

# Network Address Translation Overview

This lesson introduces Network Address Translation, its implementation and its considerations.

---

## Overview

---

### Introduction

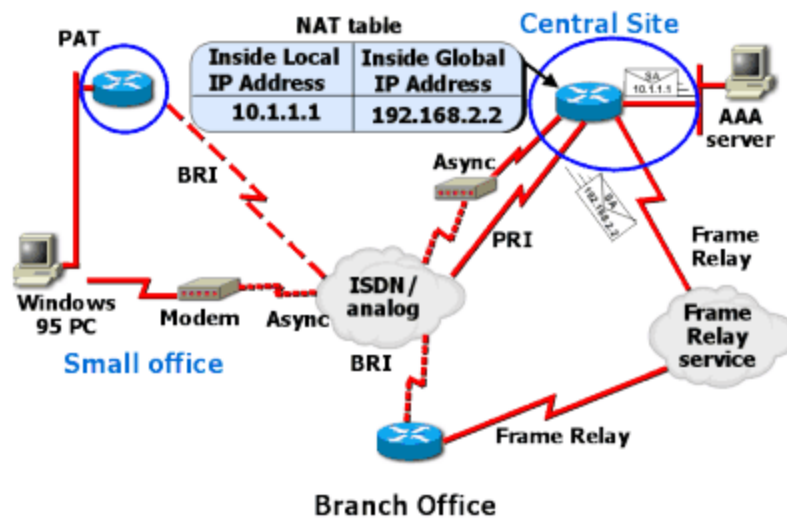
This lesson introduces Network Address Translation, its implementation, and its considerations.

### Objectives

Upon completion of this lesson, you should be able to perform the following tasks:

- ? Describe Network Address Translation.
- ? Define the terminology associated with NAT.
- ? Identify when Network Address Translation should be used.
- ? List considerations to evaluate before implementing NAT.
- ? Identify the Components of NAT Operation.
- ? Explain the operation of NAT.
- ? Describe Address overloading.
- ? Describe the function of TCP load distribution.
- ? Identify how NAT handles overlapping networks.

### Visual Objective



## Outline

This lesson includes the following topics:

- ? Overview
- ? What Is Network Address Translation?
- ? What Are the Components of NAT?
- ? When to Use NAT
- ? Considerations for Implementing NAT
- ? Examining NAT Operation
- ? How Are Inside Local Addresses Translated?
- ? How Are Inside Global Addresses Overloaded?
- ? How Is TCP Load Distributed?
- ? How Are Overlapping Networks Handled?
- ? Summary

---

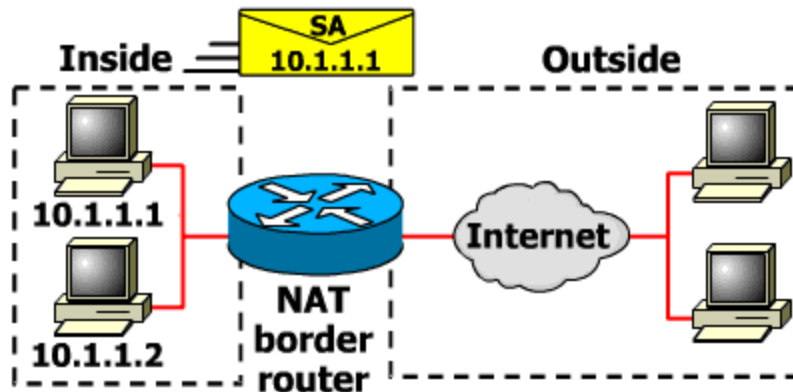
## What Is Network Address Translation?

---

## What Is Network Address Translation?

This section introduces Network Address Translation (NAT) and some of its uses.

### Network Address Translation



IP address depletion is a key problem facing the public network. To maximize the use of your registered IP addresses, Cisco IOS™ Release 11.2 software and subsequent releases implement NAT. This feature, which is Cisco's implementation of RFC 1631, The IP Network Address Translator, is a solution that provides a way to use the same IP addresses in multiple internal subnetworks, thereby reducing the need for registered IP addresses.

## What Are the Two Types of NAT Translations?

The translation performed using NAT can be either static or dynamic and are also used in load sharing.

### Static Translation

Static translation occurs when you specifically configure addresses in a lookup table. A specific inside address maps into a prespecified outside address. The inside and outside addresses are statically mapped one-for-one.

### Dynamic Translations

Dynamic mapping occurs when the NAT border router is configured to understand which inside addresses must be translated, and which pool of addresses may be used for the outside addresses. There can be multiple pools of outside addresses.

Multiple internal hosts can also share a single outside IP address, which conserves address space. Address sharing is accomplished by port multiplexing, or changing the source port on the outbound packet so that replies can be directed back to the appropriate router.

### Load Sharing

For load sharing, you can map outside IP addresses to inside IP addresses using the Transmission Control Protocol (TCP) load distribution feature. Load distribution can

also be accomplished using NAT where one external address maps to this address. Then the round robin between inside machines occurs. In this case, incoming new connections are distributed across several routers. Each connection may involve state information that a given connection must remain on one router.

---

## What Are the Components of NAT?

---

### What Are the Components of NAT?

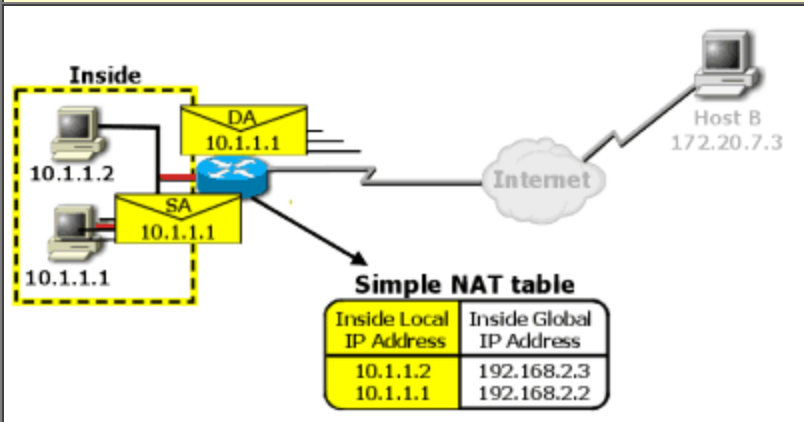
This section identifies the major components of NAT operation.

