

Cisco ONS 15800 Series and Cisco Transport Manager Data Communication Network Redundancy Using Network Address Translation

Introduction

Cisco Transport Manager is the element management system (EMS) for the Cisco ONS 15000 family of optical networking system products. Integrating fault, configuration, and performance management capabilities, Cisco Transport Manager streamlines and strengthens optical network operation, administration, maintenance, and provisioning (OAM&P).

One of the new features introduced with the Cisco Transport Manager Release 3.0 is the management of the double IP address to support access to the Cisco ONS 15800 Series nodes through two different gateways using Layer 3 routing instead of Layer 2 bridging. This capability requires configuration of the data communication network (DCN) using the Network Address Translation (NAT) approach as it is described in this document.

A feature enabled by the Internet Protocol Version 4 (IPv4) and later versions, NAT is usually exploited in two different situations:

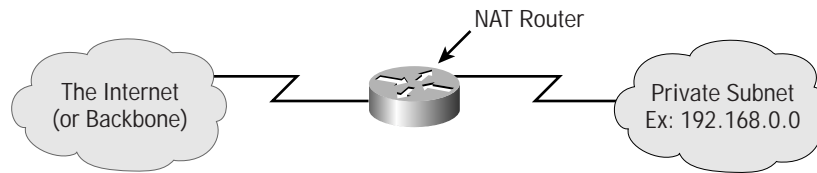
- *When Internet service providers or, in general, any administrative domains, have a shortage of public IP addresses*—The typical situation is a larger subnet covered with a small private pool of IP addresses that need access to the Internet
- *When a subnet needs to be visible and gets access to the Internet through alternative routes*—This is the implementation for the Cisco ONS 15800 Series DCN

Scope of NAT

NAT is a router function that may be configured as shown in Figure 1; note that only the border router requires the NAT configuration modifications.

With basic NAT functionality, the addresses inside a domain may be reused by any other domain. For instance, many domains could use the same private Class B address space. At each exit point between a domain and backbone, NAT is installed to translate the private Class B address into a valid public routable IP address.

