Network Address Translation

Session 109

Laura Jeanne Knapp
Network Consultant
1-919-224-2205
Laura@lauraknapp.com
www.lauraknapp.com

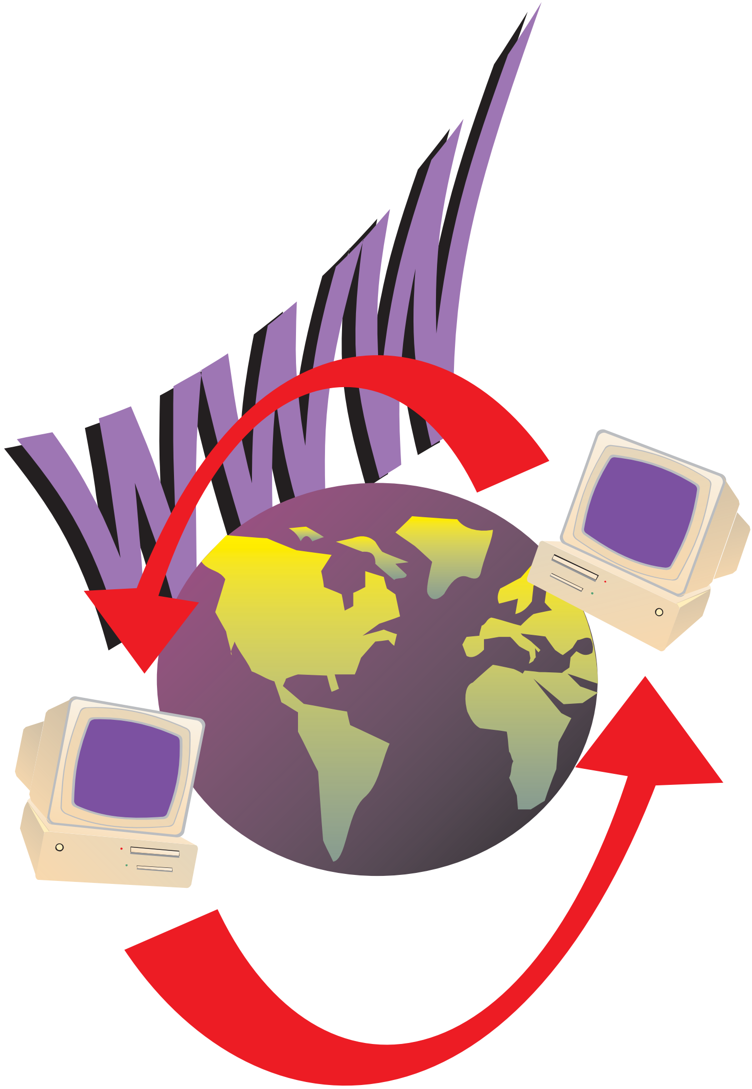
Evolving System

Concepts of NAT (Network Address Translation) and PAT (Port Address Translation)