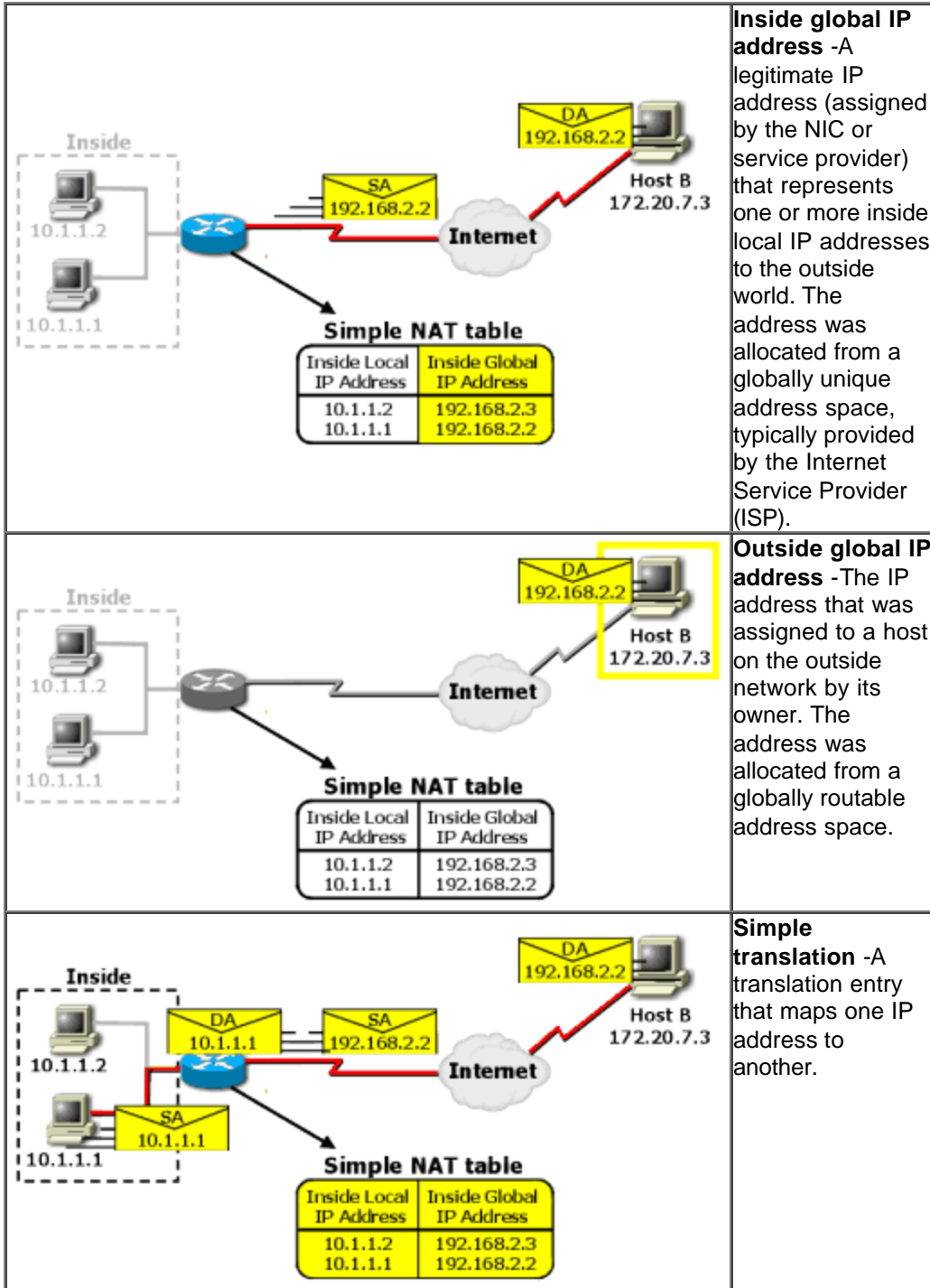
### Where Does NAT Take Place?

The NAT functionality allows privately addressed networks to connect to public networks such as the Internet. The privately addressed "inside" network sends a packet through the NAT router, and the addresses are converted to legal, registered IP addresses, enabling the packets to be passed to the public network such as the Internet. These features were formerly available only through pass-through firewall gateways. This functionality is now available in all Cisco enterprise routers.

### What Are the Major NAT Components?

Cisco's implementation of NAT uses the following terms related to NAT:

Slide Show Images	Text						
 <p>The diagram illustrates a NAT setup. On the left, an 'Inside' network is enclosed in a dashed yellow box. It contains two hosts: one with IP 10.1.1.2 and another with IP 10.1.1.1. A central router has two interfaces: 'DA' (Destination Address) with IP 10.1.1.1 and 'SA' (Source Address) with IP 10.1.1.1. The router is connected to an 'Internet' cloud, which contains 'Host B' with IP 172.20.7.3. Below the router is a 'Simple NAT table' with the following entries:</p> <table border="1" data-bbox="617 1480 901 1591"> <thead> <tr> <th>Inside Local IP Address</th> <th>Inside Global IP Address</th> </tr> </thead> <tbody> <tr> <td>10.1.1.2</td> <td>192.168.2.3</td> </tr> <tr> <td>10.1.1.1</td> <td>192.168.2.2</td> </tr> </tbody> </table>	Inside Local IP Address	Inside Global IP Address	10.1.1.2	192.168.2.3	10.1.1.1	192.168.2.2	<p><b>Inside local IP address</b> -The IP address assigned to a host on the inside network. The address was globally unique but obsolete, allocated from RFC 1918, Address Allocation for Private Internet Space, or randomly picked.</p>
Inside Local IP Address	Inside Global IP Address						
10.1.1.2	192.168.2.3						
10.1.1.1	192.168.2.2						



**Inside global IP address** -A legitimate IP address (assigned by the NIC or service provider) that represents one or more inside local IP addresses to the outside world. The address was allocated from a globally unique address space, typically provided by the Internet Service Provider (ISP).

**Outside global IP address** -The IP address that was assigned to a host on the outside network by its owner. The address was allocated from a globally routable address space.

**Simple translation** -A translation entry that maps one IP address to another.

[View](#) Summary of terms related to NAT.



Descriptions for outside local IP address and extended translation

Descriptions for outside local IP address and extended translation entry are not represented graphically.

## How Does Easy IP Relate to NAT?

Easy IP is a related feature to NAT available on Cisco routers. Configuring Easy IP is not taught in this course. The Easy IP (Phase 1) feature combines NAT and Point-to-point (PPP)/Internet Protocol Control Protocol (IPCP). This feature enables a Cisco router to automatically negotiate its own registered WAN interface IP address from a central server and enable all remote hosts to access the global Internet using this single registered IP address.

Because Easy IP (Phase 1) uses existing port-level multiplexed NAT functionality within the Cisco IOS software, IP addresses on the remote LAN are invisible to the Internet.



Note

For a complete description of the Easy IP configuration commands, refer to the “Easy IP Commands” chapter in the Dial Solutions Command Reference.