Figure 1
NAT Router to Provide Internet Access to the Private Subnet

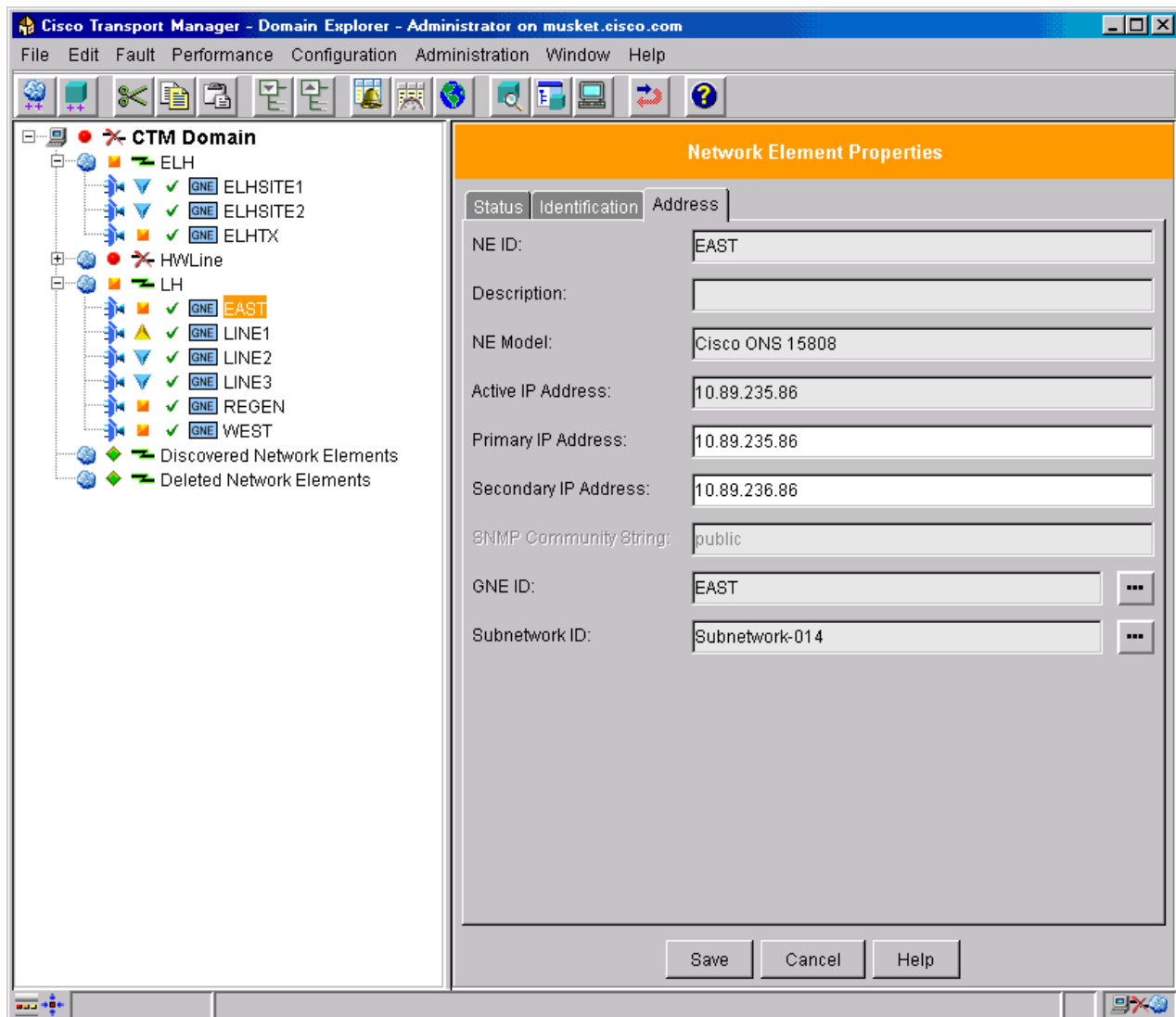


Double IP Address Management on Cisco Transport Manager

Cisco Transport Manager Release 3.0 manages the following IP addresses for the network elements of the Cisco ONS 15800 Series (Cisco ONS 15800, ONS 15801 and ONS 15808 platforms):

- **Active IP address**—This is the IP address currently used by Cisco Transport Manager to reach the Cisco ONS 15800 Series node.
- **Primary IP address**—This is the one configured on Control Monitor Processor (CMP) and used during normal working conditions to get IP access to the network element through the default gateway.
- **Secondary IP address**—This is the one used during the fault condition to reach the node through the NAT router. If the secondary IP address is not used/configured, the address is the same as the primary IP address.

Figure 2
View of the Domain Explorer with Double IP Address Settings



The primary IP address can be changed from the address panel on either the domain explorer or the network-element explorer. The change of the primary IP address is reflected by a change of the IP address stored on the CMP, and the CMP is rebooted to make the new IP address active.

When the primary IP address is changed, the secondary IP address is reset to the same address as the primary. Before reconfiguring the secondary IP address, the user should remap the NAT on the new static IP address.

The secondary IP address can be changed just in the address panel of the domain explorer; because it is a Cisco Transport Manager configuration parameter and not a network-element configuration parameter, the CMP does not have to be rebooted.

The secondary IP address should be the proper address specified in the translation table of the NAT router to ensure that Cisco Transport Manager can reach the node. During normal conditions the active IP address is the same as the primary IP address, if a fault occurs the Cisco Transport Manager switch on the secondary IP address. When both the primary and secondary IP addresses are unreachable, Cisco Transport Manager declares the communication state unavailable.

After switching to the secondary IP address, Cisco Transport Manager tries continuously to re-establish the connection to the primary IP address by checking the availability at each polling cycle (the frequency of the polling cycle is a configuration parameter within the Cisco Transport Manager server).

Implementing NAT on Cisco ONS 15800 Data Communication Network

NAT is used in the DCN to provide a fully redundant path from Cisco Transport Manager to the dense wavelength division multiplexing (DWDM) network elements. With NAT, if a fiber break occurs on the optical link it is still possible to reach each network element from Cisco Transport Manager, thus providing continuous, uninterrupted network monitoring capability.

From Cisco Transport Manager, the network elements are accessible by using two different IP addresses, as specified before. The first IP address (or primary IP address) configured on the CMP is used during normal working conditions to get IP access to the network element through the default gateway; the second (or secondary IP address) is used during a fault condition such as a fiber break. The network elements on the side of the break (that is, opposite their default gateway router) would not be reachable anymore because their IP packets cannot reach the default gateway. Because both the Ethernet LAN and the IP protocol are up, CMP packets can exploit a second router (connected on the other end of the optical line) as a "pseudogateway."