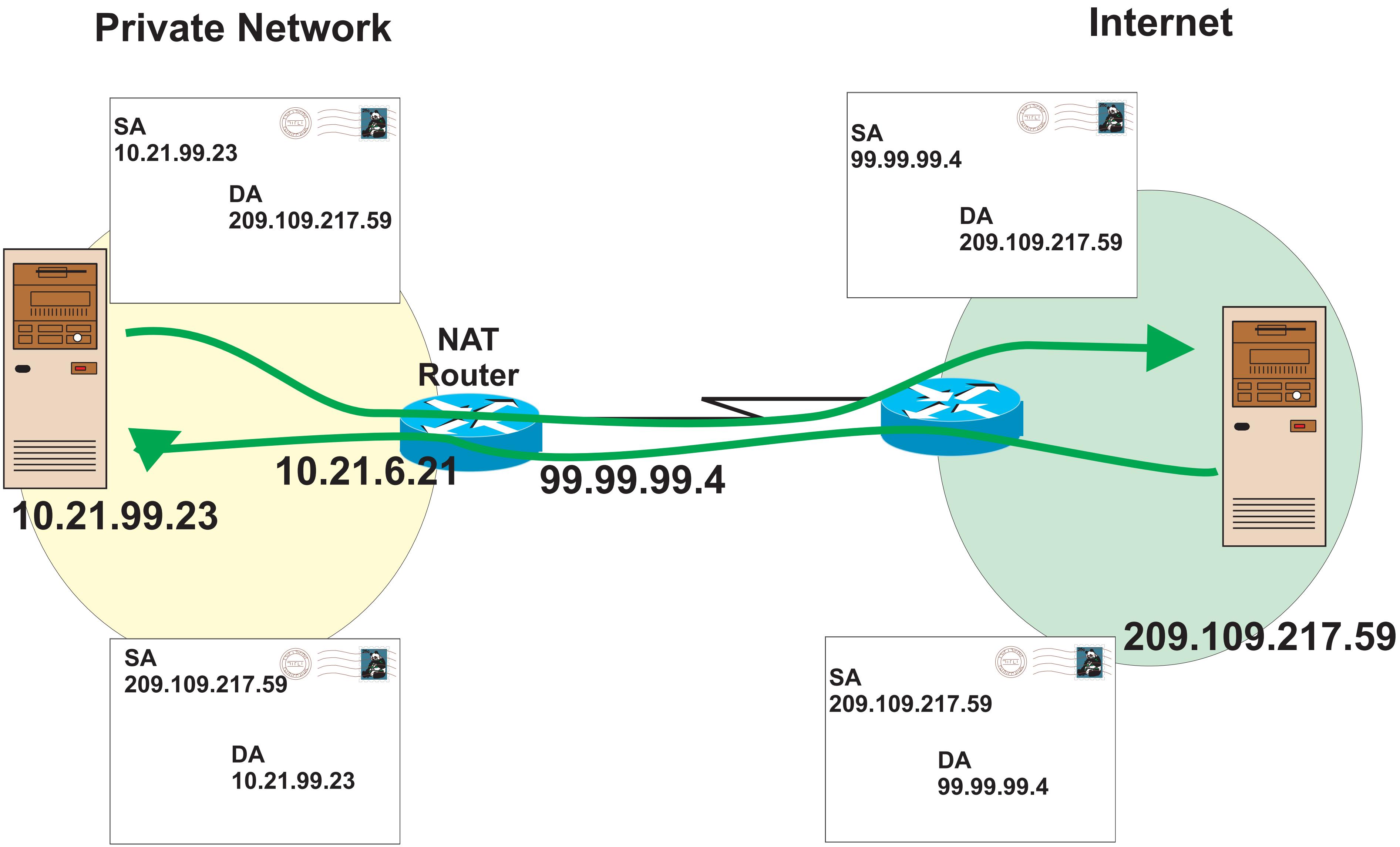
Virtual Private Networks Considerations

Other Considerations

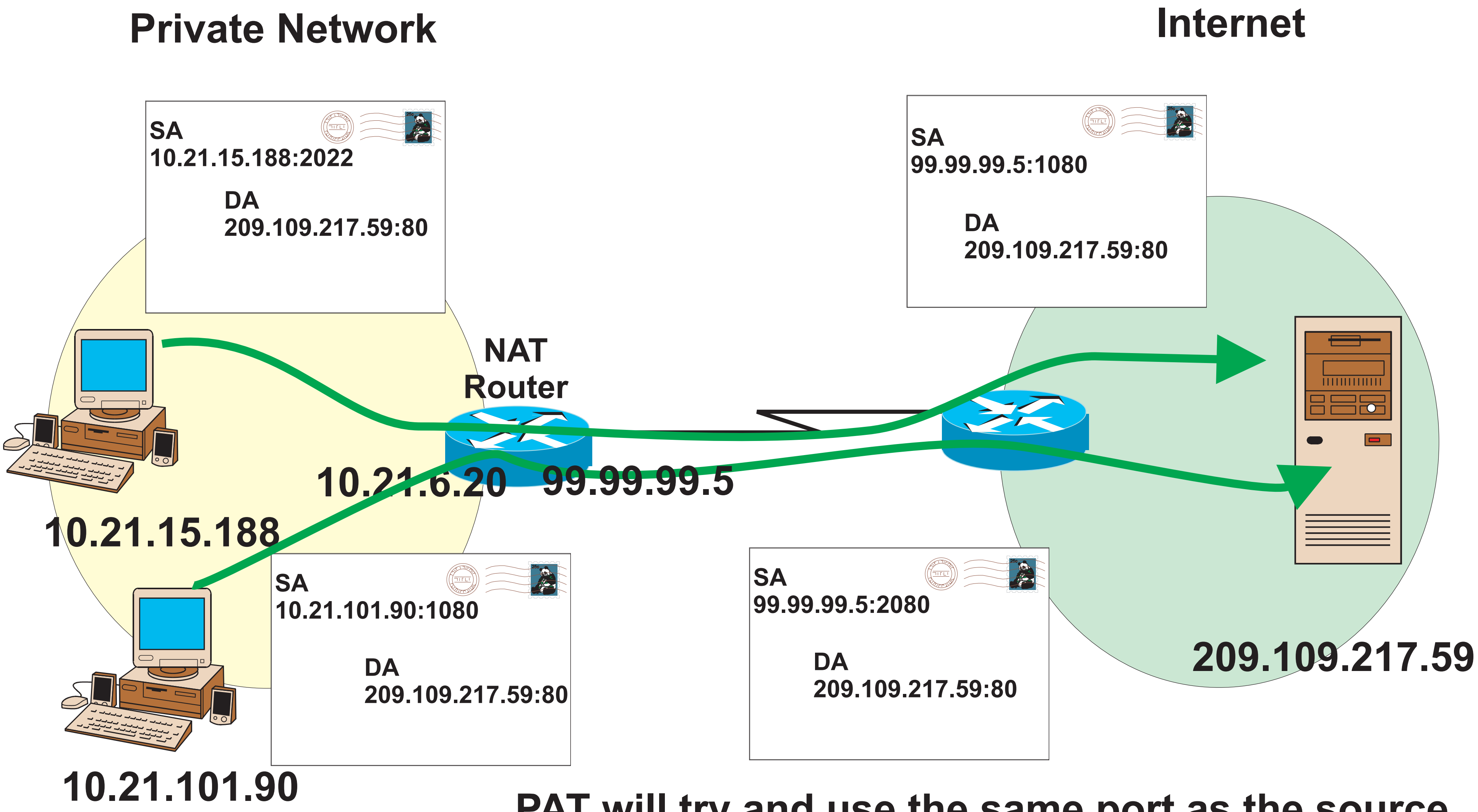
Summary



Network Address Translation in a Nutshell



Port Address Translation (PAT) in a Nutshell



Private Network

Internet

SA
10.21.15.188:2022

DA
209.109.217.59:80

SA
99.99.99.5:1080

DA
209.109.217.59:80

NAT
Router

10.21.6.20

99.99.99.5

10.21.15.188

SA
10.21.101.90:1080

DA
209.109.217.59:80

SA
99.99.99.5:2080

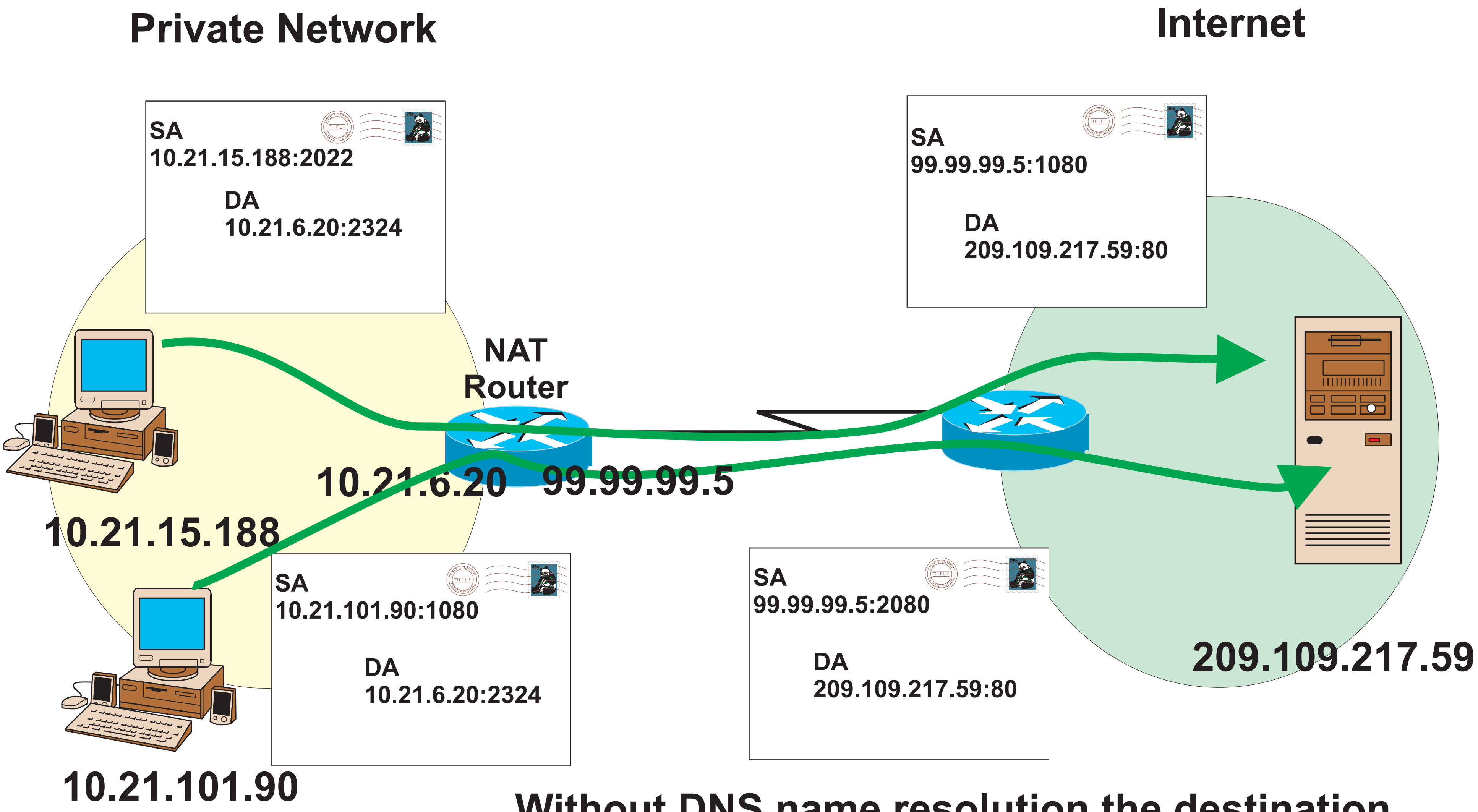
DA
209.109.217.59:80

209.109.217.59

10.21.101.90

PAT will try and use the same port as the source, but if it is already used, it will assign an available free port number

Port Address Translation (PAT) in a Nutshell without DNS