## NAT Components

---

---

## When to Use NAT

---

### When to Use NAT

This section examines when to utilize NAT.

### When Should NAT Be Utilized?

Use NAT if:

- ? You need to connect to the Internet and your hosts do not have globally unique

IP addresses.

- ? You change over to a new ISP that requires you to renumber your network.
- ? Two intranets with duplicate addresses merge.
- ? You want to support basic load sharing.

## How Is NAT Used to Solve IP Addressing Issues?

NAT technology enables private IP internetworks that use nonregistered IP addresses to connect to the public network such as the Internet. A NAT router is placed on the border of a stub domain (inside network) and a public network (outside network), and translates the internal local addresses into globally unique IP addresses before sending packets to the outside network.

NAT takes advantage of the fact that relatively few hosts in a stub domain communicate outside of the domain at any given time. Therefore, only a subset of the IP addresses in a stub domain must be translated into globally unique IP addresses for outside communication.

## What Are the Advantages of NAT?

If your internal addresses must change because you have changed service providers or two intranets merged (two companies merged, for example), NAT can be used to translate the appropriate addresses. NAT enables you to change addresses incrementally, without changes to hosts or routers other than those bordering stub domains, thereby eliminating duplicate address ranges without readdressing host computers.

## How Does NAT Use Load Sharing?

For load sharing, you can map outside IP addresses to inside IP addresses using the Transmission Control Protocol (TCP) load distribution feature. Load distribution can also be accomplished using NAT where one external address maps to this address. Then the round robin between inside machines occurs. In this case, incoming new connections are distributed across several routers. Each connection may involve state information that a given connection must remain on one router.

## Examples of Using NAT

Examples when NAT may be employed include two companies that have duplicate internal addressing schemes merge, or a company changes its Internet Service Provider (ISP) but does not want to change its internal address scheme.

---

# Considerations for Implementing NAT

---

## Considerations for Implementing NAT

This section introduces the advantages and disadvantages of NAT.

## NAT Implementation Considerations

The following table allows you to see the advantages and disadvantages of NAT.

Advantages	Disadvantages
Conserves legally registered addresses	Translation introduces switching path delays
Reduces address overlap occurrence	Loss of end-to-end IP traceability
Increases flexibility when connecting to Internet	Certain applications will not function with NAT enabled
Eliminates address renumbering as network changes	

## NAT Advantages

Before implementing NAT, you should evaluate the following considerations. Typical NAT advantages follow:

- ? NAT conserves the legally registered addressing scheme by allowing privatization of intranets, yet allows legal addressing scheme pools to be set up to gain access to the Internet.
- ? NAT also reduces the instances in which addressing schemes overlap. If a scheme was originally set up within a private network, then the network was connected to the public network (which may use the same addressing scheme) without address translation, the potential for overlap exists globally.
- ? NAT increases the flexibility of connection to the public network. Multiple pools, backup pools, and load sharing/balancing pools can be implemented to help ensure reliable public network connections. Network design is also simplified as planners have more flexibility when creating an address plan.
- ? Deprivatization of a network requires renumbering of the existing network; the costs can be associated to the number of hosts that require conversion to the new addressing scheme. NAT allows the existing scheme to remain, and still supports the new assigned addressing scheme outside the private network.

## NAT Disadvantages

Typical NAT disadvantages follow:

- ? NAT increases delay. Switching path delays, of course, are introduced because of the translation of each IP address within the packet headers. Performance may be a consideration because NAT is currently done using process switching. The CPU must look at every packet to decide if it has to translate it, and then alter the IP header and possibly the TCP header. It is not likely that this process will be easily cacheable.



- ? One significant disadvantage when implementing and using NAT is the loss of end-to-end IP trace ability. It becomes much harder to trace packets that undergo numerous packet address changes over multiple NAT hops. This scenario does, however, lead to more secure links because hackers who want to determine a packet's source will find it difficult, if not impossible to trace or obtain the origination source or destination address.
- ? NAT also forces some applications that use IP addressing to stop functioning because it hides end-to-end IP addresses. Applications that use physical addresses instead of a qualified domain name will not reach destinations that are translated across the NAT router. Sometimes this problem can be avoided by implementing static NAT mappings.

---

## Examining NAT Operation

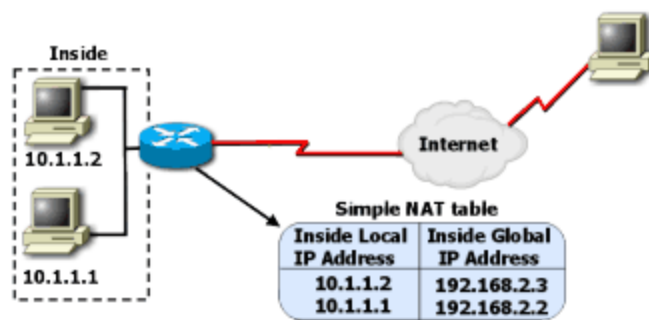
---

### Examining NAT Operation

This section introduces the major functions of NAT.

#### What Are the Components of NAT?

- ? Translating inside local addresses
- ? Overloading inside global addresses
- ? TCP load distribution
- ? Handling overlapping networks



#### Translating Inside Local Addresses

Establishes a mapping between inside local and global addresses.

#### Overloading Inside Global Addresses

You can conserve addresses in the inside global address pool by allowing source ports in TCP connections or User Datagram Protocol (UDP) conversations to be translated. When different inside local addresses map to the same inside global address, each inside host's TCP or UDP port numbers are used to distinguish between them.

#### TCP Load Distribution

A dynamic form of destination translation can be configured for some outside-to-inside traffic. When a mapping scheme is established, destination addresses matching an access list are replaced with an address from a rotary pool. Allocation is done on a round-robin basis, and only when a new connection is opened from the outside to the inside. All non-TCP traffic is passed untranslated (unless other translations are in effect).

## Handling Overlapping Networks

NAT can be used to resolve addressing issues that arise when inside addresses overlap with addresses in the outside network. This can occur when two companies merge, both with duplicate addresses in the networks. It can also occur if you switch ISPs and the address you were assigned by your old ISP has been reassigned to another client.

## NAT Functions

---

---

## How Are Inside Local Addresses Translated?

---

### How Are Inside Local Addresses Translated?

This section explains how inside local address translation works.

