Global Knowledge®

Expert Reference Series of White Papers

The Basics of Configuring and Using Cisco Network Address Translation

The Basics of Configuring and Using Cisco Network Address Translation

Raymond B. Dooley, MBA, CCSI, CCNA, CCNP, CCDA, CCDP, SE, FE, Global Knowledge Course Director

Introduction

While the Internet uses IP addresses assigned by an Internet authority such as the American Registry for Internet Numbers (ARIN), there are too few of these numbers to uniquely identify the millions of computers and computing devices in the world. Therefore, most enterprises use private addresses which allow them to identify the aforementioned computers. Of course, these IP numbers cannot be allowed on the Internet because all private networks use the same ones so there would be vast overlapping of addresses, and the addresses are not compliant anyway.

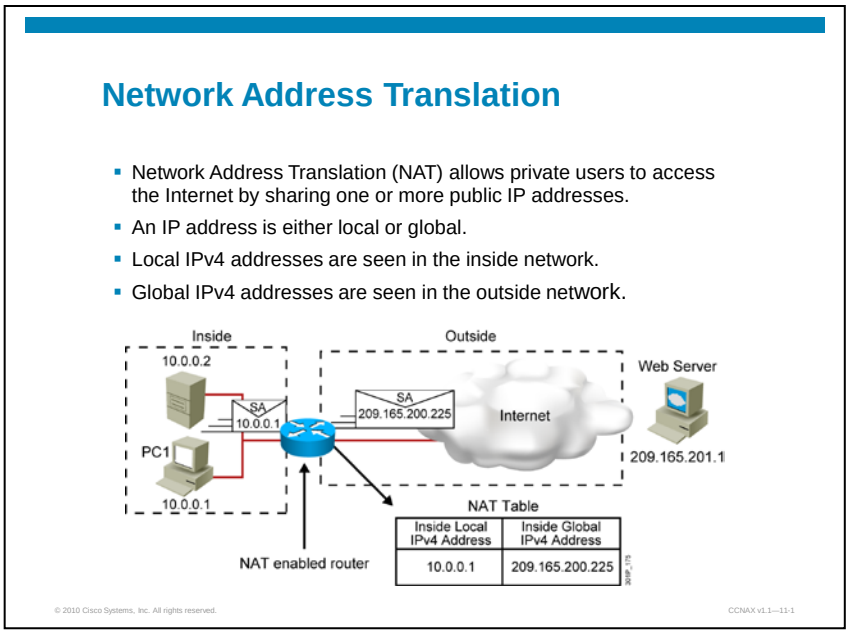
Therefore, it is necessary to change the identity of a private host to a legal public host. This process is called Network Address Translation (NAT) and may be implemented on Cisco firewall products and Cisco routers. The firewall device(s) at the Internet demarcation point is by far the more popular way to implement NAT, but routers are used in small offices or small-to-medium-sized networks in which a separate firewalling solution is not possible or affordable. The focus of this paper is on the router-based NAT solution.

The objective is to provide a fundamental explanation of Cisco NAT with the following topics:

1. Defining NAT and Port Address Translation (PAT)
2. Configuring Static NAT
3. Configuring Dynamic NAT
4. Configuring PAT
5. Troubleshooting NAT/PAT
6. Troubleshooting Example

Copyright ©2014 Global Knowledge Training LLC. All rights reserved.

Defining NAT and PAT



The following is list of important NAT/PAT definitions:

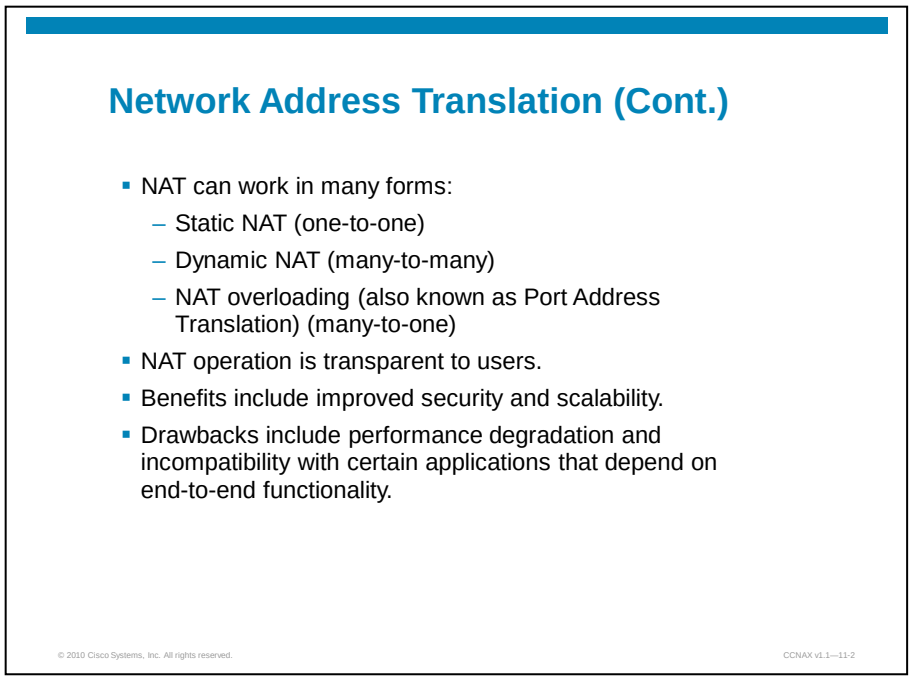
Inside Local Addresses are the private addresses used within the enterprise network and cannot be used in the public network (the Internet).

Inside Global Addresses are assigned by either an Internet authority or an Internet Service Provider (ISP) and are allowed on the Internet.

Outside Global Addresses are assigned by either an Internet authority or an ISP to Internet users in companies and organizations, as well as to individuals that are located where the local translation occurs. For example, from Acme Corp, the IP address for cisco.com would be an outside global address. Remember that these definitions are based on perspective from the locally translated address location that is looking outward.

Outside Local Addresses are the private (inside local) addresses of entities on the other side of the Internet and should never be known to a local entity doing NAT except in one special case. Occasionally during a merger, an organization will find itself with overlapping private addresses, such as many hosts with duplicate addresses in the 10.0.0.0/8 network. In this case, a special kind of NAT called NAT Overlap is used temporarily and will not be described further, since the final solution is IP address renumbering. However, in this one instance, the outside local address is known since both sides of NAT are within the organization and there is no Internet involved.