SA
10.21.15.188:2022

DA
10.21.6.20:2324

SA
99.99.99.5:1080

DA
209.109.217.59:80

SA
10.21.101.90:1080

DA
10.21.6.20:2324

SA
99.99.99.5:2080

DA
209.109.217.59:80

Without DNS name resolution the destination internal address is the NAT router internal address defined to the outside address

NAT and PAT

NAT - Network Address Translation

- 1 to 1 association
- Changes IP address in the header
- RFC 1631
- Layer 3
- Maps one internal (local) address to one external (global) address

PAT - Port Address Translation

(overload in Cisco speak)

- 1 to many
- Associates source port with each flow
- Layer 3 and 4
- Maps multiple internal (local) addresses to one external (global address)
- Also called NAPT in IETF documents
- A single IP address can address 65,536 unique ports

Terminology

Inside Zone

- Intranet/private address
- Typically uses private addresses
- “Local address” is real IP address of host
- Not routable in the Internet

Outside Zone

- Internet/Public address
- Registered addresses only
- “Global address” is the virtual host address
- Routable in the Internet

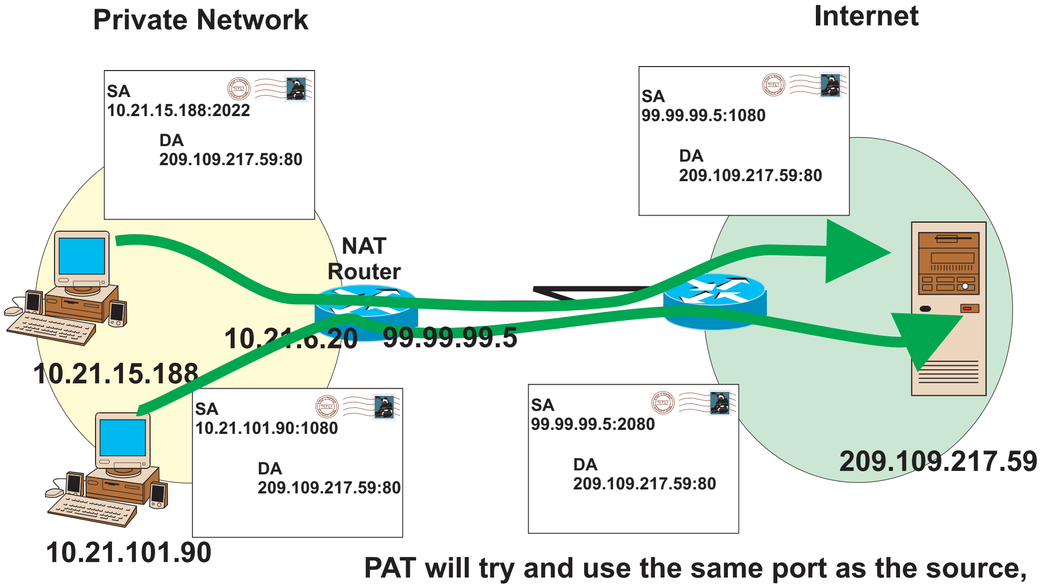
Static

- Commonly used for inbound traffic
- Permanent
- “Local” address is always known by the same “global” address
- ‘ip nat inside source static 10.21.99.23 99.99.99.4’

Dynamic

- Typically used for outbound traffic
- Changes
- “Local” address may have variable “global” address
- ‘ ip nat inside source list 1 pool nat-pool’

Why do we need NAT?