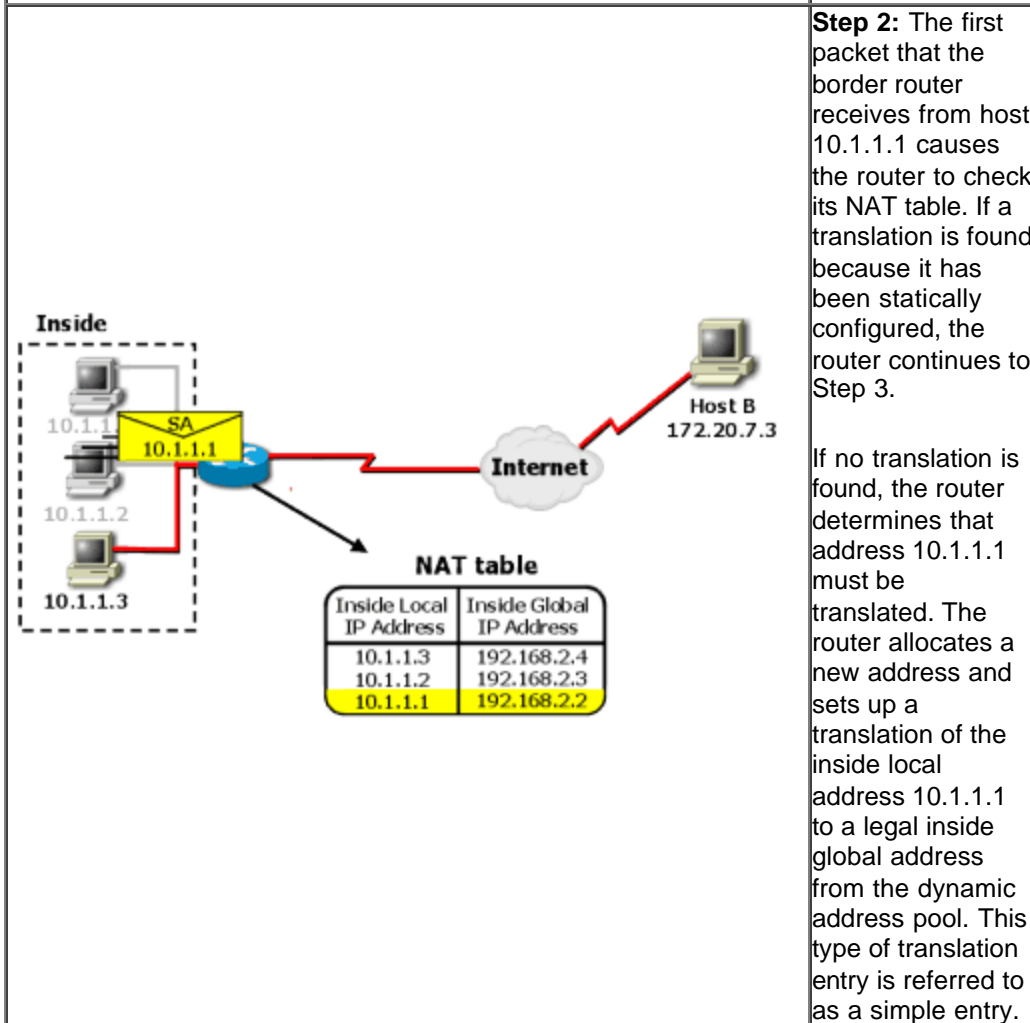
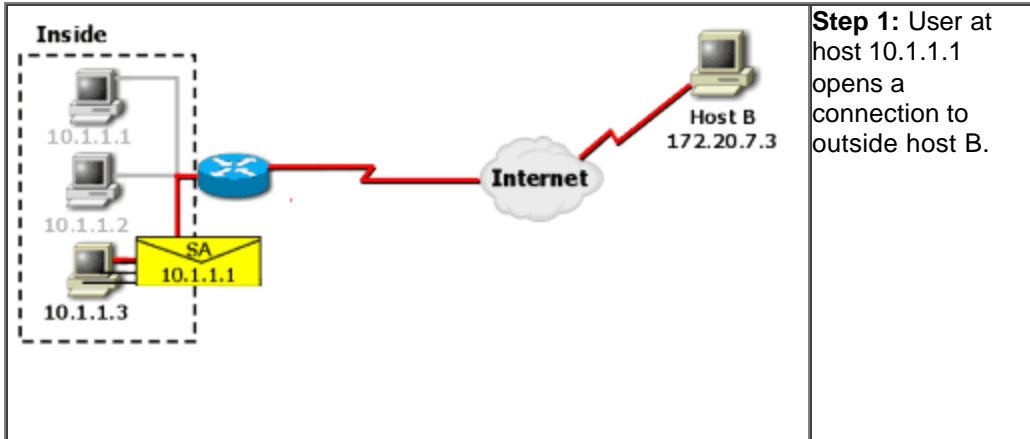
### How Does Inside Address Translation Operate?

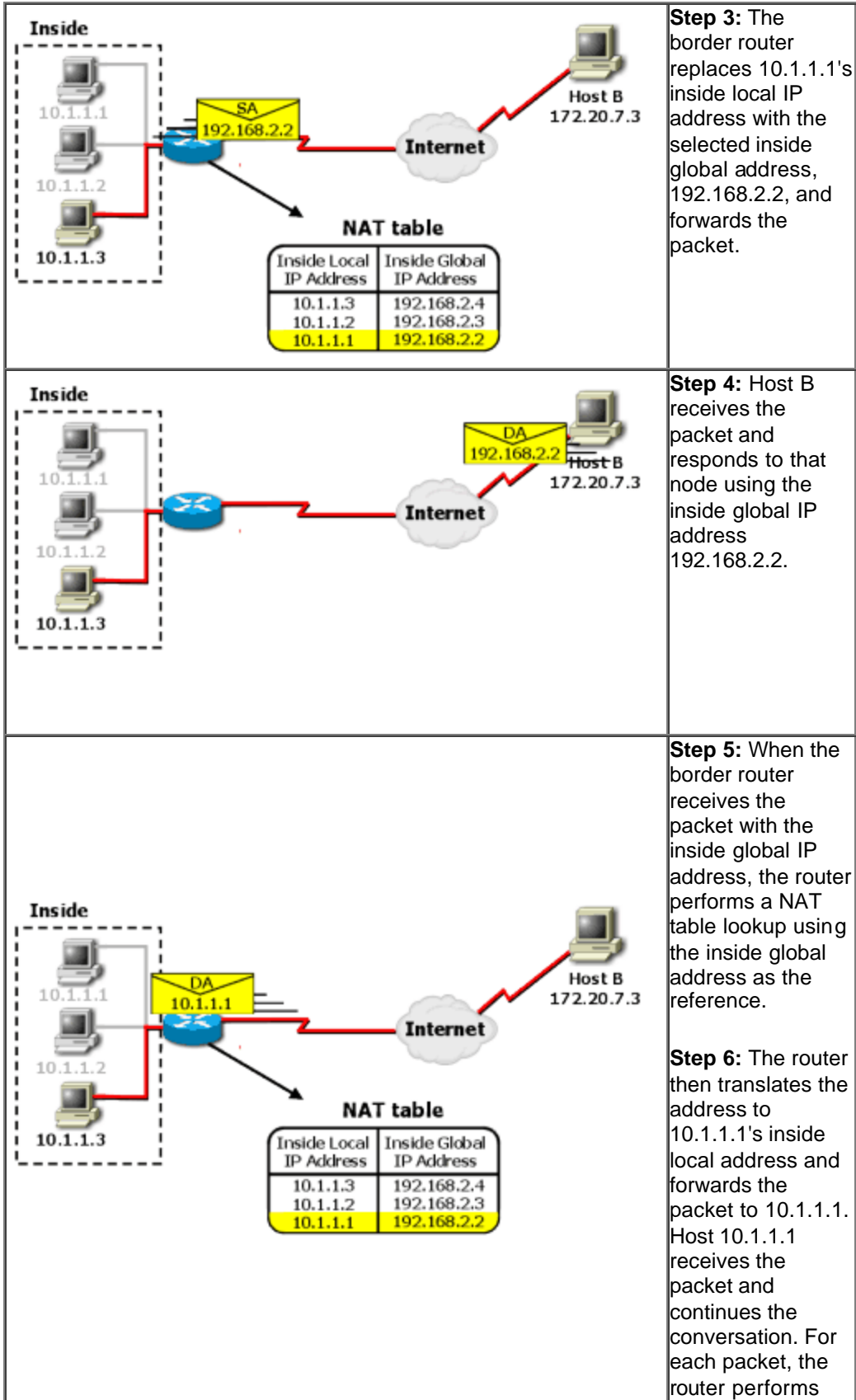
This slideshow illustrates NAT operation when it is used to translate addresses from inside your network to destinations outside of your network. To view this process as a printer-friendly table, click [here](#).

