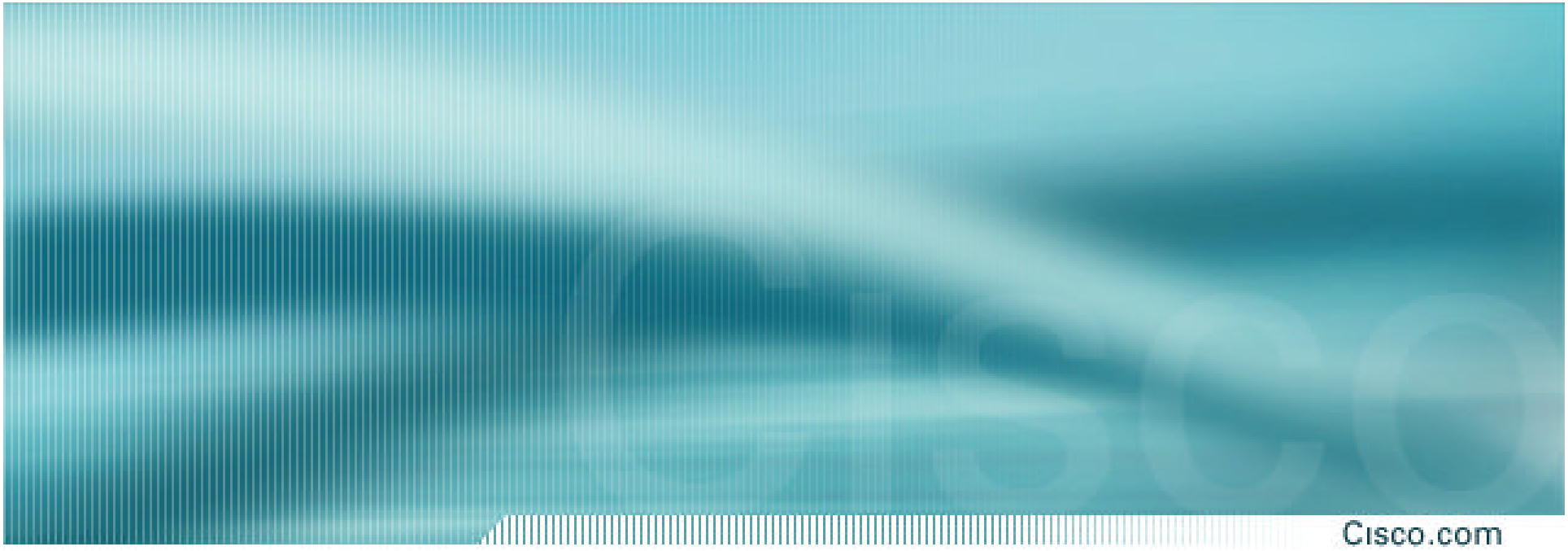

Cisco Systems



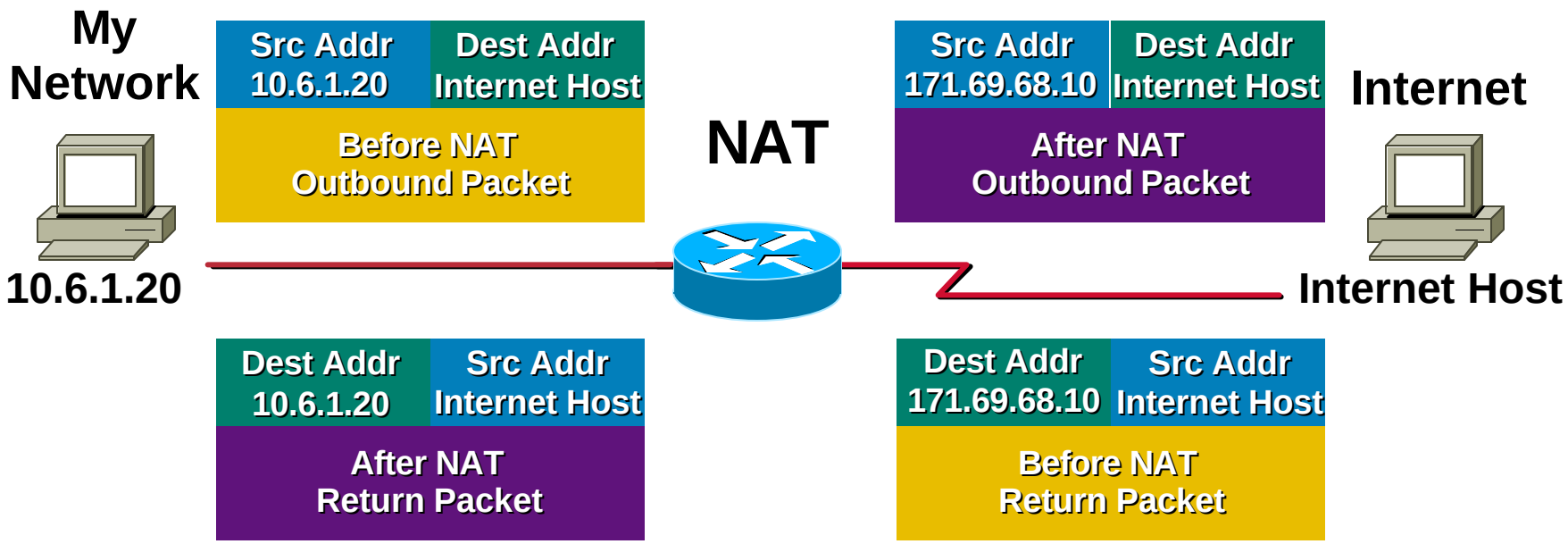
Introduction to Network Address Translation

Session IPS-120

Agenda

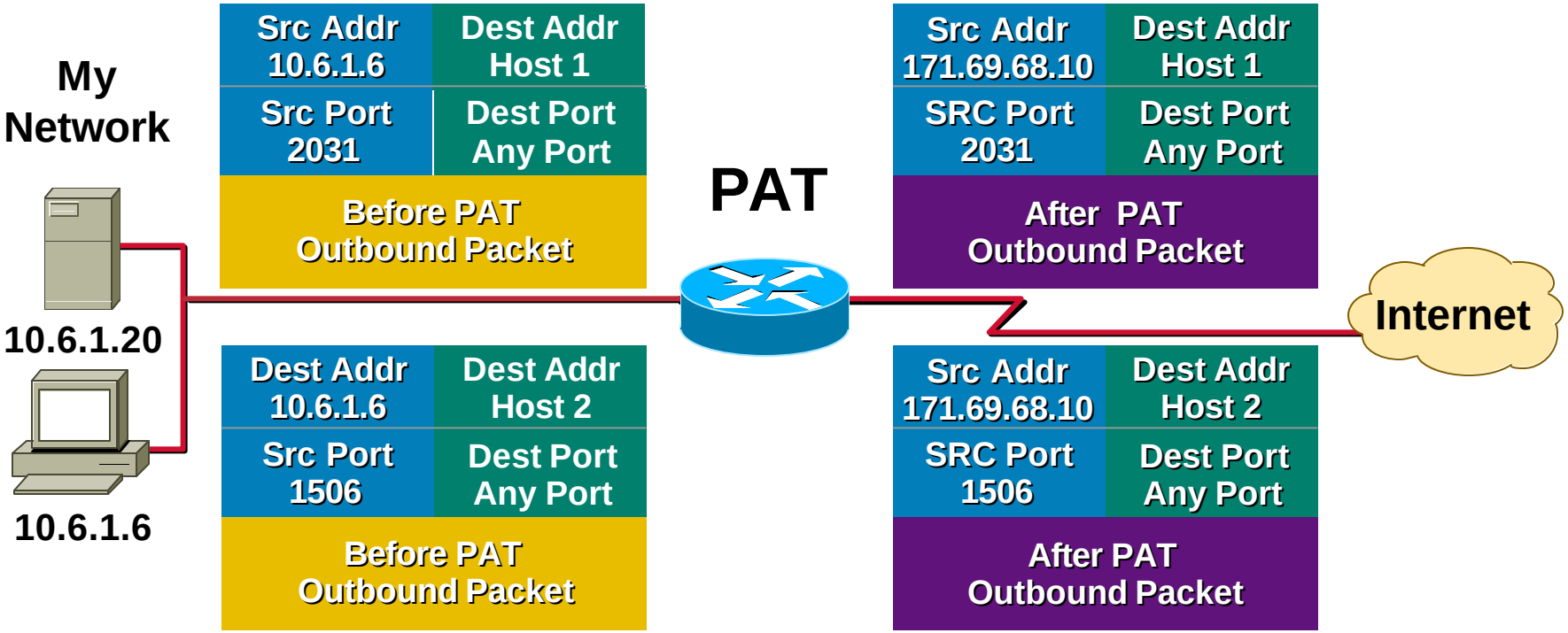
- **Basic Concept of**
  - **Network Address Translation (NAT)**
  - **Port Address Translation (PAT)**
- **Definition, Benefits, Availability and Application Support**
- **NAT Concepts and Terminology**
- **Port Address Translation (PAT)**
- **NAT Technical Information**