Copyright ©2014 Global Knowledge Training LLC. All rights reserved.



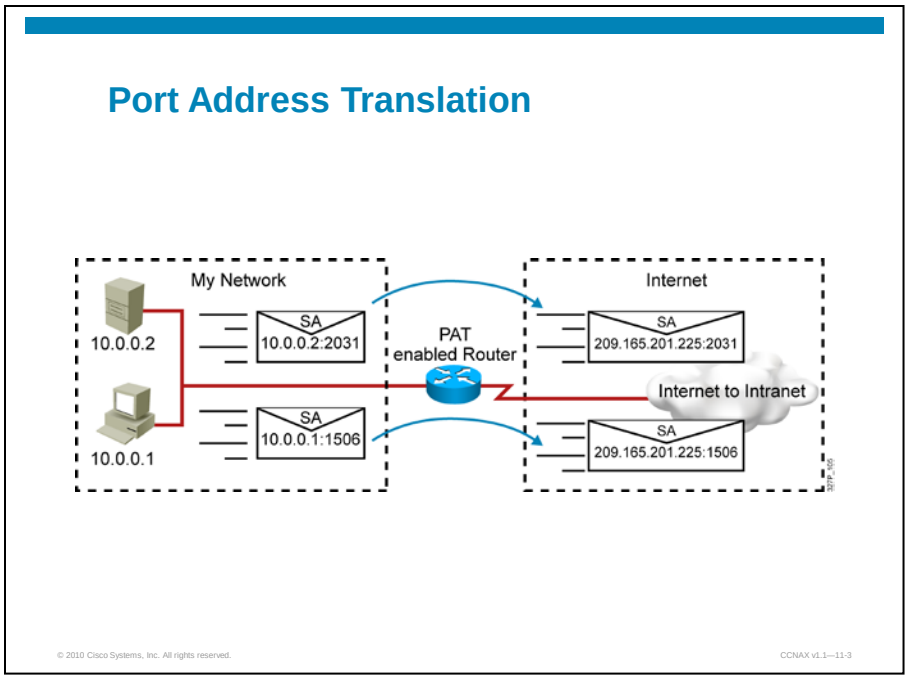
Static NAT, as the name implies, provides a permanent private (inside local) to public (inside global) translation, which never ages out of the translation table and is much like a static route. It creates a security issue because it allows outside hosts to come through NAT inbound, but may be necessary for small companies to provide access to their website where various wares are being sold.

Dynamic NAT implies that there are exactly the same number of inside local hosts as inside global hosts. This is rarely the case with the scarcity of public addresses.

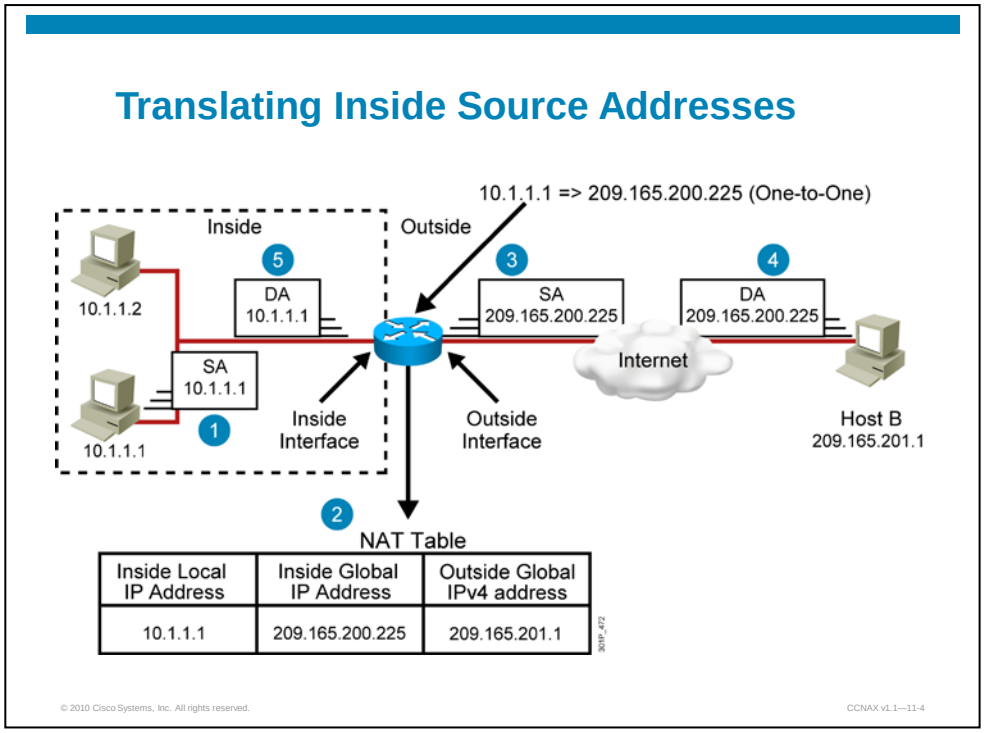
Port Address Translation (called NAT overload in the Cisco IOS) is by far the most common NAT installation.

The last bullet in the graphic refers to older applications with hard-coded (embedded) IP addresses in the application.

Copyright ©2014 Global Knowledge Training LLC. All rights reserved.



The graphic further clarifies the idea of PAT. Along with the inside local address to be translated to an inside global address as the packet exits the router, the port number (both source and destination) is recorded. In the case where non-TCP packets are used, such as ping packets, NAT/PAT creates a source and destination port. This enables several thousand inside local hosts to be translated to one inside global host IP address.



1. The packet is generated by the host with an inside local address.
2. The packet arrives at the NAT inside interface (configured as part of the NAT installation).
3. The inside local address is translated to an inside global address.
4. The packet arrives at outside global host B.
5. The return packet is translated back from the NAT outside interface to the originating inside local host.

Copyright ©2014 Global Knowledge Training LLC. All rights reserved.

Configuring Static NAT

Configuring and Verifying Static Translation

```
RouterX(config)#
ip nat inside source static 10.1.1.1 209.165.200.225
```

- Establish static translation between an inside local address (10.1.1.1) and an inside global address (209.165.200.225).

```
RouterX(config-if)#
ip nat inside
```

- Mark the interface as connected to the inside.

```
RouterX(config-if)#
ip nat outside
```

- Mark the interface as connected to the outside.

```
RouterX#
show ip nat translations
```

- Display active translations.