NAT enables solving the routing problem with the network element when the default gateway is not available.

Figures 3 and 4 show how the routers interconnect the DCN. The side routers are configured with an Ethernet interface in the same LAN and a serial interface toward the network operations center (NOC) router.

An IP address translation table is set up on the NAT router to map a set of secondary IP addresses (destination IP NAT) for all the nodes in the DWDM line to their actual addresses. (These secondary IP addresses must be part of the legal subnet that links the NAT router with the DCN.) An additional pool of dynamically allocated IP addresses should also be configured on the NAT router so that the Element Management System can access the network-element LAN as if it were on the same subnet (source IP NAT).

If a fiber breaks, Cisco Transport Manager can still access the network elements using their secondary addresses through the NAT router. The NAT router receives the TCP/IP packet for the secondary address, changes the destination address to the actual address of the node, and changes the Cisco Transport Manager source IP address with a dynamically allocated one from the optical-line subnet and forwards the packet to its correct destination. The response packet goes back to the router, where it changes both source and destination addresses back to the original ones and sends the packet to the Cisco Transport Manager.

Note: The router containing the NAT configuration should never advertise the path to the real network-element line subnet-it should advertise the NAT address only to the other routers. This scenario eliminates routing problems when the path is down but the Ethernet subnet and the protocols are still up and operating.

Figure 3
Functional View of Data-Communication Network: Normal Condition

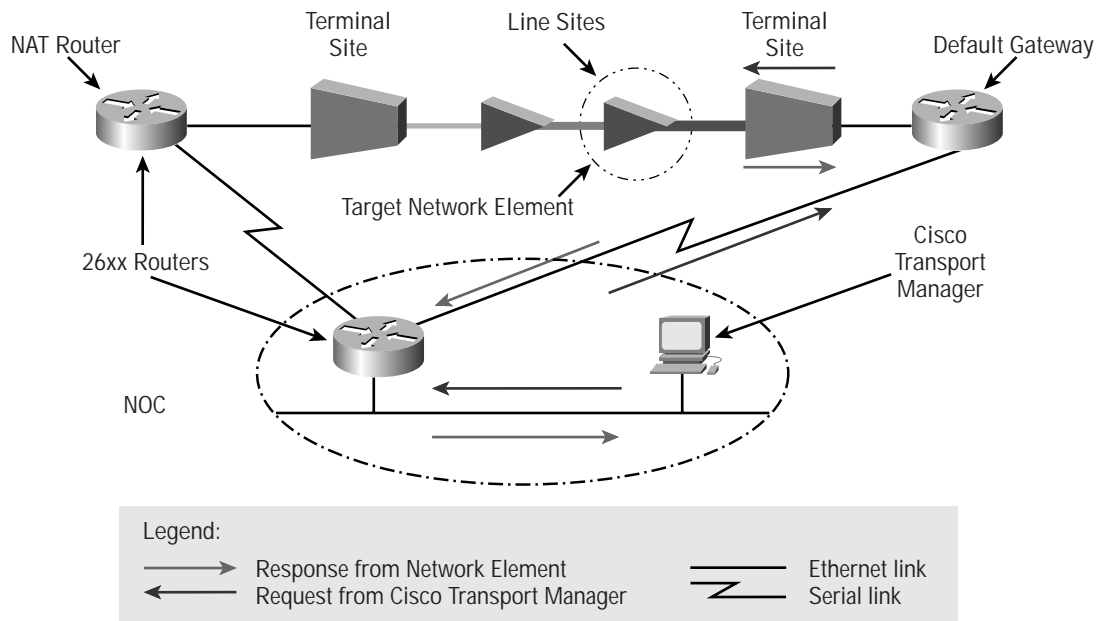
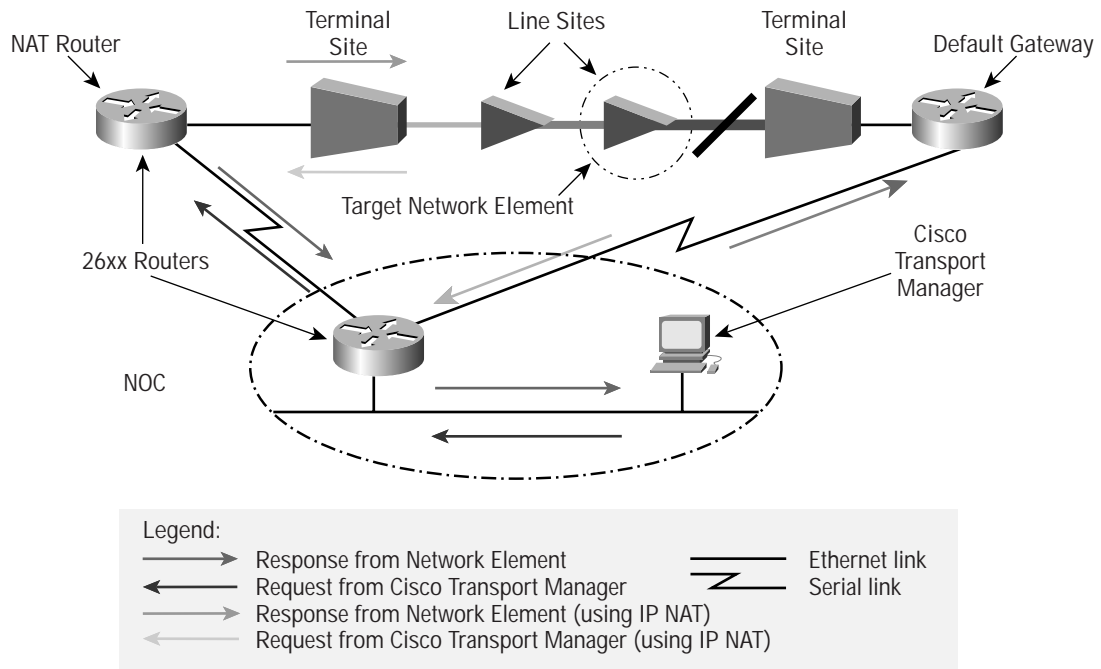


