IP Networking

This chapter describes how you must manage ONS 15454 nodes within a TCP/IP network environment. For IP setup instructions, refer to the *Cisco ONS 15454 Procedure Guide*.

The following topics are covered in this chapter:

- IP Networking Overview, page 8-1
- IP Addressing Scenarios, page 8-2
- Routing Table, page 8-21
- Provisioning an External Firewall, page 8-23
- Open GNE, page 8-25
- Provisionable Patchcords, page 8-28

IP Networking Overview

Every ONS 15454 requires a unique, valid IP address. The CTC application utilizes TCP/IP to communicate with nodes in the ONS 15454 network, which requires each node to have a unique IP address. The node's IP address is equivalent to a terminal identification (TID) number.

You can connect ONS 15454s within an IP environment in any of the following ways:

- 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.
- Static routes can be created to enable connections among multiple CTC sessions with ONS 15454 nodes 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 SOCKS proxy server controls the visibility and accessibility between CTC computers and ONS 15454 nodes.

IP Addressing Scenarios

ONS 15454 IP addressing generally has nine common scenarios or configurations. Use the following scenarios as building blocks for more complex network configurations. as building blocks for more complex network configurations. Table 8-1 provides a general list of items to check when setting up ONS 15454 nodes in IP networks.

Table 8-1 General ONS 15454 IP Troubleshooting Checklist

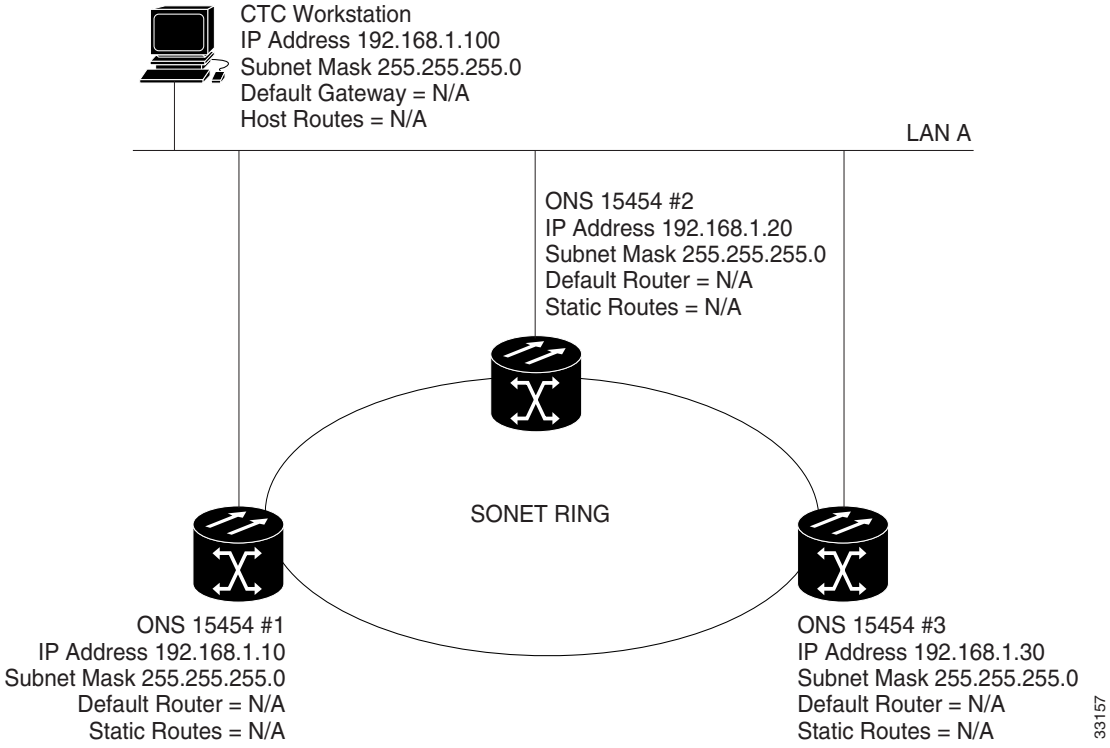
Item	What to Check
Link integrity	Verify that link integrity exists between: • CTC computer and network hub/switch • ONS 15454s (backplane wire-wrap pins or RJ-45 port) and network hub/switch • Router ports and hub/switch ports
ONS 15454 hub/switch ports	If connectivity problems occur, set the hub or switch port that is connected to the ONS 15454 to 10 Mb/s half-duplex.
Ping	Ping the node to test connections between computers and ONS 15454 nodes.
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.

Note The TCC2P secure mode option allows two IP addresses to be provisioned for the node, one for the backplane LAN port and one for the TCC2P TCP/IP port. Secure mode IP addressing examples are provided in the "Scenario 9: IP Addressing with Secure Mode Enabled" section. IP addresses shown in the other scenarios assume that secure mode is not enabled. If secure mode is enabled, the IP addresses shown in the examples apply to the backplane LAN port.

Scenario 1: CTC and ONS 15454 Nodes on the Same Subnet

Figure 8-1 shows a basic ONS 15454 LAN configuration. The ONS 15454 nodes and CTC computer reside on the same subnet. All ONS 15454 nodes connect to LAN A, and all ONS 15454 nodes have DCC connections.

Figure 8-1 CTC and ONS 15454 Nodes on Same Subnet

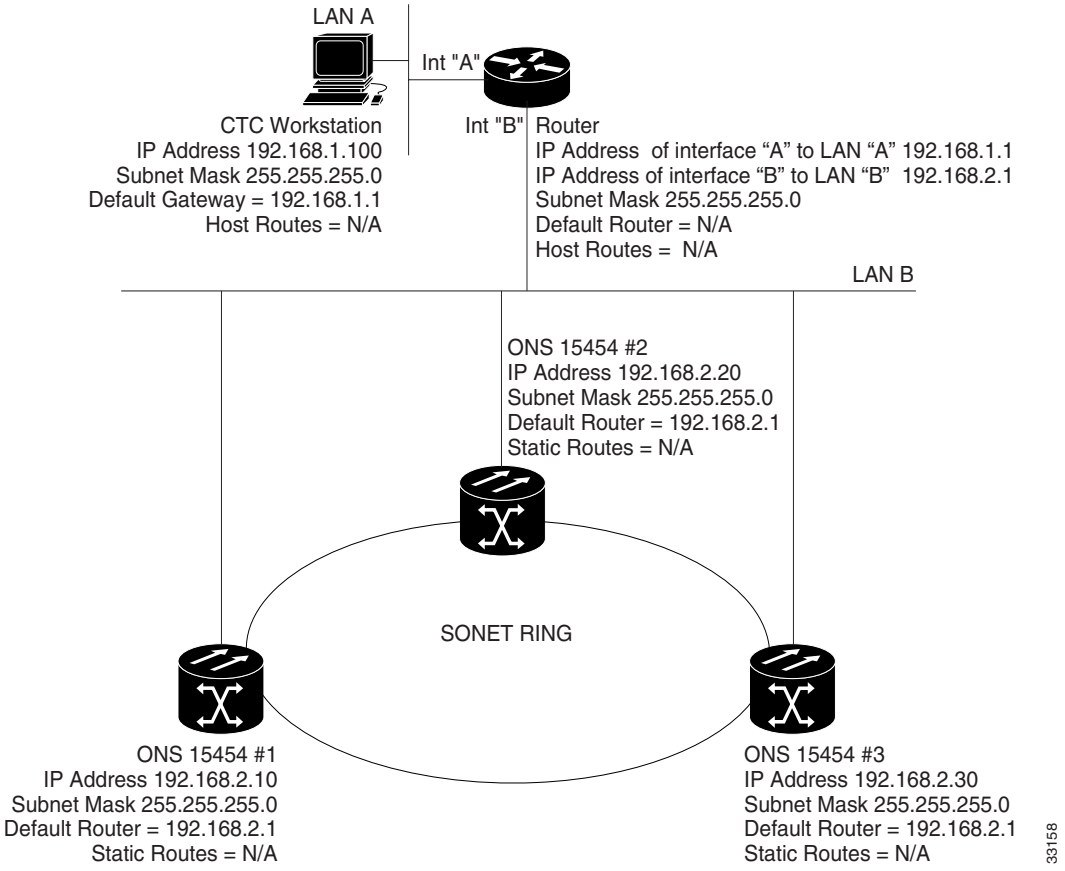


Scenario 2: CTC and ONS 15454 Nodes Connected to a Router

In Figure 8-2 the CTC computer resides on subnet 192.168.1.0 and attaches to LAN A. The ONS 15454 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 DHCP (Dynamic Host Configuration Protocol), the default gateway and IP address are assigned automatically. In the Figure 8-2 example, a DHCP server is not available.