SLIDESHOW Preview!

MediaWidth = 400, MediaHeight = 220, TextWidth = 500, TextHeight = 100,  
AutoPlayMode = 0, AutoPlayDelay= 5000, In\_numImages = 5,

<b>Slide Show Images</b>	<b>Text</b>
--------------------------	-------------





Step 2 through Step 5.



Note

You are able to use either static NAT configuration or dynamic NAT configuration.

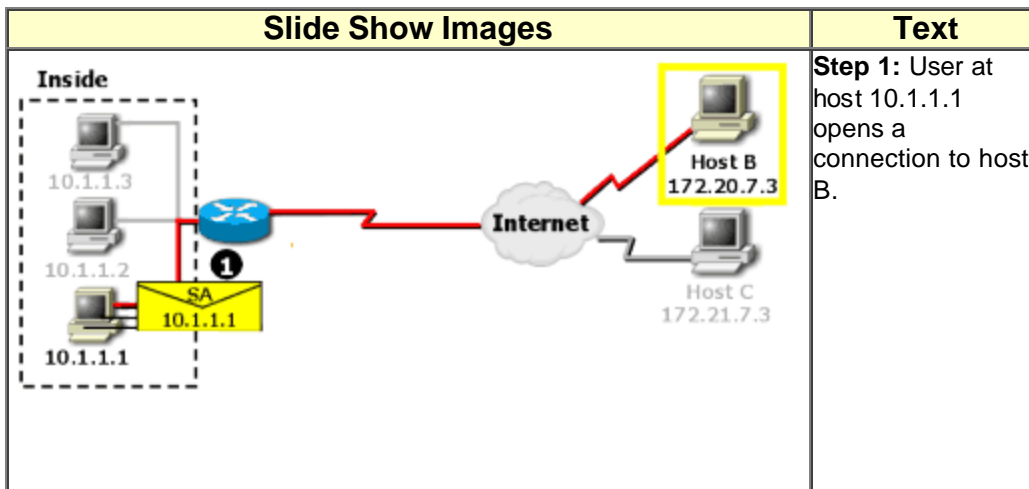
## How Are Inside Global Addresses Overloaded?

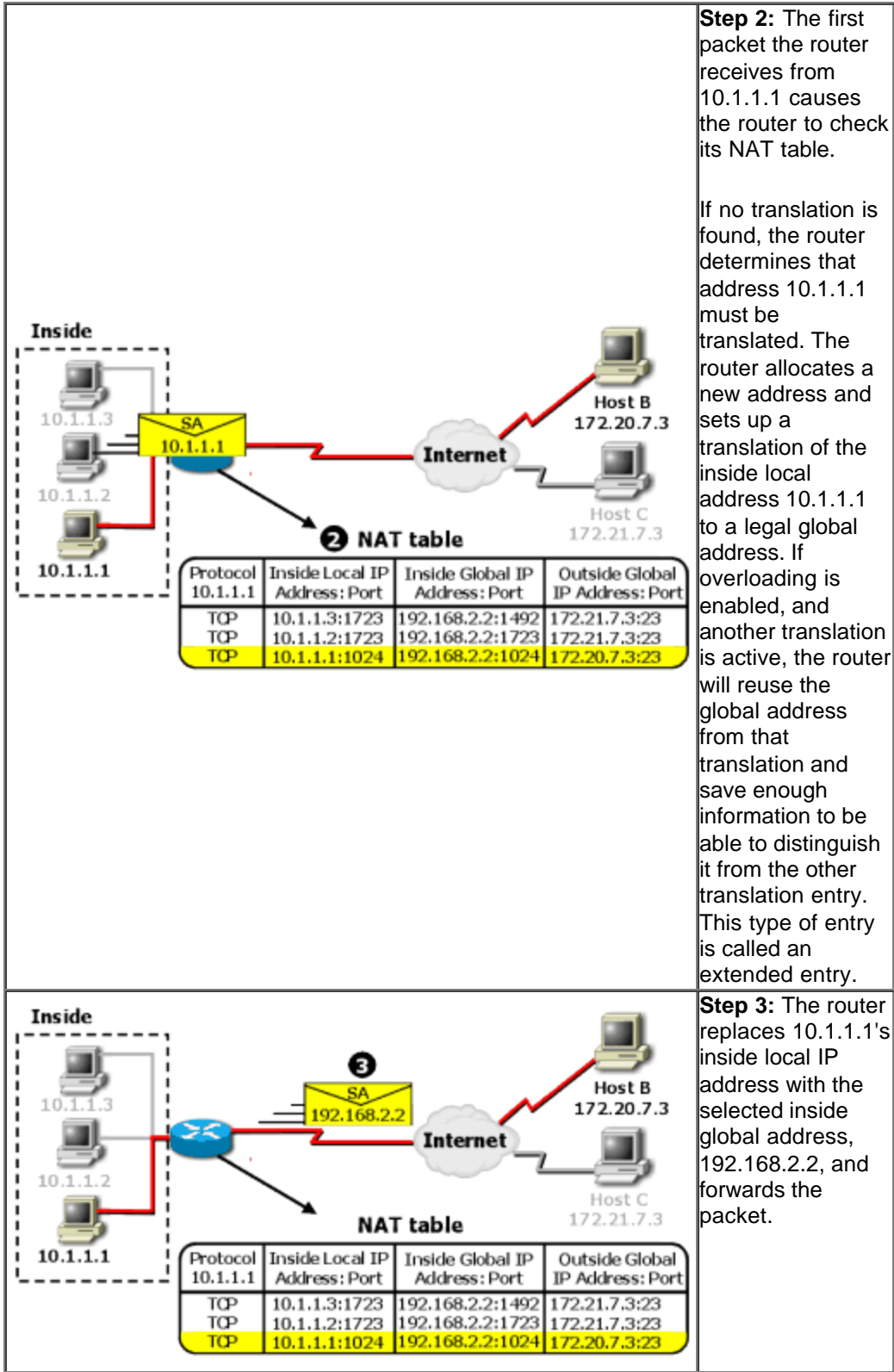
### How Are Inside Global Addresses Overloaded?