Private Network

Internet

SA
10.21.15.188:2022
DA
209.109.217.59:80

SA
99.99.99.5:1080
DA
209.109.217.59:80

NAT
Router

10.21.6.20 99.99.99.5

10.21.15.188

SA
10.21.101.90:1080
DA
209.109.217.59:80

SA
99.99.99.5:2080
DA
209.109.217.59:80

209.109.217.59

10.21.101.90

PAT will try and use the same port as the source, but if it is already used, it will assign an available free port number

Use of non-Internet-routable private address in private networks

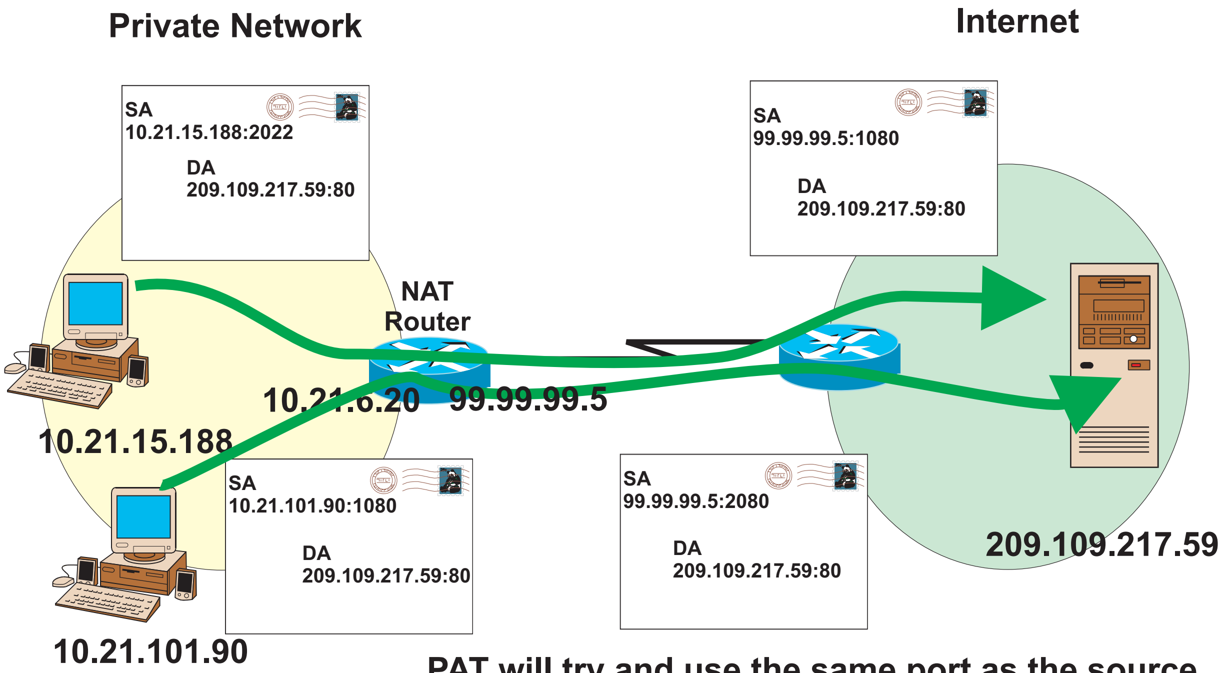
Merging corporations with conflicting IP address space

Changing Internet Service Providers (ISPs)

Can assist in changing IP addressing schemes

Secures internal network since private addresses are hidden

Where is NAT Implemented?