Figure 8-2 CTC and ONS 15454 Nodes Connected to Router



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

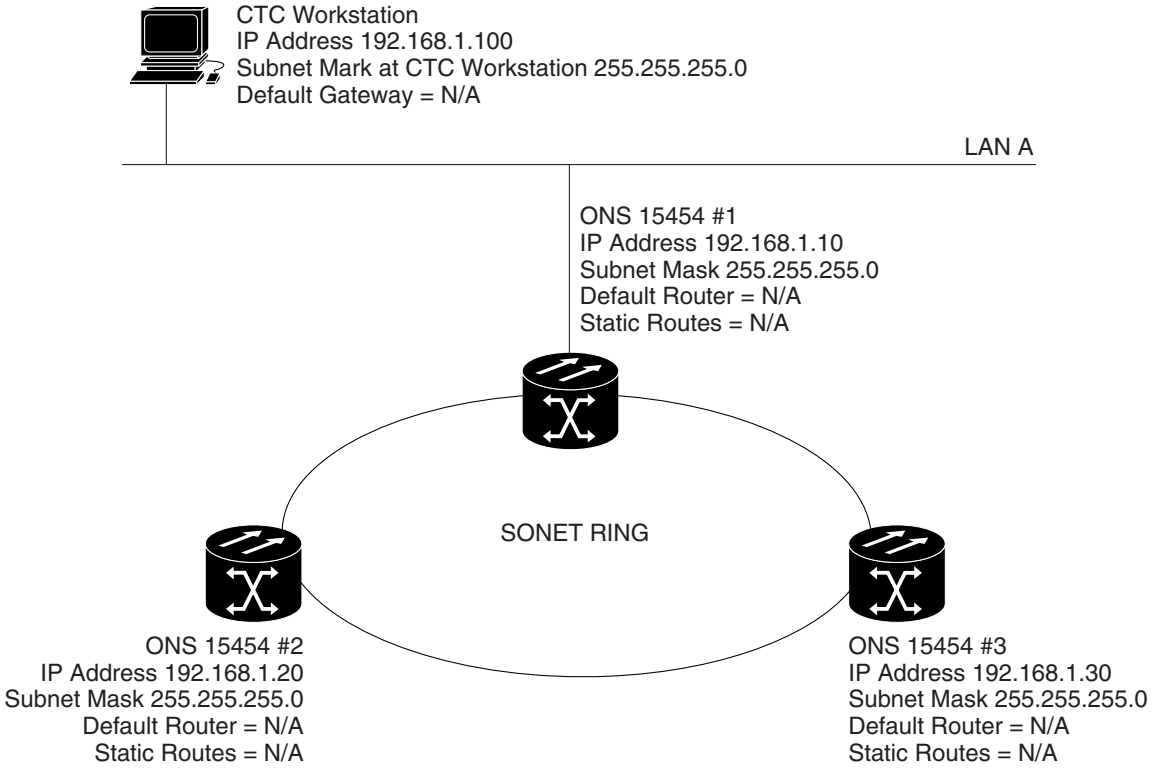
ARP matches higher-level IP addresses to the physical addresses of the destination host. It uses a lookup table (called ARP cache) to perform the translation. When the address is not found in the ARP cache, a broadcast is sent out on the network with a special format called the ARP request. If one of 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 15454 nodes 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 (node #1) connects to the LAN (see Figure 8-3). Two ONS 15454 nodes (#2 and #3) connect to ONS 15454 #1 through the SONET DCC. Because all three ONS 15454 nodes are on the same subnet, Proxy ARP enables ONS 15454 #1 to serve as a gateway network element (GNE) 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 SOCKS Proxy Server shown in Scenario 7.

Figure 8-3 Using Proxy ARP

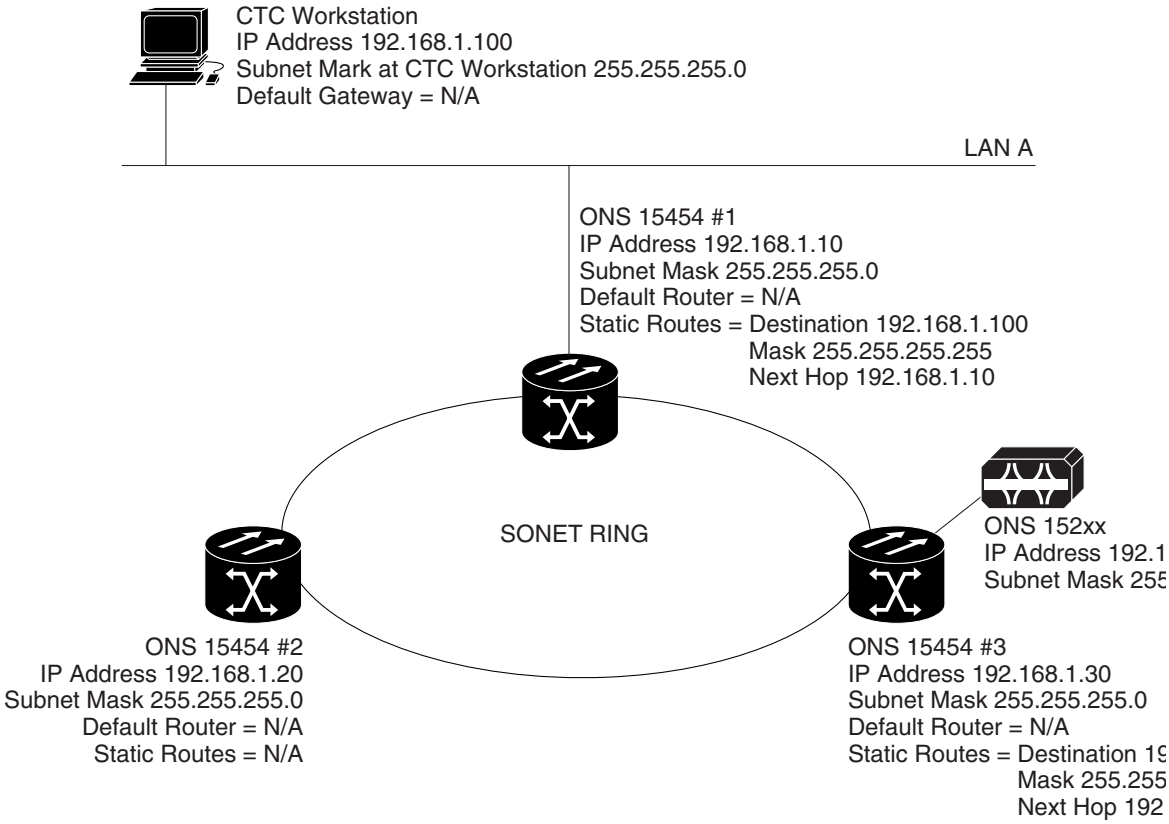


You can also use proxy ARP to communicate with hosts attached to the craft Ethernet ports of DCC-connected nodes (see Figure 8-4). The node with an attached host must have a static route to the host. Static routes are propagated to all DCC peers using OSPF. The existing proxy ARP node is the gateway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

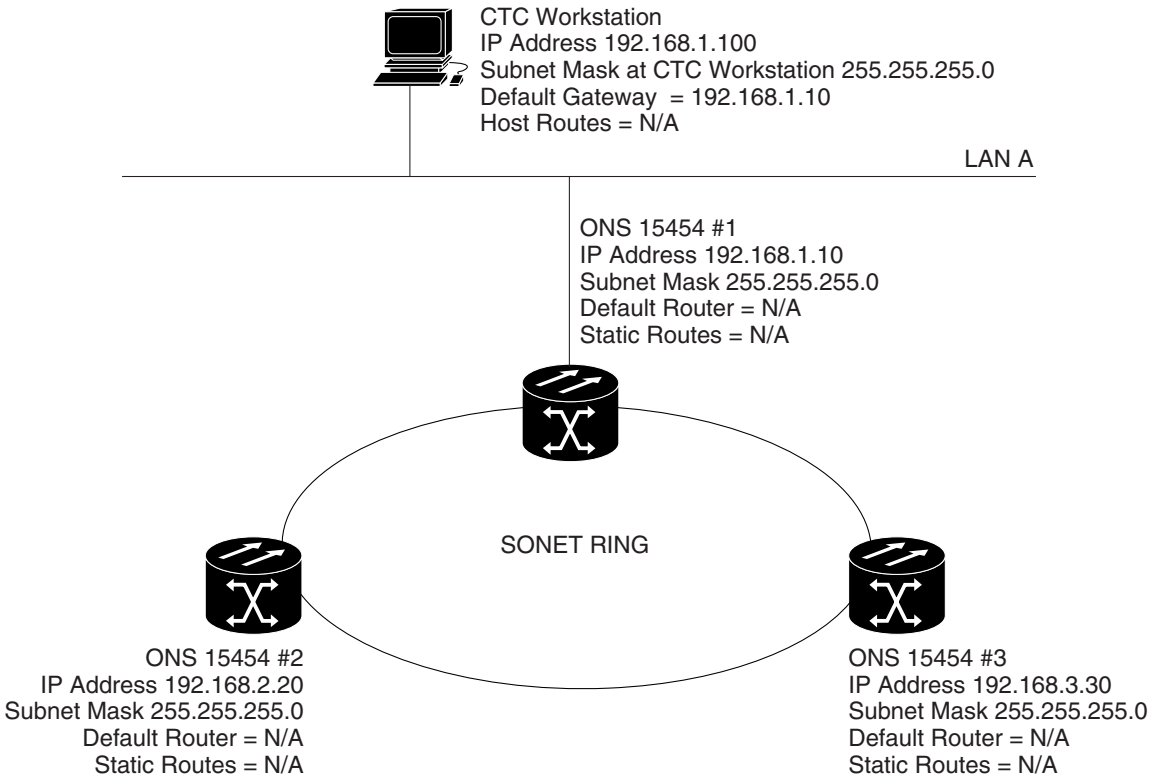
Figure 8-4 Scenario 3: Using Proxy ARP with Static Routing



Scenario 4: Default Gateway on the 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 (seeFigure 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 ONS 15454 nodes #2 and #3, ONS 15454 #1 is entered as the default gateway on the CTC computer.