Figure 4
Functional View of Data-Communication Network: A Fault Occurs on the Line



Figures 5 and 6 show how IP routing works in normal and fault conditions, respectively.

Figure 5

IP Functional Scheme: An Example of IP Routing in Normal Conditions

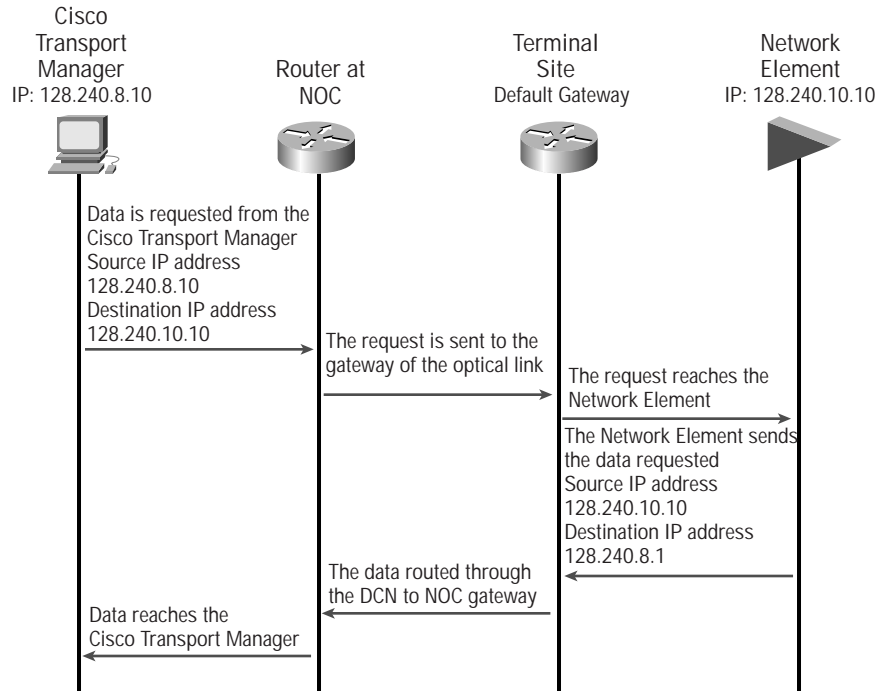
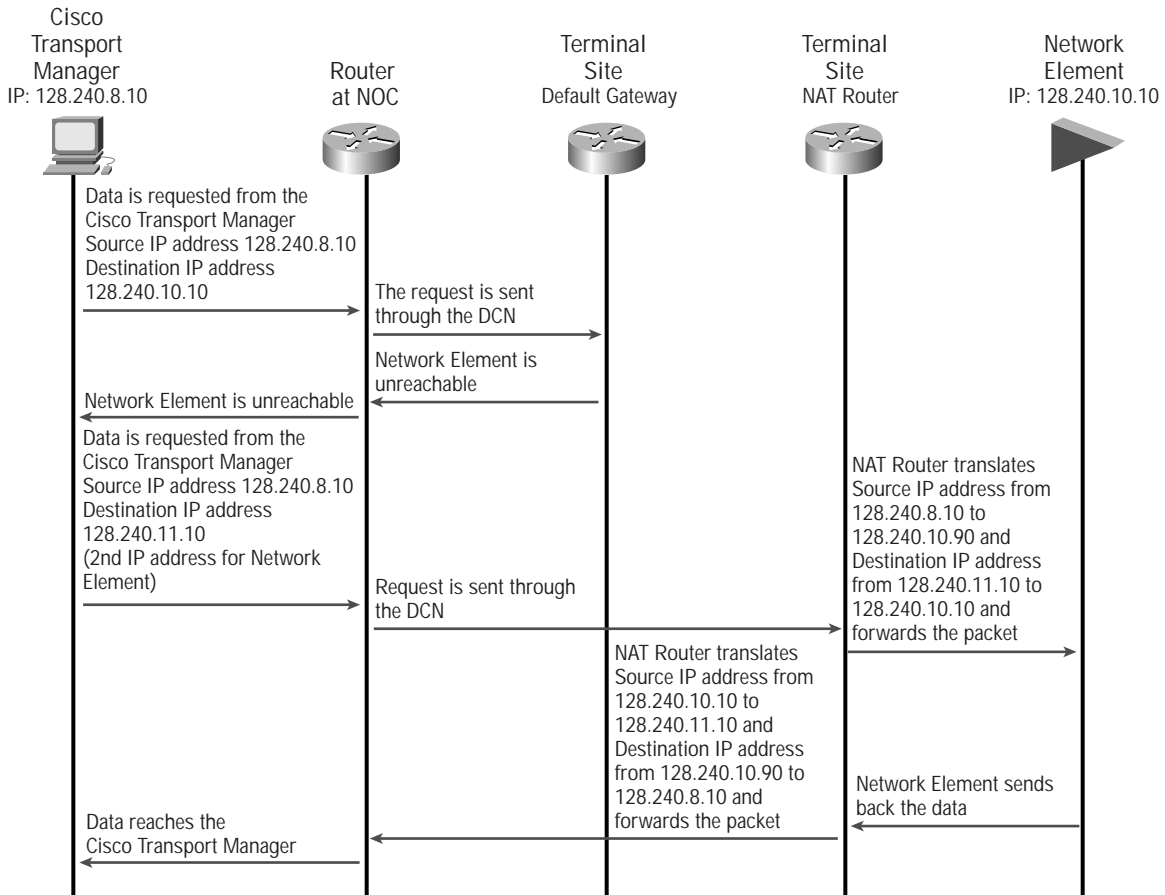


Figure 6

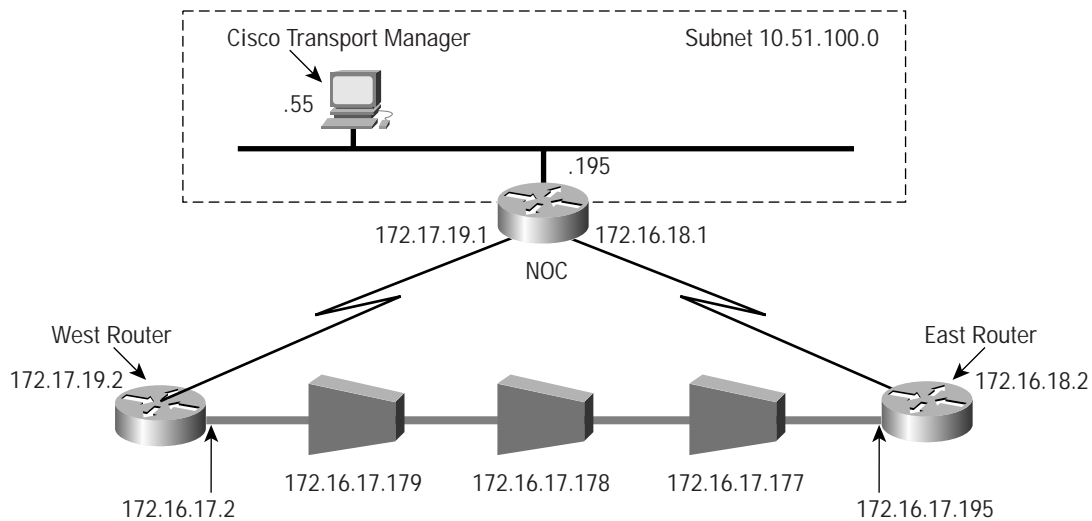
IP Functional Scheme: An Example of IP Routing when a Fault Occurs