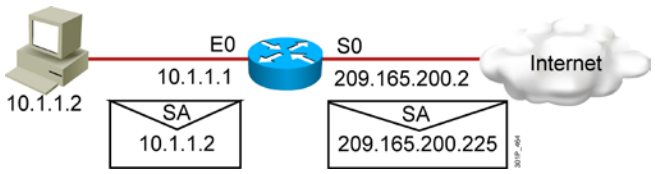
© 2010 Cisco Systems, Inc. All rights reserved.

The graphic illustrates the commands used to configure static NAT:

- The inside and outside NAT interfaces must be defined.
- The static NAT translation details are defined.

The configuration can be verified with the **show ip nat translation** command. This graphic provides an example of a static NAT configuration and verification on a Cisco router:

Enabling Static NAT Address Mapping Example




```
interface s0
ip address 209.165.200.2 255.255.255.240
ip nat outside
!
interface e0
ip address 10.1.1.1 255.255.255.0
ip nat inside
!
ip nat inside source static 10.1.1.2 209.165.200.225
```

```
RouterX#show ip nat translations
     Pro Inside global     Inside local   Outside local   Outside global
     --- 209.165.200.225   10.1.1.2          ---             ---
```

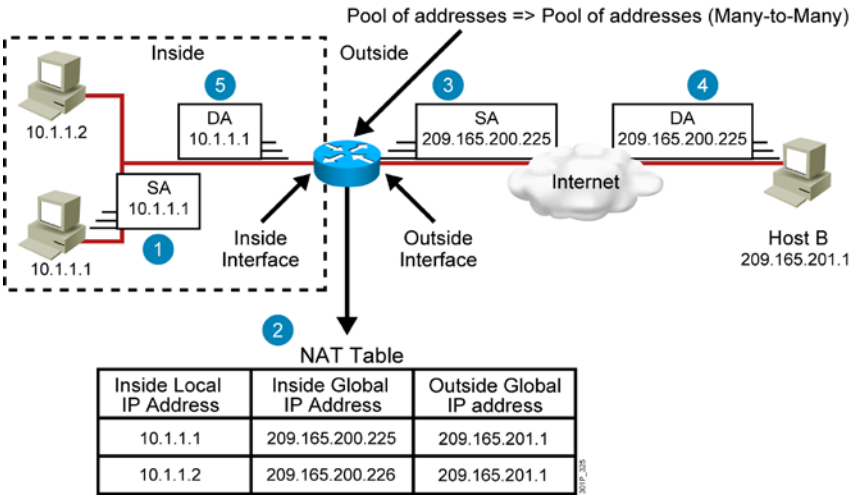
© 2010 Cisco Systems, Inc. All rights reserved.

Copyright ©2014 Global Knowledge Training LLC. All rights reserved.

Configuring Dynamic NAT

This graphic is similar to a previous one and shows the same five translation steps with a bit more detail in the address tables. Remember with dynamic NAT, the number of inside hosts should be the same as the number of outside (inside global) hosts.

Dynamic Addresses Translation



Inside Local IP Address	Inside Global IP Address	Outside Global IP address
10.1.1.1	209.165.200.225	209.165.201.1
10.1.1.2	209.165.200.226	209.165.201.1

© 2010 Cisco Systems, Inc. All rights reserved.

Configuring and Verifying Dynamic Translation

```
RouterX(config)#
ip nat pool NET209 209.165.200.225 209.165.200.238
netmask 255.255.255.240
```

- Define a pool **NET209** of global addresses (from 209.165.200.225/28 to 209.165.200.238/28) to be allocated as needed.

```
RouterX(config)#
access-list 1 permit 192.168.1.0 0.0.0.255
```

- Define a standard IP ACL 1 permitting inside local addresses 192.168.1.0/24 that are to be translated.

```
RouterX(config)#
ip nat inside source list 1 NET209
```

- Establish dynamic source translation, specifying the ACL that was defined in the previous step (ACL 1).

```
RouterX(config)#
show ip nat translations
```

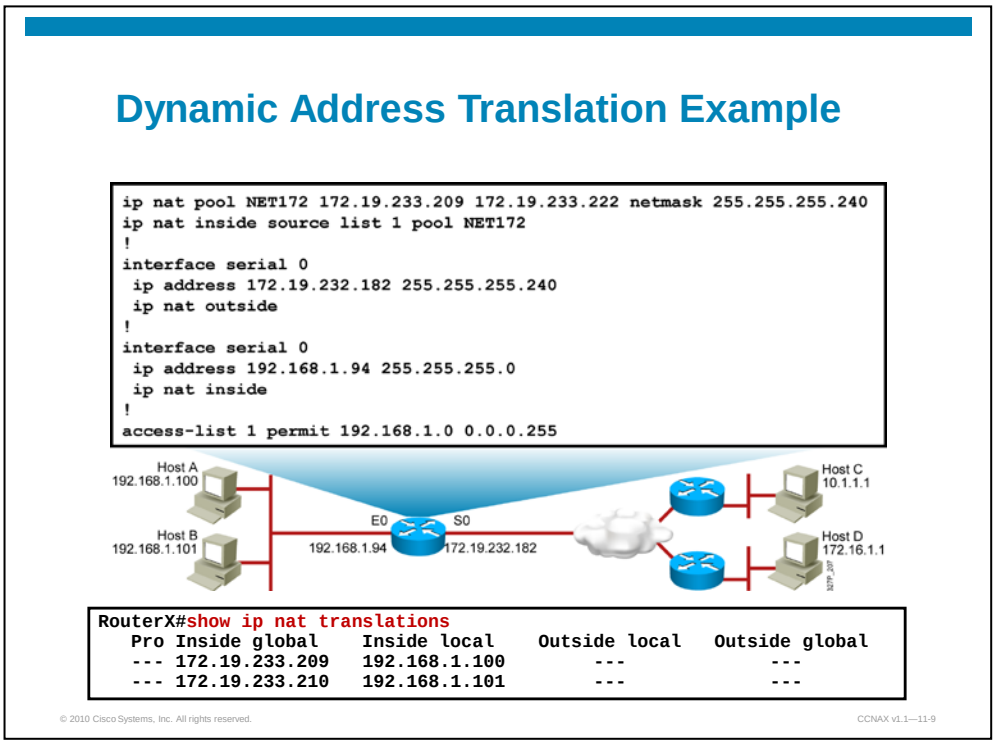
- Display active translations

© 2010 Cisco Systems, Inc. All rights reserved.