Basic Concept of NAT



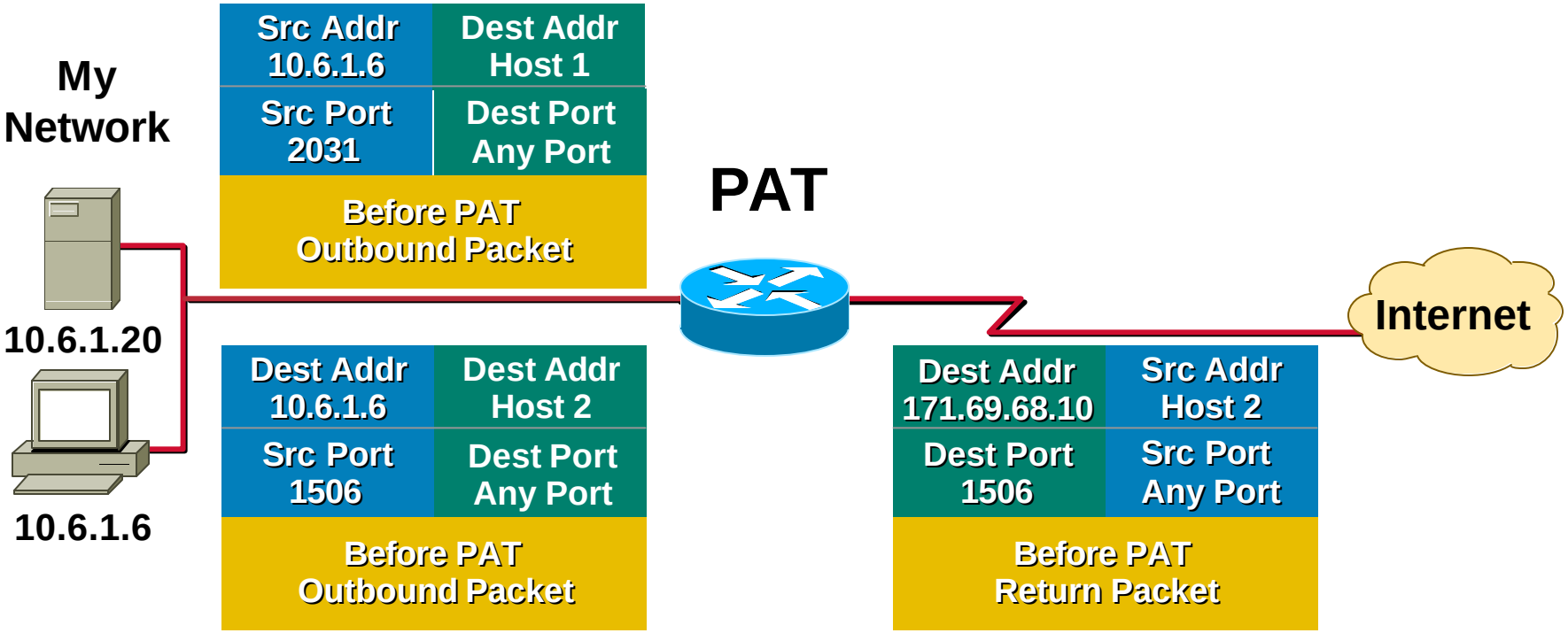
- **NAT changes the IP addresses in the IP header**

Basic Concept of PAT



- **Port Address Translation (PAT) extends NAT from "one-to-one" to "many-to-one" by associating the source port with each flow**

Basic Concept of PAT



- **Port Address Translation (PAT) extends NAT from "one-to-one" to "many-to-one" by associating the source port with each flow**

Agenda

- Basic Concept of NAT and PAT
- Definition, Benefits, Availability and Application Support
- NAT Concepts and Terminology
- PAT
- NAT Technical Information

NAT Defined

- First described in RFC 1631
- Changes source and/or destination IP addresses in IP header and the IP addresses in application data streams
- Cisco IOS® NAT is superset of that described in RFC 1631

Private IP Addresses

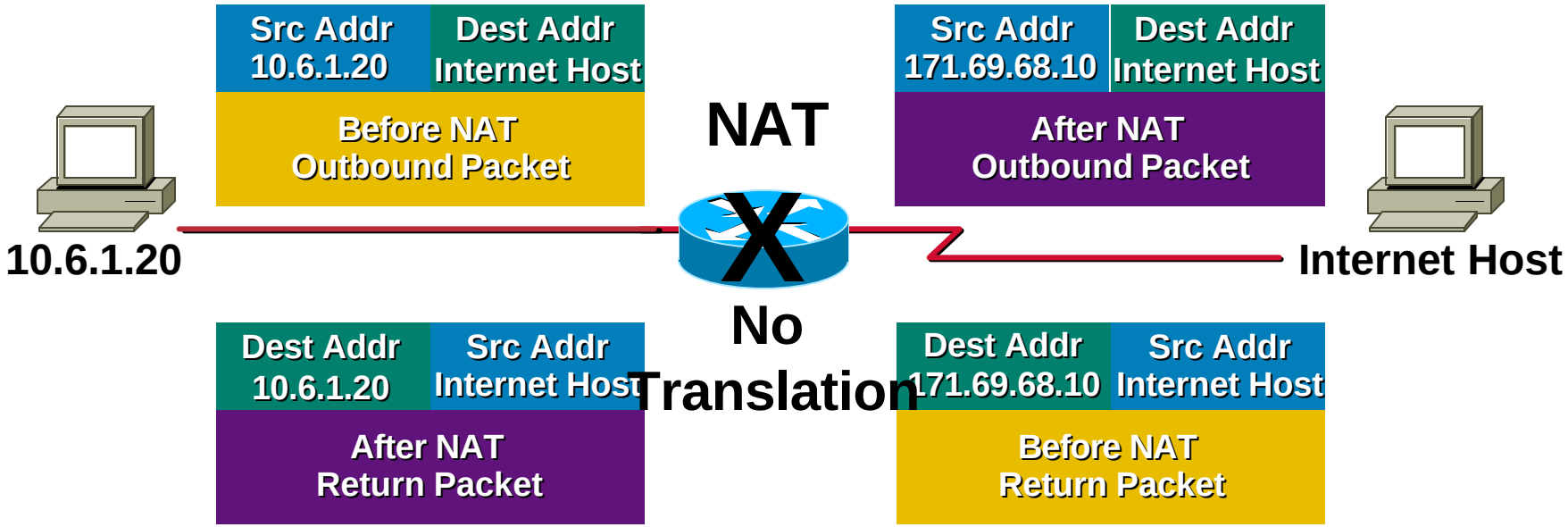
- **Problem: IP address space is limited and obtaining a large block of registered addresses is difficult**
- **Solution: Use private IP addresses (RFC 1918) internally on your network**
- **The private IP addresses you can use on your internal network are:**

