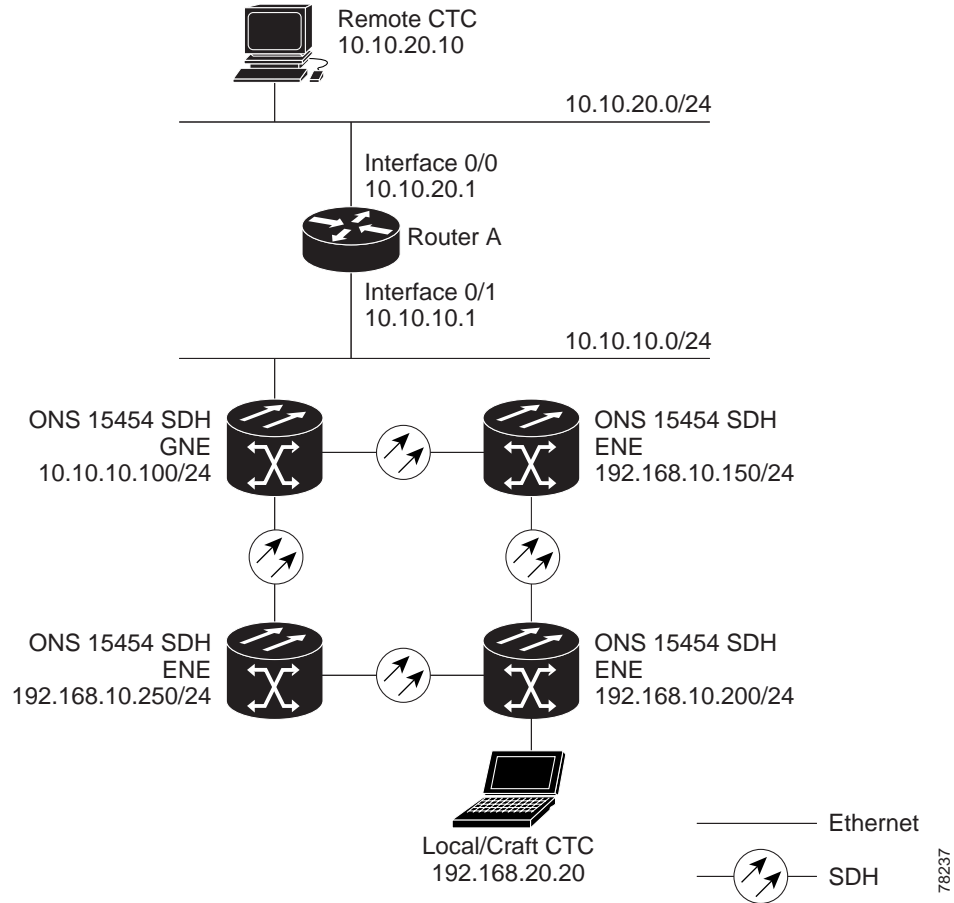


Figure 13-12 on page 13-15 shows the implementation with ONS 15454 SDH ENEs in multiple rings. In the example, ONS 15454 SDH GNEs and ENEs are provisioned with the settings shown in Table 13-2.