Copyright ©2014 Global Knowledge Training LLC. All rights reserved.

The configuration now involves additional elements:

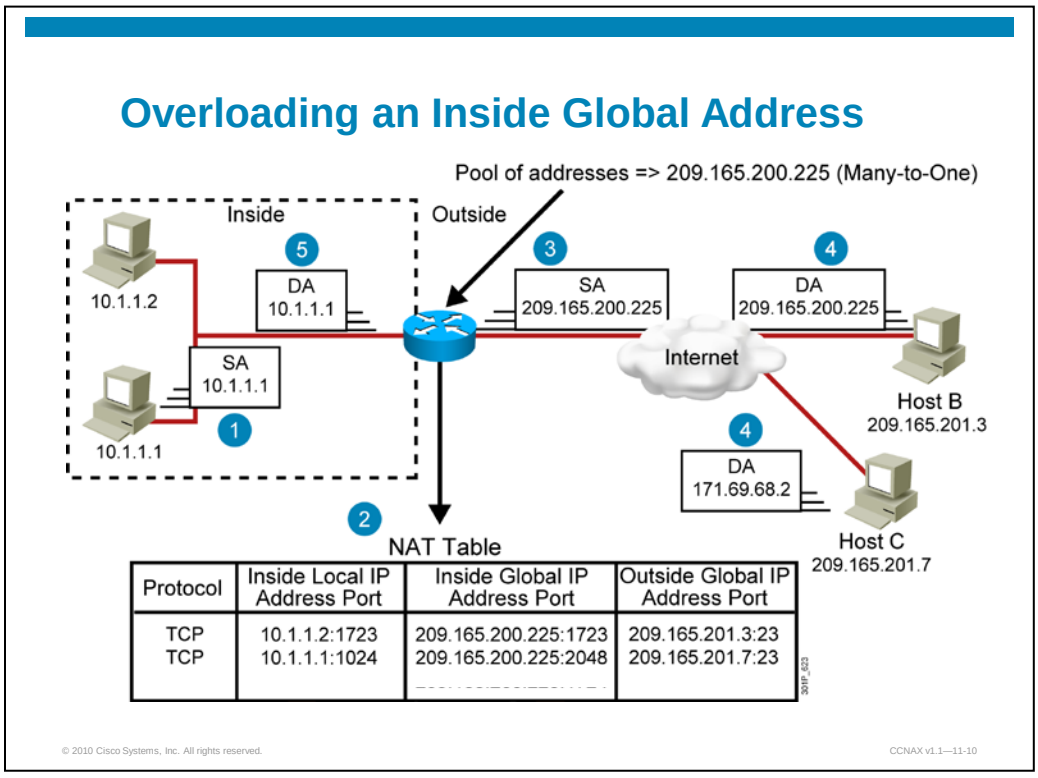
- A block of inside global addresses is identified with an ACL.
- A pool of outside local addresses is identified with a pool name. With NAT overload or PAT, there is another way to do this.
- A command is needed to define the inside local to inside global translation mapping of the ACL and the pool name.
- The inside and outside IP NAT interfaces must still be defined.
- The verification is **show ip nat translations** as before.



The graphic shows a completed dynamic NAT configuration. Note that the translation configuration line includes a network mask or prefix following the address pool.

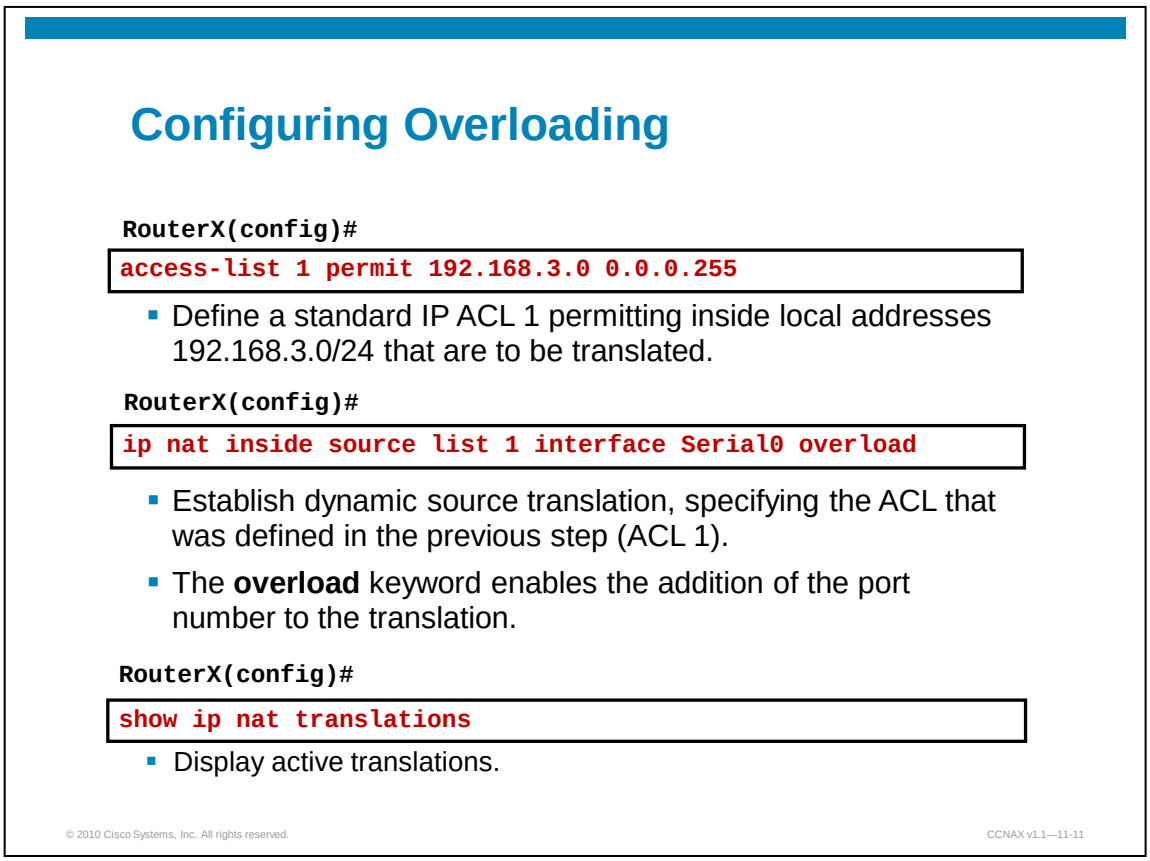
Copyright ©2014 Global Knowledge Training LLC. All rights reserved.