Figure 8-5 Default Gateway on the CTC Computer



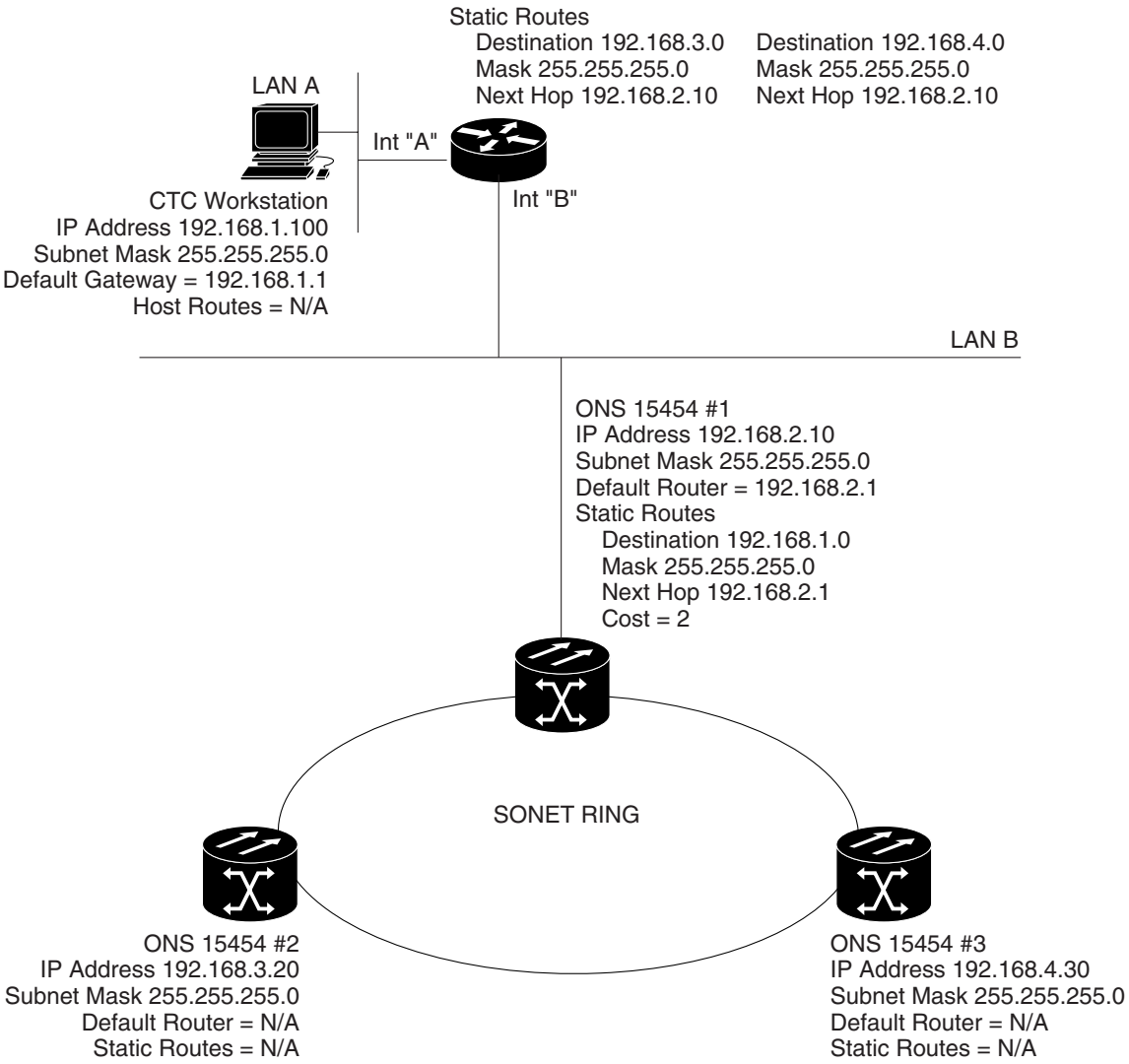
Scenario 5: Using Static Routes to Connect to LANs

Static routes are used for two purposes:

1. 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.)
2. To enable multiple CTC sessions among ONS 15454s 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 15454 nodes residing on different subnets are connected through ONS 15454 #1 to the router through interface B. Because ONS 15454 nodes #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 8-6 Static Route With One CTC Computer Used as a Destination

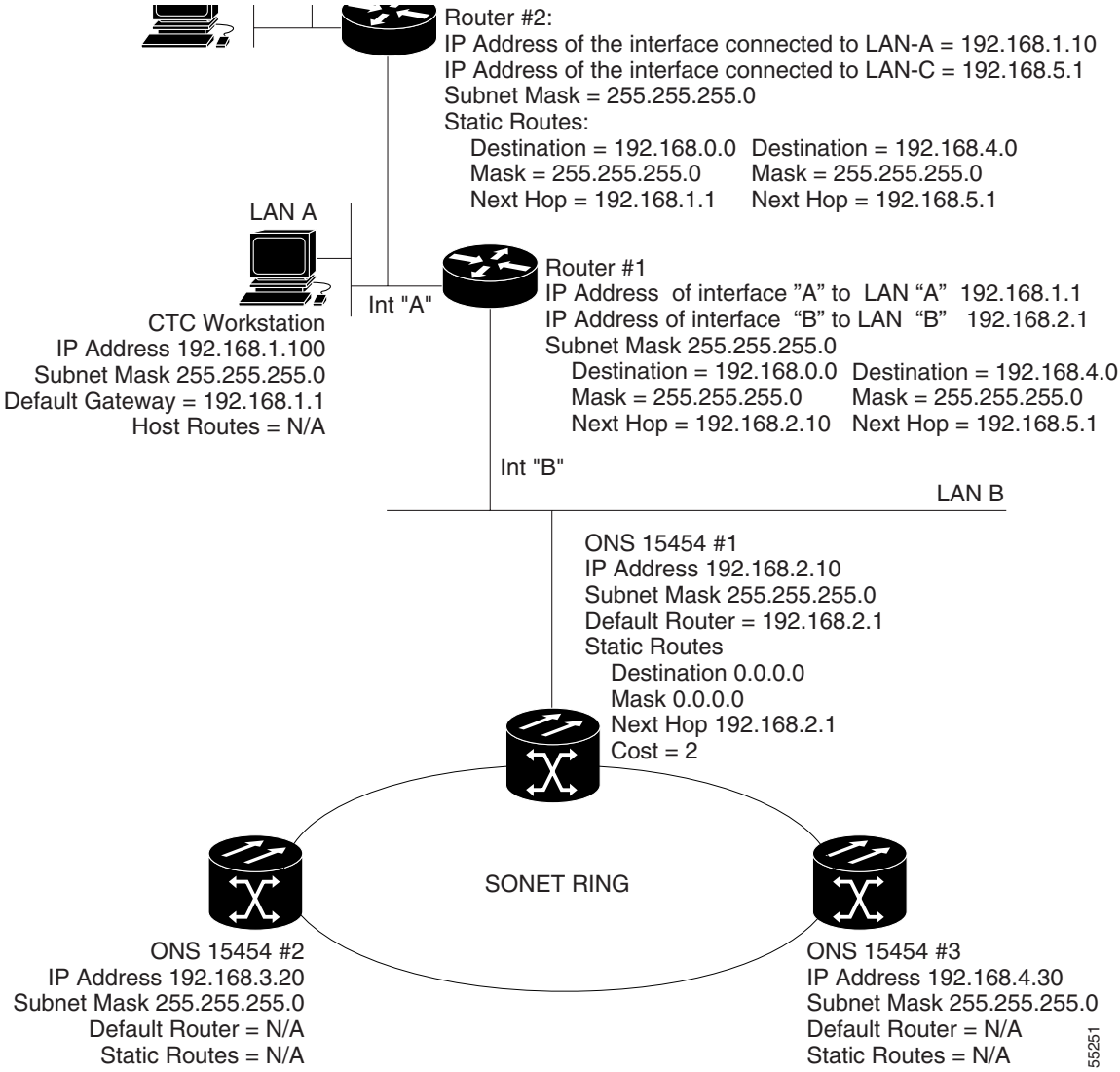


The destination and subnet mask entries control access to the ONS 15454 nodes as follows:

- 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 Static Route With Multiple LAN Destinations



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 15454 nodes 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 8-8 shows a network enabled for OSPF. Figure 8-9 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 15454 nodes should be assigned the same OSPF area ID.