Figure 13-12 Scenario 7: ONS 15454 SDH Proxy Server With ENEs on Multiple Rings

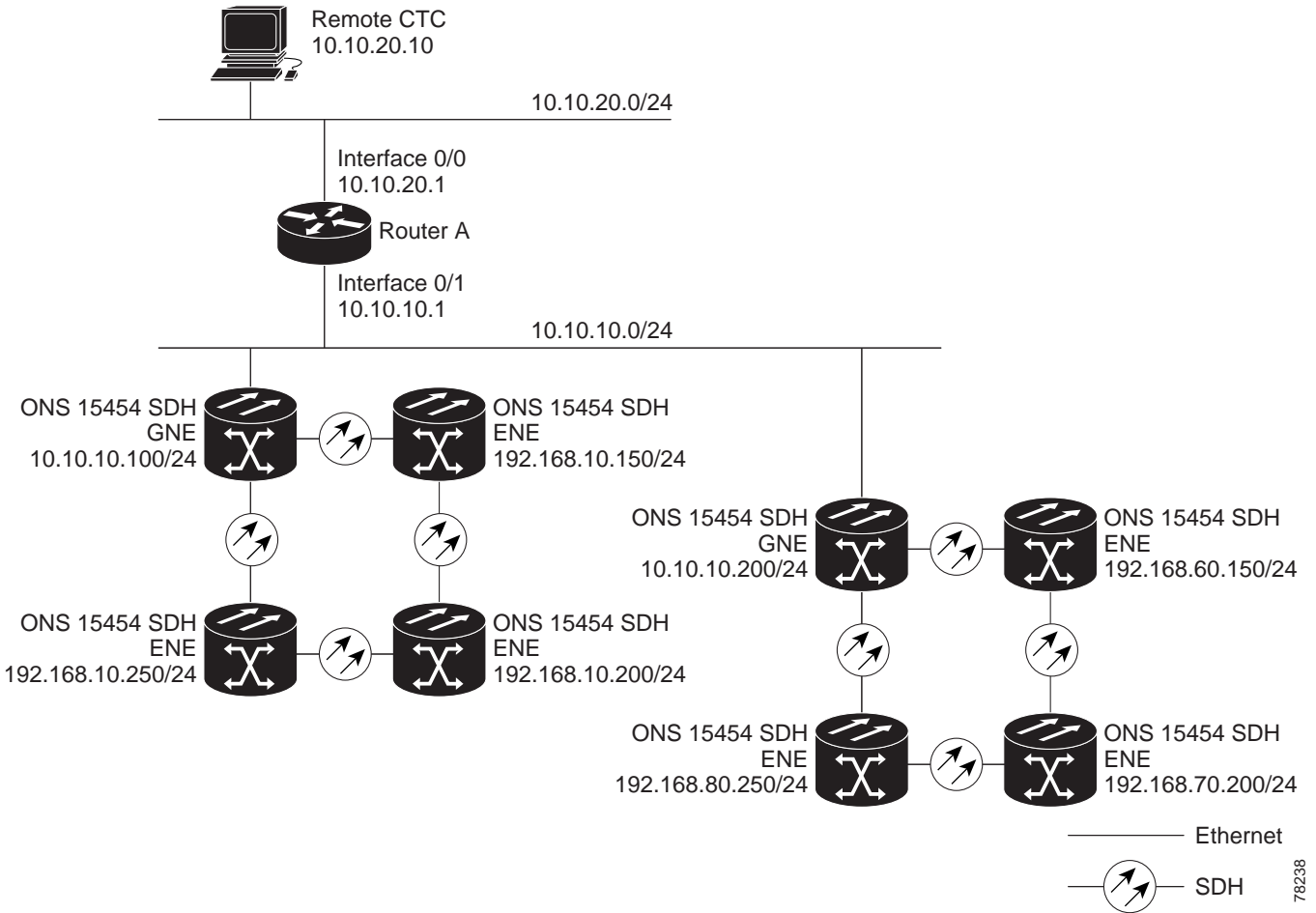


Table 13-3 shows the rules the ONS 15454 SDH follows to filter packets when Enable Firewall is enabled. If the packet is addressed to the ONS 15454 SDH, additional rules, shown in Table 13-4 on page 13-16, are applied. Rejected packets are silently discarded.

Table 13-3 Proxy Server Firewall Filtering Rules

Packets Arriving At:	Are Accepted if the IP Destination Address is:
TCC2 Ethernet interface	<ul style="list-style-type: none"> <li>The ONS 15454 SDH itself</li> <li>The ONS 15454 SDHs subnet broadcast address</li> <li>Within the 224.0.0.0/8 network (reserved network used for standard multicast messages)</li> <li>Subnet mask = 255.255.255.255</li> </ul>
DCC interface	<ul style="list-style-type: none"> <li>The ONS 15454 SDH itself</li> <li>Any destination connected through another DCC interface</li> <li>Within the 224.0.0.0/8 network</li> </ul>

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

Packets Arriving At	Accepts	Rejects
TCC2 Ethernet interface	<ul style="list-style-type: none"> <li>All UDP packets except those in the Rejected column</li> </ul>	<ul style="list-style-type: none"> <li>UDP packets addressed to the SNMP trap relay port (391) are rejected</li> </ul>
DCC interface	<ul style="list-style-type: none"> <li>All UDP packets</li> <li>All TCP packets except those in the Rejected column</li> <li>OSPF packets</li> <li>ICMP packets</li> </ul>	<ul style="list-style-type: none"> <li>TCP packets addressed to the Telnet port are rejected.</li> <li>TCP packets addressed to the proxy server port are rejected.</li> <li>All packets other than UDP, TCP, OSPF, and ICMP</li> </ul>