Configuring NAT Overload—PAT



As described earlier, PAT or NAT overload deploys the same five-step process as before, except that the source and destination UPD/TCP port number is recorded along with the IP address as part of the translation. This is how thousands of inside local IP hosts may be translated to one inside global host.

Copyright ©2014 Global Knowledge Training LLC. All rights reserved.



The ACL is still used to define the inside local address block.

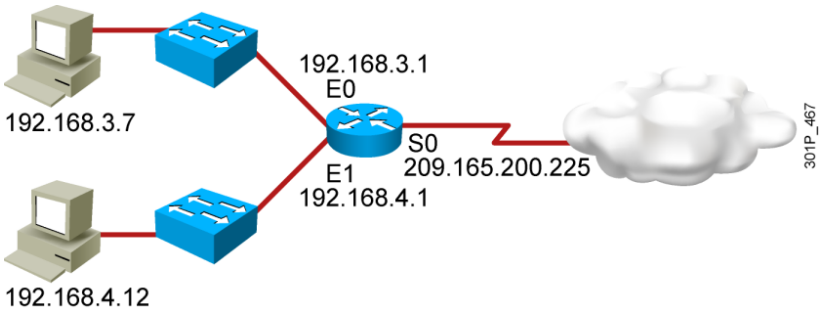
The translation command now has a new argument in place of the pool name described in dynamic NAT. The inside local address can be translated to whichever IP host address is configured on the IP NAT outside interface with the additional argument **overload**.

The command **show ip nat translations** has the same function as before.

Copyright ©2014 Global Knowledge Training LLC. All rights reserved.

The next two graphics provide a working example with two inside NAT interfaces and one outside.

Overloading an Inside Global Address Example



- Two private networks - 192.168.3.0/24 and 192.168.4.0/24
- Overload to router outside S0 interface address - 209.165.200.225/32

© 2010 Cisco Systems, Inc. All rights reserved.

Overloading an Inside Global Address Example (Cont.)

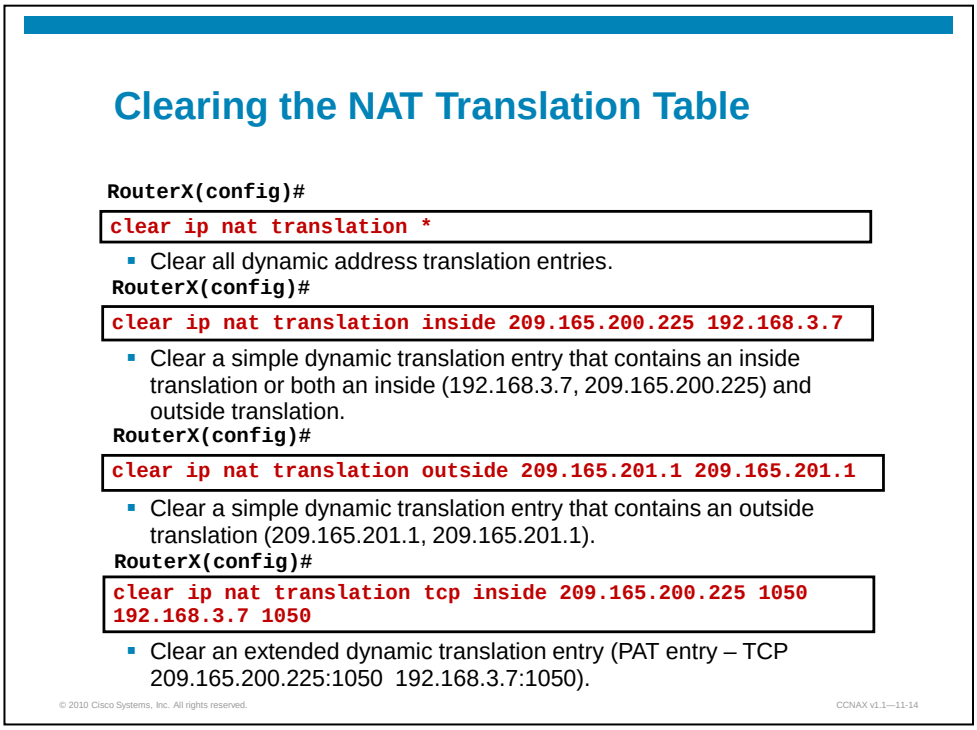
```
hostname RouterX
!
interface Ethernet0
 ip address 192.168.3.1 255.255.255.0
 ip nat inside
!
interface Ethernet1
 ip address 192.168.4.1 255.255.255.0
 ip nat inside
!
interface Serial0
 description To ISP
 ip address 209.165.200.225 255.255.255.240
 ip nat outside
!
ip nat inside source list 1 interface Serial0 overload
!
ip route 0.0.0.0 0.0.0.0 Serial0
!
access-list 1 permit 192.168.3.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.0.255
```

```
RouterX#show ip nat translations
Pro Inside global         Inside local       Outside local      Outside global
TCP 209.165.200.225:1050  192.168.3.7:1050   209.165.201.1:23   209.165.201.1:23
TCP 209.165.200.225:1776  192.168.4.12:1776  209.165.202.1:25   209.165.202.1:25
```

© 2010 Cisco Systems, Inc. All rights reserved.

Copyright ©2014 Global Knowledge Training LLC. All rights reserved.

The graphic shows the completed configuration with the verification of the translations taking place.