Figure 8-8 OSPF Enabled

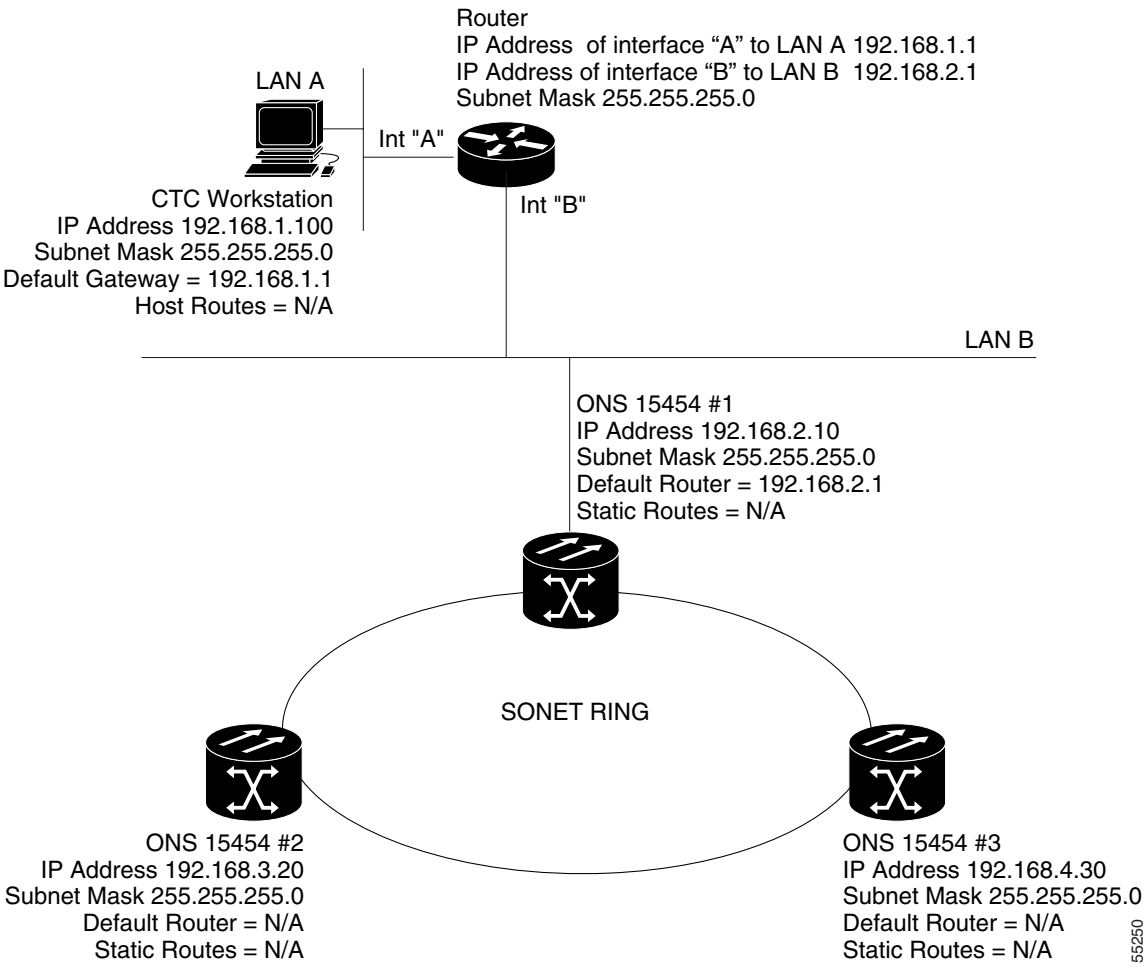
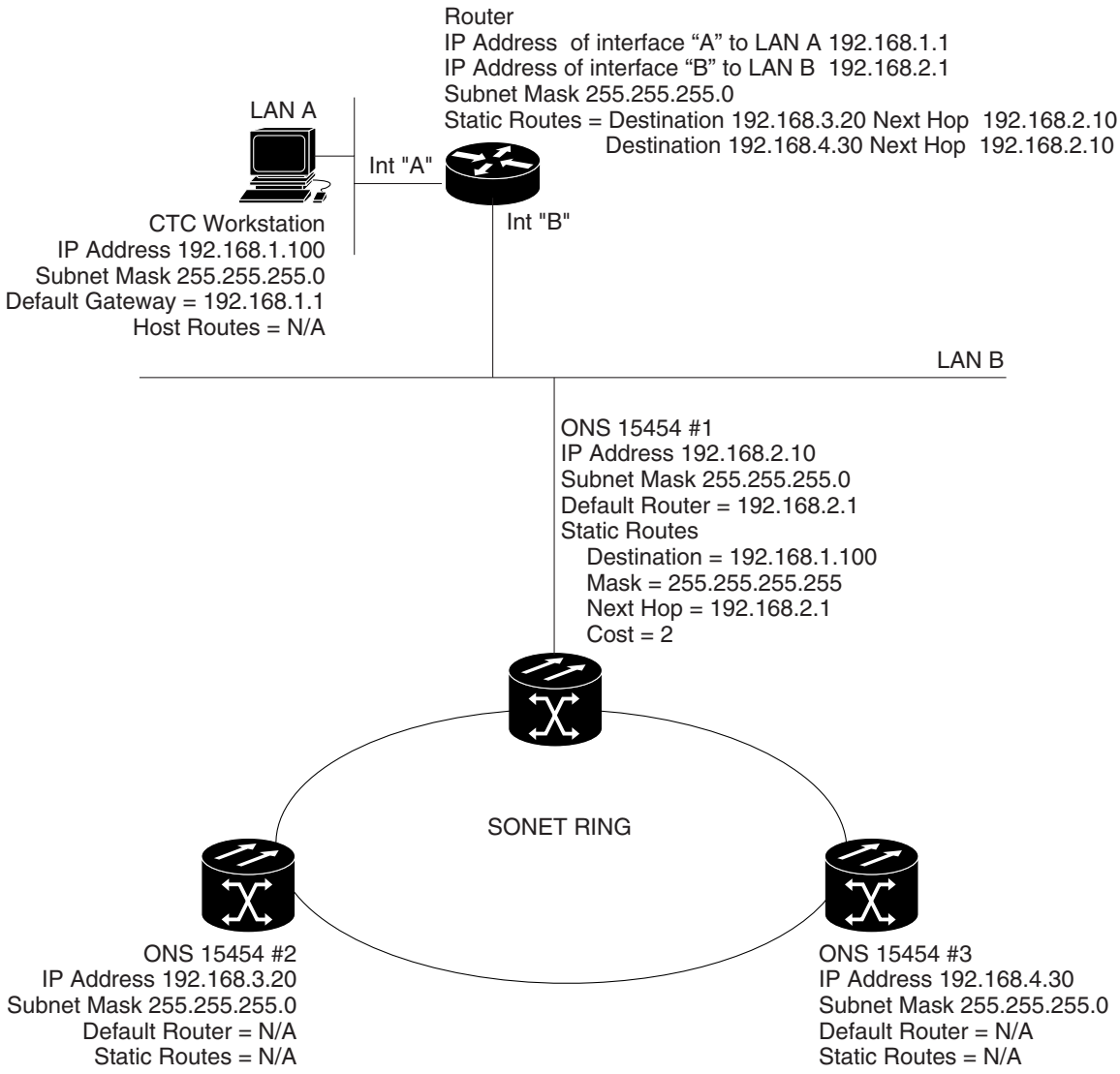


Figure 8-9 OSPF Not Enabled



Scenario 7: Provisioning the ONS 15454 SOCKS Proxy Server

The ONS 15454 SOCKS proxy server is a set of functions that allows you to network ONS 15454 nodes in environments where visibility and accessibility between ONS 15454 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 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 8-3 and Table 8-4 depend on whether the packet arrives at the ONS 15454 DCC or TCC2/TCC2P 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 15454 nodes 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.
- Processes SNMPv1 traps. The GNE ONS 15454 receives SNMPv1 traps from the ENE ONS 15454 nodes and forwards them to all provisioned SNMPv1 trap destinations.

The ONS 15454 SOCKS proxy server is provisioned using the Enable SOCKS proxy server on port check box on the Provisioning > Network >General tab (see Figure 8-10). If checked, the ONS 15454 serves as a proxy for connections between CTC clients and ONS 15454 nodes that are DCC-connected to the proxy ONS 15454. The CTC client establishes connections to DCC-connected nodes through the proxy node. The CTC client can connect to nodes that it cannot directly reach from the host on which it runs. If not selected, the node does not proxy for any CTC clients, although any established proxy connections continue until the CTC client exits. In addition, you can set the SOCKS proxy server as an ENE or a GNE as follows:

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 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.

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

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

Proxy Server Port Reduction

In releases prior to 4.0, CTC was able to manage nodes behind routers that performed NAT, but required that intermediate routers allow connections on many ports. Additionally, these intermediate routers needed to be configured to allow connections to be initiated from both CTC and the GNE. With Release

4.0 and higher, CTC can now manage nodes behind routers that perform NAT or PAT. Intermediate routers need only be configured to allow connections from CTC to the GNE on ports 80 (HTTP) and 1080 (SOCKS) and packets for established connections from the GNE to CTC. The superuser can enable this functionality on the node level Provisioning > Network tab.

Figure 8-10 SOCKS Proxy Server Gateway Settings

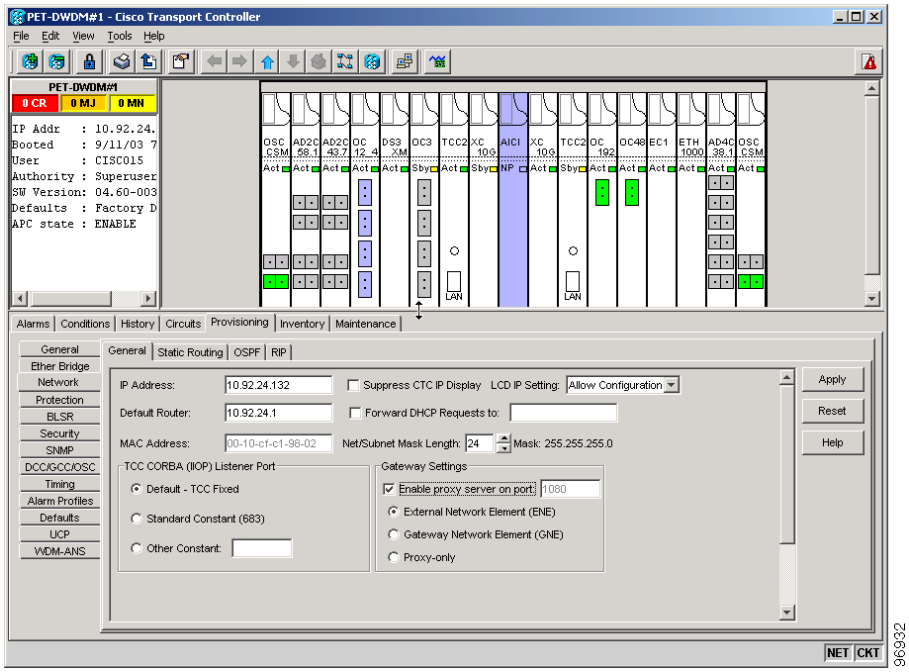


Figure 8-11 shows an ONS 15454 SOCKS proxy server implementation. A GNE ONS 15454 is connected to a central office LAN and to ENE ONS 15454s. The central office LAN is connected to a NOC LAN, which has CTC computers. The NOC CTC computer and craft technicians must both be able to access the ONS 15454 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 8-11 ONS 15454 SOCKS Proxy Server with GNE and ENEs on the Same Subnet