  Class A: 10.x.x.x

  Class B range: 172.16.x.x–172.31.x.x

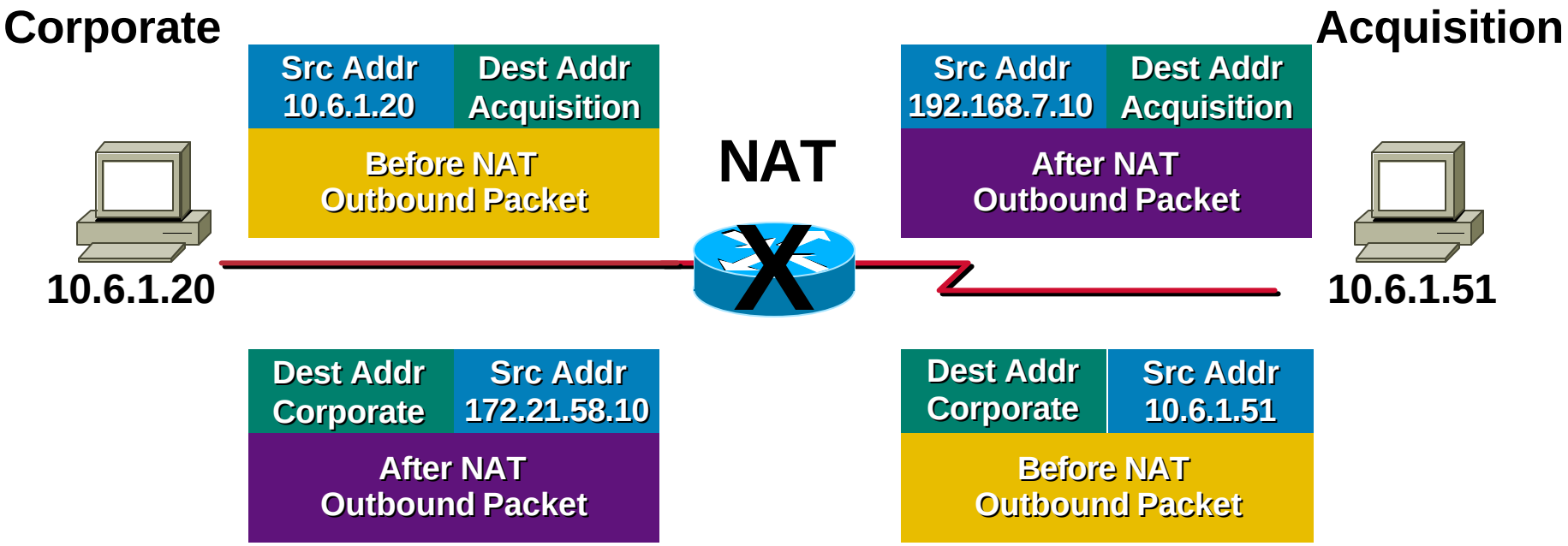
  Class C range: 192.168.1.x–192.168.254.x

Benefits



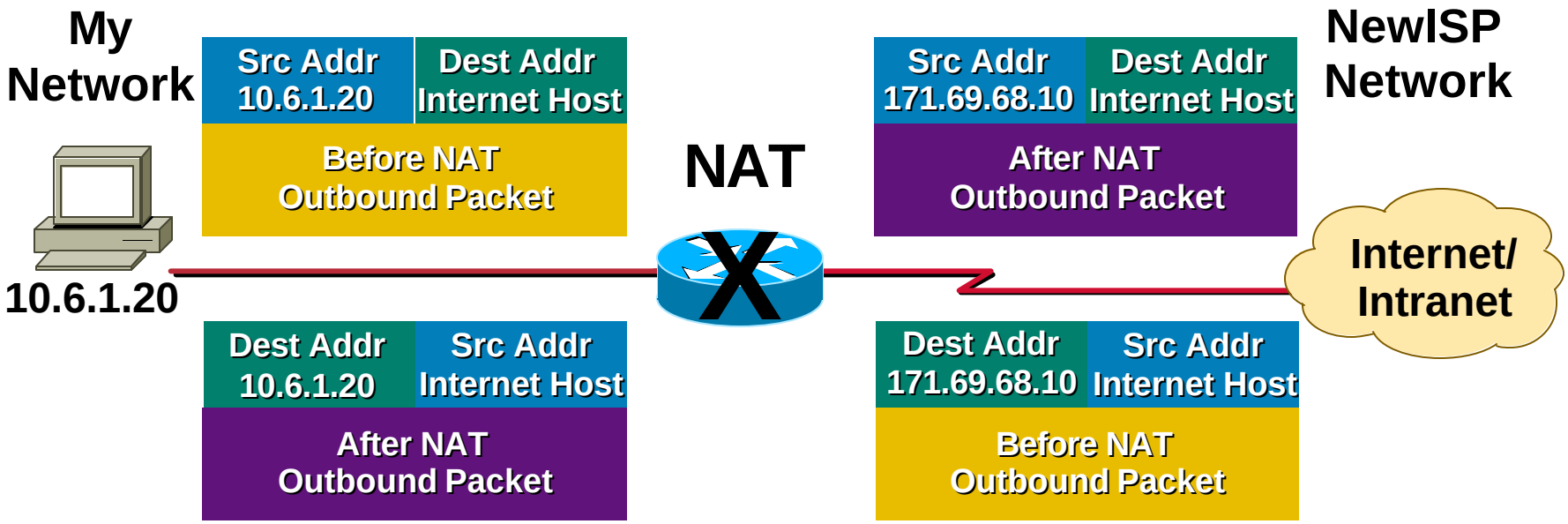
- **Problem: Hosts can't access registered networks such as the Internet, when assigned private IP addresses**
- **Solution: NAT replaces the source address with a routable address and enables privately addressed hosts to access registered networks, such as the Internet, without requiring globally unique IP addresses on end hosts**

Benefits



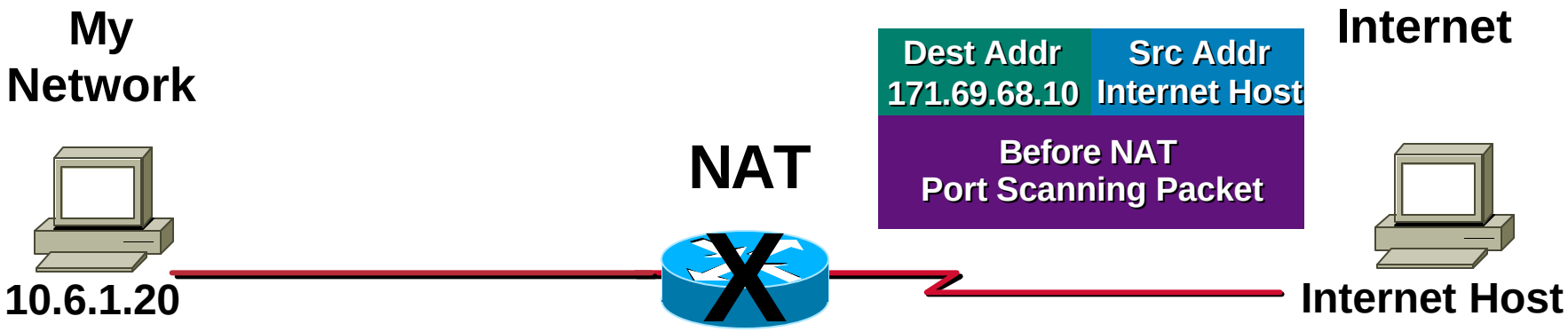
- **Problem: Merging corporations with conflicting private IP address space need connectivity to each other and/or the Internet**
- **Solution: NAT provides transparent, scalable, and bi-directional connectivity between corporate headquarters and acquisitions**

Benefits



- **Problem: Changing ISPs**
- **Solution: NAT eliminates the need for host renumbering when changing ISPs or IP addressing schemes**

Benefits



- **Problem: Internal network should not be visible to external users**
- **Solution: NAT enhances network privacy since assigned addresses are hidden. NAT defeats port scanning of the subnet**

Availability and Platform Support

Cisco.com

- **Introduced in Cisco IOS software release 11.2(1) October 1996**
- **Available in all Cisco IOS releases after 11.2**
- **Supported on Cisco IOS-based systems except on Cisco 7000 unless it has an RSP7000**
- **Also supported on Catalyst 5xxx RSM and Catalyst 6xxx MSFC, as well as Catalyst 6xxx Supervisor IOS**

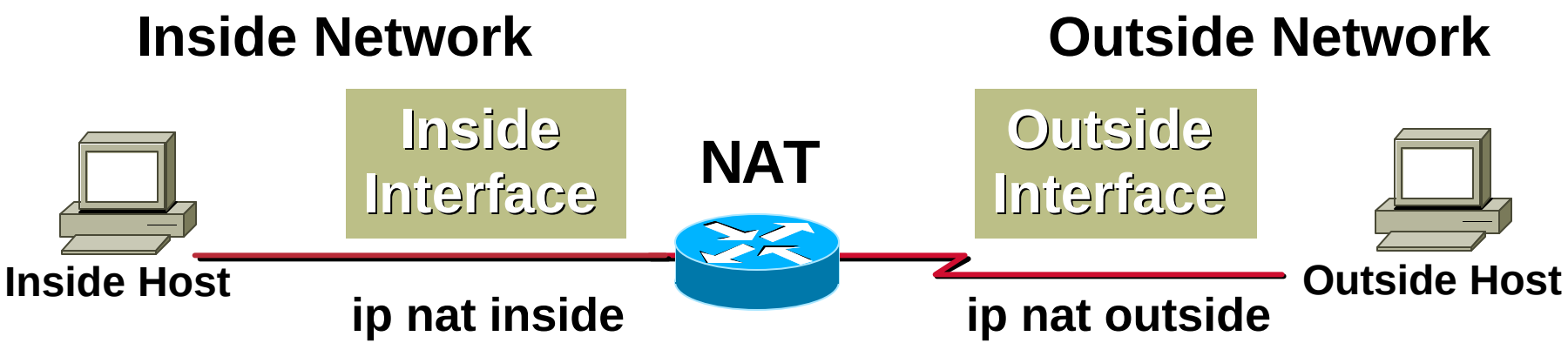
Application Support

- **Applications are transparent to Cisco IOS NAT, except when applications**
  - **Require specific or negotiated ports**
  - **Have embedded IP addresses**
- **Cisco IOS NAT performs ‘stateful inspection’ on applications it has awareness of**

Agenda

- Basic Concept of NAT and PAT
- Definition, Benefits, Availability and Application Support
- NAT Concepts and Terminology
- PAT
- NAT Technical Information

NAT Concepts



- An interface on the router can be defined as inside or outside
- Translations occur only from inside to outside interfaces or vice versa—never between the same type of interface

NAT Concepts

- **NAT translations are static or dynamic**

  Static translation are entered directly into the configuration and are always in the translation table

  ip nat inside source static 10.6.1.20 171.69.68.10

  Dynamic translations use access lists to identify IP addresses that NAT should create translations for

  ip nat inside source list 1 pool nat-pool

  access-list 1 permit 10.0.0.0 0.255.255.255

Static vs. Dynamic Translations

- **Static translations**

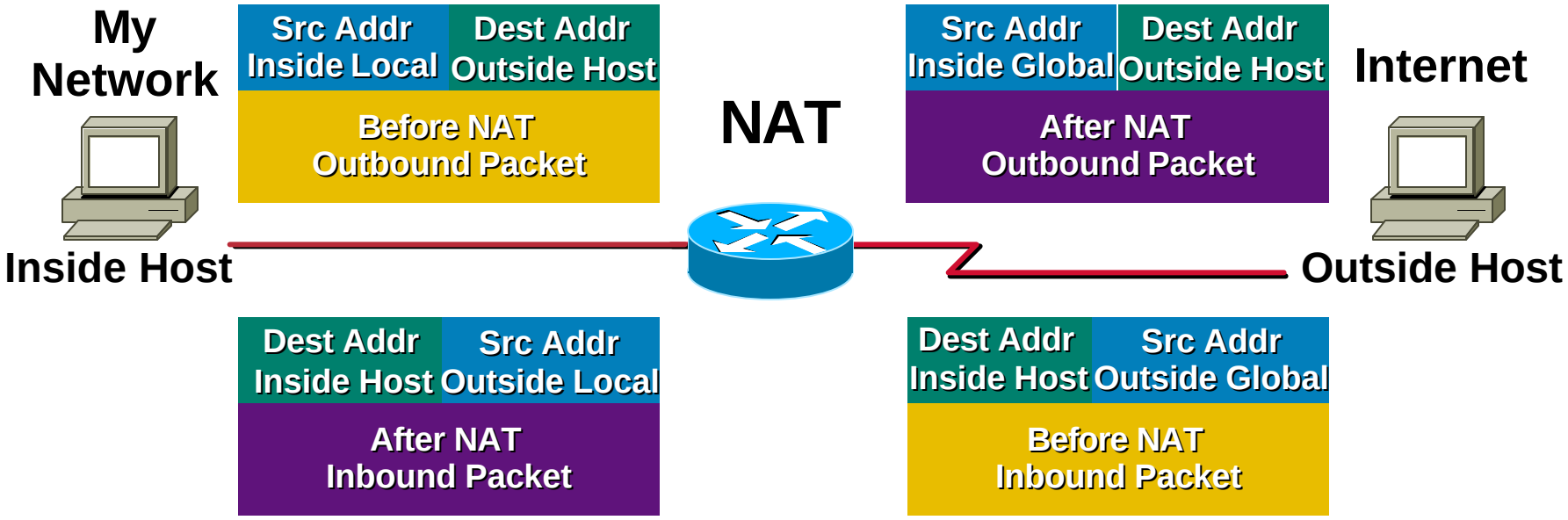
  When you need to be able to initiate a connection from both the inside and outside interfaces (e.g. SMTP, Web)

  Or you want a specific host to be translated to a specific IP address

- **Dynamic translations**

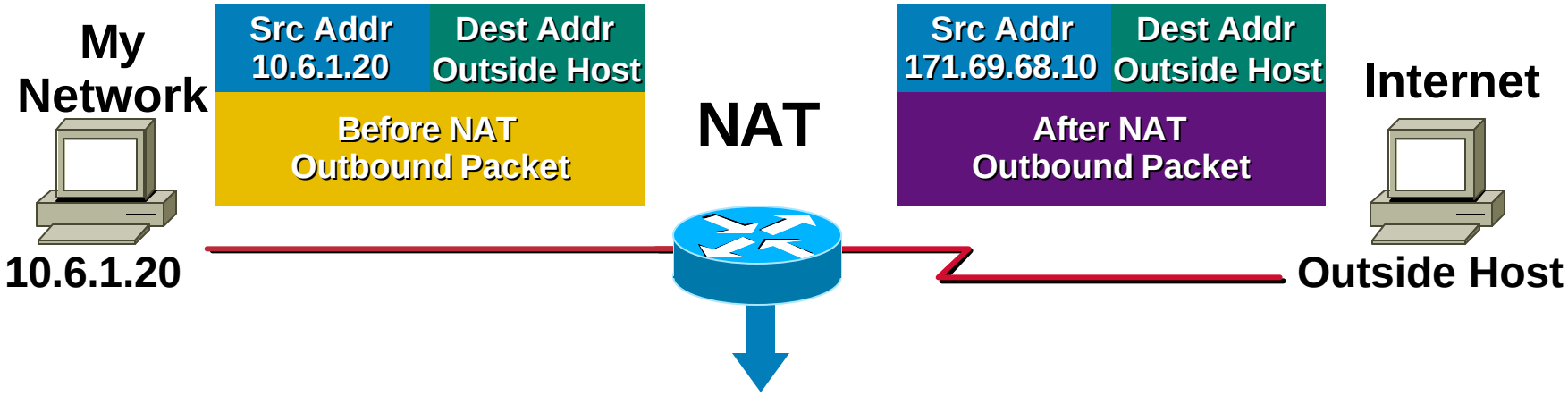
  When you want to initiate a connection from only the inside or only the outside

NAT Concepts



- An IP address is either local or global
- Local IP addresses are seen in the inside network
- Global IP addresses are seen in the Outside network

Inside Local/Inside Global Example

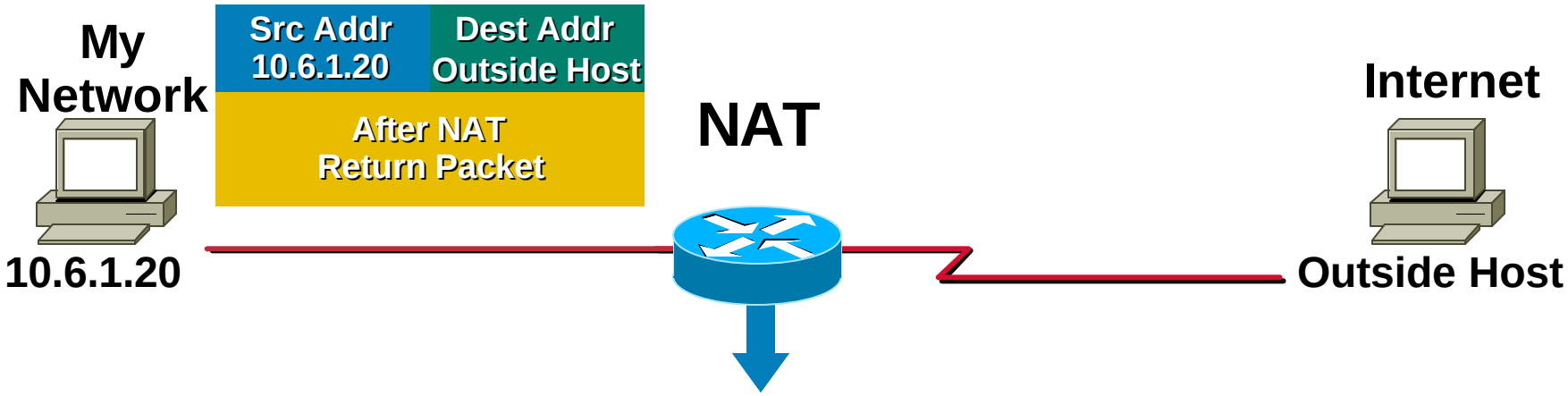


Pro	Inside Global	Inside Local	Outside Local	Outside Global
---	171.69.68.10	10.6.1.20	---	---

NAT Address Pool
- - -
171.69.68.11
171.69.68.12
171.69.68.13

For Outbound Packets an Address Is Dynamically Allocated from the NAT Address Pool

Inside Local/Inside Global Example



Pro	Inside Global	Inside Local	Outside Local	Outside Global
---	---	---	---	---

NAT Address Pool
171.69.68.10
171.69.68.11
171.69.68.12
171.69.68.13

The NAT Address Translation Entry in the Translation Table Is Used to Translate Return Packets

NAT Terminology

- **Inside local**

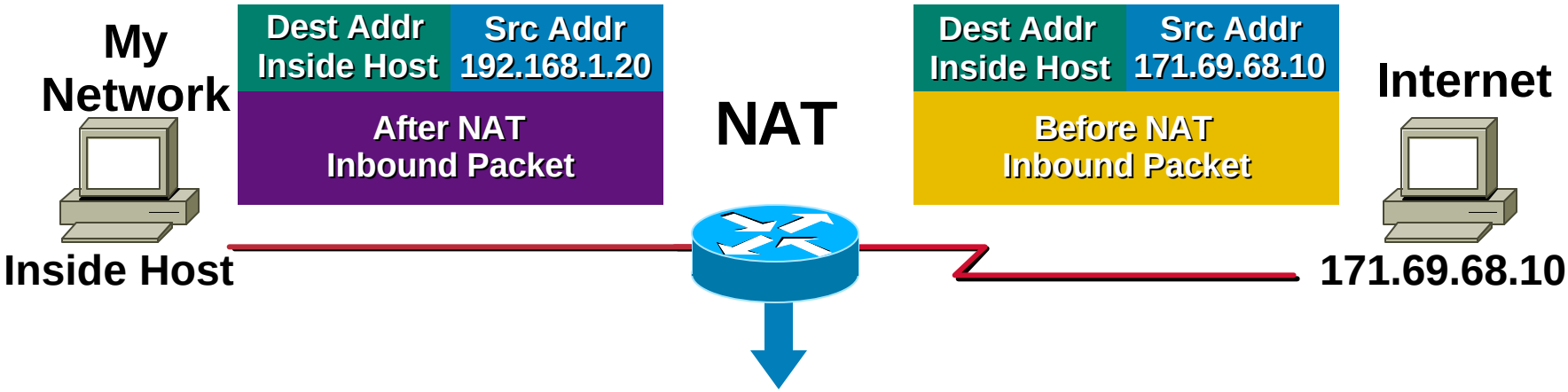
  Configured IP address assigned to a host on the inside network; address may be globally unique, allocated out of the private address space defined in RFC 1918, or may be officially allocated to some other organization

- **Inside global**

  The IP address of an inside host as it appears to the outside host and network, “Translated IP Address”; addresses can be allocated from a globally unique address space, typically provided by the ISP (if the enterprise is connected to the global Internet)

Outside Local/Outside Global Example

Cisco.com



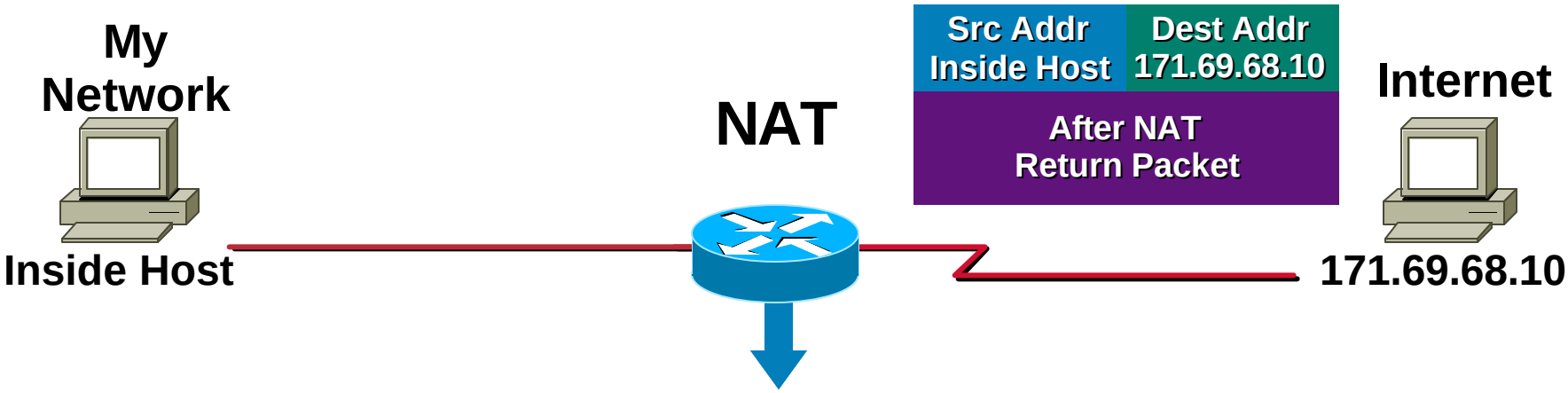
Pro	Inside Global	Inside Local	Outside Local	Outside Global
---	---	---	192.168.1.20	171.69.68.10

NAT Address Pool
- - -
192.168.1.21
192.168.1.22
192.168.1.23

For Inbound Packets an Address Is Dynamically Allocated from the NAT Address Pool

Outside Local/Outside Global Example

Cisco.com



Pro	Inside Global	Inside Local	Outside Local	Outside Global
---	---	---	---	---

NAT Address Pool
192.168.1.21
192.168.1.21
192.168.1.22
192.168.1.23

The NAT Address Translation Entry in the Translation Table Is Used to Translate Return Packets

NAT Terminology

- **Outside local**

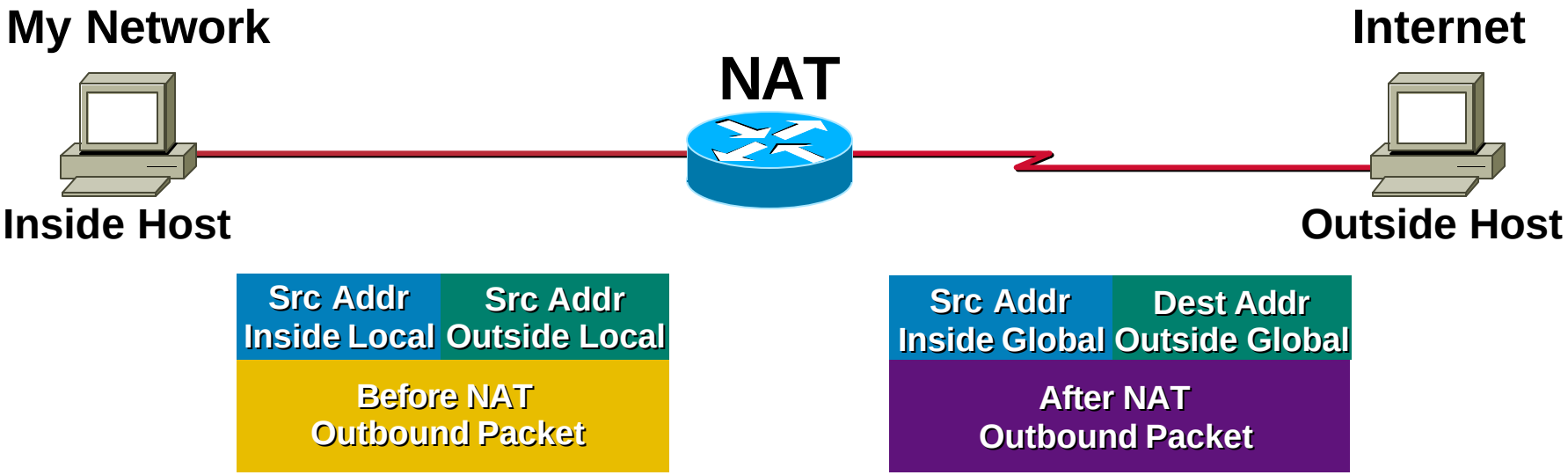
  The IP address of an outside host as it appears to the inside network. These addresses can be allocated from the RFC 1918 space if desired

- **Outside global**

  The configured IP address assigned to a host on the outside network

NAT Concepts

Cisco.com



- **Local IP addresses are seen on the inside network while global IP addresses are seen on the outside network**

NAT Concepts

Cisco.com

Router# show ip nat translations

Pro	Inside Global	Inside Local	Outside Local	Outside Global
---	171.69.70.15	192.168.1.80	---	---
tcp	171.69.68.10:1202	10.6.15.2:1202	204.71.200.67:80	204.71.200.67:80
tcp	171.69.68.10:1460	10.8.20.25:1460	204.71.200.69:80	204.71.200.69:80

- **A NAT translation is 1 to 1 or many to 1**

  1 to 1 translations (NAT) assign a different IP address for each translation

  Many to 1 (PAT) translations can assign the same IP address for each translation

NAT Concepts

Router# show ip nat translations

Pro	Inside Global	Inside Local	Outside Local	Outside Global
tcp	171.69.68.5:1405	10.6.15.2:1405	204.71.200.69:80	204.71.200.69:80
---	171.69.68.20	172.21.58.20	204.71.200.67	204.71.200.67

- **A NAT translation is simple or extended**
  - **Both NAT and PAT can have extended translations**
  - **Only NAT can have simple translations**

Inside Source and Outside Source

- **ip nat inside source**

  Creates a translation, if necessary, and translates the source IP address for packets going from inside Þ outside

  Translates the destination IP address for packets going from outside Þ inside

- **ip nat outside source**

  Creates a translation, if necessary, and translates the source IP address for packets going from outside Þ inside

  Translates the destination IP address for packets going from inside Þ outside

Inside Source vs. Outside Source

- **Inside source translation**

  When you have hosts with IP addresses that should not be seen on the outside network

- **Outside source translation**

  When the same IP addresses are being used on both the inside and outside network (overlapping networks) or you have multiple gateways; generally used in conjunction with inside source translation

Agenda

Cisco.com

- Basic Concept of NAT and PAT
- Definition, Benefits, Availability and Application Support
- NAT Concepts and Terminology
- PAT
- NAT Technical Information

PAT

Router# show ip nat translations

Pro	Inside Global	Inside Local	Outside Local	Outside Global
tcp	171.69.68.5:1405	10.6.15.2:1405	204.71.200.69:80	204.71.200.69:80

- **PAT (Port Address Translation) includes ports in addition to IP addresses**
  - **Many-to-one translation**
  - **Maps multiple IP addresses to 1 or a few IP addresses**
  - **Unique source port number identifies each session**
  - **Conserves registered IP addresses**
  - **Also called NAPT in IETF documents**

Outside Address Assignment

- **Use a pool of IP addresses**
- **Can use an interface name**

  Interface IP addresses can be assigned:

  1) Statically configured

  2) Via PPP (IPCP)

  3) Via DHCP on Ethernet interfaces [12.1(2)T]. More types of interfaces to follow

NAT vs. PAT

- **NAT**

  When there is sufficient number of IP addresses for 1 to 1 translations

- **PAT**

  When there are an insufficient number of IP addresses available to translate all of the inside addresses

Agenda

Cisco.com

- Basic Concept of NAT and PAT
- Definition, Benefits, Availability and Application Support
- NAT Concepts and Terminology
- PAT
- NAT Technical Information

Switching Paths for NAT

- All embedded applications are process switched (e.g DNS, FTP control session packets; FTP data session packets are CEF switched though!)
- First packet without translation is process switched and creates a fast switch cache entry; if CEF switching is enabled, all subsequent packets are CEF switched

How Much Memory?

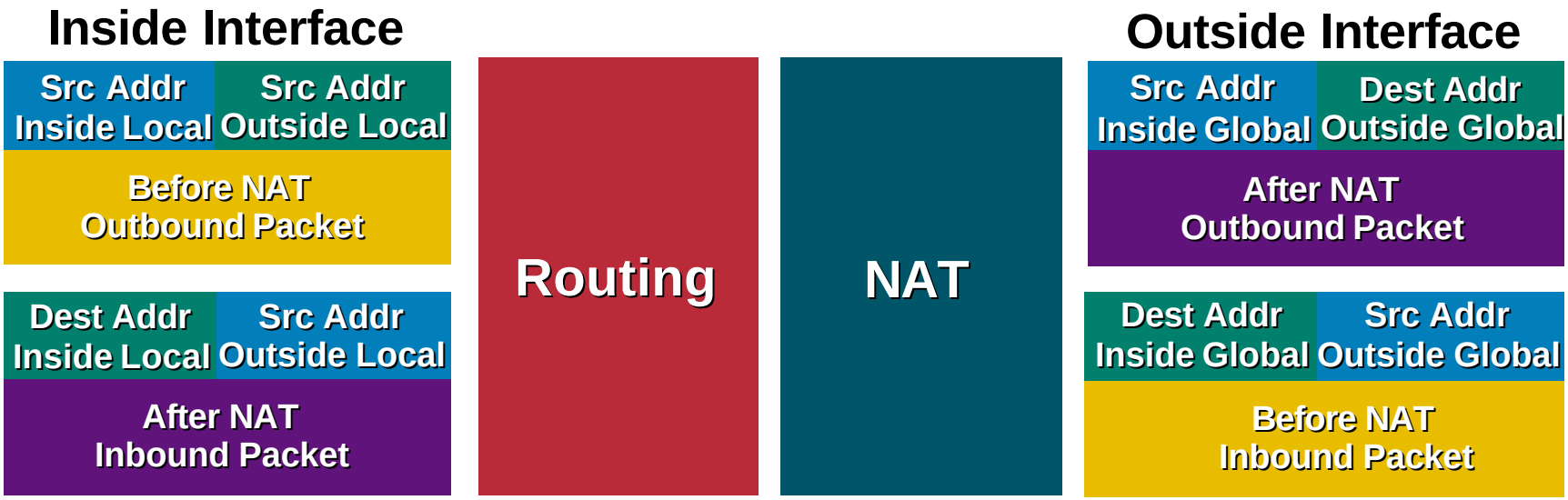
- **Memory**

  Needs 42 Kb of system memory to enable NAT

  160–200 bytes for each entry in the NAT translation table

  1,000 entries use approximately 205 Kb of memory (includes 42 Kb)

NAT Order of Operation



- NAT always checks translation table for entry before access lists
- For a full NAT order of operation see http://www.cisco.com/warp/public/556/5.html

Summary

Cisco.com

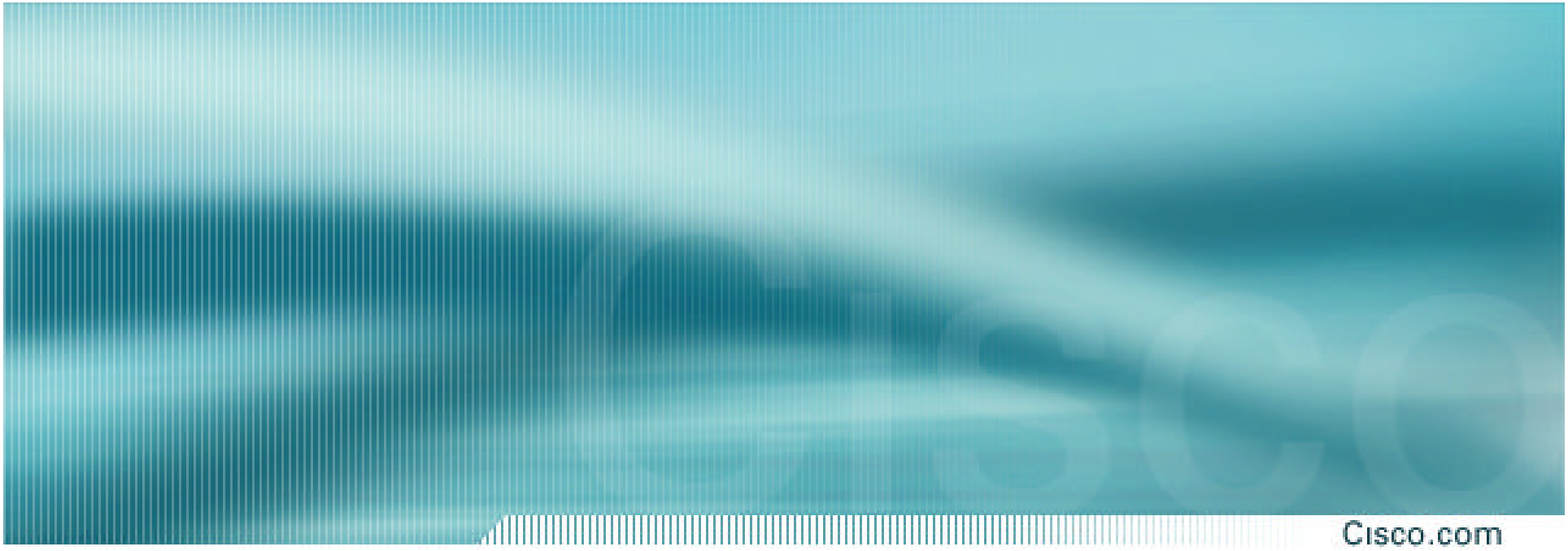
- NAT provides transparent and bi-directional connectivity between networks having arbitrary addressing schemes
- NAT eliminates costs associated with host renumbering
- NAT eases IP address management
- NAT enhances network privacy

References

- RFC 1631—The IP Network Address Translator
- RFC 2663—IP Network Address Translator (NAT) Terminology and Considerations
- http://www.ietf.org/html.charters/nat-charter.html
- NAT Technical Tips
  http://www.cisco.com/warp/public/556/index.shtml
- NAT FAQ (includes platform support)
  http://www.cisco.com/warp/public/458/41.html
- TAC NAT page
  http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Internetworking:NAT

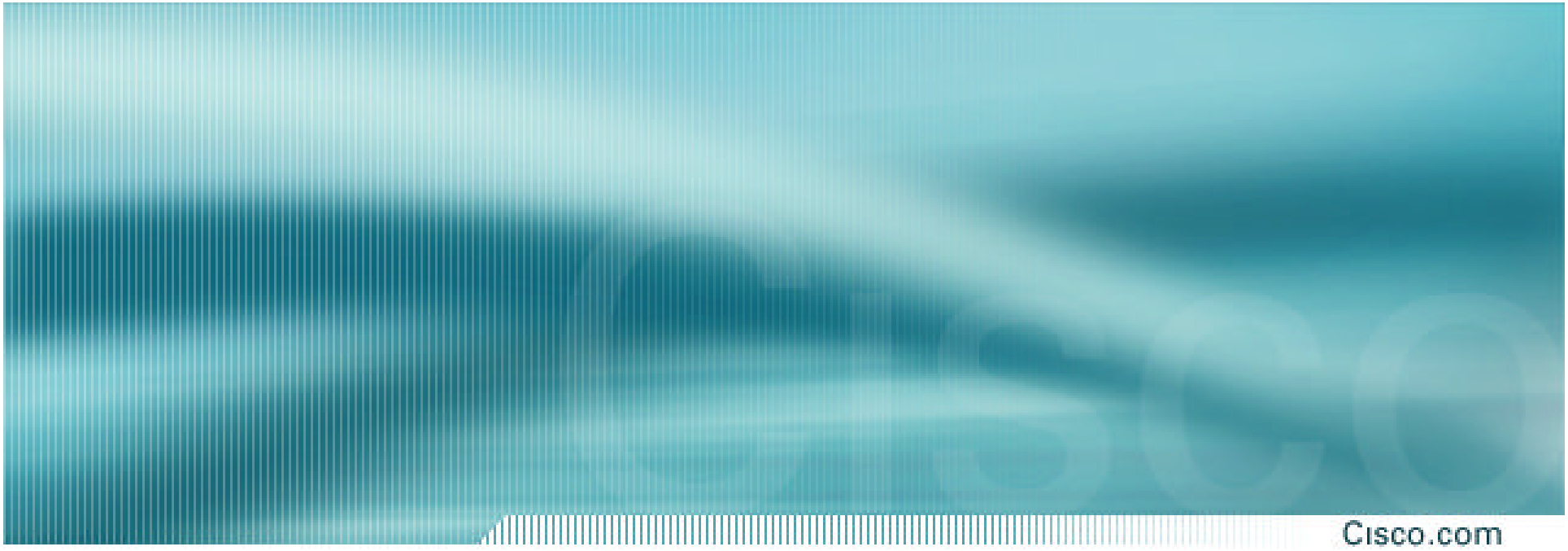
Other Related Presentations

- **IPS-220: Deploying Network Address Translation**
- **IPS-320: Troubleshooting Network Address Translation**



Introduction to Network Address Translation

Session IPS-120



Please Complete Your Evaluation Form

Session IPS-120

Additional Slides

- These slides are for your information and will *NOT* be part of the NAT presentation
- Please feel free to come up after the presentation if you have any questions about them

Application Support List Continues to Grow…

Traffic Types/Applications Supported

Any TCP/UDP Traffic that Does Not Carry IP Addresses in the Application Data Stream or Change Ports during a flow. These include:

- Telnet
- Archie
- Finger
- NTP (Network Time Protocol)
- rlogin, rsh, rcp
- NFS
- HTTP (Web)
- TFTP

Protocols or Applications that require Special Support (Carry IP Addresses in the Application Data Stream or Change Ports) and are Supported by Cisco IOS® NAT:

- VDOLive—11.3(4)/11.3(4)T
- Vxtreme—11.3(4)/11.3(4)T
- IP Multicast—12.0(1)T Source Translation Only
- ICMP
- PPTP support with PAT – 12.1(2)T
- H.323v2 for NetMeeting v.2.x and v3.x
  - H.323v1 for NetMeeting v2.x - 12.0(1)/12.0(1)T
  - H.323v2 for NetMeeting v3.x - 12.0(7)T
- SMTP (Mail)
- FTP (Including PORT and PASV Commands)
- NetBIOS over TCP/IP
- Progressive Networks' RealAudio
- White Pines' CuSeeMe
- DNS "A" and "PTR" Queries
- Xing Technologies' StreamWorks

Application Support (Cont.)

Cisco.com

Traffic Types/Applications Supported

Any TCP/UDP Traffic that Does Not Carry IP Addresses in the Application Data Stream or Change Ports during a flow. These include:	Protocols or Applications that require Special Support (Carry IP Addresses in the Application Data Stream or Change Ports) and are Supported by Cisco IOS® NAT: RAS – 12.2(1)T SIP – 12.2(3)T

NAT Configuration Command Examples

Cisco.com

Static

```
ip nat inside source static 10.1.1.10 140.16.1.254          ! Inside Source Static translation
ip nat outside source static 10.1.1.10 192.168.1.254        ! Outside Source Static translation
```

Dynamic

```
ip nat pool iga 140.16.1.1 140.16.1.253 netmask 255.255.255.0  ! Dynamic IL->IG address xlations
ip nat pool ola 192.168.1.1 192.168.1.253 netmak 255.255.255.0 ! Dynamic OG->OL address xlations
ip nat inside source list 1 pool iga                        ! Command for dynamic inside source xlations
ip nat outside source list 2 pool ola                       ! Command for dynamic outside source xlations
access-list 1 permit 10.0.0.0 0.255.255.255                 ! Translate all traffic from 10/8 internal hosts
access-list 2 permit 10.0.0.0 255.0.0.0                     ! Translate all externally originated traffic
!
interface <inside>
ip address <ip-address> <net-mask>
ip nat inside
!
interface <outside>
ip address <ip-address> <net-mask>
ip nat outside
```

Show IP NAT Statistics

Cisco.com

```
Total active translations: 3 (2 static, 1 dynamic; 1 extended)
Outside interfaces:
  FastEthernet2/0
Inside interfaces:
  FastEthernet1/0
Hits: 244  Misses: 1
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list web interface FastEthernet1/0 refcount 1
```

- This is an example of “Show ip nat statistics”. There are currently 3 active translations, 2 static translations and 1 dynamic translation, with 1 of the 3 translations extended. The list of outside interfaces is composed of Fast Ethernet 2/0. The list of inside Interfaces is composed of Fast Ethernet 1/0. The NAT code has looked in the translation table a total of 245 times. 244 of these times it found a translation it could use. 1 time it did not find a translation and created one. There are 0 translations that have timed out and been removed. The dynamic translation consist of an inside source translation that is using the named access list “web” for specifying the packets to create translations for. It is using the address of Fast Ethernet 1/0 as the global address to translate to. The refcount indicates that one flow is using this dynamic mapping.

Show IP NAT Verbose

Cisco.com

```
router#show ip nat translations verbose
Pro Inside global     Inside local       Outside local      Outside global
tcp 134.79.1.1:80     172.21.58.2:80     134.79.1.2:80      134.79.1.2:80
create 00:00:12, use 00:00:10, left 23:59:49,
flags:
extended, use_count: 0
```

- The “show ip nat translations verbose” command shows the protocol if the translation is extended, the inside and outside local and global addresses, a number of different timer fields, and flags. It also shows the use_count field. The use_count field can show how many extended translations are using this static translation or it can show how many extended translations are based on this entry (e.g. FTP Control Session translation opens a FTP Data Session translation). In the timer fields, the “create” timer shows how long ago the translation was created. The “use” timer shows how long ago the translation was last used. And the “left” timer indicates how long the translations has left before deletion from the translation table. If the "left" timer is missing, the translation will not timeout and will not be removed. The flags field is implicit if not explicit. In this example, it indicates the translation is extended. If there was not an extended flag, it would mean that the translation was simple. The other flags follow this example. If there is no outside flag, then the translation is an inside source translation. No Static flag, then it is a dynamic translation. If there are no flags at all, the flag field will indicate “none”.

Debug IP Nat


```
router# debug ip nat
NAT s=192.168.1.95->172.31.233.209, d=172.31.2.132 [6825]
NAT* s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23311]
```

- The “debug ip nat” command lets you see the packets that were changed and how they were changed. The * next to NAT indicates that the packet was fast or CEF switched (process switched otherwise) . In the top debug, the source IP address 192.168.1.95 was changed to 172.31.233.209 and was process switched. The return packet was fast or CEF switched.

Debug IP NAT Detailed


```
router# debug ip nat detailed
NAT i udp (192.168.1.95, 1493) -> (172.31.2.132, 53) [22399]
NAT* o tcp (172.31.2.75, 23) -> (172.31.233.193, 1135) [22002]
```

- The “debug ip nat detail” command shows you every packet NAT examined. It displays which type of interface (inside or outside) it saw the packet come in on, what IP protocol was in the IP packet, the source IP address and source port, and finally the destination IP address and destination port.

Both Debugs

Cisco.com

> 1d05h NAT* i tcp (172.21.58.94, 2045) -> (134.79.1.10, 80) [0]

> 1d05h NAT* s=172.21.58.94->101.0.0.92, d=134.79.1.10 [0]

> 1d05h NAT i udp (172.21.58.34, 7778) -> (134.79.1.5, 53) [0]

> 1d05h NAT s=172.21.58.34->101.0.0.32, d=134.79.1.5 [0]

- **An example of both debugs on. The router saw a packet from 172.21.58.94 with a TCP source port of 2045 come in on an inside interface. The packet was fast or CEF switched depending on the configuration. The next line shows the source IP address translation the router did from 172.21.58.94 to 101.0.0.92. There was no translation on the destination address. The third line shows a DNS lookup and the source address was again translated. Notice that the DNS packet was process switched.**

Other Debug Messages

- **When no translation occurs because NAT could not complete it because of an error, such as trying to use the subnet zero addresses in translations, the debug ip nat command puts out the following messages:**

  NAT: translation failed (A), dropping packet s=171.16.4.4 d=171.16.6.5

  NAT: translation failed (A), dropping packet s=171.16.4.4 d=171.16.6.5

  NAT: translation failed (A), dropping packet s=171.16.4.4 d=171.16.6.5

  NAT: translation failed (A), dropping packet s=171.16.4.4 d=171.16.6.5

  NAT: translation failed (A), dropping packet s=171.16.4.4 d=171.16.6.5

- **Note: The "(A)" in the debug output means that translation failed after routing occurred**