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

- All DCC-connected ONS 15454 SDH nodes on the same Ethernet segment must have the same Craft Access Only setting. Mixed values produce unpredictable results, and may leave some nodes unreachable through the shared Ethernet segment.
- All DCC-connected ONS 15454 SDH nodes on the same Ethernet segment must have the same Enable Firewall setting. Mixed values produce unpredictable results. Some nodes may become unreachable.
- If you check Enable Firewall, always check Enable Proxy. If Enable Proxy is not checked, CTC cannot see nodes on the DCC side of the ONS 15454 SDH.
- If Craft Access Only is checked, check Enable Proxy. If Enable Proxy is not checked, CTC cannot see nodes on the DCC side of the ONS 15454 SDH.

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

- Disconnect the craft computer from the unreachable ONS 15454 SDH. Connect to the ONS 15454 SDH through another ONS 15454 SDH in the network that has a DCC connection to the unreachable ONS 15454 SDH.
- Disconnect the Ethernet cable from the unreachable ONS 15454 SDH. Connect a CTC computer directly to the ONS 15454 SDH.

## 13.2.8 Scenario 8: Dual GNEs on a Subnet

The ONS 15454 SDH 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 13-13](#) shows a network with dual GNEs on the same subnet. [Figure 13-14](#) shows a network with dual GNEs on different subnets.