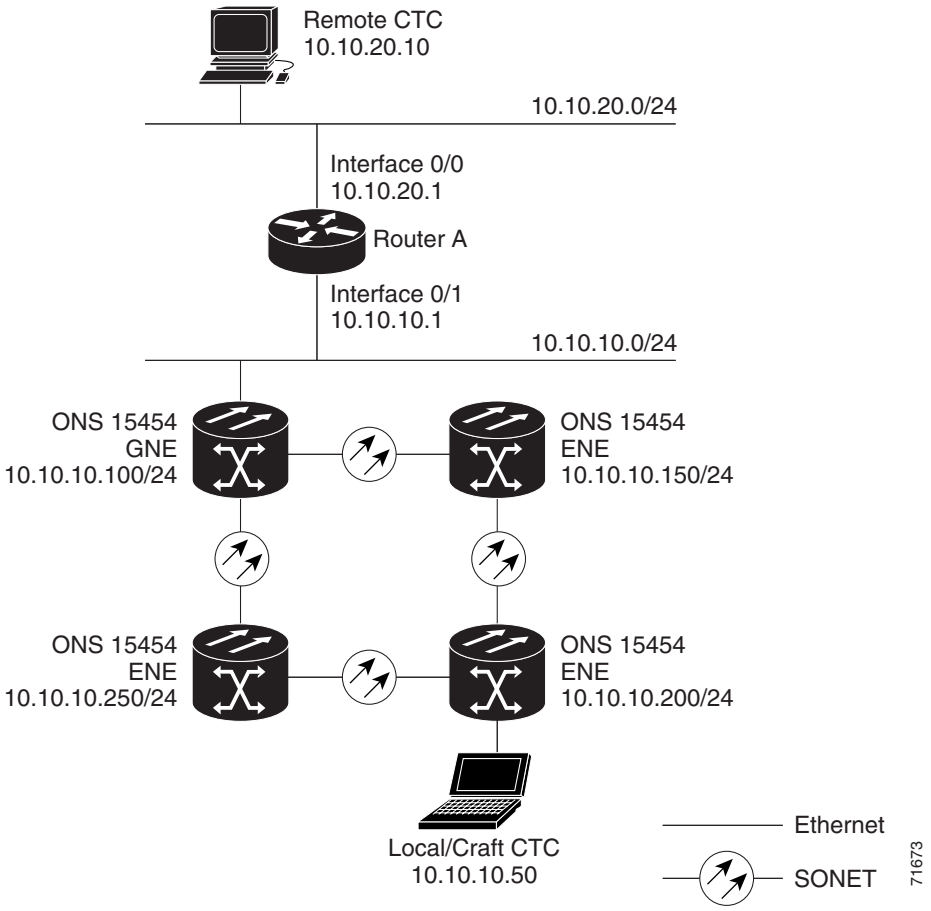


Table 8-2 shows recommended settings for ONS 15454 GNEs and ENEs in the configuration shown in Figure 8-11.

Table 8-2 ONS 15454 Gateway and ENE Settings

Setting	ONS 15454 Gateway NE	ONS 15454 ENE
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 8-12 shows the same SOCKS proxy server implementation with ONS 15454 ENEs on different subnets. Figure 8-13 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 8-2.

Figure 8-12 ONS 15454 SOCKS Proxy Server with GNE and ENEs on Different Subnets

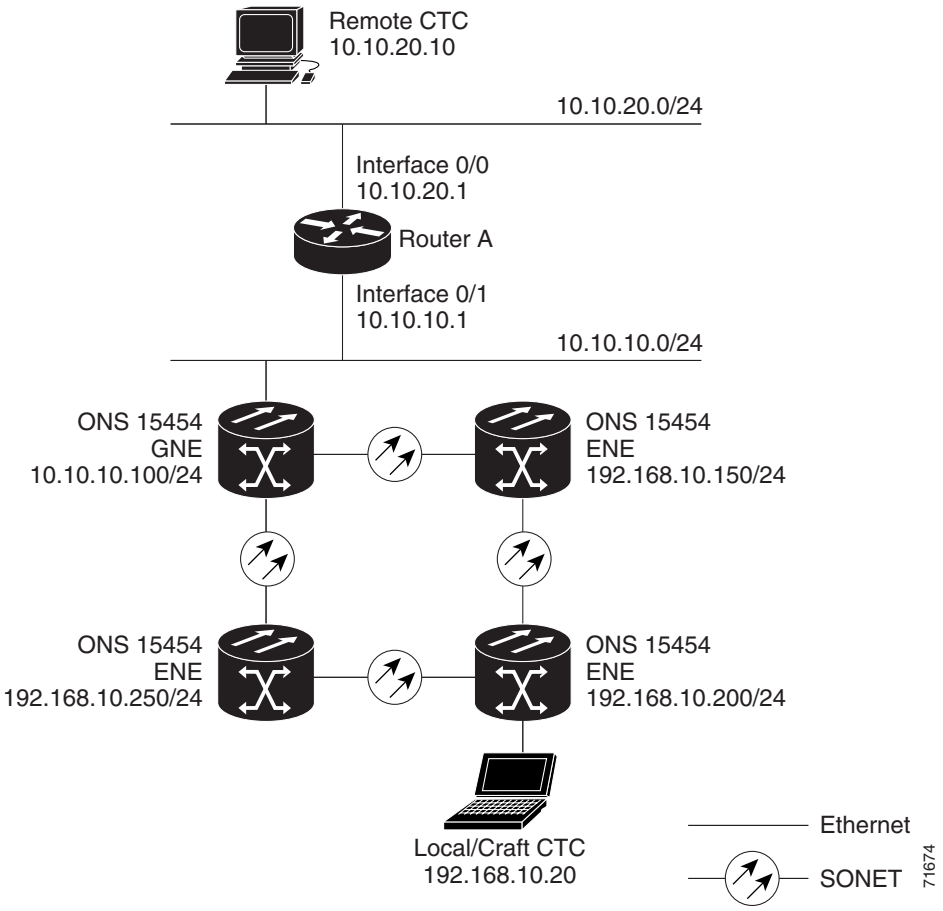


Figure 8-13 ONS 15454 SOCKS Proxy Server With ENEs on Multiple Rings

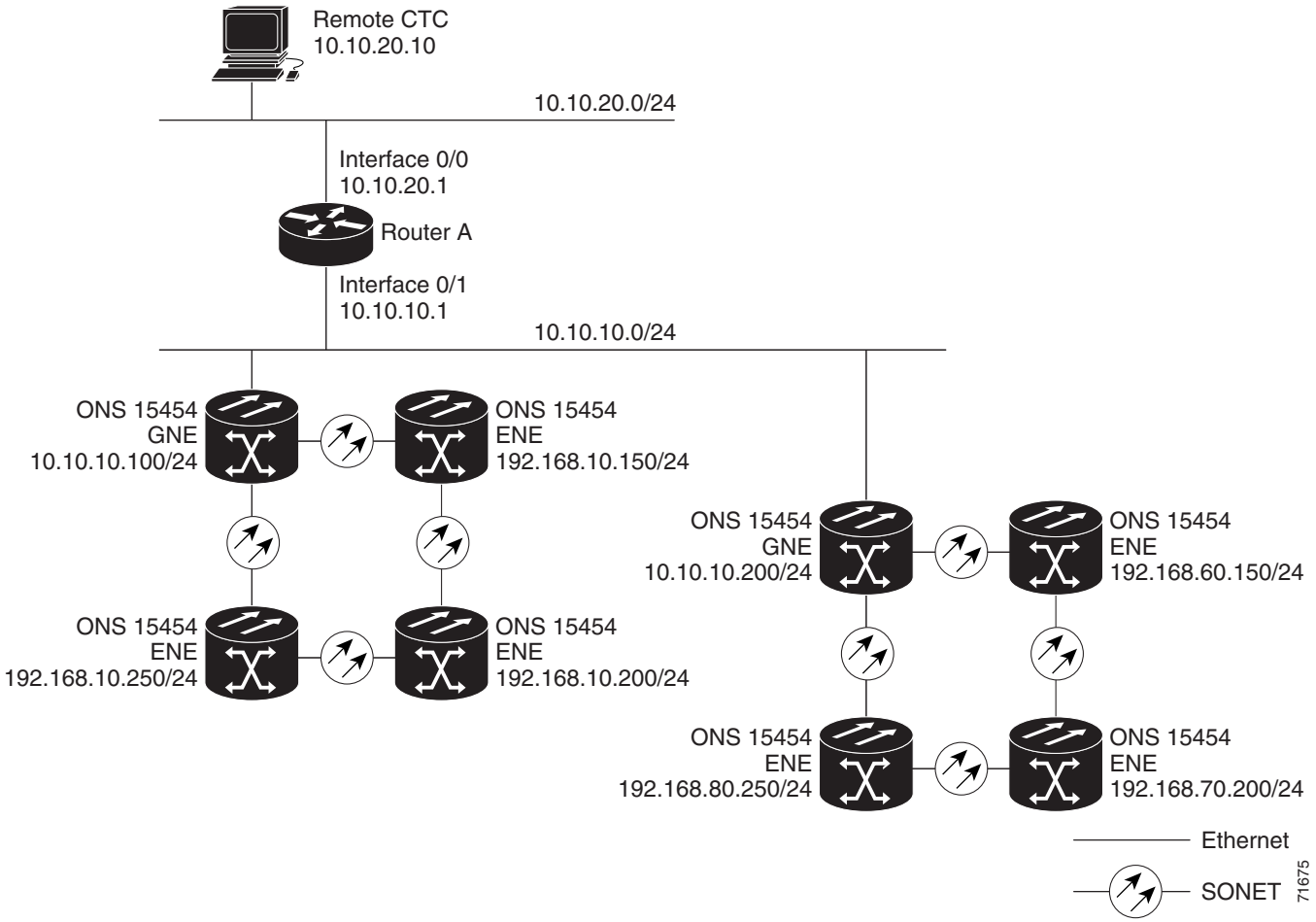


Table 8-3 shows the rules the ONS 15454 follows to filter packets when Enable Firewall is enabled. If the packet is addressed to the ONS 15454, additional rules, shown in Table 8-4, are applied. Rejected packets are silently discarded.