Private Network

Internet

SA
10.21.15.188:2022
DA
209.109.217.59:80

SA
99.99.99.5:1080
DA
209.109.217.59:80

NAT
Router

10.21.6.20

99.99.99.5

10.21.15.188

SA
10.21.101.90:1080
DA
209.109.217.59:80

SA
99.99.99.5:2080
DA
209.109.217.59:80

209.109.217.59

10.21.101.90

PAT will try and use the same port as the source, but if it is already used, it will assign an available free port number

Routers
Firewalls
VPN devices

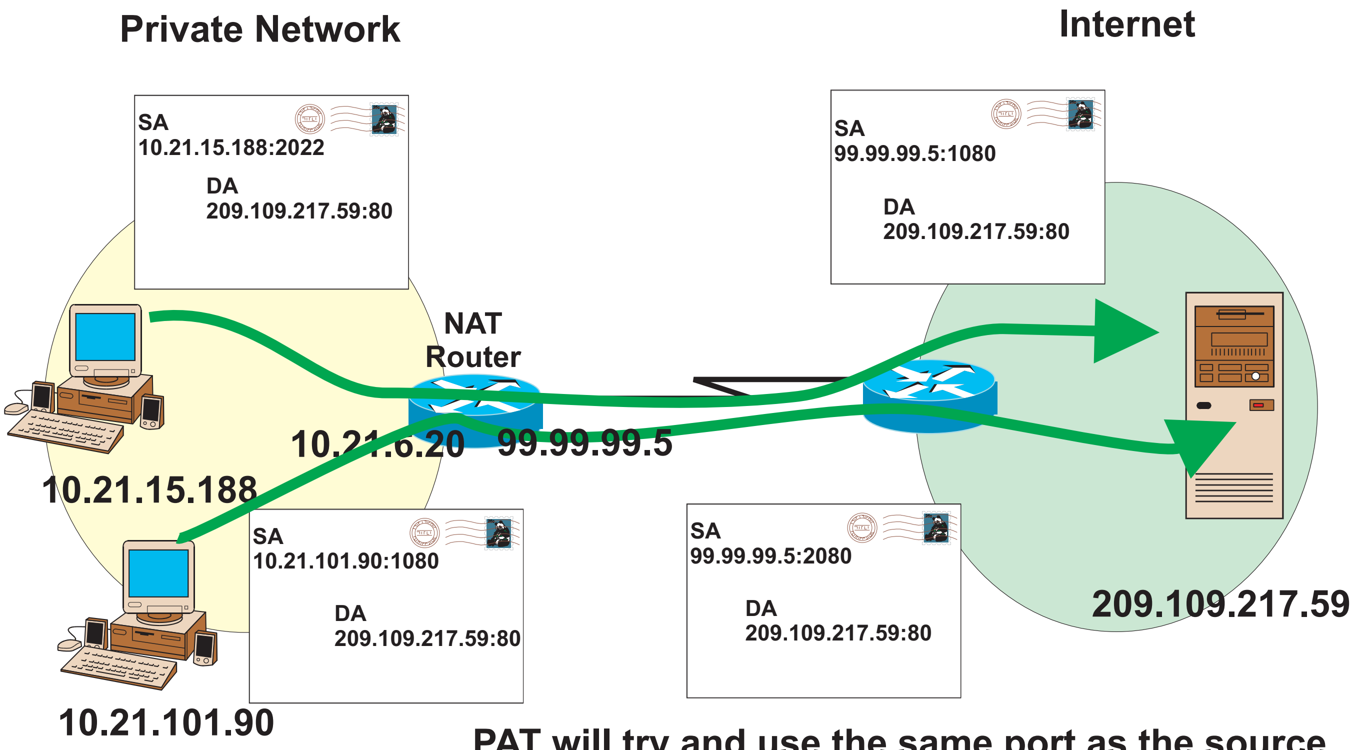
Each translation = 160 - 200 bytes

10,000 translations = 1.6 megabytes

Performance/latency is negligible