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

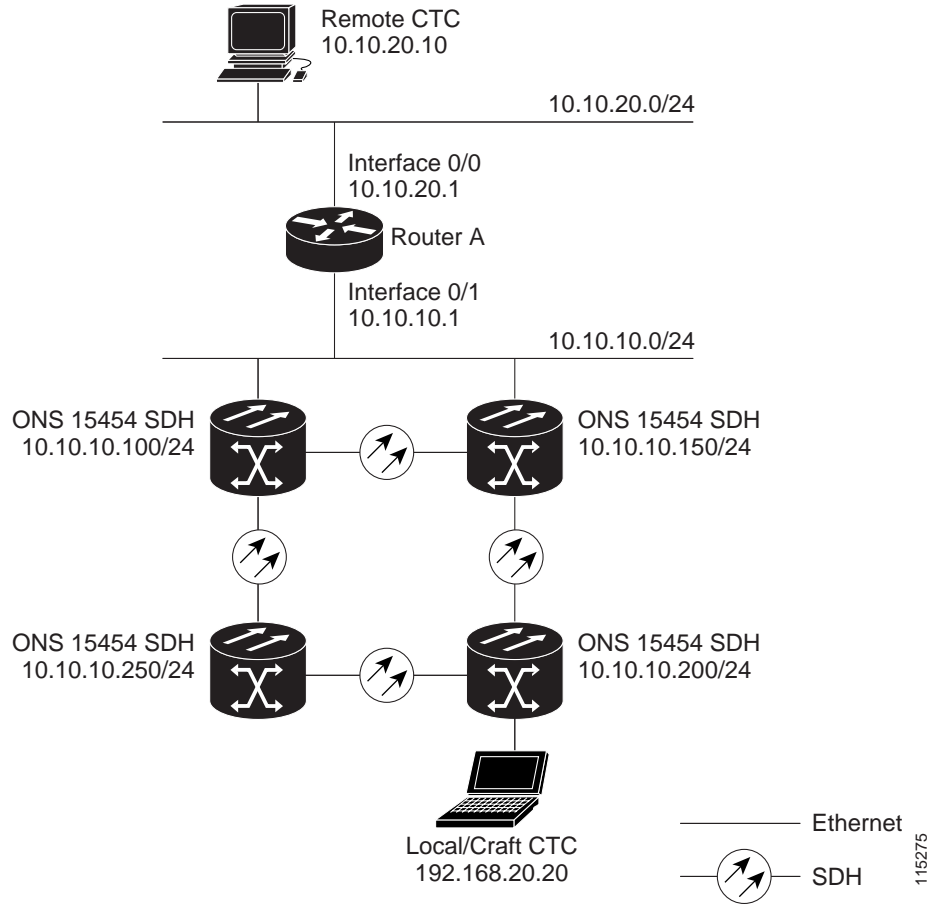
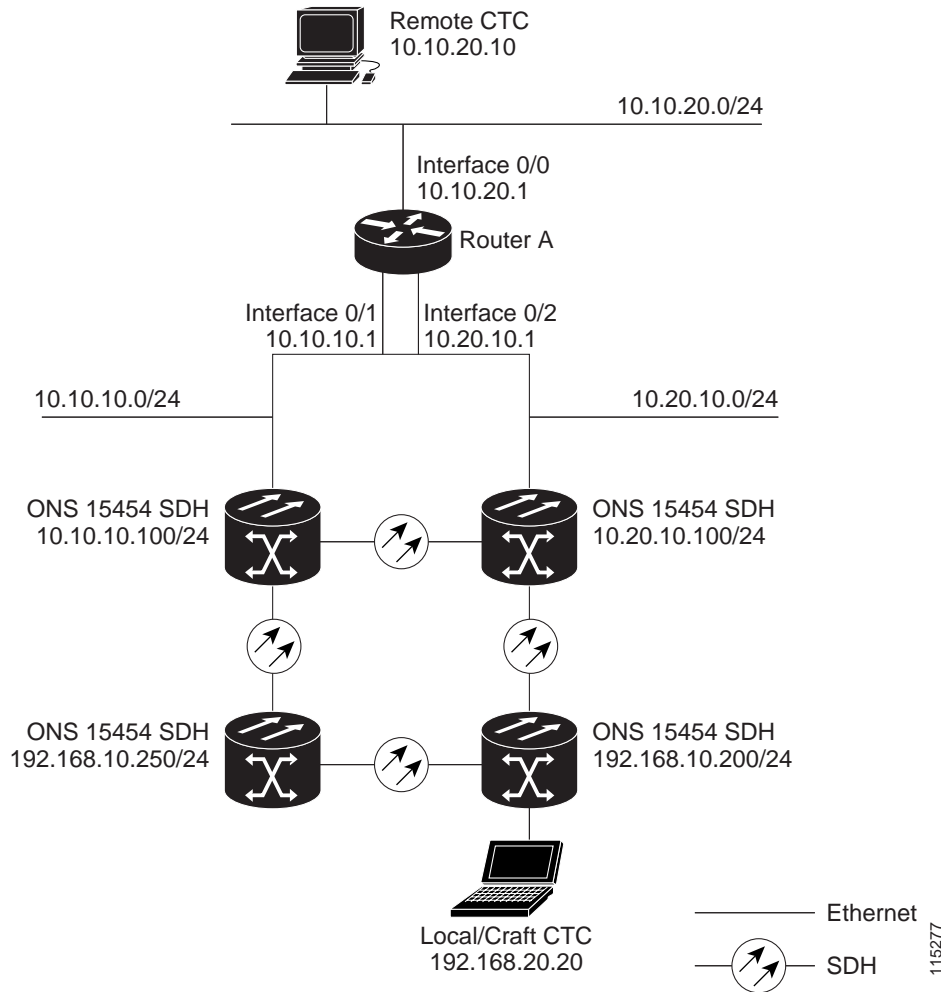


Figure 13-14 Scenario 8: Dual GNEs on Different Subnets



## 13.3 Routing Table

ONS 15454 SDH routing information is displayed on the Maintenance > Routing Table tabs (Figure 13-15 on page 13-19). 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 SDH interface used to access the destination. Values are:
  - cpm0—The ONS 15454 SDH Ethernet interface, that is, the RJ-45 jack on the TCC2 and the LAN 1 pins on the backplane
  - pdcc0—An SDCC interface, that is, an STM-N trunk card identified as the SDCC termination
  - lo0—A loopback interface