Table 8-3 SOCKS Proxy Server Firewall Filtering Rules

Packets arriving at:	Are accepted if the IP destination address is:
TCC2/TCC2P 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 8-4 SOCKS Proxy Server Firewall Filtering Rules When Packet Addressed to ONS 15454

Packets Arrive At	Accepted	Rejected
TCC2/TCC2P Ethernet Interface	All UDP[1] packets except those in the Rejected column.	UDP packets addressed to the SNMP trap relay port (391).
DCC Interface	• All UDP packets • All TCP[2] packets 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 SOCKS proxy server, note that all DCC-connected ONS 15454 nodes on the same Ethernet segment must have the same Gateway setting. Mixed values will produce unpredictable results and may 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 the Ethernet cable from the unreachable ONS 15454. Connect a CTC computer directly to the ONS 15454 and change its provisioning.

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. GNE load balancing reduces the dependency on the launch GNE and DCC bandwidth, both of which enhance CTC performance. Figure 8-14 shows a network with dual GNEs on the same subnet.

Figure 8-14 Dual GNEs on the Same Subnet

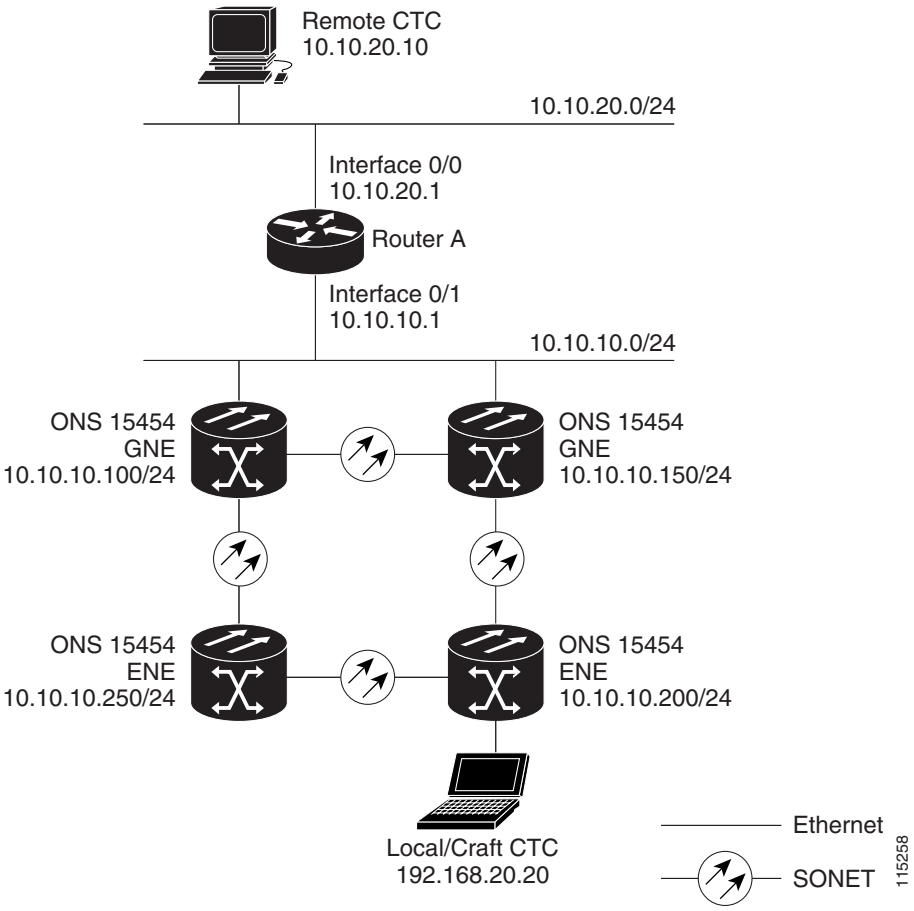
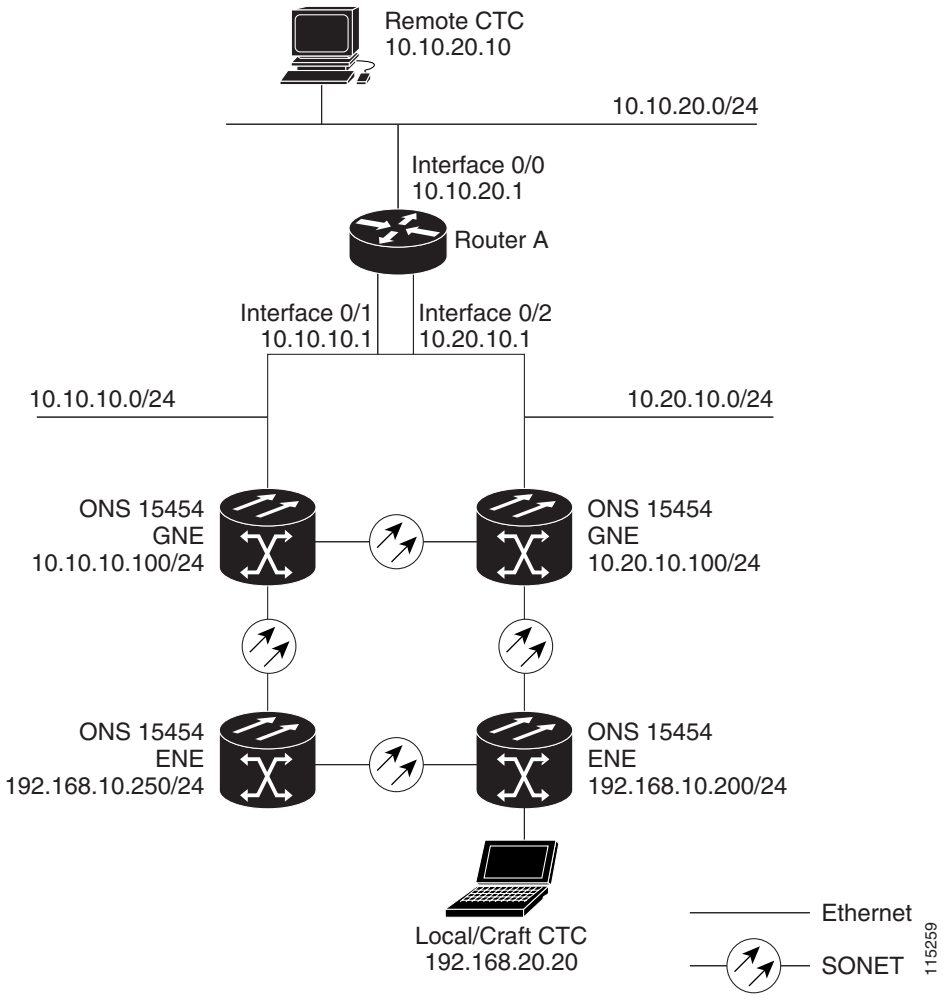


Figure 8-15 shows a network with dual GNEs on different subnets.

Figure 8-15 Dual GNEs on Different Subnets



Scenario 9: IP Addressing with Secure Mode Enabled

TCC2P cards running Software Release 5.0 and higher provide a secure mode option allowing you to provision two IP addresses for the ONS 15454. One IP address is provisioned for the ONS 15454 backplane LAN port. The other IP address is provisioned for the TCC2P TCP/IP Ethernet port. The two IP addresses provide an additional layer of separation between the TCC2P access port and the backplane LAN port. If secure mode is enabled, the IP addresses provisioned for the TCC2P TCP/IP port must follow general IP addressing guidelines. In addition, TCC2P IP addresses must reside on a different subnet from the backplane LAN port and ONS 15454 default router IP addresses.

The IP address assigned to the backplane LAN port becomes a private address, which is used to connect the ONS 15454 GNE to an OSS (Operations Support System) through a central office LAN or private enterprise network. In secure mode, the backplane's LAN IP address is not displayed on the CTC node view or to a technician directly connected to the node by default. This default can be changed to allow the backplane IP address to be viewed on CTC only by a Superuser.

Figure 8-16 shows an example of ONS 15454 nodes on the same subnet with secure mode enabled.

Note Secure mode is not available if TCC2 cards are installed, if only one TCC2P card is installed, or if TCC2P cards are installed with a software release prior to R5.0.