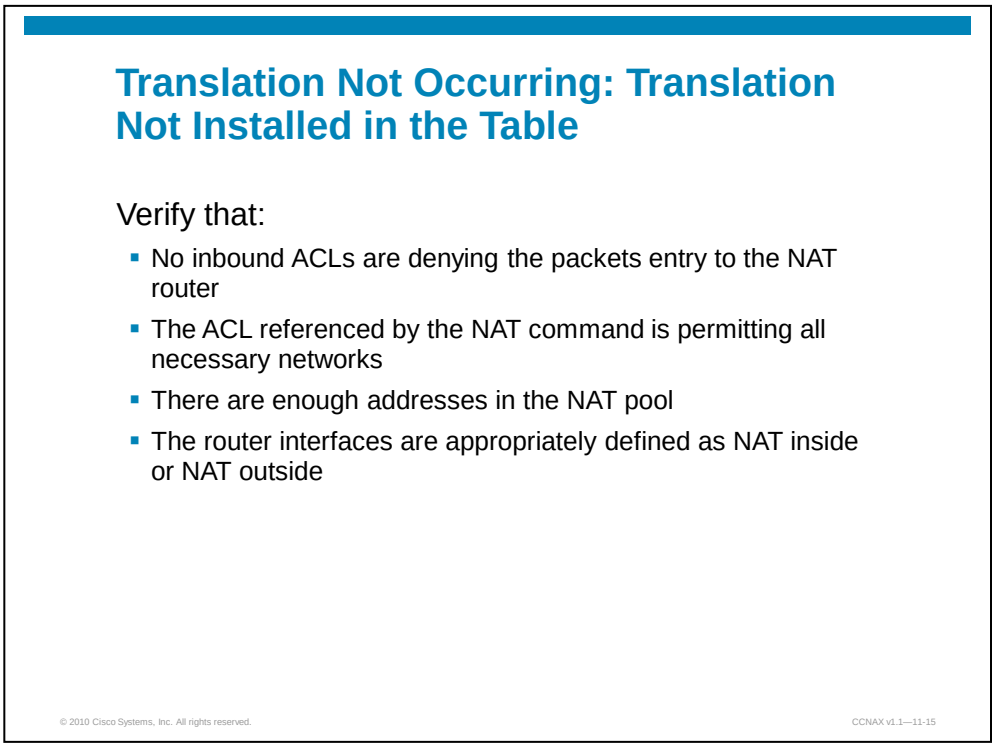
It is sometimes necessary for a network administrator to clear IP NAT translations from the table before they expire, generally for troubleshooting. The graphic shows a series of commands to do this based on the complexity of the translation being cleared. **Clear ip nat translations *** will clear all of them but could cause the administrator to seek other employment because all translations will be cleared including the one being used by the boss.

Copyright ©2014 Global Knowledge Training LLC. All rights reserved.

Troubleshooting NAT/PAT

There are very few commands for verifying and troubleshooting NAT on a Cisco router.

- **Show ip nat statistics** verifies the proper configuration of the inside and outside interfaces and the translation command from inside local to inside global.
- **Show ip nat translations** shows the actual address and port translations that have recently occurred.
- **Show access-list** can be used to verify the ACL defining the inside local block.
- **Debug ip nat** can be used to see the translations occurring in real time.



This graphic provides a list of possibilities to check if no translation is happening at all. This is almost always an error in configuration.

Many times ACLs are used in Cisco devices to filter packets crossing an interface for security and other reasons. Since addresses are being changed now, it is possible to run afoul of one of these filters.

Copyright ©2014 Global Knowledge Training LLC. All rights reserved.

Translation Occurring: Installed Translation Entry but No Connectivity

Verify:

- What the NAT configuration is supposed to accomplish
- That the NAT entry exists in the translation table and that it is accurate
- That the translation is actually taking place by monitoring the NAT process or statistics
- That the NAT router has the appropriate route in the routing table if the packet is going from inside to outside
- That all necessary routers have a return route back to the translated address

© 2010 Cisco Systems, Inc. All rights reserved.

This graphic provides some tips for things to check when the translation is happening but the destination networks are unreachable.

Displaying Information with show and debug Commands

```
RouterX#show ip nat statistics
Total translations: 5 (0 static, 5 dynamic, 5 extended)
Outside Interfaces: Serial0
Inside Interfaces: Ethernet0 , Ethernet1
Hits: 42  Misses: 44
Expired translations: 30
Dynamic mappings:
```

- Monitors the NAT statistics

```
RouterX#debug ip nat

NAT: s=192.168.3.254->209.165.200.225, d=209.165.201.1 [62]
NAT*: s=209.165.201.1, d=209.165.200.225->192.168.3.254 [53]
NAT: s=192.168.3.254->209.165.200.225, d=209.165.201.1 [63]
NAT*: s=209.165.201.1, d=209.165.200.225->192.168.3.254 [54]
NAT: s=192.168.3.254->209.165.200.225, d=209.165.201.1 [64]
NAT*: s=209.165.201.1, d=209.165.200.225->192.168.3.254 [55]
NAT: s=192.168.3.254->209.165.200.225, d=209.165.201.1 [65]
NAT*: s=209.165.201.1, d=209.165.200.225->192.168.3.254 [56]
NAT: s=192.168.3.254->209.165.200.225, d=209.165.201.1 [66]
NAT*: s=209.165.201.1, d=209.165.200.225->192.168.3.254 [57]
```

- Displays information about every packet that is translated by the router

© 2010 Cisco Systems, Inc. All rights reserved.