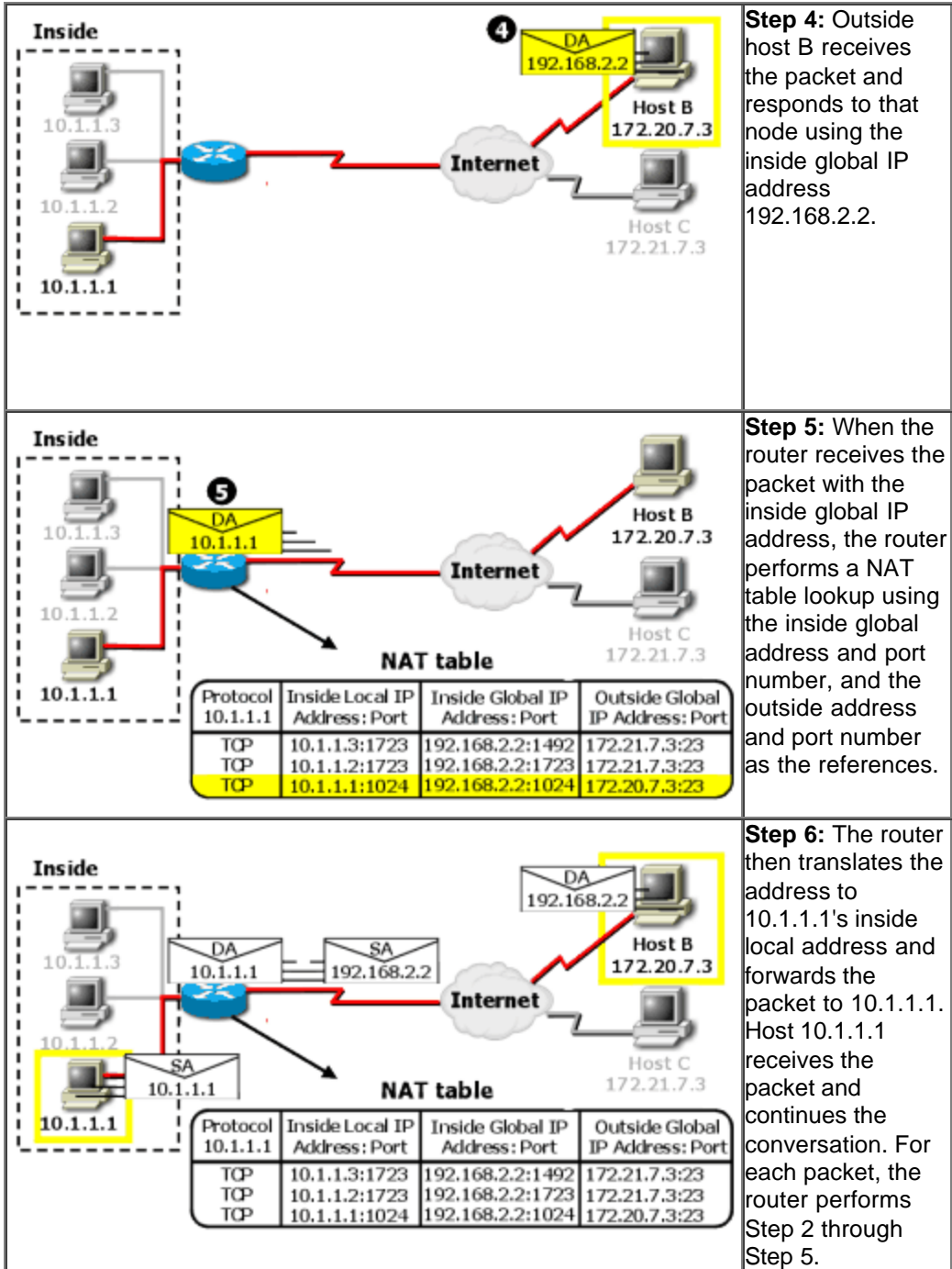
This section explains how overloading inside global addresses operates.

### How Does Global Address Overloading Operate?

This figure illustrates NAT operation when a single inside global address can be used to represent multiple inside local addresses simultaneously. In this example, an extended translation entry table is used. In the table, the combination of address and port makes each global IP address unique. The use of ports to make an address unique is actually Port Address Translation (PAT), a subset of NAT.







## Global Address Overloading Operation Summary

This following table illustrates NAT operation when a single inside global address can be used to represent multiple inside local addresses simultaneously. In this example, an extended translation entry table is used. In the table, the combination of address and port makes each global IP address unique. The use of ports to make an address unique is actually Port Address Translation (PAT), a subset of NAT.

Step	Action	Results and Notes
------	--------	-------------------

1.	User at host 10.1.1.1 opens a connection to host B.	The connection between hosts is made.
2.	The first packet the router receives from 10.1.1.1 causes the router to check its NAT table. If no translation is found, the router determines that address 10.1.1.1 must be translated.  The router allocates a new address and sets up a translation of the inside local address 10.1.1.1 to a legal global address. If overloading is enabled, and another translation is active, the router will reuse the global address from that translation and save enough information to be able to distinguish it from the other translation entry. This type of entry is called an extended entry.	The packet is received by the router to check the NAT Table.
3.	The router replaces 10.1.1.1's inside local IP address with the selected inside global address, 192.168.2.2, and forwards the packet.	Once the translation has been found the package is sent on to its intended receiver.
4.	Outside host B receives the packet and responds to that node using the inside global IP address 192.168.2.2.	The host receives the packet and responds to that node by using the global IP address.
5.	When the router receives the packet with the inside global IP address, the router performs a NAT table lookup using the inside global address and port number, and the outside address and port number as the references.	When the router receives the inside global IP address, the router performs another NAT table lookup using the the inside global address and port number, and the outside address and port number as the reference.
6.	The router then translates the address to 10.1.1.1's inside local address and forwards the packet to 10.1.1.1. Host 10.1.1.1 receives the packet and continues the conversation. For each packet, the router performs Step 2 through Step 5.	The router then translates the address inside the local address and forwards the packet. The host receives the packet continues the conversation.