Figure 8-16 ONS 15454 GNE and ENE Nodes on the Same Subnet with Secure Mode Enabled

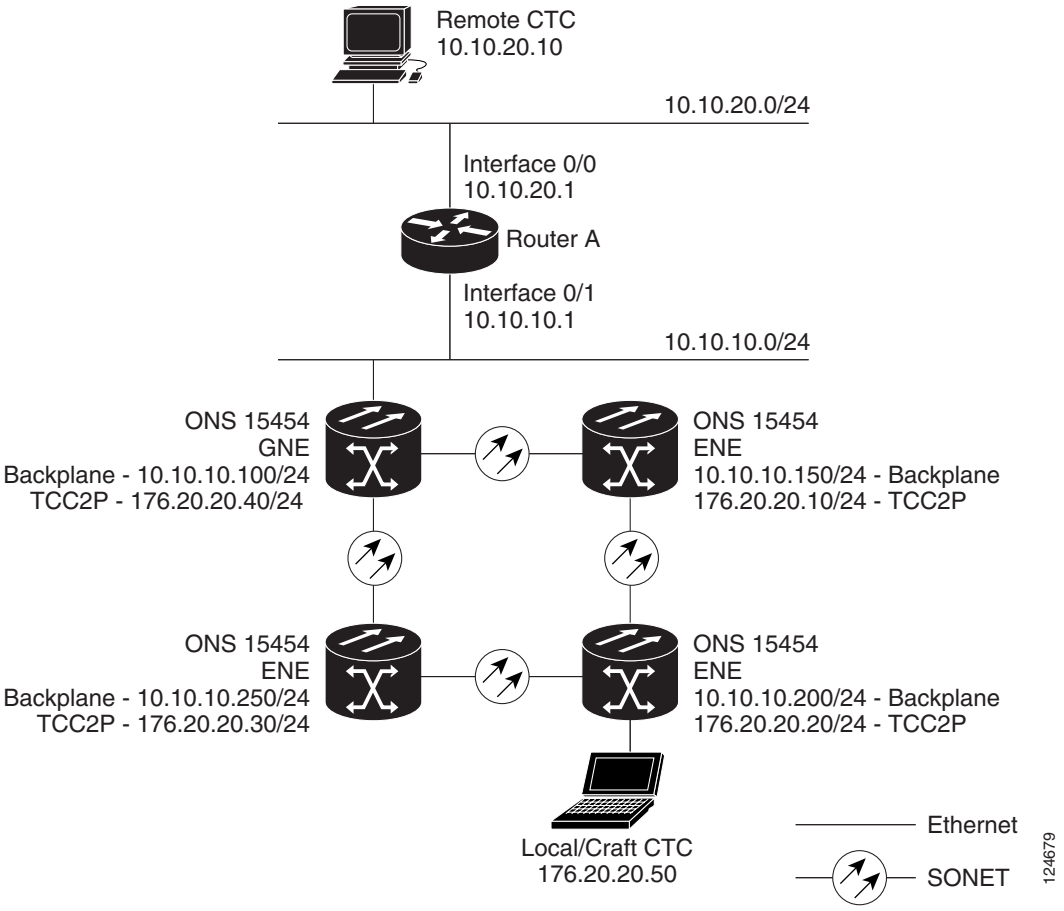
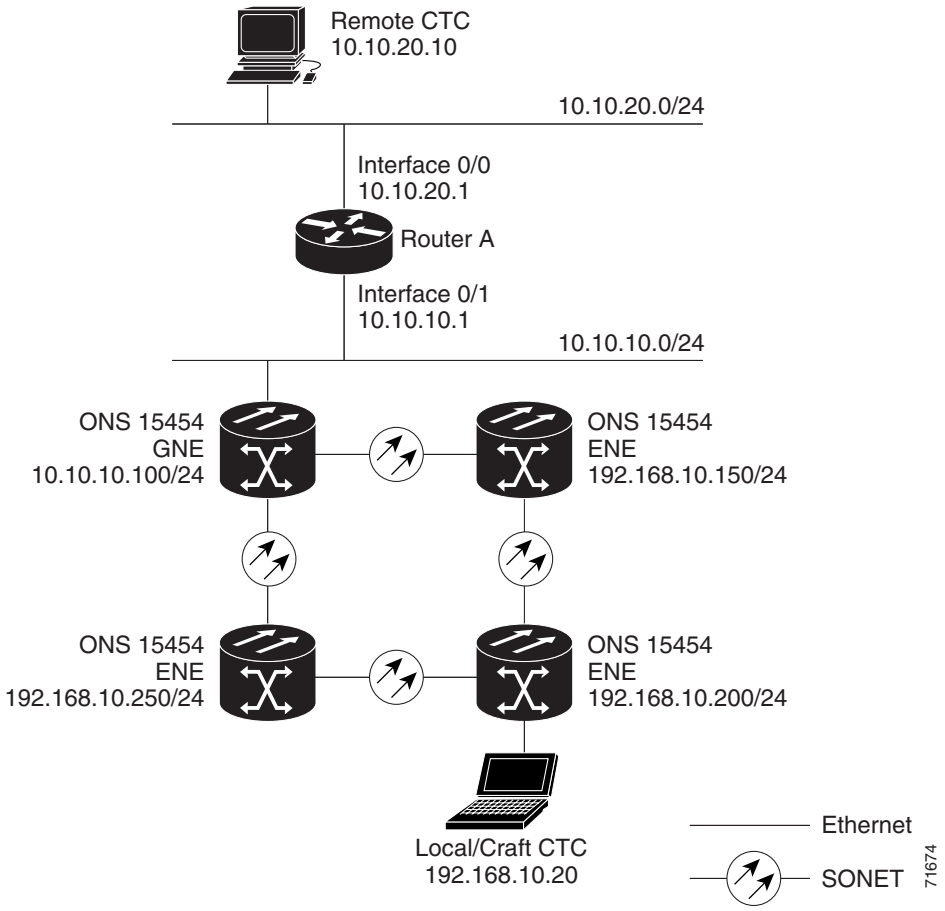


Figure 8-17 shows an example of ONS 15454 nodes connected to a router with secure mode enabled. In each example, TCC2P port addresses are on a different subnet from the node backplane addresses.

Figure 8-17 ONS 15454 GNE and ENEs on Different Subnets with Secure Mode Enabled



Routing Table

ONS 15454 routing information is displayed on the Maintenance > Routing Table tabs (see Figure 8-18. 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 TCC2/TCC2P 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

Figure 8-18 Viewing the ONS 15454 Routing Table

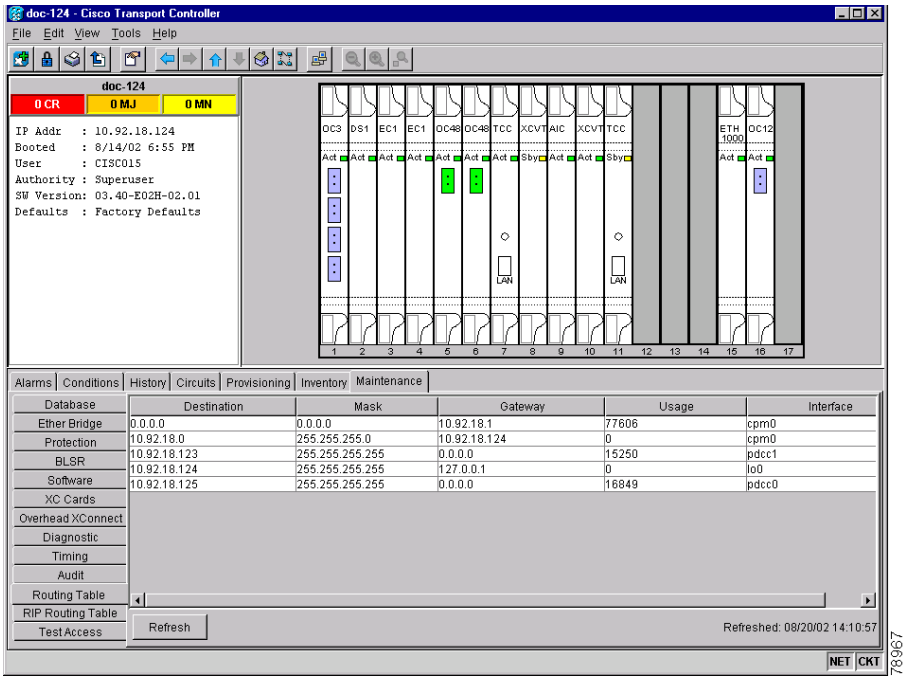


Table 8-5 shows sample routing entries for an ONS 15454.

Table 8-5 Sample Routing Table Entries

Entry	Destination	Mask	Gateway	Usage	Interface
1	0.0.0.0	0.0.0.0	172.20.214.1	265103	cpm0
2	172.20.214.0	255.255.255.0	172.20.214.92	0	cpm0
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 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.

Provisioning an External Firewall

Table 8-6 shows the ports that are used by the TCC2/TCC2P.

Table 8-6 Ports Used by the TCC2/TCC2P

Port	Function	Action[1]
0	Never used	D
20	FTP	D
21	FTP control	D
22	SSH	D
23	Telnet	D
80	HTTP	D
111	SUNRPC	NA
161	SNMP traps destinations	D
162	SNMP traps destinations	D
513	rlogin (not used; but port is in use)	D
683	CORBA IIOP	OK
1080	Proxy server	D

Table 8-6 Ports Used by the TCC2/TCC2P (continued)

Port	Function	Action[1]
2001-2017	I/O card Telnet	D
2018	DCC processor on active TCC2/TCC2P	D
2361	TL1	D
3082	Raw TL1	D
3083	TL1	D
5001	BLSR server port	D
5002	BLSR client port	D
7200	SNMP input port	D
9100	EQM port	D
9401	TCC boot port	D
9999	Flash manager	D
10240-12288	Proxy client	D
57790	Default TCC listener port	OK

1. D = deny, NA = not applicable, OK = do not deny

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 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 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 any 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 192.168.10.10 683 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 any 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 ****

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 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 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 any 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 192.168.10.10 683 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 192.168.10.10 683 host 10.10.10.100 eq 1080

*access-list 100 remark *** allows CTC communication with the 15454 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 15454 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 (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 ****

Open GNE

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

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

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

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

- If the node is configured with the SOCKS proxy server enabled in GNE or ENE mode, you must set up a proxy tunnel and/or a firewall tunnel.
- If the node is configured with the SOCKS proxy server enabled in proxy-only mode, you can set up proxy tunnels. Firewall tunnels are not allowed.
- If the node is configured with the SOCKS proxy server disabled, neither proxy tunnels or firewall tunnels are allowed.