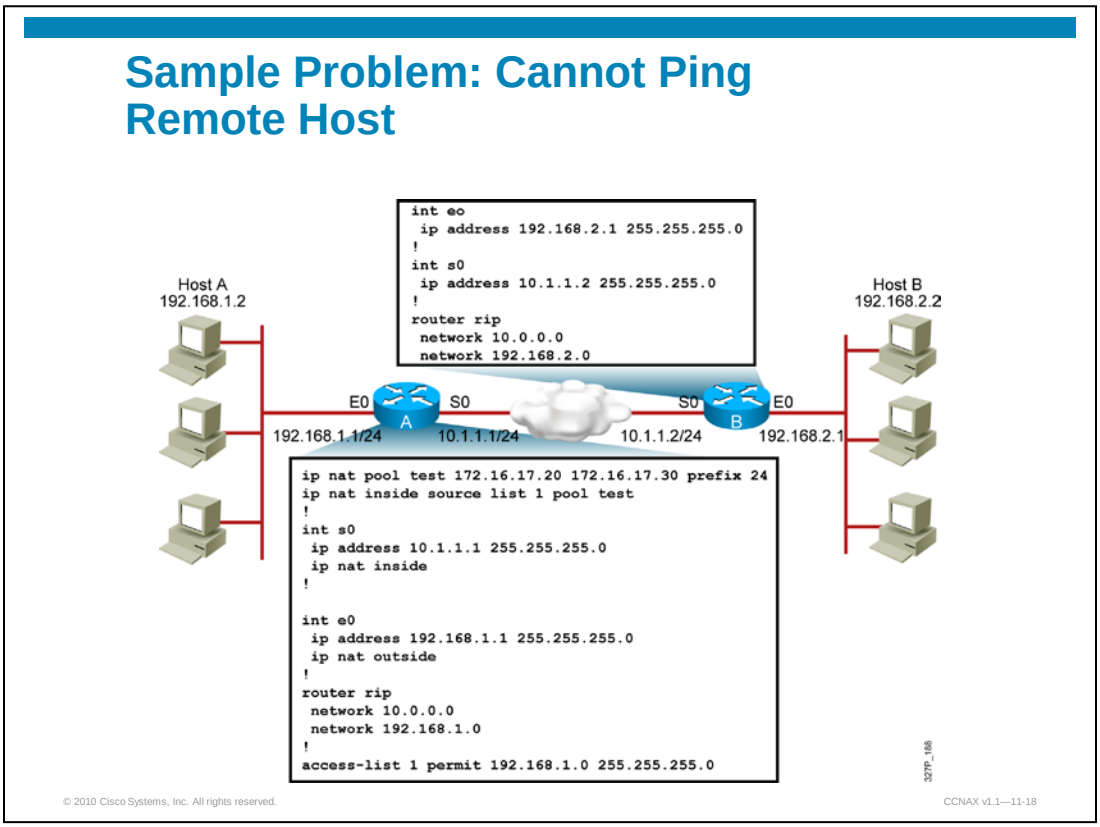
The output of the **show ip nat statistics** command is missing the translation mapping which is an important part of this output.

Copyright ©2014 Global Knowledge Training LLC. All rights reserved.

A careful analysis of the **debug ip nat** output is needed to see the outbound and the inbound translated packets. But, it is required to keep track of inbound vs. outbound.

The indexing numbers in brackets on the right side of the **debug ip nat** output reveal inbound vs. outbound packets. 62, 63, 64… are inbound and 53, 54, 55… are outbound.

Troubleshooting Example

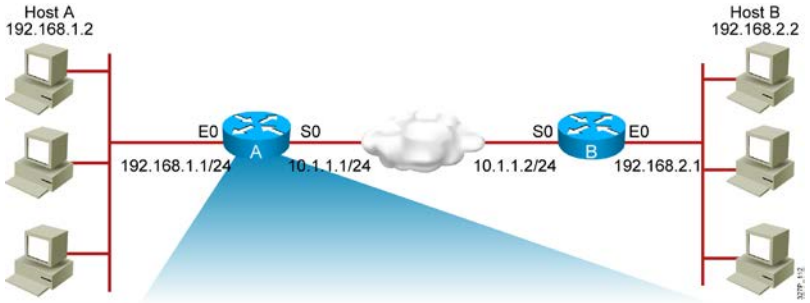


A complete NAT configuration is shown. Unfortunately, no translations or connectivity is happening.

Copyright ©2014 Global Knowledge Training LLC. All rights reserved.

Sample Problem: Cannot Ping Remote Host (Cont.)

- There are no translations in the table.



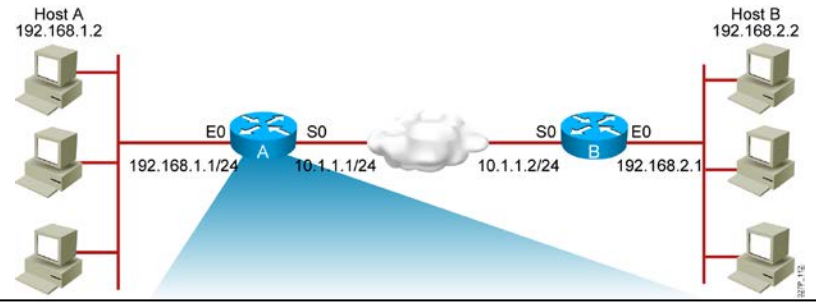

```
RouterA#show ip nat translations
     Pro Inside global   Inside local  Outside local  Outside global
     ---                                ---            ---
     ---                                ---            ---
```

© 2010 Cisco Systems, Inc. All rights reserved.

The command **show ip nat translations** verifies that nothing is happening.

Sample Problem: Cannot Ping Remote Host (Cont.)

- The router interfaces are inappropriately defined as NAT inside and NAT outside.




```
RouterA#show ip nat statistics
      Total active translations: 0 (0 static, 0 dynamic; 0 extended)
      Outside interfaces:
      Ethernet0
      Inside interfaces:
      Serial0
<output omitted>
```

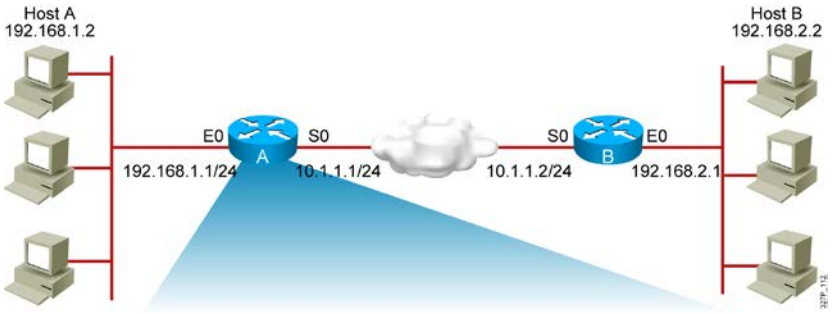
© 2010 Cisco Systems, Inc. All rights reserved.

The **show ip nat statistics** command reveals that the ip nat inside and ip nat outside interfaces are reversed.

Copyright ©2014 Global Knowledge Training LLC. All rights reserved.

Sample Problem: Cannot Ping Remote Host (Cont.)

- Pings are still failing and there are still no translations in the table.
- An incorrect wildcard bit mask in the ACL defines the addresses to be translated.