Note

Overloading inside global address translation is Port Address Translation (PAT). How to configure PAT on a Cisco 700 series router is described later in this chapter.

---

## How Are Overlapping Networks Handled?



---

## How Are Overlapping Networks Handled?

This section describes NAT operation when addresses in the inside network overlap with address that are in the outside network.

### Overlapping Network Operation



**Note**

For each packet sent between 10.1.1.1 and host C, the router does a lookup, replaces the destination address with the inside local address, and replaces the source address with the outside local address.

### Overlapping Network Operation Summary

The table below list the steps of Overlapping Network Operation.

Step	Action	Results and Notes
1.	User at 10.1.1.1 opens a connection to host C (10.1.1.3), and 10.1.1.1 does a name-to-address lookup to a Domain Name System (DNS) server.	User opens a connection and does a name-to-address lookup to a DNS server.
2.	The router sets up a translation that maps the inside local address and inside global address.	The router maps the inside local address and inside global address.
3.	The packet continues to the DNS server.	The packet continues to the DNS server.
4.	The DNS server does a name-to-address lookup.	The DNS server does a name-to-address lookup.
5.	The router intercepts the DNS reply and translates the returned address if there is an overlap. In this case, 10.1.1.3 overlaps with an inside address. To translate the return address of host C, the router creates a simple translation entry that maps the overlapping address 10.1.1.3 to an address from a separately configured outside local address pool. In this example, the address is 193.3.3.3.	The router intercepts the DNS reply and translates the returned address if there is no overlap.
6.	The router then forwards the DNS reply to 10.1.1.1. The reply has host C's address as 193.3.3.3.	The router then forwards the DNS reply.
7.	10.1.1.1 opens a connection to 193.3.3.3.	The host opens a connection.

8.	When the router receives the packet for host C, the router sets up a translation that maps the inside local address, and the global, outside global, and local addresses. The router replaces the source address of 10.1.1.1 with the inside global address 192.2.2.2, and replaces the destination address of 193.3.3.3 with host C's outside global address 10.1.1.3.	When the router receives the packet for the host, the router sets up a translation that maps the inside local address, and the global, outside global, and local addresses.
9.	Host C receives a packet and continues the conversation.	The host receives the packet and continues the conversation.

x

## How Is TCP Load Distributed?

### How Is TCP Load Distributed?

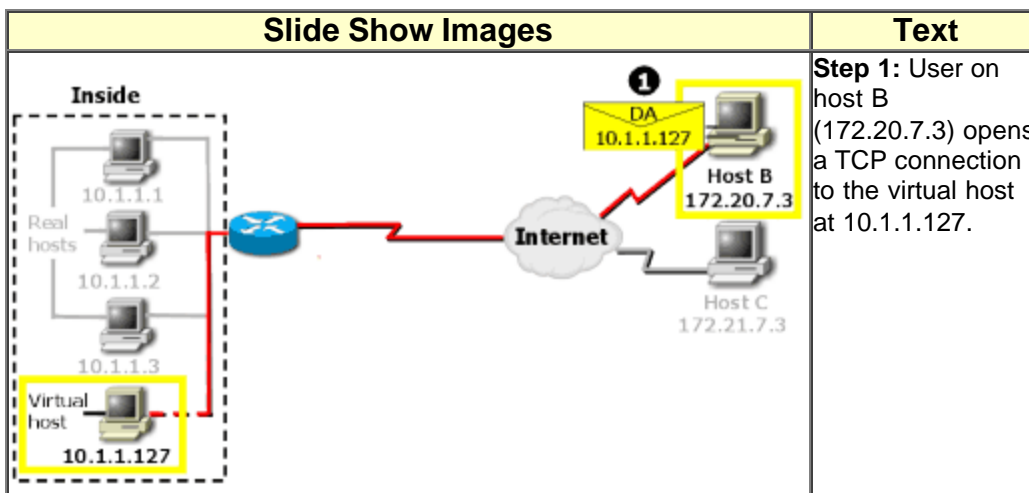
This section describes TCP load distribution operation.

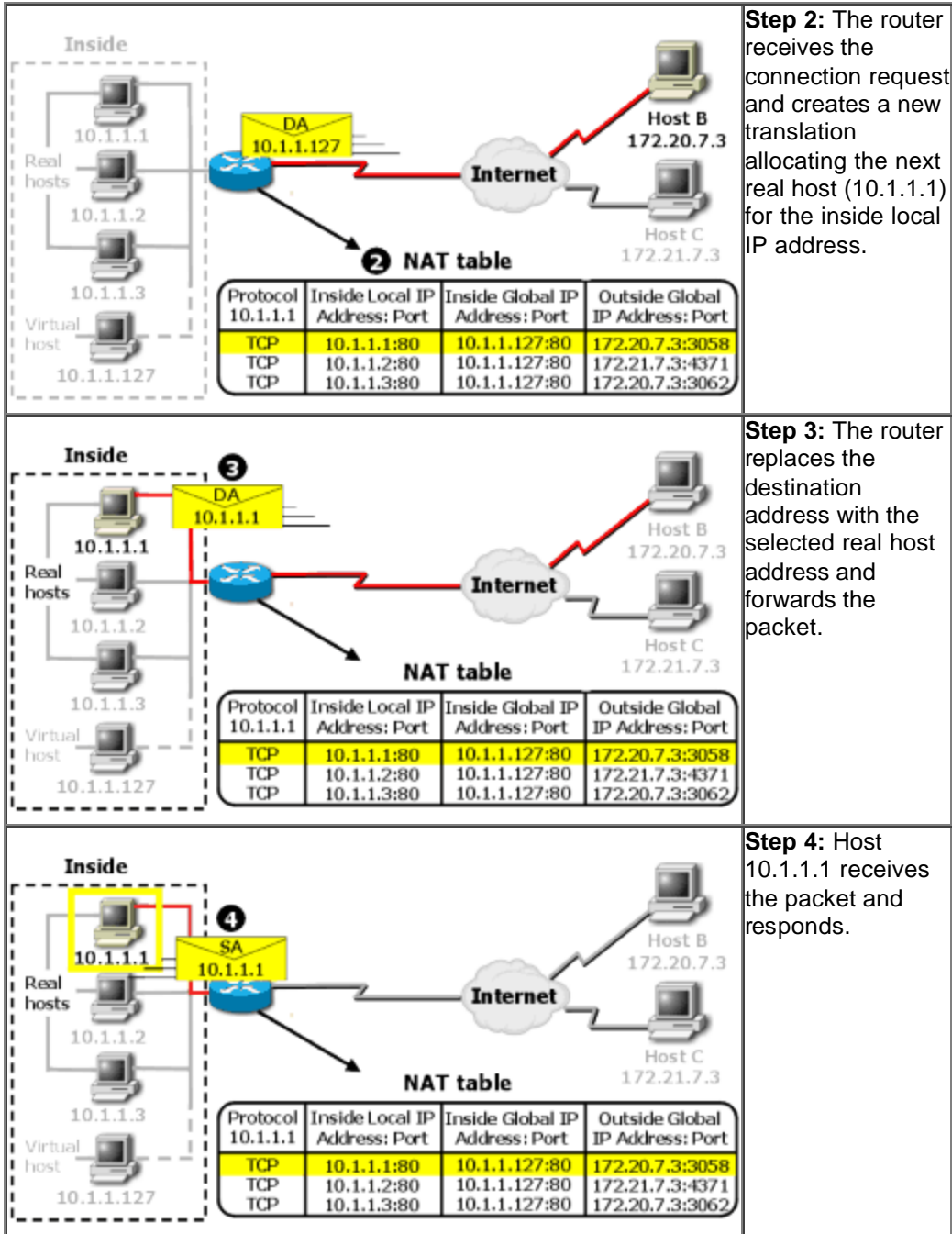
### When Is TCP Load Distribution Used?