Figure 8-19 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 8-19 Proxy and Firewall Tunnels for Foreign Terminations

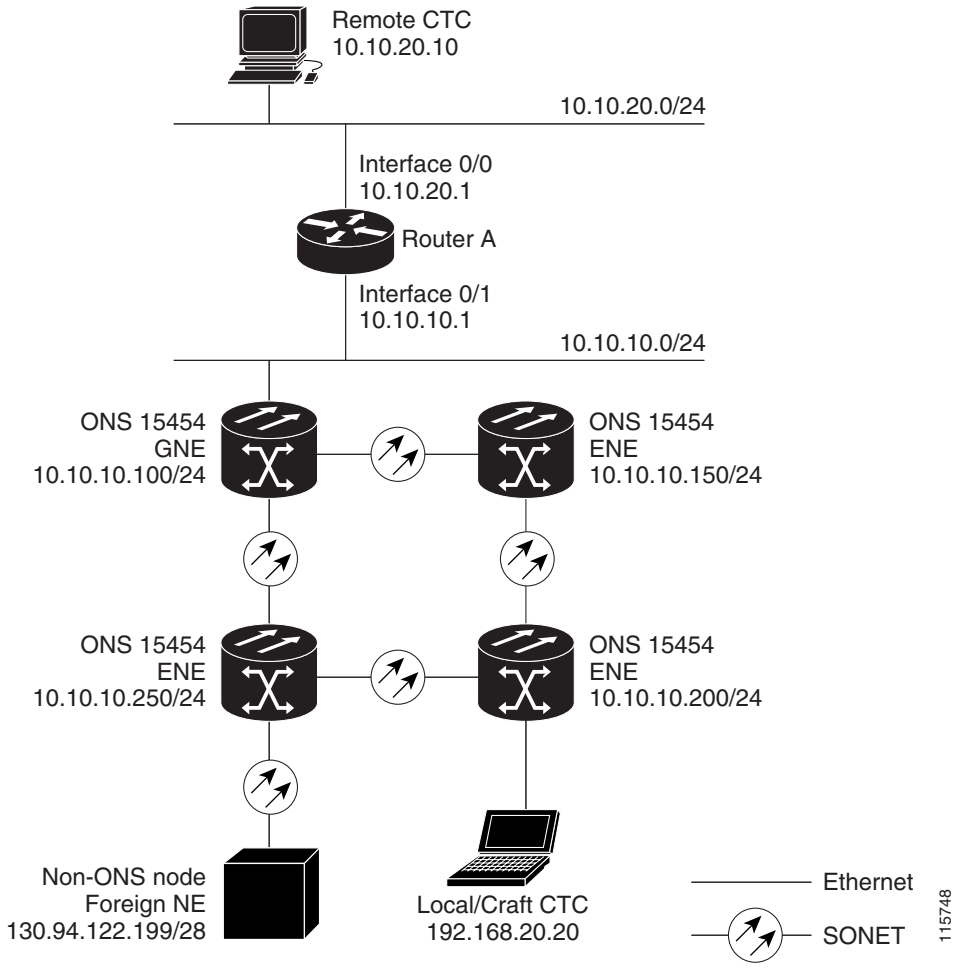
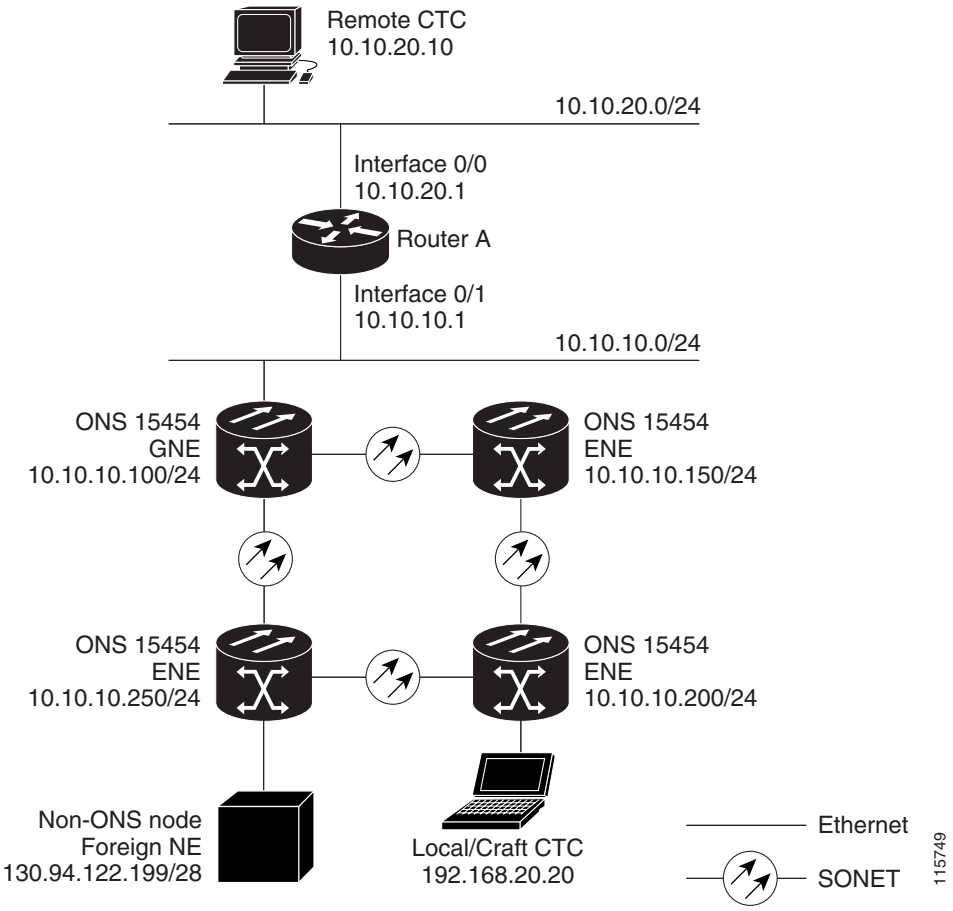


Figure 8-20 shows a remote node connected to an ENE Ethernet port. Proxy and firewall tunnels are useful in this example because the GNE would otherwise block IP access between the PC and foreign node. This configuration also requires a firewall tunnel on the ENE.

Figure 8-20 Foreign Node Connection to an ENE Ethernet Port



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 in the following situations:

- An optical port is connected to a transponder or muxponder client port provisioned in transparent mode.
- An optical ITU port is connected to a DWDM optical channel card.
- Two transponder or muxponder trunk ports are connected to a DWDM optical channel card and the generic control channel (GCC) is carried transparently through the ring.
- Transponder or muxponder client and trunk ports are in a regenerator group, the cards are in transparent mode, and DCC/GCC termination is not available.

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 8-7 lists the supported card combinations for client and trunk ports in a provisionable patchcord.

Table 8-7 Cisco ONS 15454 Client/Trunk Card Combinations for Provisionable Patchcords

	Client Cards						
Trunk Cards	**MXP_2.5G_10G TXP_MR_10G**	**TXP(P)_MR_2.5G**	**MXP_2.5G_10E TXP_MR_10E**	**32MUX-O 32DMX-O**	**32-WSS 32-DMX**	**ADxC**	**4MD**
MXP_2.5G_10G TXP_MR_10G	—	—	—	Yes	Yes	Yes	Yes
TXP(P)_MR_2.5G	—	—	—	Yes	Yes	Yes	Yes
MXP_2.5G_10E TXP_MR_10E	—	—	—	Yes	Yes	Yes	Yes
MXP(P)_MR_2.5G	—	—	—	Yes	Yes	Yes	Yes
OC-192	Yes	—	Yes	—	—	—	—
OC-48	Yes	Yes	Yes	—	—	—	—
OC-192 ITU	—	—	—	Yes	Yes	Yes	Yes
OC-48 ITU	—	—	—	Yes	Yes	Yes	Yes

Note If the OCSM card is installed in Slot 8, provisionable patchcords from OC-N ports to the following cards are not supported on the same node: MXP_2.5G_10G, TXP_MR_10G, TXP(P)_MR_2.5G, MXP_2.5G_10E, TXP_MR_10E, 32MUX-O, 32DMX-O, 32-WSS, or 32-DMX.

Table 8-8 lists the supported card combinations for client-to-client ports in a patchcord.

Table 8-8 Cisco ONS 15454 Client/Client Card Combinations for Provisionable Patchcords

Client Cards	**MXP_2.5G_10G TXP_MR_10G**	**TXP(P)_MR_2.5G**	**MXP_2.5G_10E TXP_MR_10E**
MXP_2.5G_10G TXP_MR_10G	Yes	—	Yes
TXP(P)_MR_2.5G	—	Yes	—
MXP_2.5G_10E TXP_MR_10E	Yes	—	Yes

Table 8-9 lists the supported card combinations for trunk-to-trunk ports in a patchcord.

Table 8-9 Cisco ONS 15454 Trunk/Trunk Card Combinations for Provisionable Patchcords

Client Cards	**MXP_2.5G_10G TXP_MR_10G**	**TXP(P)_MR_2.5G**	**MXP_2.5G_10E TXP_MR_10E**
MXP_2.5G_10G TXP_MR_10G	Yes	—	Yes

Table 8-9 Cisco ONS 15454 Trunk/Trunk Card Combinations for Provisionable Patchcords (continued)

Client Cards	MXP_2.5G_10G TXP_MR_10G	TXP(P)_MR_2.5G	MXP_2.5G_10E TXP_MR_10E
TXP(P)_MR_2.5G	—	Yes	—
MXP_2.5G_10E TXP_MR_10E	Yes	—	Yes

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

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

Transponder and muxponder ports have the following requirements when used in a provisionable patchcord:

- Two patchcords are required when a transponder/muxponder port is connected to an add/drop multiplexer or multiplexer/demultiplexer port. CTC automatically prompts the user to set up the second patchcord.
- If a patchcord is on a client port in a regenerator group, the other end of the patchcord must be on the same node and on a port within the same regenerator group.
- A patchcord is allowed on a client port only if the card is in transparent mode.

DWDM cards support provisionable patchcords only on optical channel ports. Each DWDM optical channel port can have only one provisionable patchcord.

Note For TXP, MXP, and DWDM card information refer to the Cisco ONS 15454 DWDM Installation and Operations Guide.