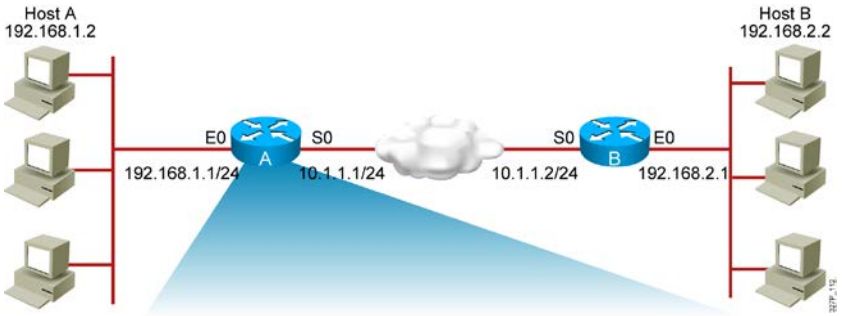

```
RouterA#show access-list

Standard IP access list 20
    10 permit 0.0.0.0, wildcard bits 255.255.255.0
```

© 2010 Cisco Systems, Inc. All rights reserved.

The ACL defining the inside local addresses is misconfigured as shown in the graphic.

Sample Problem: Cannot Ping Remote Host (Cont.)

- Translations are now occurring.
- Pings are still failing.




```
RouterA#show ip nat translations
   Pro Inside global   Inside local    Outside local   Outside global
   ---  172.16.17.20    192.168.1.2         ---             ---
```

© 2010 Cisco Systems, Inc. All rights reserved.

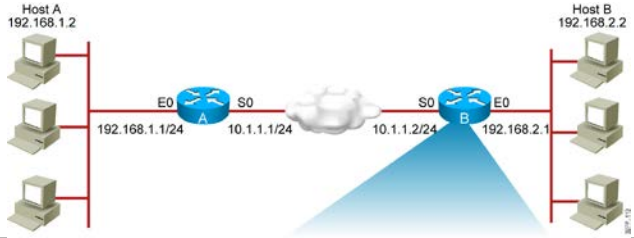
Copyright ©2014 Global Knowledge Training LLC. All rights reserved.

Once those two problems are solved, a translation is occurring but there is no connectivity to the networks on the west side (router B) of the original graphic for the example.

It is important to note that the remaining problem applies to only this example and would not be present if translation is occurring to an ISP. The ISP would be responsible for routing translated packets. In the example, it has to be solved.

Sample Problem: Cannot Ping Remote Host (Cont.)

- Router B has no route to the translated network address of 172.16.0.0.




```
RouterB#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0/24 is directly connected, Serial0
    192.168.2.0/24 is subnetted, 1 subnets
R       192.168.2.0/24 is directly connected, Ethernet0
     192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
R       192.168.1.0/24 [120/1] via 10.1.1.1, 2d19h, Serial0
```

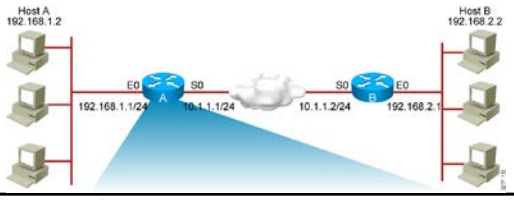
© 2010 Cisco Systems, Inc. All rights reserved.

A check of the routing table on router B verifies that there is no route back to the 172.16.0.0 network.

Copyright ©2014 Global Knowledge Training LLC. All rights reserved.

Sample Problem: Cannot Ping Remote Host (Cont.)

- Router A is advertising the network that is being translated (192.168.1.0), instead of the network address that the router is translating into (172.16.0.0).

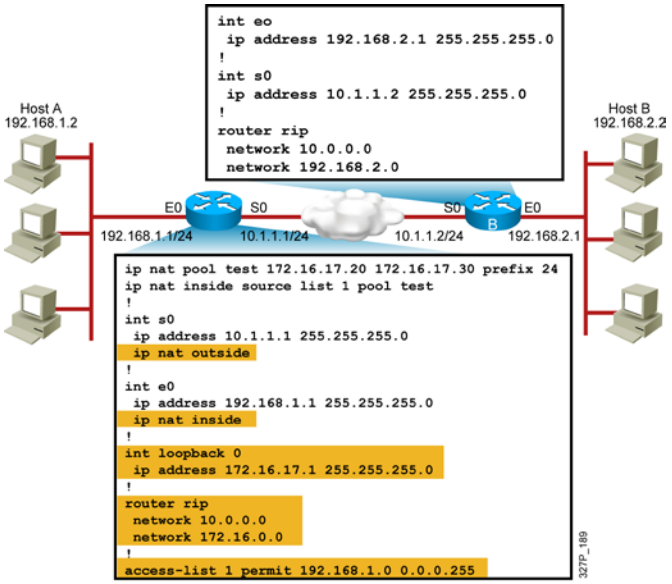



```
RouterA#show ip protocol
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 0 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Default version control: send version 1, receive any version
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    192.168.0.0
    10.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 120)
```

© 2010 Cisco Systems, Inc. All rights reserved.

On Router A, the **show ip protocols** command verifies that there is no network statement for 172.16.0.0 configured. The graphic shows the corrected configuration.

Solution: Corrected Configuration



© 2010 Cisco Systems, Inc. All rights reserved.

Copyright ©2014 Global Knowledge Training LLC. All rights reserved.

Conclusion

There are few (if any) networks in the world that do not implement NAT/PAT for IP version 4. IP version 6 will eliminate a lot of the need for NAT. Even though NAT is usually implemented as a firewalling function, it can be important on Cisco routers as well. From this, it is simple to conclude that understanding, designing, implementing, and troubleshooting NAT is a required skill for network engineers. The topic also appears in the CCNA examination in multiple questions and simulations.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

ICND1 v2.0 - Interconnecting Cisco Networking Devices, Part 1

ICND2 v2.0 - Interconnecting Cisco Networking Devices, Part 2

CCNAX v2.0 - CCNA Routing and Switching Boot Camp

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

Ray Dooley has been a network professional for over 30 years. He is a Global Knowledge Course Director for CCDA, ARCH, SWITCH, ROUTE, TSHOOT, and ICMI. Ray has developed courses for Global Knowledge, Cisco, and General Electric.

Copyright ©2014 Global Knowledge Training LLC. All rights reserved.