Needs about 42 Kbytes of system memory

NAT Basic Information



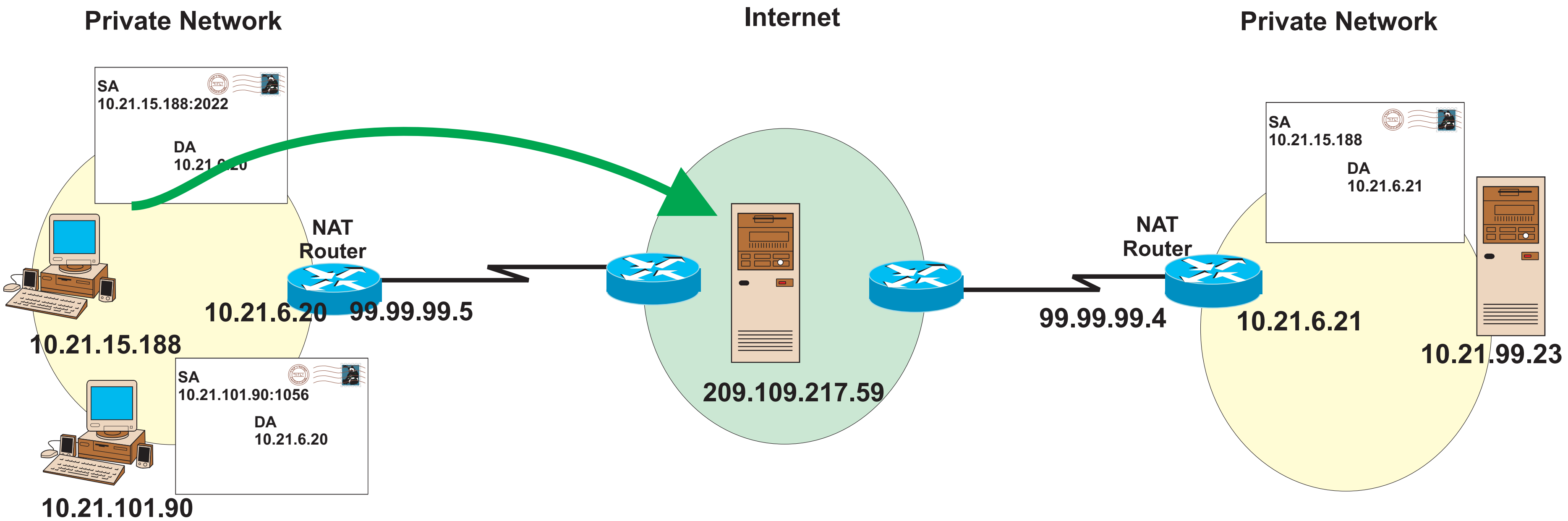
PAT will try and use the same port as the source, but if it is already used, it will assign an available free port number

An interface can be defined as inside or outside

Translations occur from ‘inside to outside’ interfaces or from ‘outside to inside’

Translations never occur from ‘inside to inside’ or ‘outside to outside’

Inside and Outside Definitions



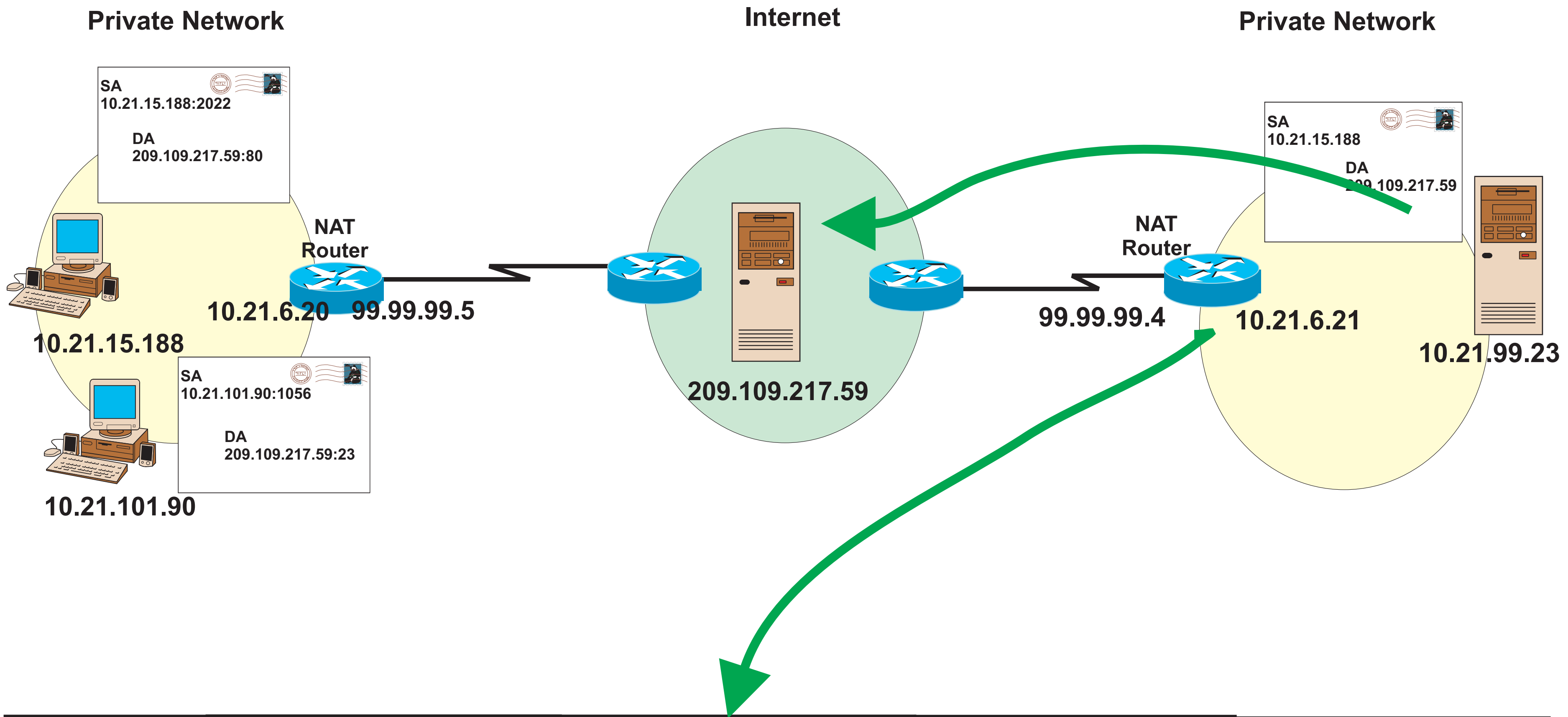
Inside Local: The IP address assigned to a device on the inside network