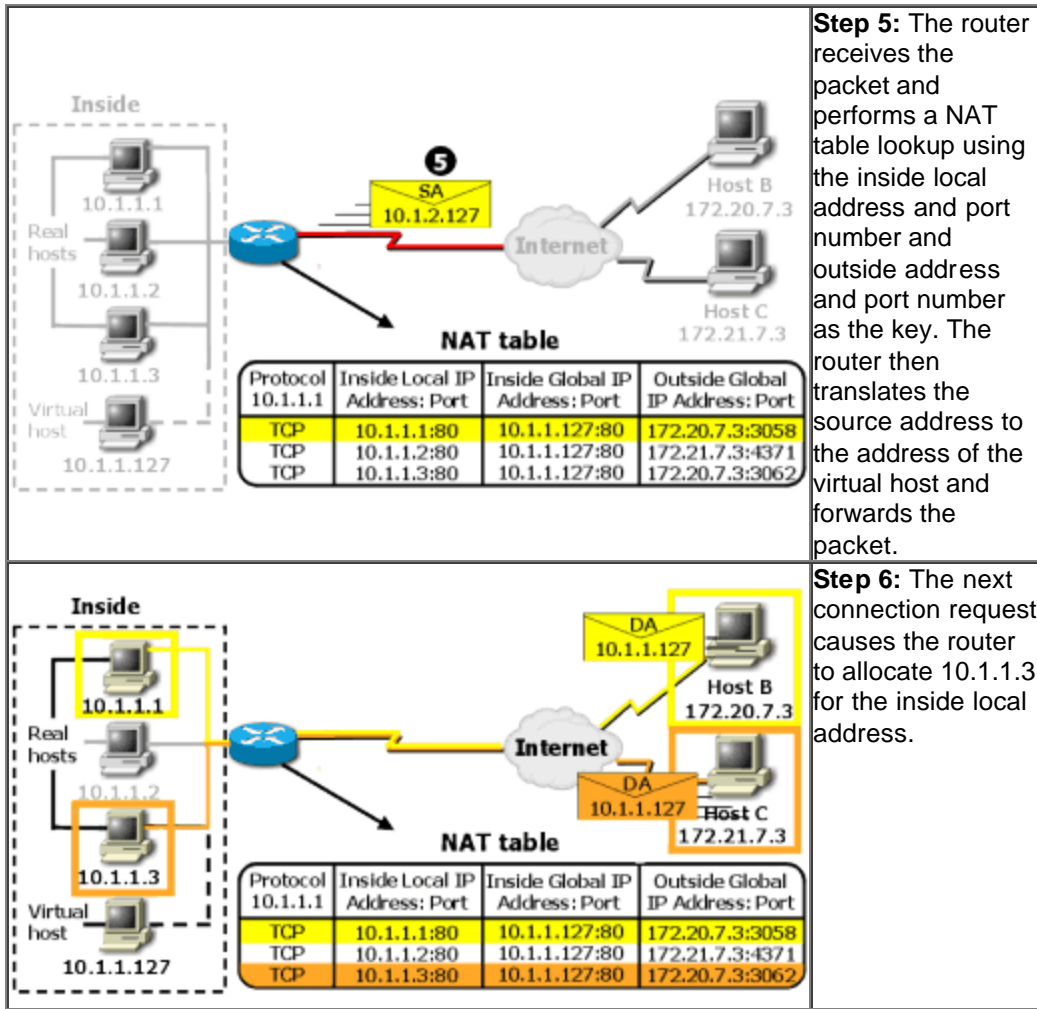
Load distribution is used when multiple inside stations have mirrored resources, requiring a unique virtual addressing scheme.

### How Does TCP Load Distribution Operate?

The figure illustrates NAT operation when NAT is used to map one virtual host to several real hosts.







### TCP Load Distribution Summary

The table illustrates NAT operation when NAT is used to map one virtual host to several real hosts.

Step	Action	Results and Notes
1.	User on host B (172.20.7.3) opens a TCP connection to the virtual host at 10.1.1.127.	User opens a TCP connection to a virtual host.
2.	The router receives the connection request and creates a new translation allocating the next real host (10.1.1.1) for the inside local IP address.	Router receives a connection request and creates a new translation allocating the next real host for inside local IP address.
3.	The router replaces the destination address with the selected real host address and forwards the packet.	The router replaces the destination address with the selected real host address and forward the

		packet.
<b>4.</b>	Host 10.1.1.1 receives the packet and responds.	The host receives the packet and responds.
<b>5.</b>	The router receives the packet and performs a NAT table lookup using the inside local address and port number and outside address and port number as the key. The router then translates the source address to the address of the virtual host and forwards the packet.	The router receives the packet and performs a NAT table lookup using the inside local address and port number and outside address and port number as the key. The router translates the source address to the virtual host and forwards the packet.
<b>6.</b>	The next connection request causes the router to allocate 10.1.1.2 for the inside local address.	The next connection request causes the router to allocate a real host of the inside local address.