Figure 13-15 Viewing the ONS 15454 SDH Routing Table

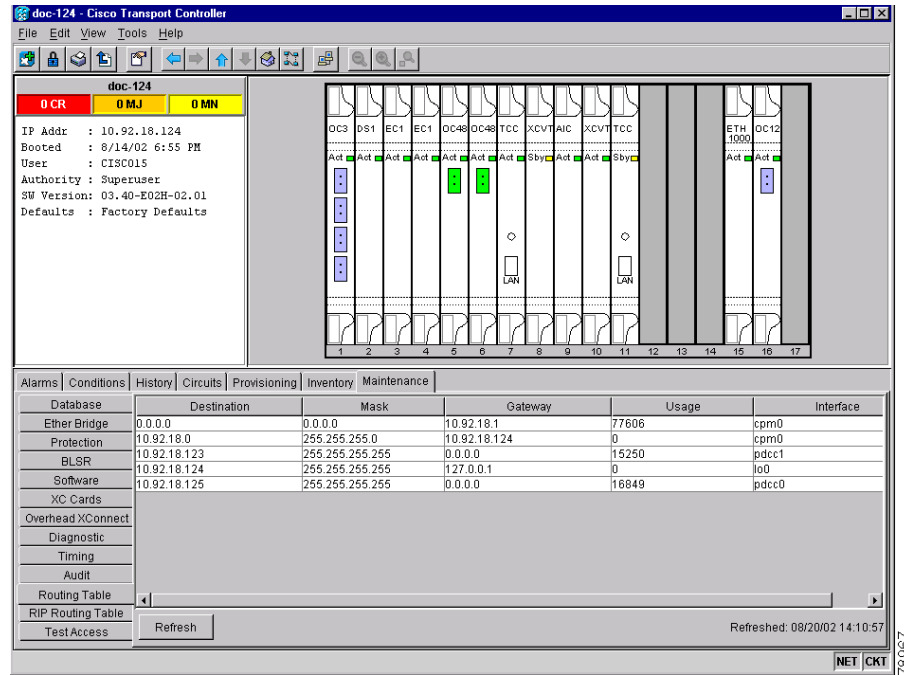


Table 13-5 shows sample routing entries for an ONS 15454 SDH.

Table 13-5 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 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 are sent to this gateway.
- Interface (cpm0) indicates that the ONS 15454 SDH 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 SDH 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 SDH 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 SDH SDCC interface is used to reach the gateway.

## 13.4 Provisioning an External Firewall

Table 13-6 shows the ports that are used by the TCC2.

**Table 13-6 Ports Used by the 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 TCC2
2361	TL1
3082	TL1

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

Port	Function
3083	TL1
5001	MS-SPRing server port
5002	MS-SPRing 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

## 13.4.1 Access Control List Example With Proxy Server Not Enabled

The following access control list (ACL) example 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 SDH address is 10.10.10.100. The firewall is attached to the GNE CTC, 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 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 any host 10.10.10.100 eq www
access-list 100 remark *** allows initial contact with the 15454 SDH using http (port 80) ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 683 host 10.10.10.100 eq 57790
access-list 100 remark *** allows CTC communication with the 15454 SDH 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 SDH GNE ***

access-list 101 remark *** Outbound ACL, NE -> CTC ***
access-list 101 remark
access-list 101 permit tcp host 10.10.10.100 any host 192.168.10.10 eq 683
access-list 101 remark *** allows alarms etc., from the 15454 SDH (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 SDH GNE to CTC ***

```

## 13.4.2 Access Control List Example With Proxy Server Enabled

The following ACL example 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 SDH address is 10.10.10.100. The firewall is attached to the GNE CTC, so inbound is CTC to the GNE and outbound is from the GNE to CTC. CTC CORBA Standard constant (683) and TCC CORBA Default 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 any host 10.10.10.100 eq www
access-list 100 remark *** allows initial contact with the 15454 SDH using http (port 80) ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 683 host 10.10.10.100 eq 57790
access-list 100 remark *** allows CTC communication with the 15454 SDH GNE (port 57790) ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 683 host 10.10.10.100 eq 1080
access-list 100 remark *** allows CTC communication with the 15454 SDH GNE proxy server (port
1080) ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 683 host 10.10.10.100 range 10240 10495
access-list 100 remark *** allows CTC communication with the 15454 SDH ENEs (ports 10240 -
10495) via the GNE proxy server
***
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 SDH GNE ***

access-list 101 remark *** Outbound ACL, NE -> CTC ***
access-list 101 remark
access-list 101 permit tcp host 10.10.10.100 any host 192.168.10.10 eq 683
access-list 101 remark *** allows alarms and other communications from the 15454 SDH (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 SDH GNE to CTC ***

```