Example of Configuration

Figure 7 shows a typical DCN configuration scheme for data-communication redundancy exploiting NAT. Configuration of the actual router is included.

Figure 7
Test bed Layout



Current Configuration of NOC Router

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname gwos1  
!  
enable password test!  
!  
username root  
!  
ip subnet-zero  
ip name-server 144.254.74.7  
!  
cns event-service server  
!  
process-max-time 200  
!  
interface FastEthernet0/0  
 ip address 10.51.100.195 255.255.255.0  
 no ip directed-broadcast  
!  
interface Serial0/2  
 ip address 172.17.19.1 255.255.255.0  
 no ip directed-broadcast  
 no ip mroute-cache  
 no fair-queue  
!  
interface Serial0/3  
 ip address 172.16.18.1 255.255.255.0  
 no ip directed-broadcast  
 no ip mroute-cache  
 no fair-queue  
!
```

```
router eigrp 17
 network 10.0.0.0
 network 172.16.0.0
 network 172.17.0.0
 no auto-summary
!
ip classless
no ip http server
!
line con 0
line aux 0
line vty 0 4
!
no scheduler allocate
end
```

East Router Current configuration:

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname gwterm1-c
!
enable password test!
!
username root
ip subnet-zero
!
interface Ethernet0
 ip address 172.16.17.195 255.255.255.0
 no ip directed-broadcast
!
interface Serial0
 ip address 172.16.18.2 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 no fair-queue
 clockrate 1000000
!
router eigrp 17
 network 172.16.0.0
 no auto-summary
!
ip classless
!
line con 0
line aux 0
line vty 0 4
!
end
```

West Router Current configuration:

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname gwterm2-d
!
enable password test!
!
username root
```

```
ip subnet-zero
ip name-server 144.254.42.167
!
interface Ethernet0
 ip address 172.16.17.2 255.255.255.0
 no ip directed-broadcast
 ip nat inside
!
interface Serial0
 ip address 172.17.19.2 255.255.255.0
 no ip directed-broadcast
 ip nat outside
 no ip mroute-cache
 no fair-queue
 clockrate 1000000
!
router eigrp 17
 network 172.17.0.0
!
ip nat pool gwterm2d-nat 172.16.17.10 172.16.17.15 prefix-length 24
ip nat inside source static 172.16.17.177 172.17.19.177
ip nat inside source static 172.16.17.178 172.17.19.178
ip nat inside source static 172.16.17.179 172.17.19.179
ip nat outside source list 1 pool gwterm2d-nat
ip classless
ip route 172.16.17.10 255.255.255.255 Serial0
ip route 172.16.17.11 255.255.255.255 Serial0
ip route 172.16.17.12 255.255.255.255 Serial0
ip route 172.16.17.13 255.255.255.255 Serial0
ip route 172.16.17.14 255.255.255.255 Serial0
ip route 172.16.17.15 255.255.255.255 Serial0
!
access-list 1 permit any
!
line con 0
line aux 0
line vty 0 4
!
end
```

References

For more technical information regarding features of Cisco Transport Manager, refer to the following sites:

<http://www.cisco.com/warp/public/cc/pd/nemnsw/ctm/index.shtml>

<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/optnet/ctm/>

For more technical information regarding NAT, refer to the related Cisco Web page at <http://www.cisco.com/warp/public/556/nat-cisco.shtml>; it contains an explanation of the various fields of application for NAT, in addition to other references to public domain bibliography on the subject.

CISCO SYSTEMS



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: 65 317 7777
Fax: 65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe