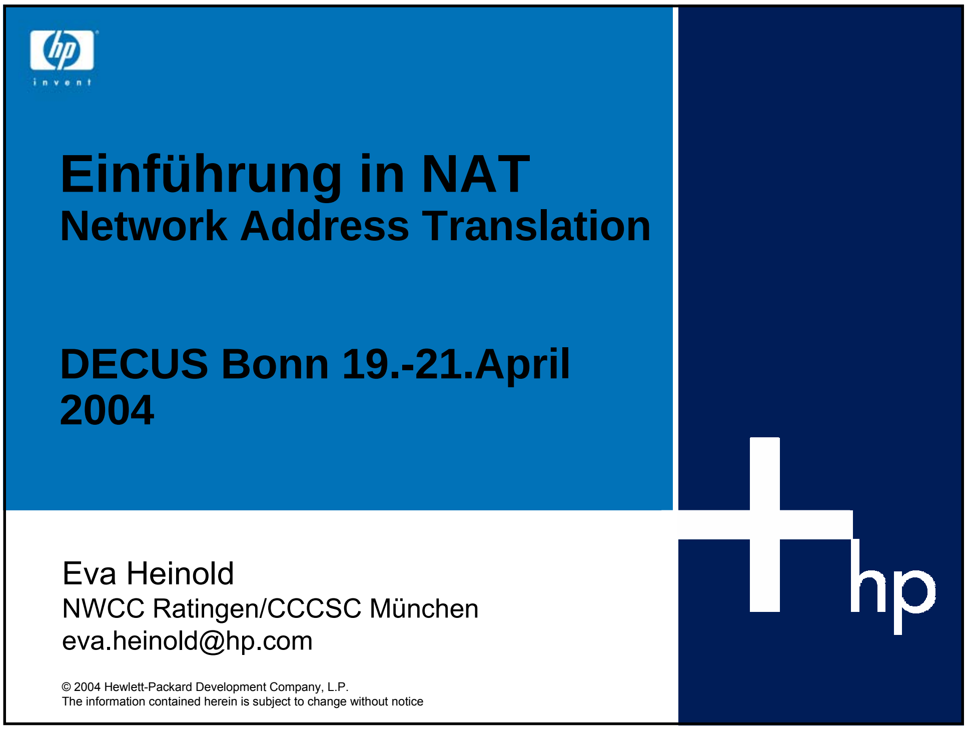
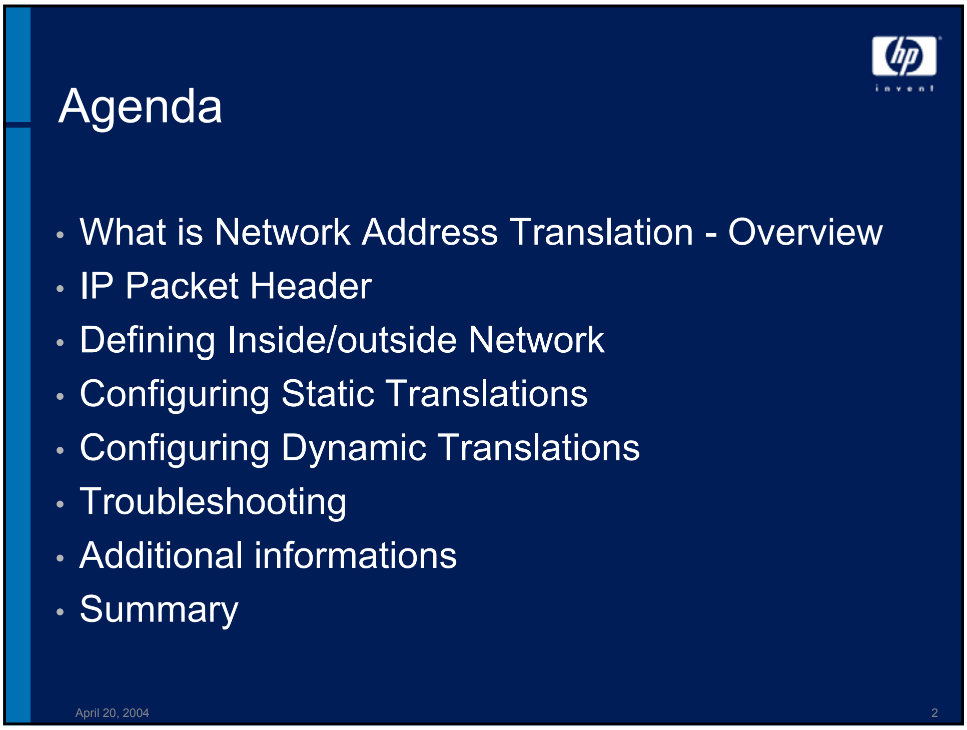


Einführung in NAT
Network Address Translation

DECUS Bonn 19.-21.April 2004

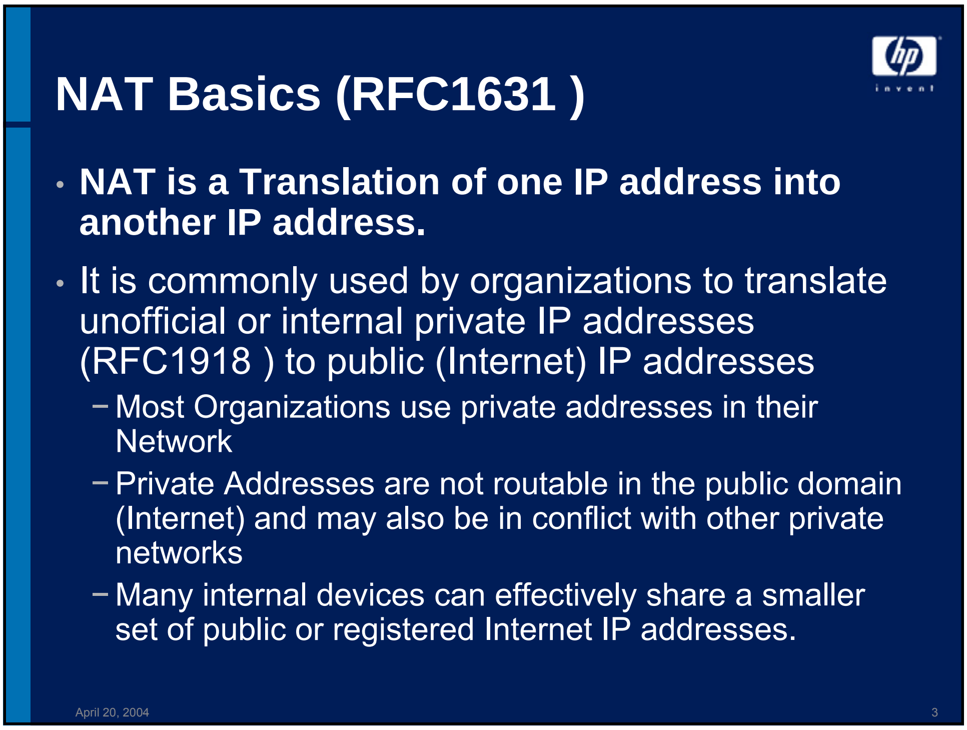
Eva Heinold
NWCC Ratingen/CCCSC München
eva.heinold@hp.com



Agenda

- What is Network Address Translation - Overview
- IP Packet Header
- Defining Inside/outside Network
- Configuring Static Translations
- Configuring Dynamic Translations
- Troubleshooting
- Additional informations
- Summary

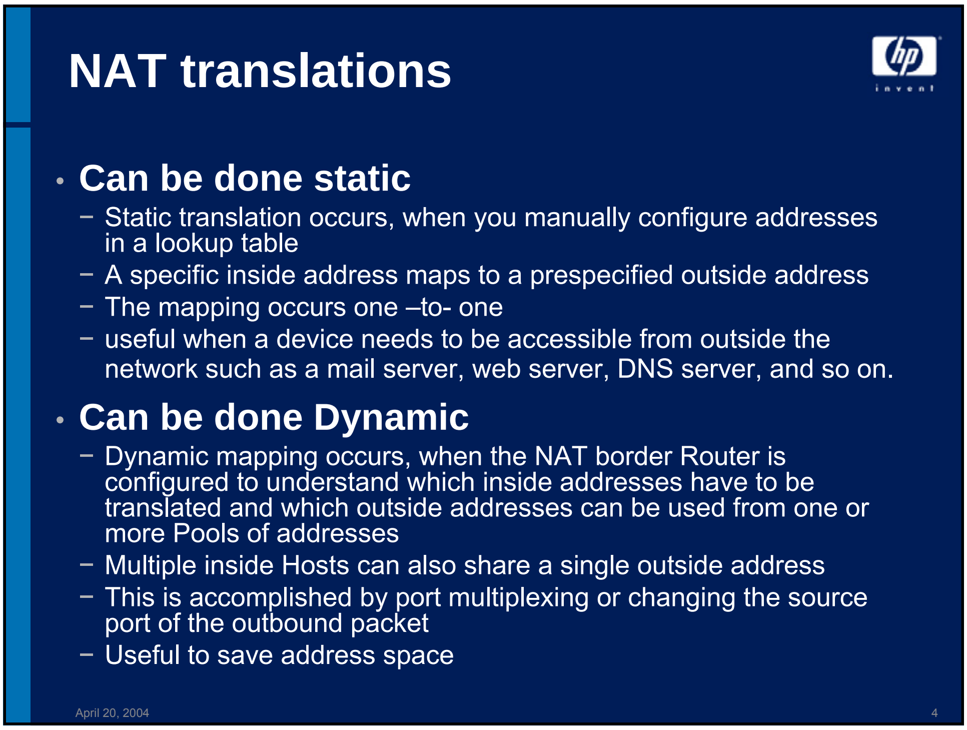
April 20, 2004 2



NAT Basics (RFC1631)

- **NAT is a Translation of one IP address into another IP address.**
- It is commonly used by organizations to translate unofficial or internal private IP addresses (RFC1918) to public (Internet) IP addresses
  - Most Organizations use private addresses in their Network
  - Private Addresses are not routable in the public domain (Internet) and may also be in conflict with other private networks
  - Many internal devices can effectively share a smaller set of public or registered Internet IP addresses.

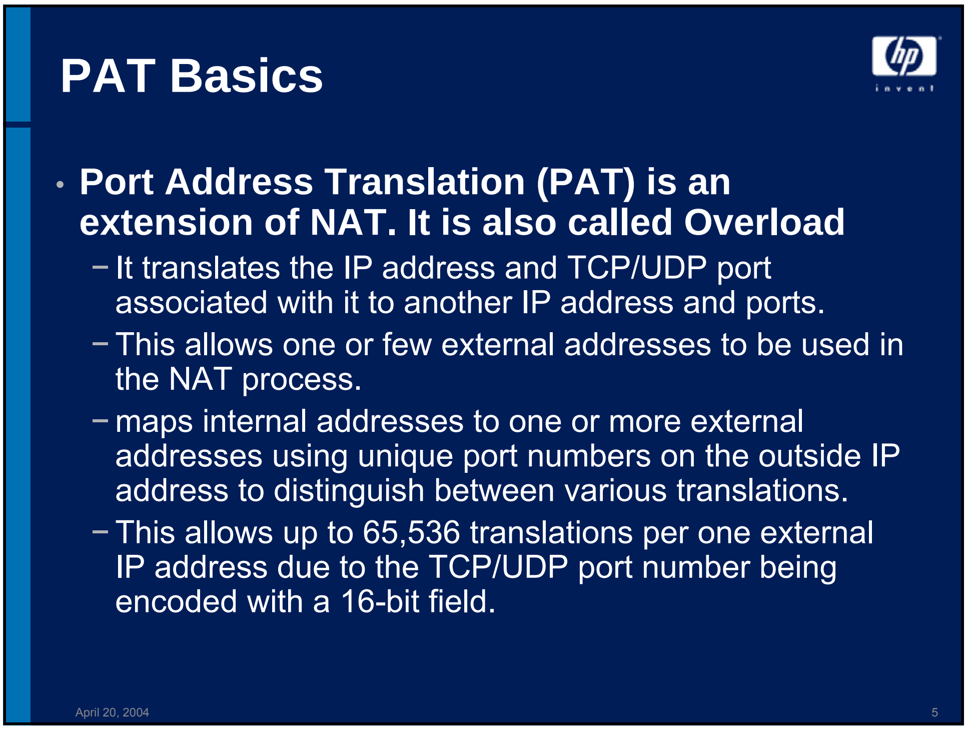
April 20, 2004 3



NAT translations

- **Can be done static**
  - Static translation occurs, when you manually configure addresses in a lookup table
  - A specific inside address maps to a prespecified outside address
  - The mapping occurs one –to- one
  - useful when a device needs to be accessible from outside the network such as a mail server, web server, DNS server, and so on.
- **Can be done Dynamic**
  - Dynamic mapping occurs, when the NAT border Router is configured to understand which inside addresses have to be translated and which outside addresses can be used from one or more Pools of addresses
  - Multiple inside Hosts can also share a single outside address
  - This is accomplished by port multiplexing or changing the source port of the outbound packet
  - Useful to save address space

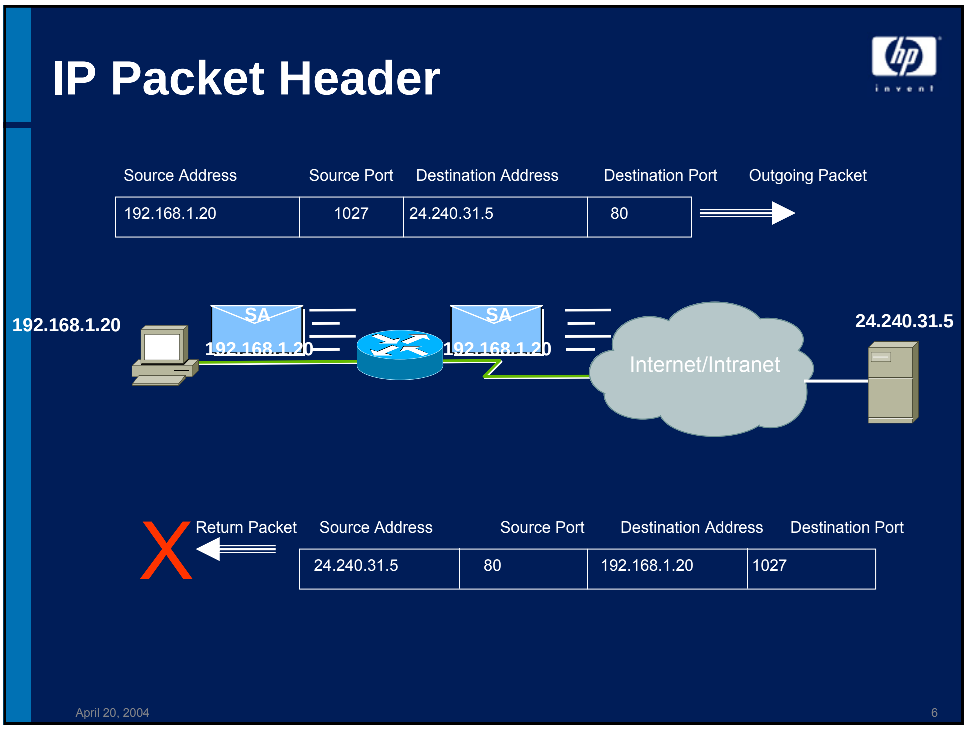
April 20, 2004 4



PAT Basics

- **Port Address Translation (PAT) is an extension of NAT. It is also called Overload**
  - It translates the IP address and TCP/UDP port associated with it to another IP address and ports.
  - This allows one or few external addresses to be used in the NAT process.
  - maps internal addresses to one or more external addresses using unique port numbers on the outside IP address to distinguish between various translations.
  - This allows up to 65,536 translations per one external IP address due to the TCP/UDP port number being encoded with a 16-bit field.

April 20, 2004 5



IP Packet Header

Source Address	Source Port	Destination Address	Destination Port	Outgoing Packet
192.168.1.20	1027	24.240.31.5	80	⇒

192.168.1.20

SA 192.168.1.20

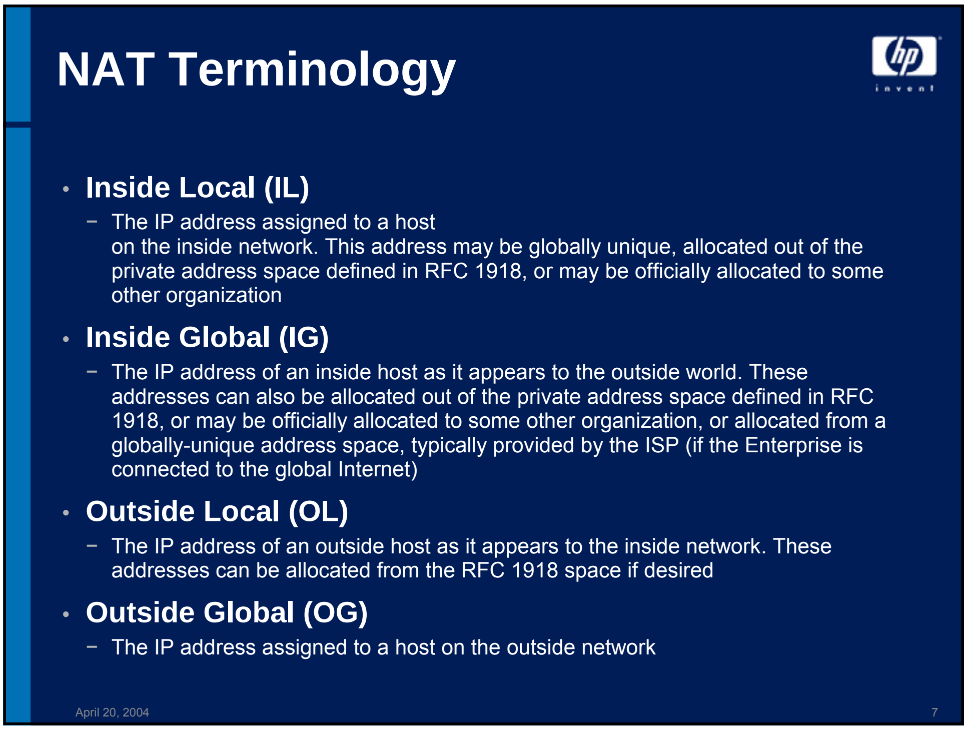
SA 192.168.1.20

Internet/Intranet

24.240.31.5

Return Packet	Source Address	Source Port	Destination Address	Destination Port
X ⇐	24.240.31.5	80	192.168.1.20	1027

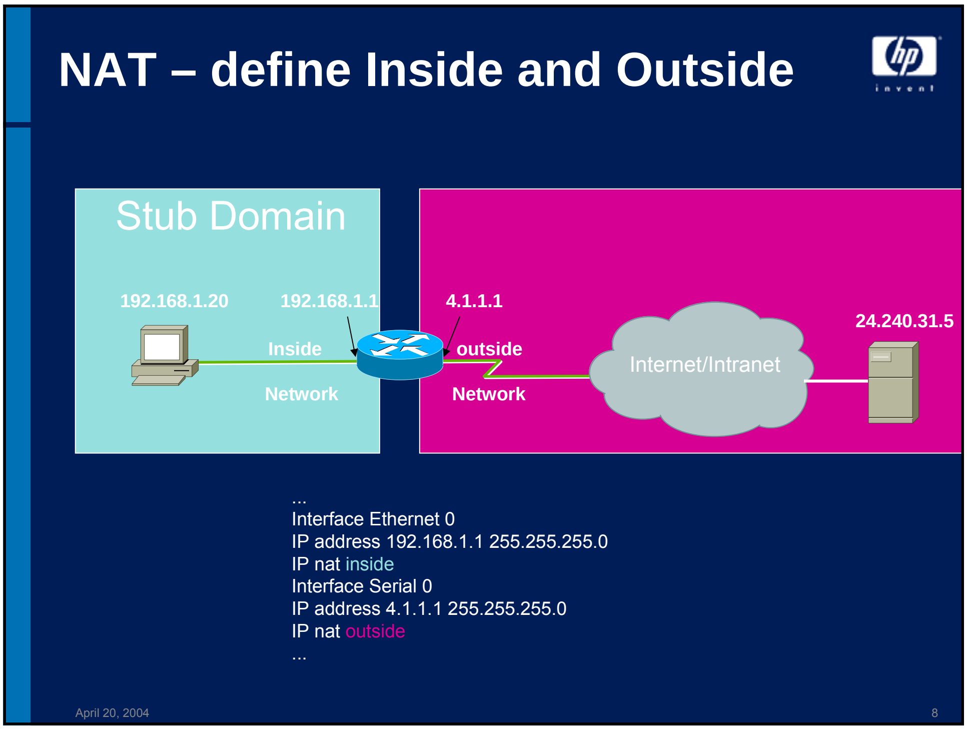
April 20, 2004 6



NAT Terminology

- **Inside Local (IL)**
  - The IP address assigned to a host on the inside network. This 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 (IG)**
  - The IP address of an inside host as it appears to the outside world. These addresses can also be allocated out of the private address space defined in RFC 1918, or may be officially allocated to some other organization, or allocated from a globally-unique address space, typically provided by the ISP (if the Enterprise is connected to the global Internet)
- **Outside Local (OL)**
  - 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 (OG)**
  - The IP address assigned to a host on the outside network

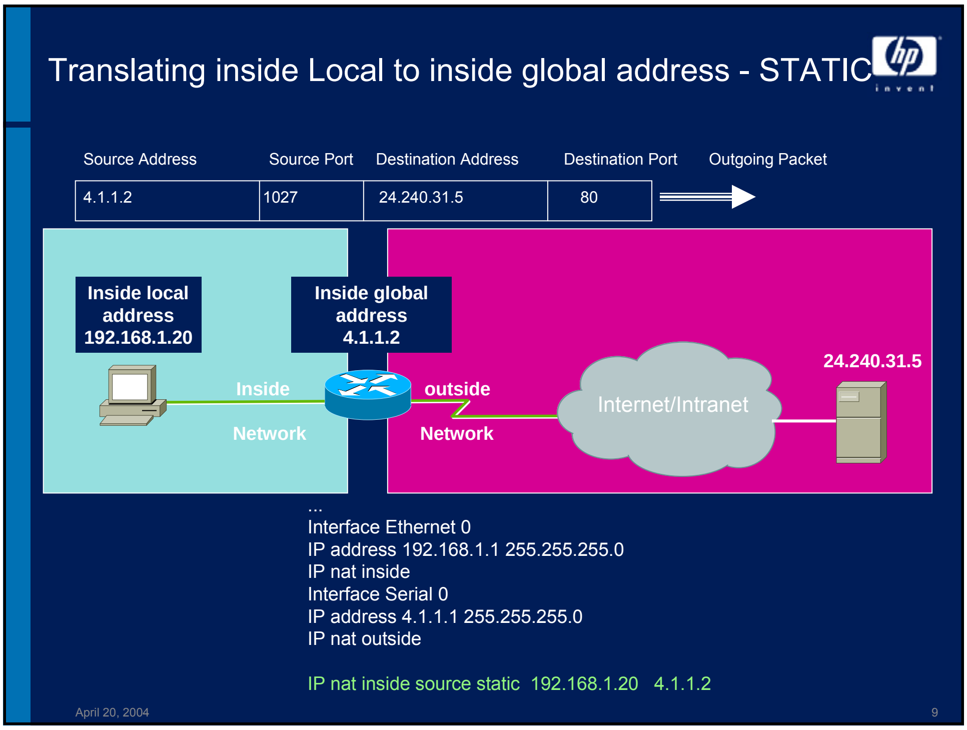
April 20, 2004 7



NAT – define Inside and Outside

```
...
Interface Ethernet 0
IP address 192.168.1.1 255.255.255.0
IP nat inside
Interface Serial 0
IP address 4.1.1.1 255.255.255.0
IP nat outside
...
```

April 20, 2004 8



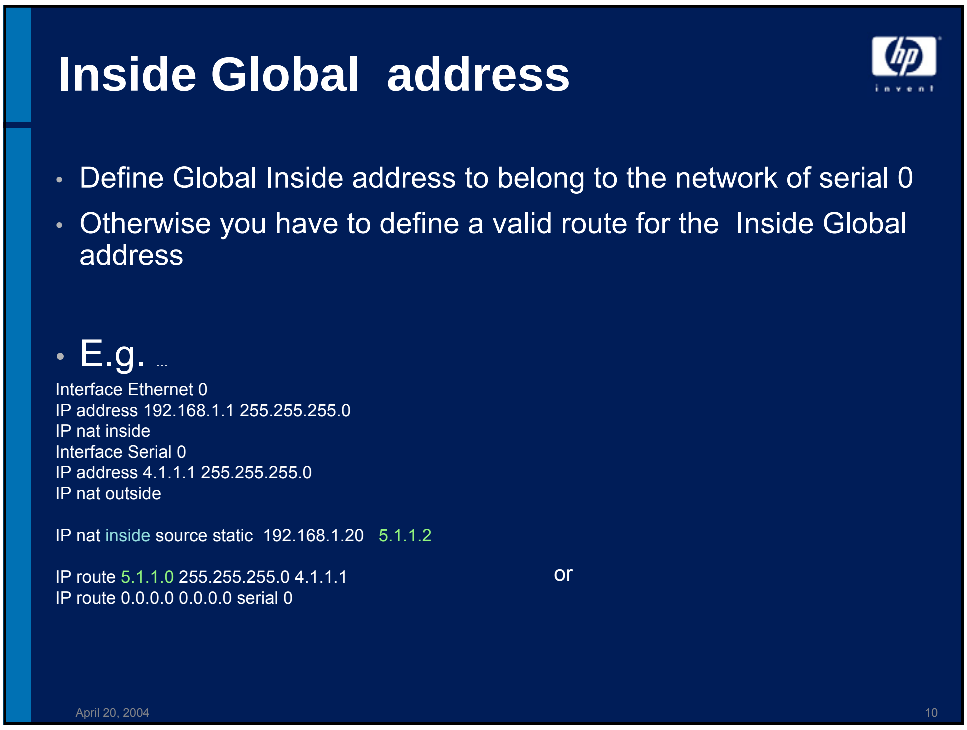
Translating inside Local to inside global address - STATIC

Source Address	Source Port	Destination Address	Destination Port	Outgoing Packet
4.1.1.2	1027	24.240.31.5	80	⟹

Inside local address 192.168.1.20
Inside global address 4.1.1.2
Inside
Network
outside
Network
Internet/Intranet
24.240.31.5

```
...
Interface Ethernet 0
IP address 192.168.1.1 255.255.255.0
IP nat inside
Interface Serial 0
IP address 4.1.1.1 255.255.255.0
IP nat outside

IP nat inside source static  192.168.1.20   4.1.1.2
```

April 20, 2004 9

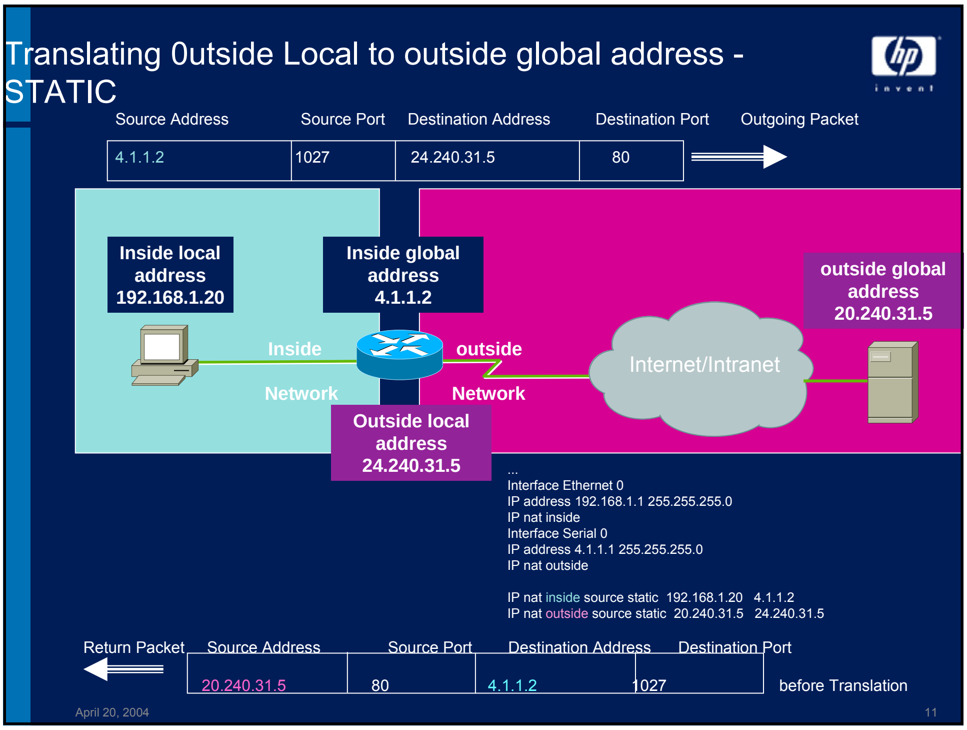


Inside Global address

- Define Global Inside address to belong to the network of serial 0
- Otherwise you have to define a valid route for the Inside Global address
- E.g. ...

```
Interface Ethernet 0
IP address 192.168.1.1 255.255.255.0
IP nat inside
Interface Serial 0
IP address 4.1.1.1 255.255.255.0
IP nat outside

IP nat inside source static  192.168.1.20   5.1.1.2

IP route 5.1.1.0 255.255.255.0 4.1.1.1                              or
IP route 0.0.0.0 0.0.0.0 serial 0
```

April 20, 2004 10



Translating 0utside Local to outside global address - STATIC

Source Address	Source Port	Destination Address	Destination Port	Outgoing Packet
4.1.1.2	1027	24.240.31.5	80	

Inside local address 192.168.1.20

Inside global address 4.1.1.2

outside global address 20.240.31.5

Inside Network

outside Network

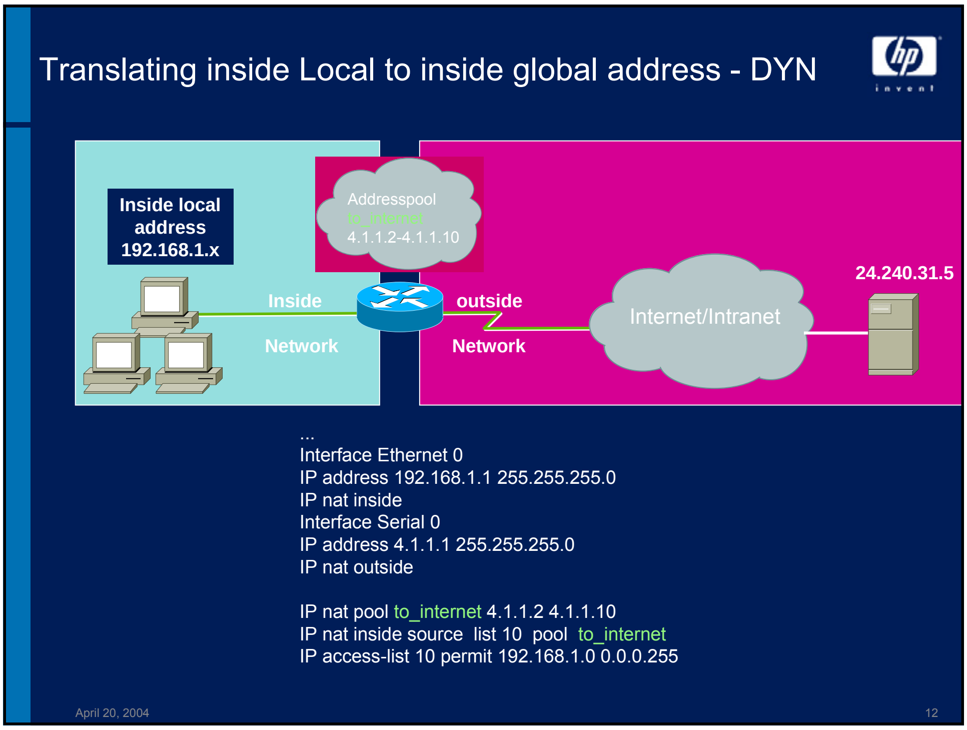
Internet/Intranet

Outside local address 24.240.31.5

```
...
Interface Ethernet 0
IP address 192.168.1.1 255.255.255.0
IP nat inside
Interface Serial 0
IP address 4.1.1.1 255.255.255.0
IP nat outside

IP nat inside source static  192.168.1.20   4.1.1.2
IP nat outside source static  20.240.31.5   24.240.31.5
```

Return Packet	Source Address	Source Port	Destination Address	Destination Port	
	20.240.31.5	80	4.1.1.2	1027	before Translation

April 20, 2004 11



Translating inside Local to inside global address - DYN

Inside local address 192.168.1.x

Addresspool
to_internet
4.1.1.2-4.1.1.10

Inside Network

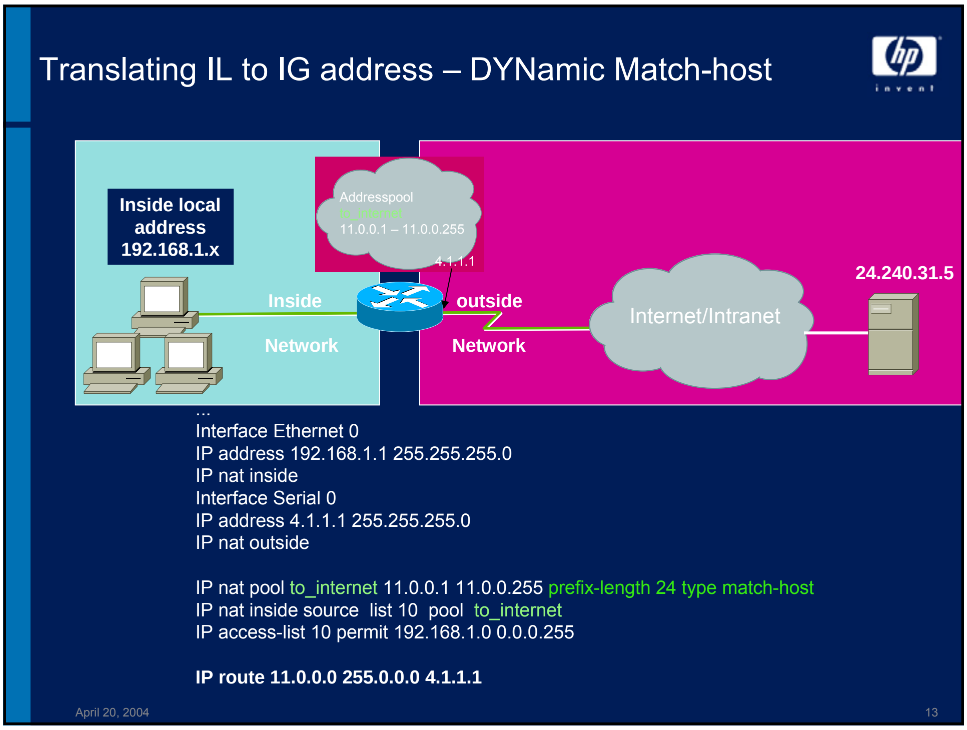
outside Network

Internet/Intranet

24.240.31.5

```
...
Interface Ethernet 0
IP address 192.168.1.1 255.255.255.0
IP nat inside
Interface Serial 0
IP address 4.1.1.1 255.255.255.0
IP nat outside

IP nat pool to_internet 4.1.1.2 4.1.1.10
IP nat inside source  list 10  pool  to_internet
IP access-list 10 permit 192.168.1.0 0.0.0.255
```

April 20, 2004 12

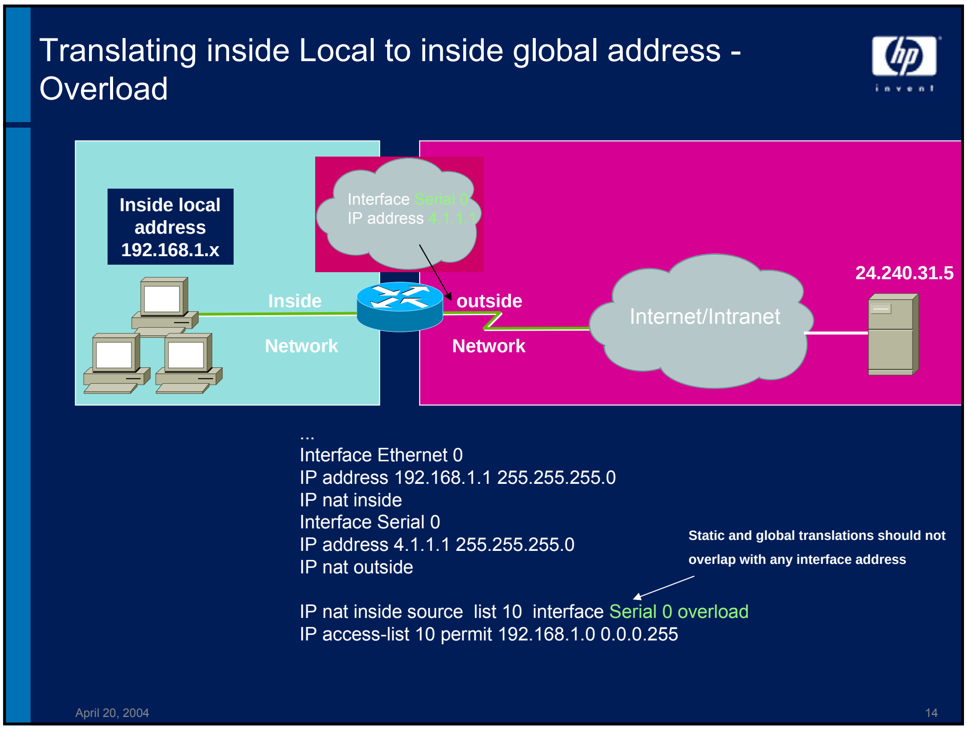


Translating IL to IG address – DYNamic Match-host

```
...
Interface Ethernet 0
IP address 192.168.1.1 255.255.255.0
IP nat inside
Interface Serial 0
IP address 4.1.1.1 255.255.255.0
IP nat outside

IP nat pool to_internet 11.0.0.1 11.0.0.255 prefix-length 24 type match-host
IP nat inside source  list 10  pool  to_internet
IP access-list 10 permit 192.168.1.0 0.0.0.255

IP route 11.0.0.0 255.0.0.0 4.1.1.1
```

April 20, 2004

13



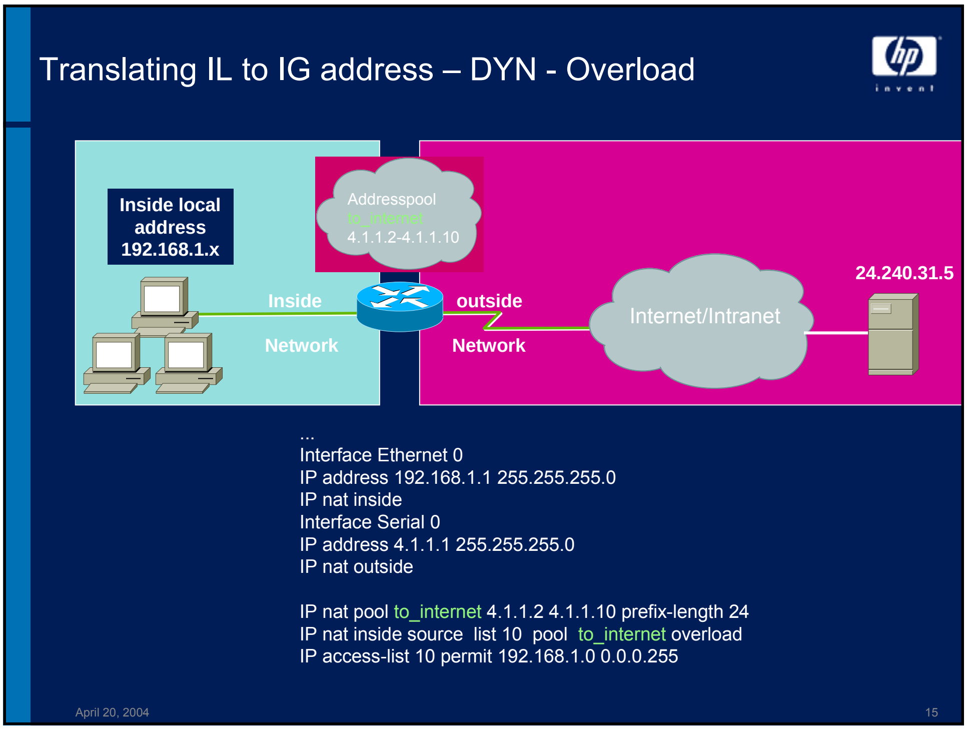
Translating inside Local to inside global address - Overload

```
...
Interface Ethernet 0
IP address 192.168.1.1 255.255.255.0
IP nat inside
Interface Serial 0
IP address 4.1.1.1 255.255.255.0
IP nat outside

IP nat inside source  list 10  interface Serial 0 overload
IP access-list 10 permit 192.168.1.0 0.0.0.255
```

Static and global translations should not overlap with any interface address

April 20, 2004

14

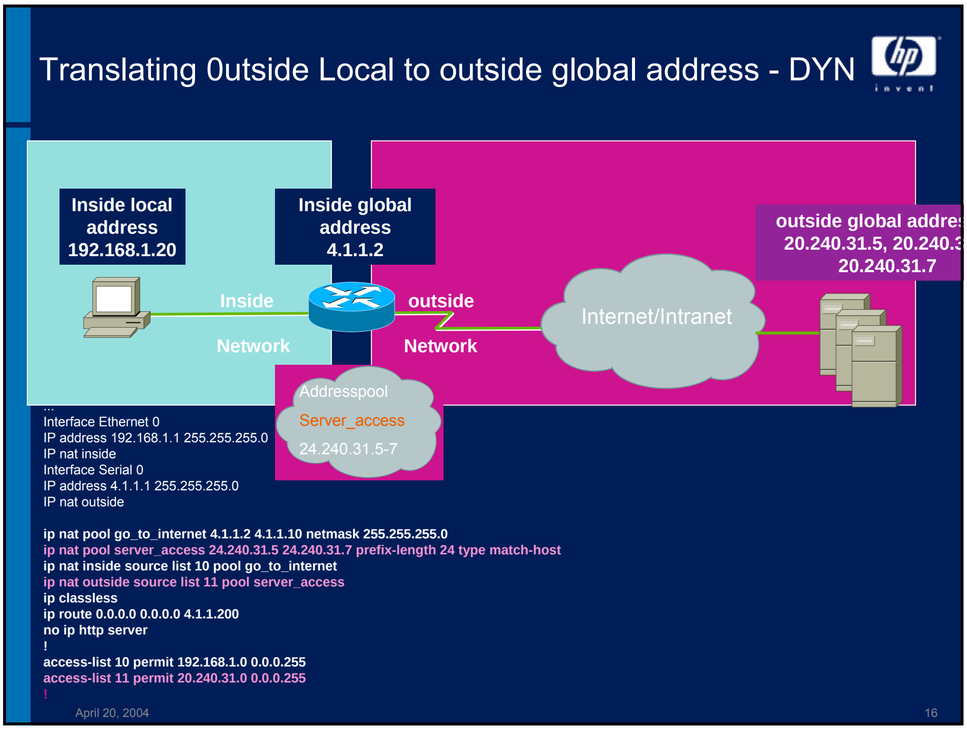


Translating IL to IG address – DYN - Overload

```
...
Interface Ethernet 0
IP address 192.168.1.1 255.255.255.0
IP nat inside
Interface Serial 0
IP address 4.1.1.1 255.255.255.0
IP nat outside

IP nat pool to_internet 4.1.1.2 4.1.1.10 prefix-length 24
IP nat inside source  list 10  pool  to_internet overload
IP access-list 10 permit 192.168.1.0 0.0.0.255
```

April 20, 2004

15

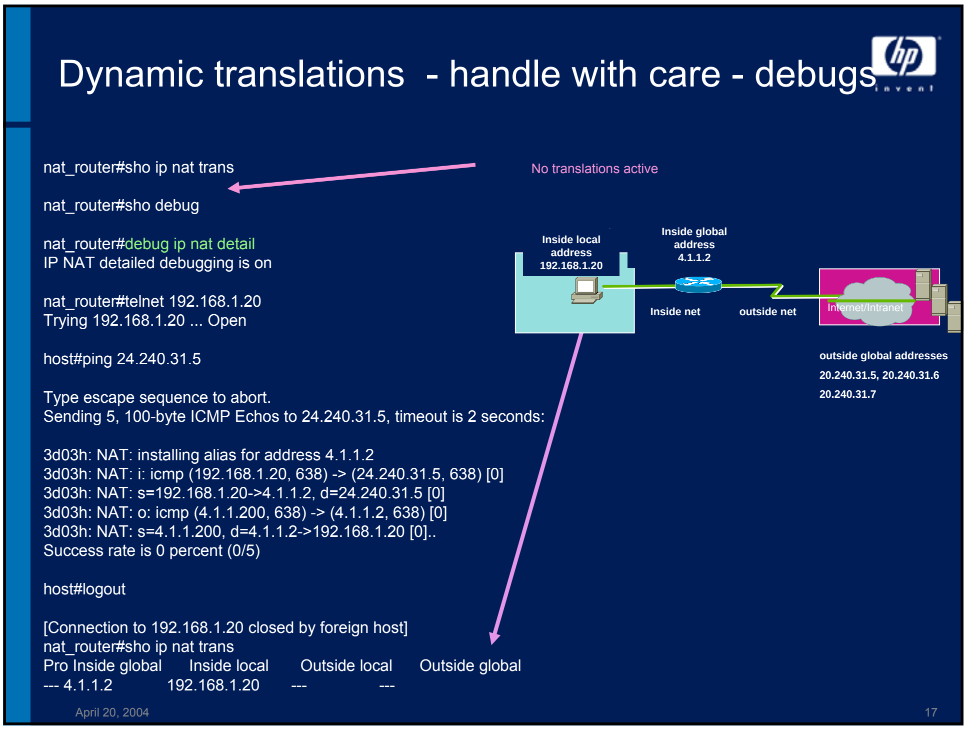


Translating 0utside Local to outside global address - DYN

```
...
Interface Ethernet 0
IP address 192.168.1.1 255.255.255.0
IP nat inside
Interface Serial 0
IP address 4.1.1.1 255.255.255.0
IP nat outside

ip nat pool go_to_internet 4.1.1.2 4.1.1.10 netmask 255.255.255.0
ip nat pool server_access 24.240.31.5 24.240.31.7 prefix-length 24 type match-host
ip nat inside source list 10 pool go_to_internet
ip nat outside source list 11 pool server_access
ip classless
ip route 0.0.0.0 0.0.0.0 4.1.1.200
no ip http server
!
access-list 10 permit 192.168.1.0 0.0.0.255
access-list 11 permit 20.240.31.0 0.0.0.255
!
```

April 20, 2004

16



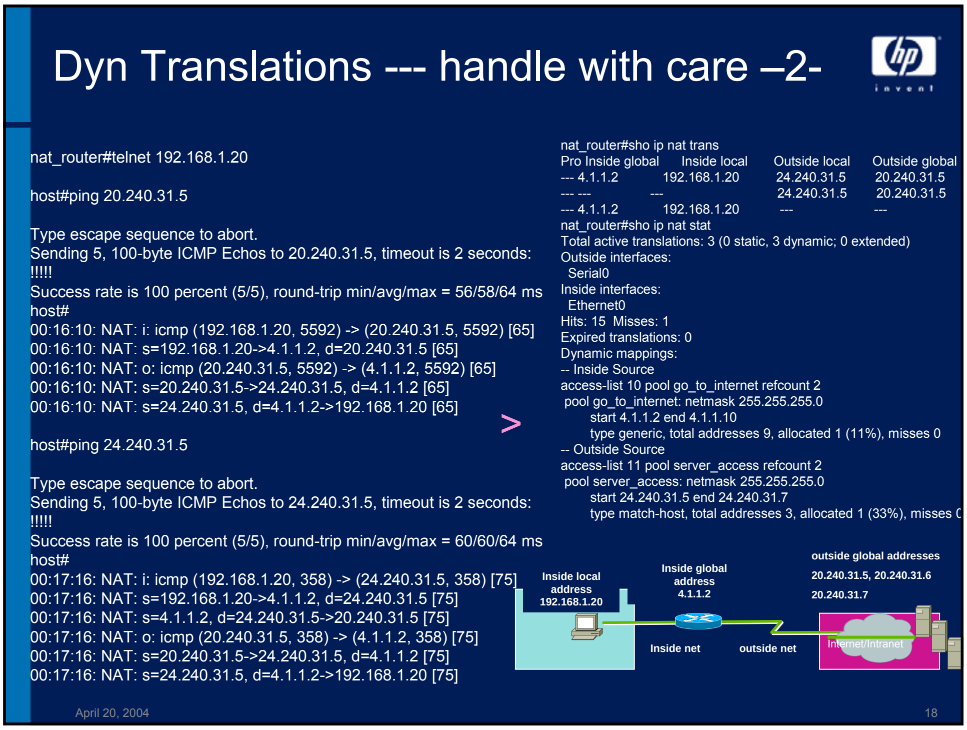
Dynamic translations - handle with care - debugs

```
nat_router#sho ip nat trans

nat_router#sho debug

nat_router#debug ip nat detail
IP NAT detailed debugging is on

nat_router#telnet 192.168.1.20
Trying 192.168.1.20 ... Open

host#ping 24.240.31.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 24.240.31.5, timeout is 2 seconds:

3d03h: NAT: installing alias for address 4.1.1.2
3d03h: NAT: i: icmp (192.168.1.20, 638) -> (24.240.31.5, 638) [0]
3d03h: NAT: s=192.168.1.20->4.1.1.2, d=24.240.31.5 [0]
3d03h: NAT: o: icmp (4.1.1.200, 638) -> (4.1.1.2, 638) [0]
3d03h: NAT: s=4.1.1.200, d=4.1.1.2->192.168.1.20 [0]..
Success rate is 0 percent (0/5)

host#logout

[Connection to 192.168.1.20 closed by foreign host]
nat_router#sho ip nat trans
Pro Inside global     Inside local      Outside local     Outside global
--- 4.1.1.2           192.168.1.20      ---               ---
```

No translations active

April 20, 2004

17



Dyn Translations --- handle with care –2-

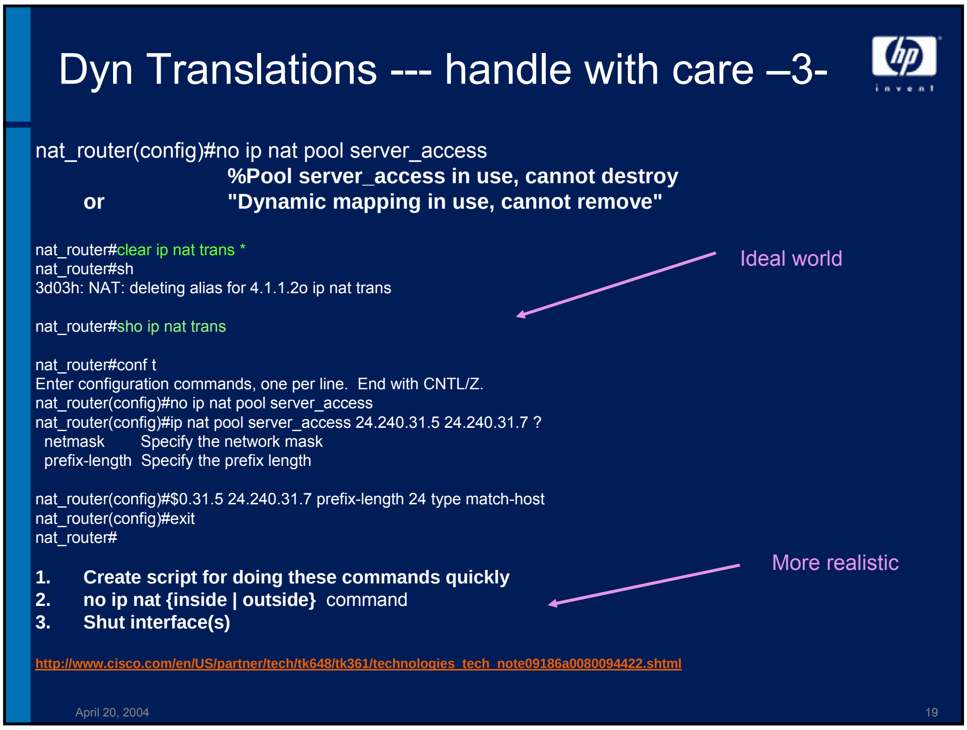
```
nat_router#telnet 192.168.1.20

host#ping 20.240.31.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.240.31.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/58/64 ms
host#
00:16:10: NAT: i: icmp (192.168.1.20, 5592) -> (20.240.31.5, 5592) [65]
00:16:10: NAT: s=192.168.1.20->4.1.1.2, d=20.240.31.5 [65]
00:16:10: NAT: o: icmp (20.240.31.5, 5592) -> (4.1.1.2, 5592) [65]
00:16:10: NAT: s=20.240.31.5->24.240.31.5, d=4.1.1.2 [65]
00:16:10: NAT: s=24.240.31.5, d=4.1.1.2->192.168.1.20 [65]

host#ping 24.240.31.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 24.240.31.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/60/64 ms
host#
00:17:16: NAT: i: icmp (192.168.1.20, 358) -> (24.240.31.5, 358) [75]
00:17:16: NAT: s=192.168.1.20->4.1.1.2, d=24.240.31.5 [75]
00:17:16: NAT: s=4.1.1.2, d=24.240.31.5->20.240.31.5 [75]
00:17:16: NAT: o: icmp (20.240.31.5, 358) -> (4.1.1.2, 358) [75]
00:17:16: NAT: s=20.240.31.5->24.240.31.5, d=4.1.1.2 [75]
00:17:16: NAT: s=24.240.31.5, d=4.1.1.2->192.168.1.20 [75]
```

>

```
nat_router#sho ip nat trans
Pro Inside global     Inside local      Outside local     Outside global
--- 4.1.1.2           192.168.1.20      24.240.31.5       20.240.31.5
--- ---               ---               24.240.31.5       20.240.31.5
--- 4.1.1.2           192.168.1.20      ---               ---
nat_router#sho ip nat stat
Total active translations: 3 (0 static, 3 dynamic; 0 extended)
Outside interfaces:
  Serial0
Inside interfaces:
  Ethernet0
Hits: 15  Misses: 1
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 10 pool go_to_internet refcount 2
 pool go_to_internet: netmask 255.255.255.0
        start 4.1.1.2 end 4.1.1.10
        type generic, total addresses 9, allocated 1 (11%), misses 0
-- Outside Source
access-list 11 pool server_access refcount 2
 pool server_access: netmask 255.255.255.0
        start 24.240.31.5 end 24.240.31.7
        type match-host, total addresses 3, allocated 1 (33%), misses 0
```

April 20, 2004

18



Dyn Translations --- handle with care –3-

```
nat_router(config)#no ip nat pool server_access
                      %Pool server_access in use, cannot destroy
      or              "Dynamic mapping in use, cannot remove"
```

```
nat_router#clear ip nat trans *
nat_router#sh
3d03h: NAT: deleting alias for 4.1.1.2o ip nat trans

nat_router#sho ip nat trans

nat_router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
nat_router(config)#no ip nat pool server_access
nat_router(config)#ip nat pool server_access 24.240.31.5 24.240.31.7 ?
  netmask        Specify the network mask
  prefix-length  Specify the prefix length

nat_router(config)#$0.31.5 24.240.31.7 prefix-length 24 type match-host
nat_router(config)#exit
nat_router#
```

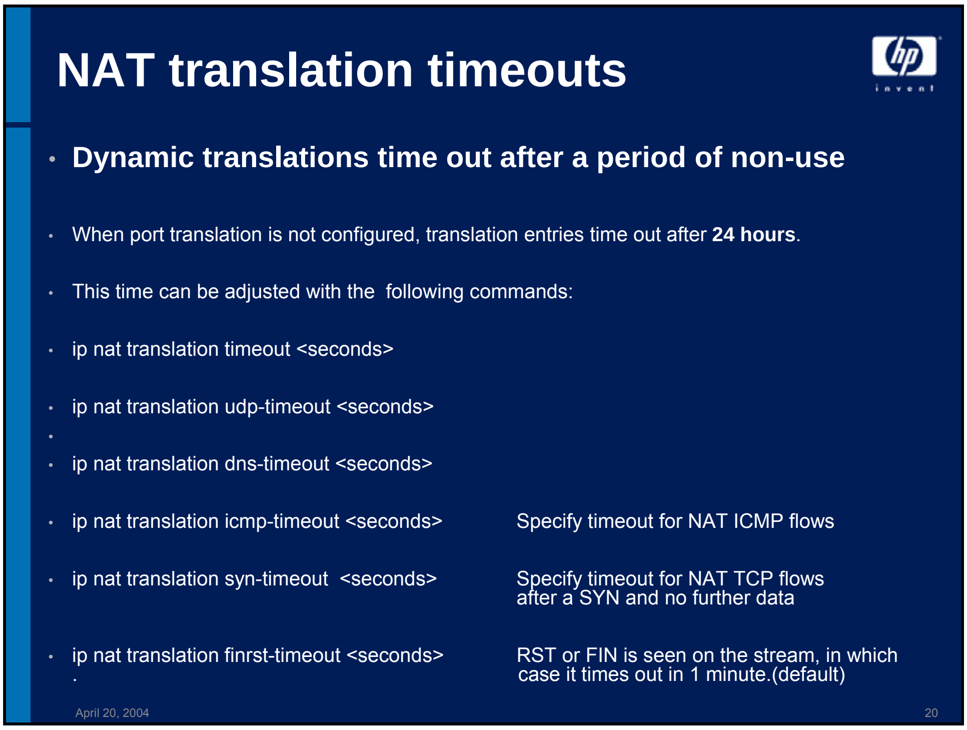
Ideal world

1. **Create script for doing these commands quickly**
2. **no ip nat {inside | outside}** command
3. **Shut interface(s)**

More realistic

http://www.cisco.com/en/US/partner/tech/tk648/tk361/technologies_tech_note09186a0080094422.shtml

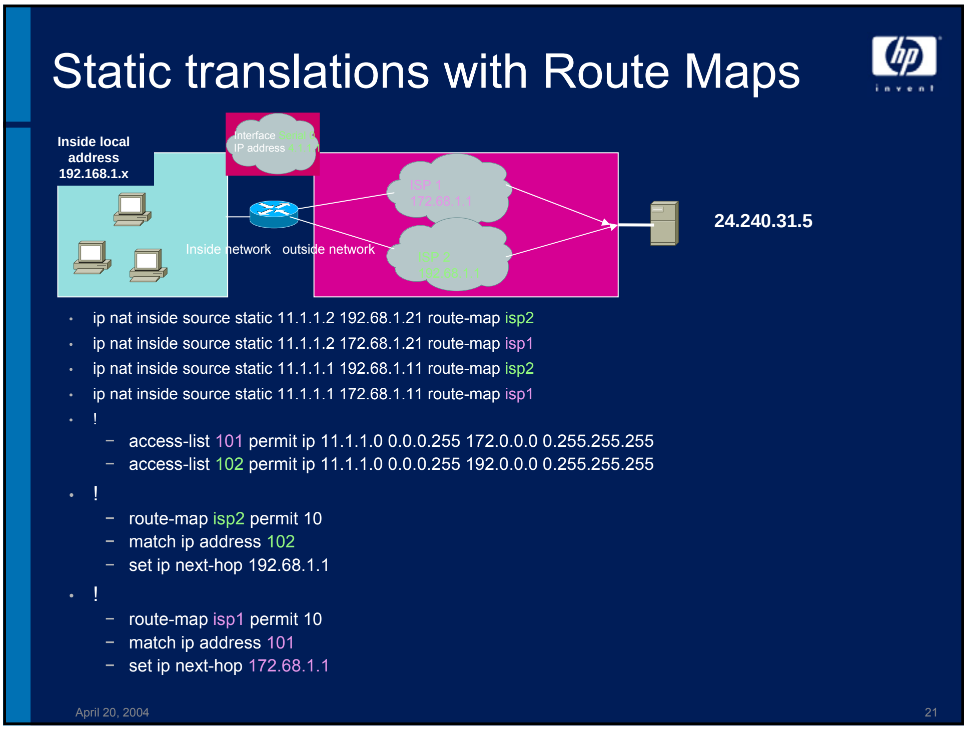
April 20, 2004 19



NAT translation timeouts

- **Dynamic translations time out after a period of non-use**
- When port translation is not configured, translation entries time out after **24 hours**.
- This time can be adjusted with the following commands:
- ip nat translation timeout <seconds>
- ip nat translation udp-timeout <seconds>
-
- ip nat translation dns-timeout <seconds>
- ip nat translation icmp-timeout <seconds> Specify timeout for NAT ICMP flows
- ip nat translation syn-timeout <seconds> Specify timeout for NAT TCP flows after a SYN and no further data
- ip nat translation finrst-timeout <seconds> RST or FIN is seen on the stream, in which case it times out in 1 minute.(default)
  .

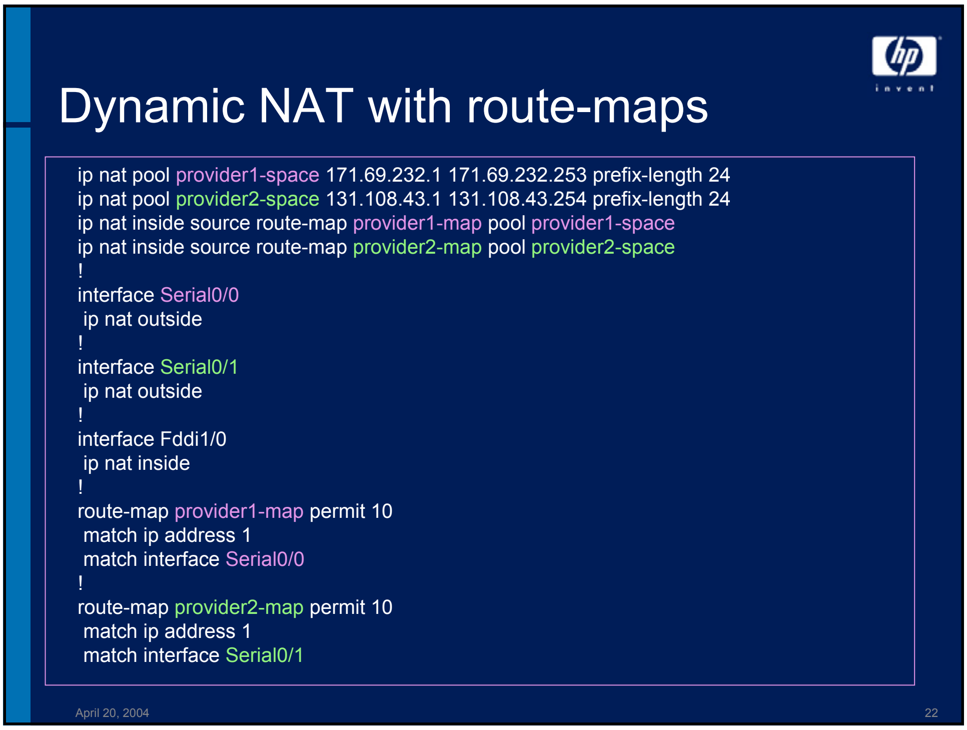
April 20, 2004 20



Static translations with Route Maps

- ip nat inside source static 11.1.1.2 192.68.1.21 route-map isp2
- ip nat inside source static 11.1.1.2 172.68.1.21 route-map isp1
- ip nat inside source static 11.1.1.1 192.68.1.11 route-map isp2
- ip nat inside source static 11.1.1.1 172.68.1.11 route-map isp1
- !
  - access-list 101 permit ip 11.1.1.0 0.0.0.255 172.0.0.0 0.255.255.255
  - access-list 102 permit ip 11.1.1.0 0.0.0.255 192.0.0.0 0.255.255.255
- !
  - route-map isp2 permit 10
  - match ip address 102
  - set ip next-hop 192.68.1.1
- !
  - route-map isp1 permit 10
  - match ip address 101
  - set ip next-hop 172.68.1.1

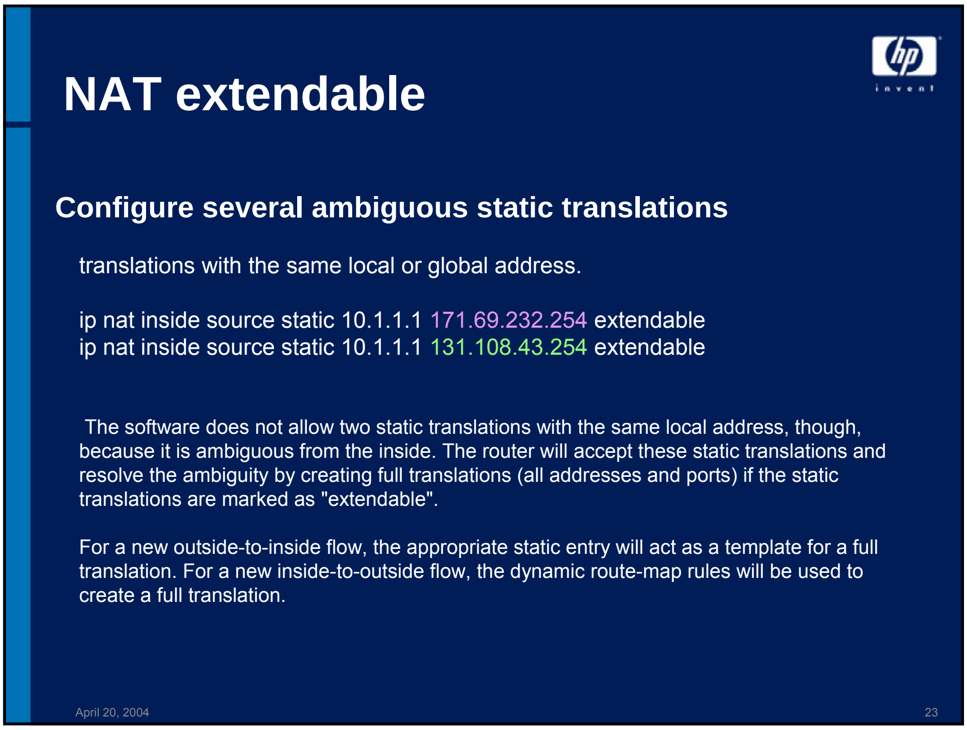
April 20, 2004 21



Dynamic NAT with route-maps

```
ip nat pool provider1-space 171.69.232.1 171.69.232.253 prefix-length 24
ip nat pool provider2-space 131.108.43.1 131.108.43.254 prefix-length 24
ip nat inside source route-map provider1-map pool provider1-space
ip nat inside source route-map provider2-map pool provider2-space
!
interface Serial0/0
 ip nat outside
!
interface Serial0/1
 ip nat outside
!
interface Fddi1/0
 ip nat inside
!
route-map provider1-map permit 10
 match ip address 1
 match interface Serial0/0
!
route-map provider2-map permit 10
 match ip address 1
 match interface Serial0/1
```

April 20, 2004 22



NAT extendable

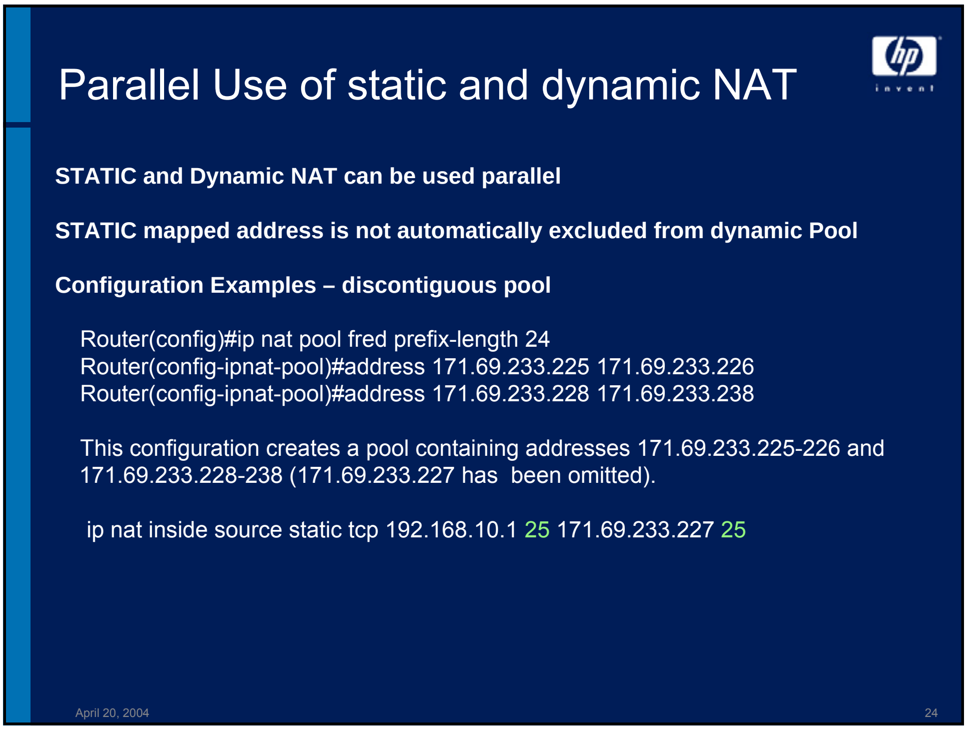
Configure several ambiguous static translations

translations with the same local or global address.

```
ip nat inside source static 10.1.1.1 171.69.232.254 extendable
ip nat inside source static 10.1.1.1 131.108.43.254 extendable
```

The software does not allow two static translations with the same local address, though, because it is ambiguous from the inside. The router will accept these static translations and resolve the ambiguity by creating full translations (all addresses and ports) if the static translations are marked as "extendable".

For a new outside-to-inside flow, the appropriate static entry will act as a template for a full translation. For a new inside-to-outside flow, the dynamic route-map rules will be used to create a full translation.



Parallel Use of static and dynamic NAT

STATIC and Dynamic NAT can be used parallel

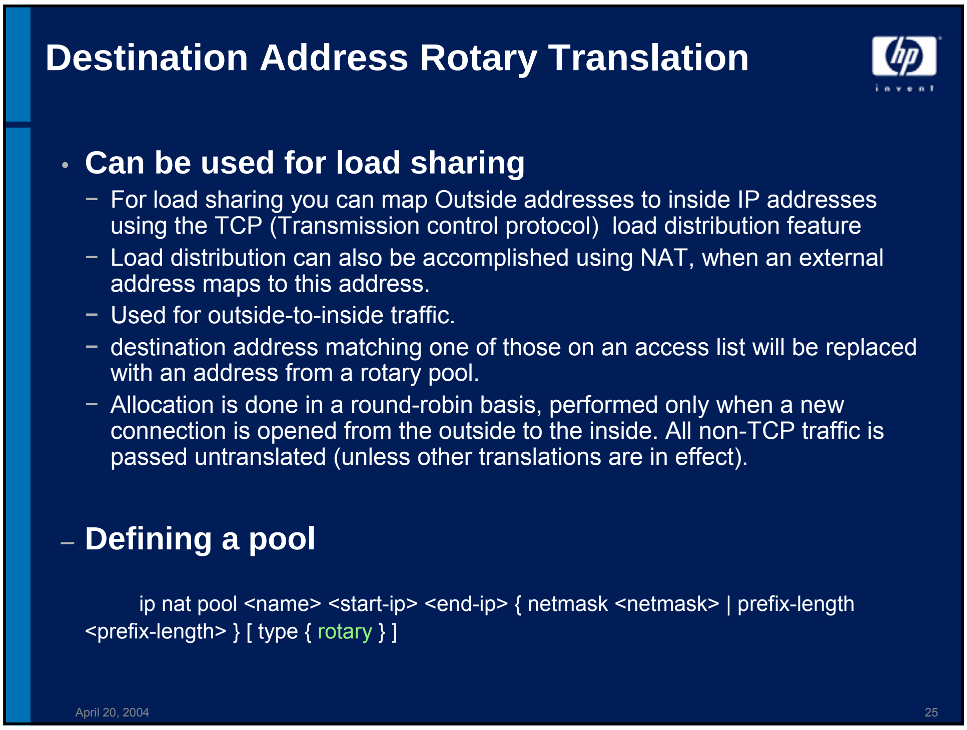
STATIC mapped address is not automatically excluded from dynamic Pool

Configuration Examples – discontiguous pool

```
Router(config)#ip nat pool fred prefix-length 24
Router(config-ipnat-pool)#address 171.69.233.225 171.69.233.226
Router(config-ipnat-pool)#address 171.69.233.228 171.69.233.238
```

This configuration creates a pool containing addresses 171.69.233.225-226 and 171.69.233.228-238 (171.69.233.227 has been omitted).

```
ip nat inside source static tcp 192.168.10.1 25 171.69.233.227 25
```



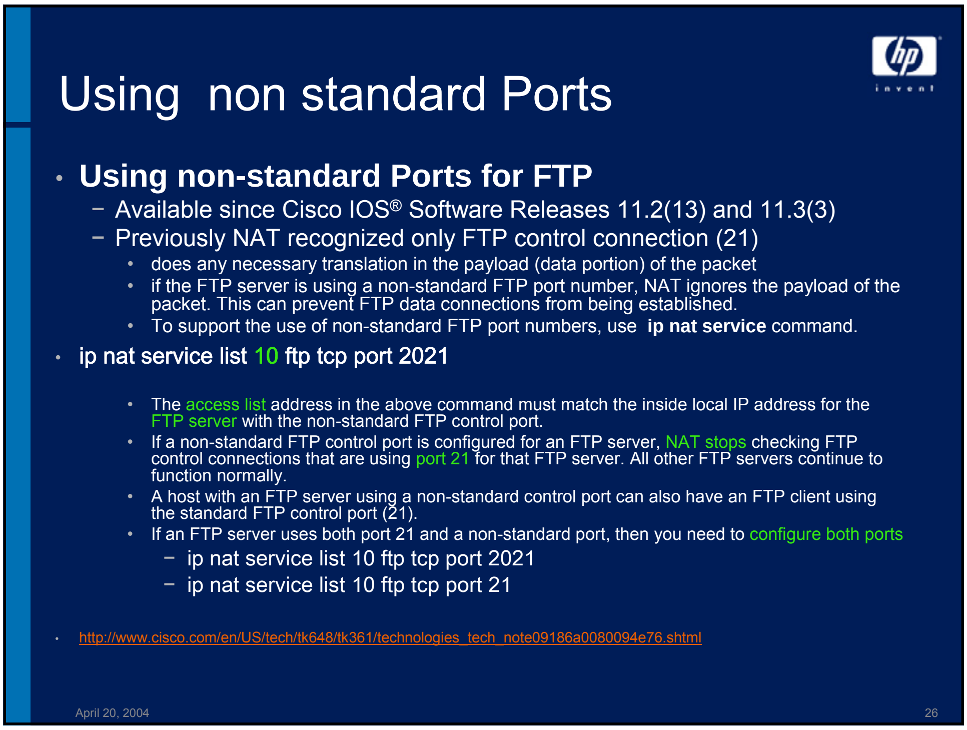
Destination Address Rotary Translation

- **Can be used for load sharing**
  - For load sharing you can map Outside addresses to inside IP addresses using the TCP (Transmission control protocol) load distribution feature
  - Load distribution can also be accomplished using NAT, when an external address maps to this address.
  - Used for outside-to-inside traffic.
  - destination address matching one of those on an access list will be replaced with an address from a rotary pool.
  - Allocation is done in a round-robin basis, performed 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).

– **Defining a pool**

ip nat pool <name> <start-ip> <end-ip> { netmask <netmask> | prefix-length <prefix-length> } [type { rotary }]

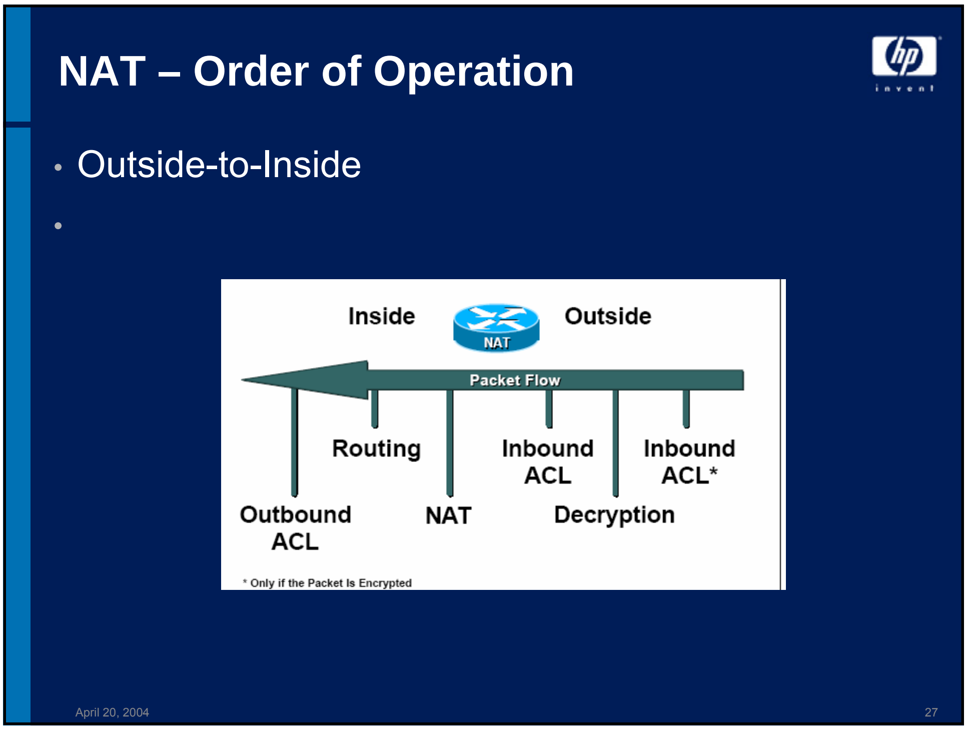
April 20, 2004 25



Using non standard Ports

- **Using non-standard Ports for FTP**
  - Available since Cisco IOS® Software Releases 11.2(13) and 11.3(3)
  - Previously NAT recognized only FTP control connection (21)
    - does any necessary translation in the payload (data portion) of the packet
    - if the FTP server is using a non-standard FTP port number, NAT ignores the payload of the packet. This can prevent FTP data connections from being established.
    - To support the use of non-standard FTP port numbers, use **ip nat service** command.
- ip nat service list 10 ftp tcp port 2021
    - The access list address in the above command must match the inside local IP address for the FTP server with the non-standard FTP control port.
    - If a non-standard FTP control port is configured for an FTP server, NAT stops checking FTP control connections that are using port 21 for that FTP server. All other FTP servers continue to function normally.
    - A host with an FTP server using a non-standard control port can also have an FTP client using the standard FTP control port (21).
    - If an FTP server uses both port 21 and a non-standard port, then you need to configure both ports
      - ip nat service list 10 ftp tcp port 2021
      - ip nat service list 10 ftp tcp port 21
- http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094e76.shtml

April 20, 2004 26



NAT – Order of Operation

- Outside-to-Inside
-

Inside

NAT

Outside

Packet Flow

Routing

Inbound ACL

Inbound ACL*

Outbound ACL

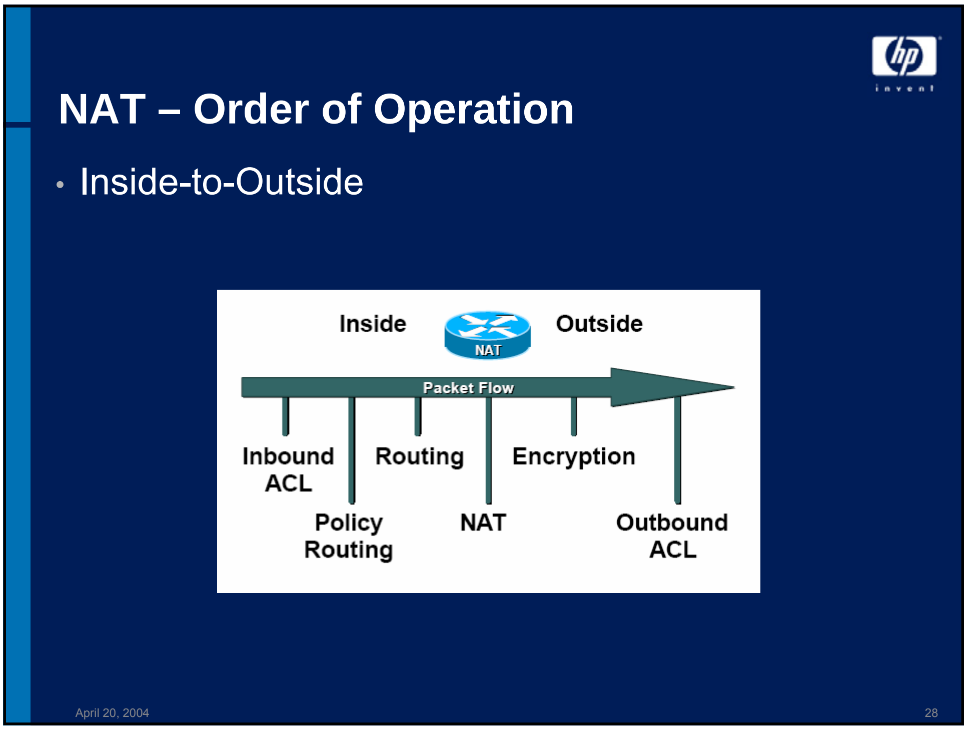
NAT

Decryption

* Only if the Packet Is Encrypted

April 20, 2004

27



NAT – Order of Operation

- Inside-to-Outside

Inside

NAT

Outside

Packet Flow

Inbound ACL

Routing

Encryption

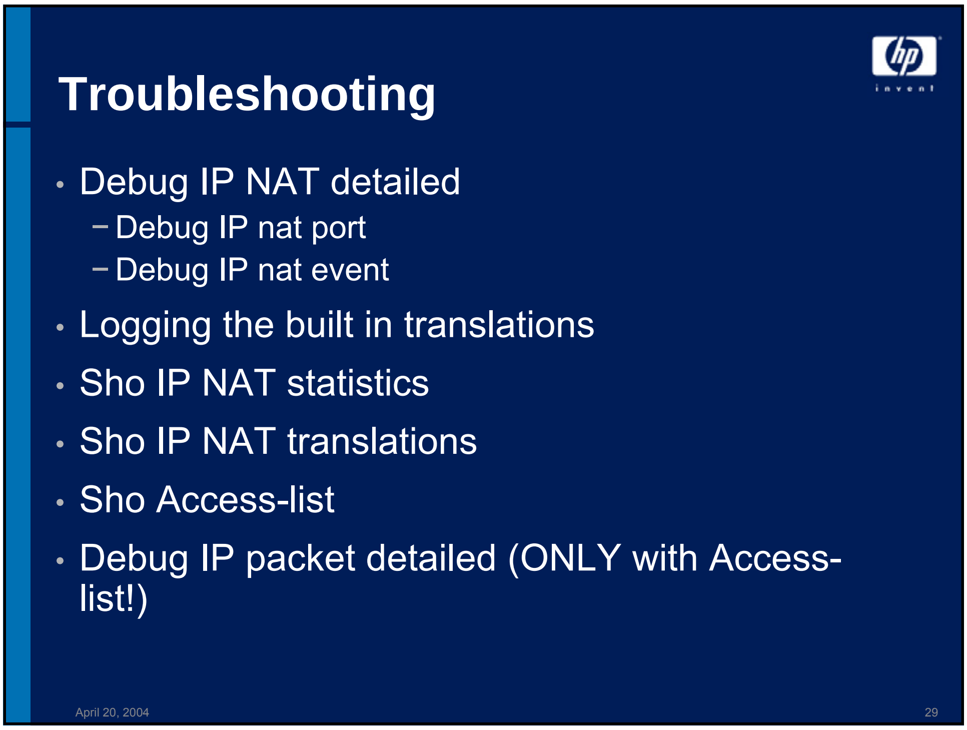
Policy Routing

NAT

Outbound ACL

April 20, 2004

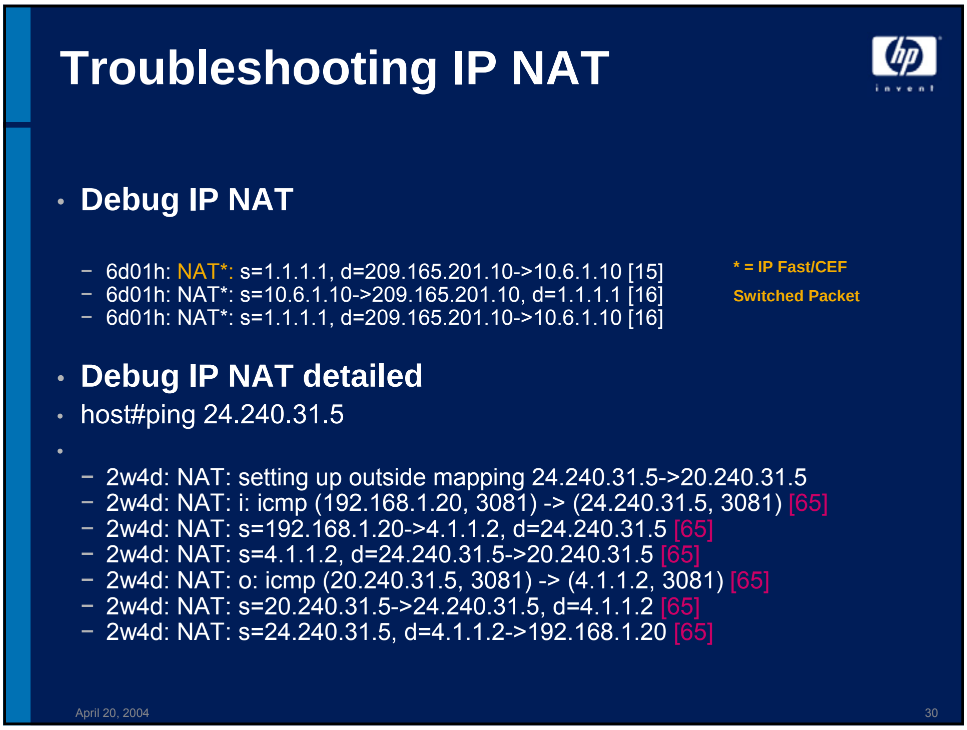
28



Troubleshooting

- Debug IP NAT detailed
  - Debug IP nat port
  - Debug IP nat event
- Logging the built in translations
- Sho IP NAT statistics
- Sho IP NAT translations
- Sho Access-list
- Debug IP packet detailed (ONLY with Access-list!)

April 20, 2004 29



Troubleshooting IP NAT

- **Debug IP NAT**

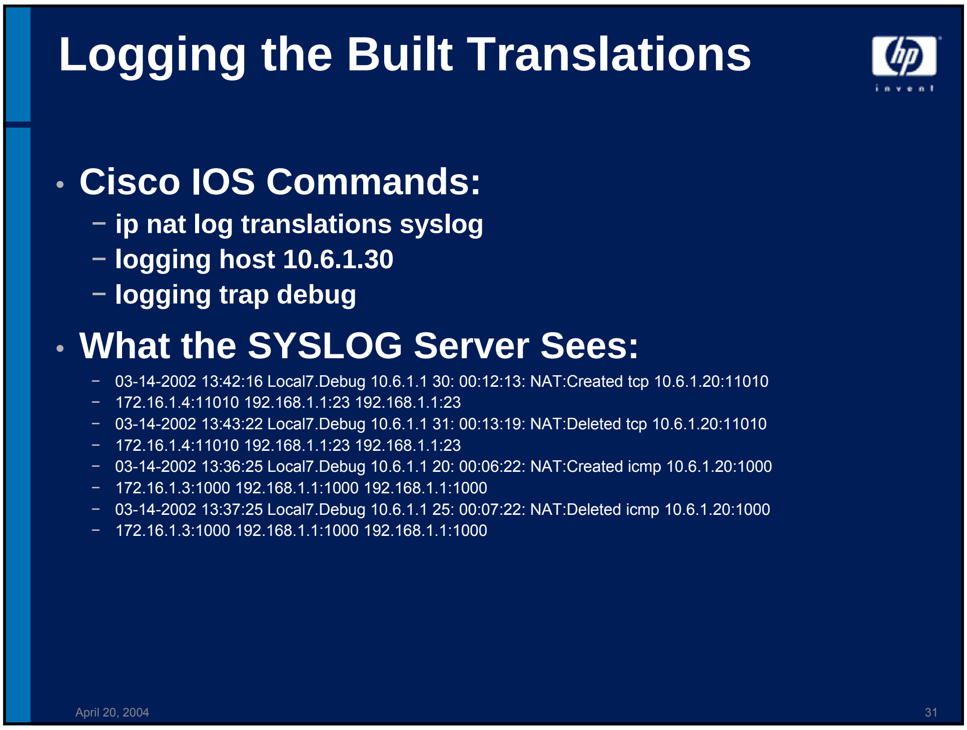
```
– 6d01h: NAT*: s=1.1.1.1, d=209.165.201.10->10.6.1.10 [15]
– 6d01h: NAT*: s=10.6.1.10->209.165.201.10, d=1.1.1.1 [16]
– 6d01h: NAT*: s=1.1.1.1, d=209.165.201.10->10.6.1.10 [16]
```

*** = IP Fast/CEF Switched Packet**

- **Debug IP NAT detailed**
- host#ping 24.240.31.5
-

```
– 2w4d: NAT: setting up outside mapping 24.240.31.5->20.240.31.5
– 2w4d: NAT: i: icmp (192.168.1.20, 3081) -> (24.240.31.5, 3081) [65]
– 2w4d: NAT: s=192.168.1.20->4.1.1.2, d=24.240.31.5 [65]
– 2w4d: NAT: s=4.1.1.2, d=24.240.31.5->20.240.31.5 [65]
– 2w4d: NAT: o: icmp (20.240.31.5, 3081) -> (4.1.1.2, 3081) [65]
– 2w4d: NAT: s=20.240.31.5->24.240.31.5, d=4.1.1.2 [65]
– 2w4d: NAT: s=24.240.31.5, d=4.1.1.2->192.168.1.20 [65]
```

April 20, 2004 30

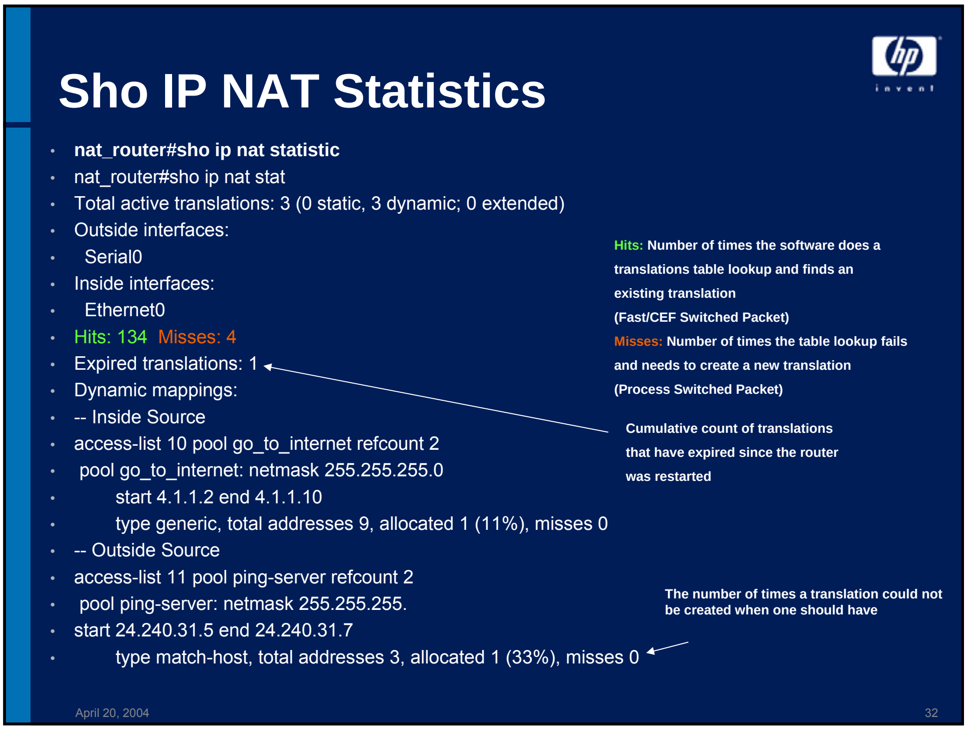


Logging the Built Translations

- Cisco IOS Commands:
  - ip nat log translations syslog
  - logging host 10.6.1.30
  - logging trap debug
- What the SYSLOG Server Sees:

```
– 03-14-2002 13:42:16 Local7.Debug 10.6.1.1 30: 00:12:13: NAT:Created tcp 10.6.1.20:11010
– 172.16.1.4:11010 192.168.1.1:23 192.168.1.1:23
– 03-14-2002 13:43:22 Local7.Debug 10.6.1.1 31: 00:13:19: NAT:Deleted tcp 10.6.1.20:11010
– 172.16.1.4:11010 192.168.1.1:23 192.168.1.1:23
– 03-14-2002 13:36:25 Local7.Debug 10.6.1.1 20: 00:06:22: NAT:Created icmp 10.6.1.20:1000
– 172.16.1.3:1000 192.168.1.1:1000 192.168.1.1:1000
– 03-14-2002 13:37:25 Local7.Debug 10.6.1.1 25: 00:07:22: NAT:Deleted icmp 10.6.1.20:1000
– 172.16.1.3:1000 192.168.1.1:1000 192.168.1.1:1000
```

April 20, 2004 31



Sho IP NAT Statistics

```
• nat_router#sho ip nat statistic
• nat_router#sho ip nat stat
• Total active translations: 3 (0 static, 3 dynamic; 0 extended)
• Outside interfaces:
•   Serial0
• Inside interfaces:
•   Ethernet0
• Hits: 134  Misses: 4
• Expired translations: 1
• Dynamic mappings:
• -- Inside Source
• access-list 10 pool go_to_internet refcount 2
•  pool go_to_internet: netmask 255.255.255.0
•        start 4.1.1.2 end 4.1.1.10
•        type generic, total addresses 9, allocated 1 (11%), misses 0
• -- Outside Source
• access-list 11 pool ping-server refcount 2
•  pool ping-server: netmask 255.255.255.
• start 24.240.31.5 end 24.240.31.7
•        type match-host, total addresses 3, allocated 1 (33%), misses 0
```

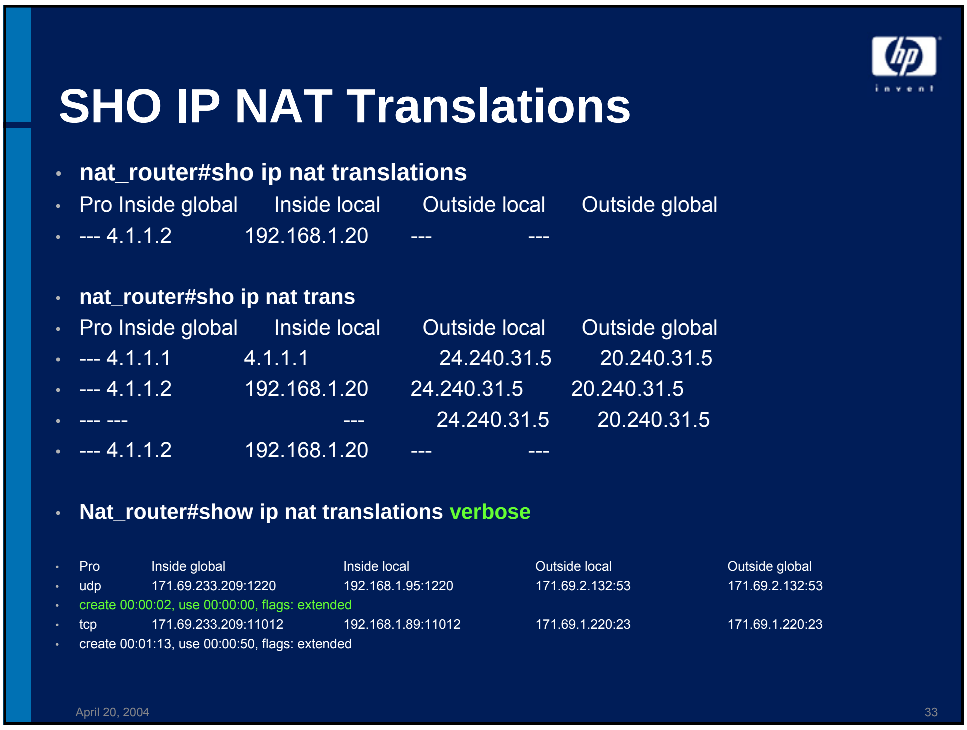
Hits: Number of times the software does a translations table lookup and finds an existing translation (Fast/CEF Switched Packet)

Misses: Number of times the table lookup fails and needs to create a new translation (Process Switched Packet)

Cumulative count of translations that have expired since the router was restarted

The number of times a translation could not be created when one should have

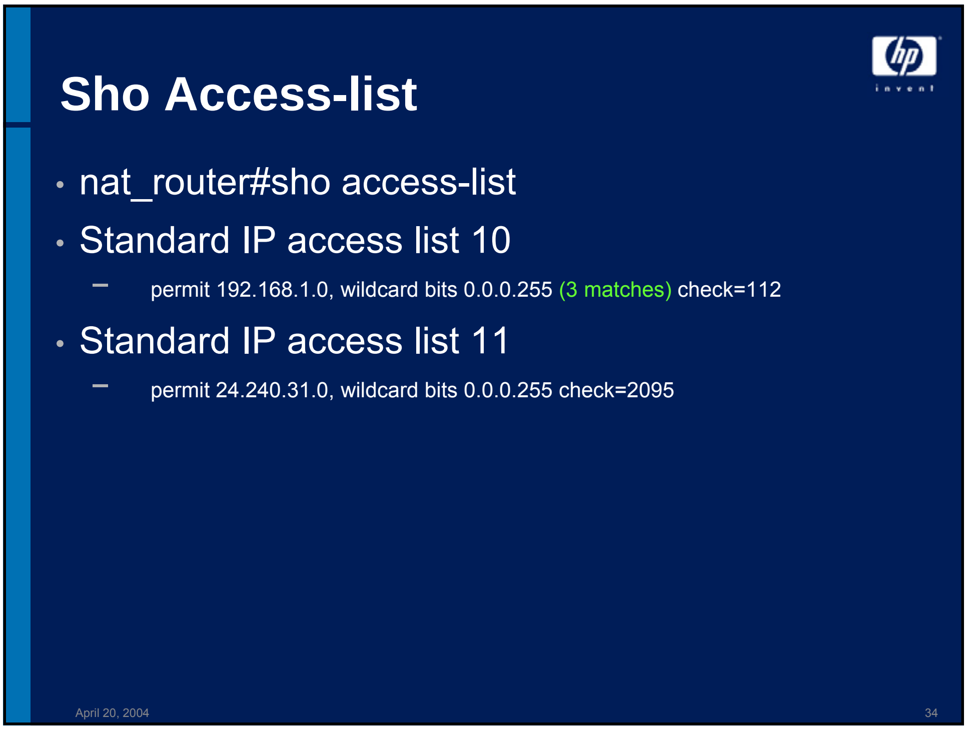
April 20, 2004 32



SHO IP NAT Translations

```
• nat_router#sho ip nat translations
• Pro Inside global     Inside local     Outside local     Outside global
• --- 4.1.1.2           192.168.1.20     ---               ---

• nat_router#sho ip nat trans
• Pro Inside global     Inside local     Outside local     Outside global
• --- 4.1.1.1           4.1.1.1             24.240.31.5       20.240.31.5
• --- 4.1.1.2           192.168.1.20     24.240.31.5       20.240.31.5
• --- ---                          ---      24.240.31.5       20.240.31.5
• --- 4.1.1.2           192.168.1.20     ---               ---

• Nat_router#show ip nat translations verbose

• Pro     Inside global          Inside local          Outside local       Outside global
• udp     171.69.233.209:1220    192.168.1.95:1220     171.69.2.132:53     171.69.2.132:53
• create 00:00:02, use 00:00:00, flags: extended
• tcp     171.69.233.209:11012   192.168.1.89:11012    171.69.1.220:23     171.69.1.220:23
• create 00:01:13, use 00:00:50, flags: extended
```

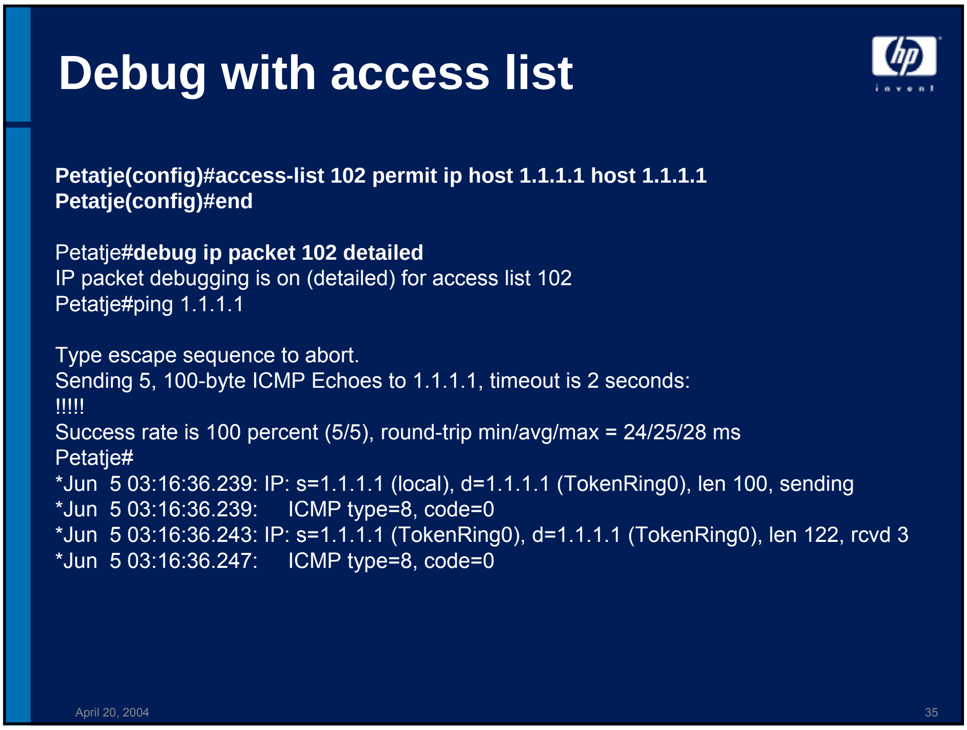
April 20, 2004 33



Sho Access-list

- nat_router#sho access-list
- Standard IP access list 10
  - permit 192.168.1.0, wildcard bits 0.0.0.255 (3 matches) check=112
- Standard IP access list 11
  - permit 24.240.31.0, wildcard bits 0.0.0.255 check=2095

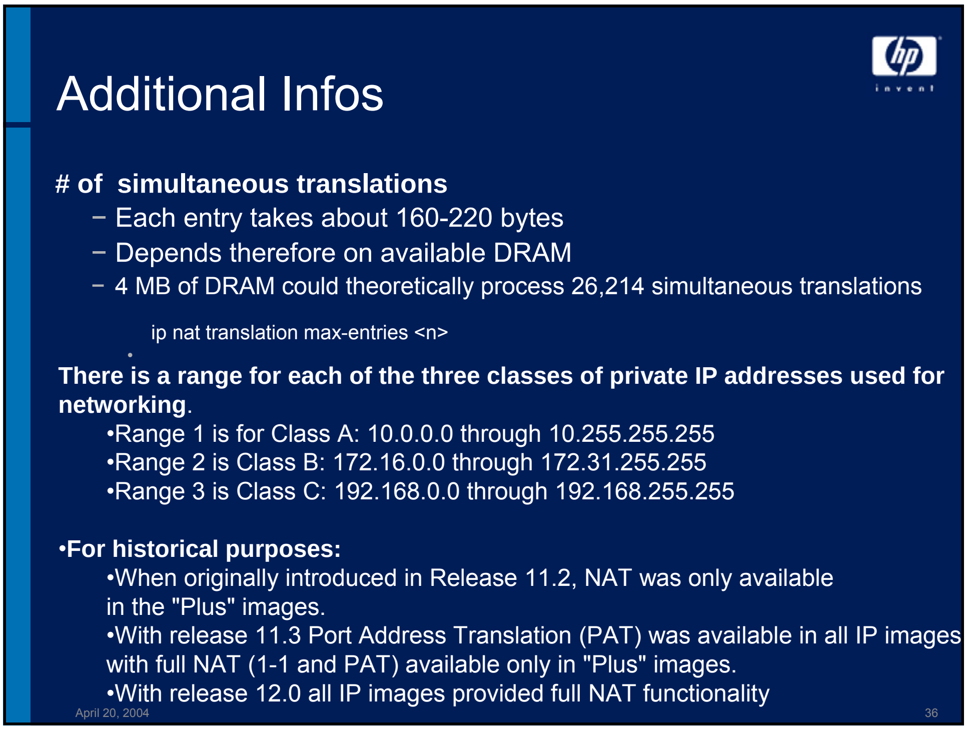
April 20, 2004 34



Debug with access list

```
Petatje(config)#access-list 102 permit ip host 1.1.1.1 host 1.1.1.1
Petatje(config)#end

Petatje#debug ip packet 102 detailed
IP packet debugging is on (detailed) for access list 102
Petatje#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/25/28 ms
Petatje#
*Jun  5 03:16:36.239: IP: s=1.1.1.1 (local), d=1.1.1.1 (TokenRing0), len 100, sending
*Jun  5 03:16:36.239:     ICMP type=8, code=0
*Jun  5 03:16:36.243: IP: s=1.1.1.1 (TokenRing0), d=1.1.1.1 (TokenRing0), len 122, rcvd 3
*Jun  5 03:16:36.247:     ICMP type=8, code=0
```

April 20, 2004 35



Additional Infos

# of simultaneous translations

- Each entry takes about 160-220 bytes
- Depends therefore on available DRAM
- 4 MB of DRAM could theoretically process 26,214 simultaneous translations

```
ip nat translation max-entries <n>
```

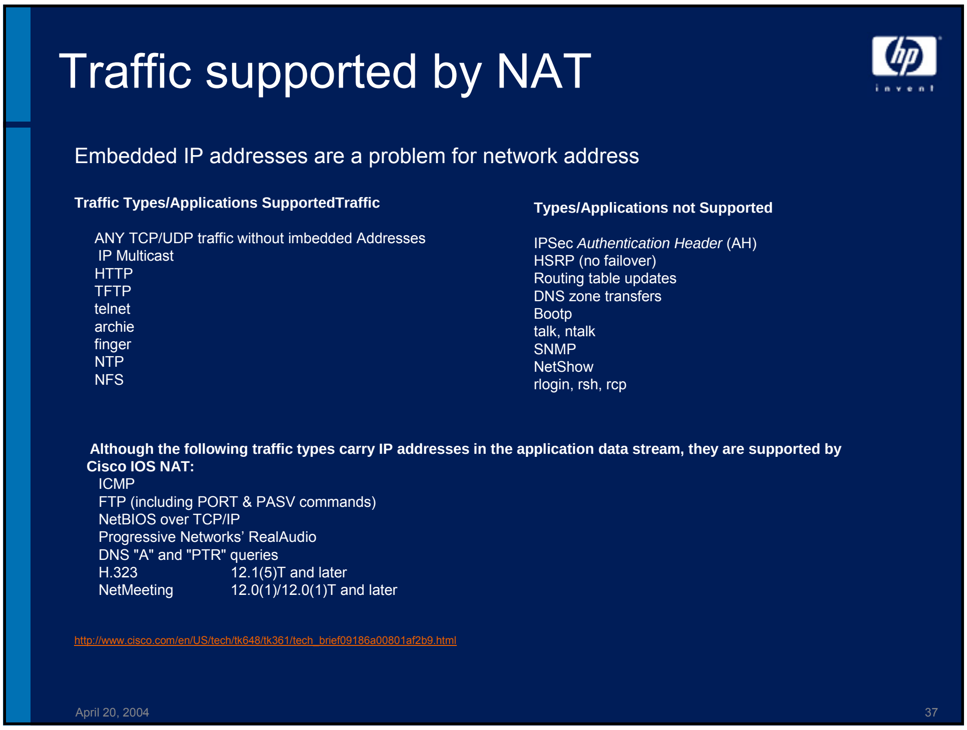
There is a range for each of the three classes of private IP addresses used for networking.

•Range 1 is for Class A: 10.0.0.0 through 10.255.255.255
•Range 2 is Class B: 172.16.0.0 through 172.31.255.255
•Range 3 is Class C: 192.168.0.0 through 192.168.255.255

•For historical purposes:

•When originally introduced in Release 11.2, NAT was only available in the "Plus" images.
•With release 11.3 Port Address Translation (PAT) was available in all IP images with full NAT (1-1 and PAT) available only in "Plus" images.
•With release 12.0 all IP images provided full NAT functionality

April 20, 2004 36



Traffic supported by NAT

Embedded IP addresses are a problem for network address

Traffic Types/Applications SupportedTraffic

ANY TCP/UDP traffic without imbedded Addresses
IP Multicast
HTTP
TFTP
telnet
archie
finger
NTP
NFS

Types/Applications not Supported

IPSec *Authentication Header* (AH)
HSRP (no failover)
Routing table updates
DNS zone transfers
Bootp
talk, ntalk
SNMP
NetShow
rlogin, rsh, rcp

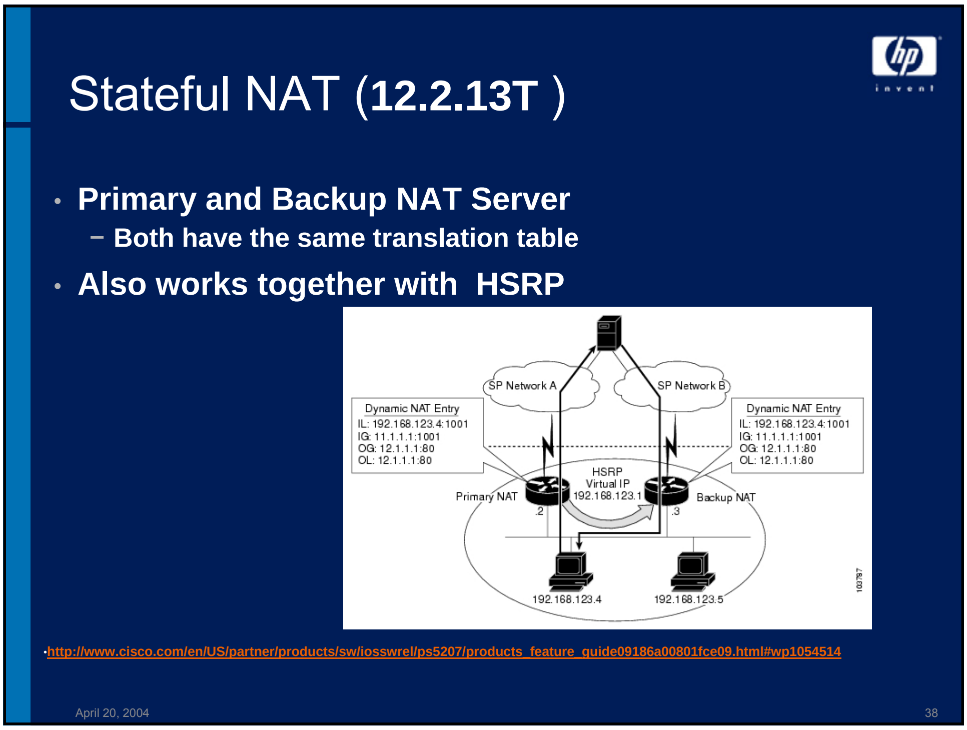
Although the following traffic types carry IP addresses in the application data stream, they are supported by Cisco IOS NAT:

ICMP
FTP (including PORT & PASV commands)
NetBIOS over TCP/IP
Progressive Networks' RealAudio
DNS "A" and "PTR" queries

H.323	12.1(5)T and later
NetMeeting	12.0(1)/12.0(1)T and later

http://www.cisco.com/en/US/tech/tk648/tk361/tech_brief09186a00801af2b9.html

April 20, 2004 37

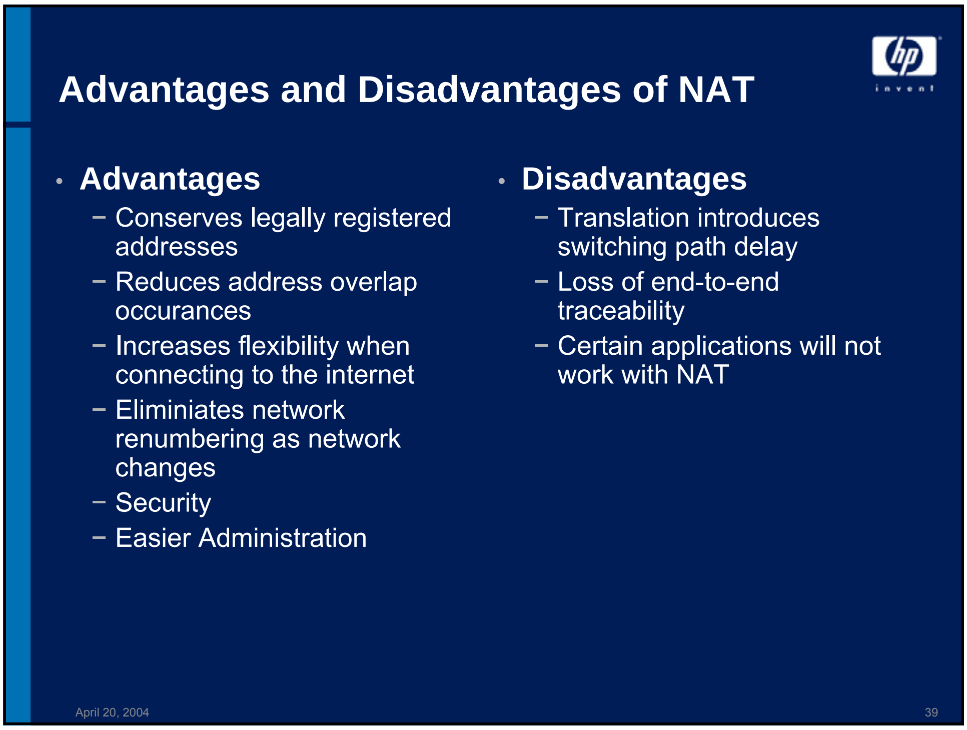


Stateful NAT (12.2.13T)

- **Primary and Backup NAT Server**
  - **Both have the same translation table**
- **Also works together with HSRP**

•http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_feature_guide09186a00801fce09.html#wp1054514

April 20, 2004 38



Advantages and Disadvantages of NAT

- **Advantages**
  - Conserves legally registered addresses
  - Reduces address overlap occurances
  - Increases flexibility when connecting to the internet
  - Eliminiates network renumbering as network changes
  - Security
  - Easier Administration
- **Disadvantages**
  - Translation introduces switching path delay
  - Loss of end-to-end traceability
  - Certain applications will not work with NAT

April 20, 2004

39