Inside Global: The IP address of an inside device as it is known to the outside

Outside Local: The IP address of an outside device as it is known to the inside network

Outside Global: The IP address assigned to a device on the outside network

NAT Configuration



Private Network

Internet

Private Network

SA
10.21.15.188:2022

DA
209.109.217.59:80

NAT
Router

10.21.6.20

99.99.99.5

10.21.15.188

SA
10.21.101.90:1056

DA
209.109.217.59:23

10.21.101.90

209.109.217.59

SA
10.21.15.188

DA
209.109.217.59

NAT
Router

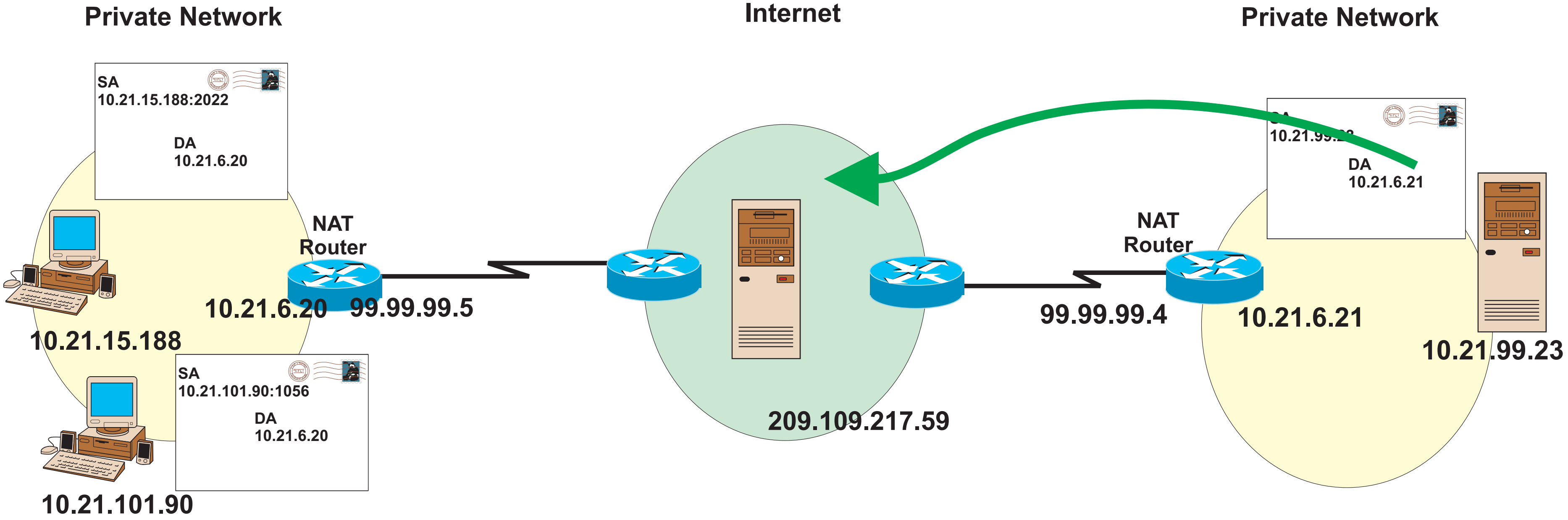
99.99.99.4

10.21.6.21

10.21.99.23

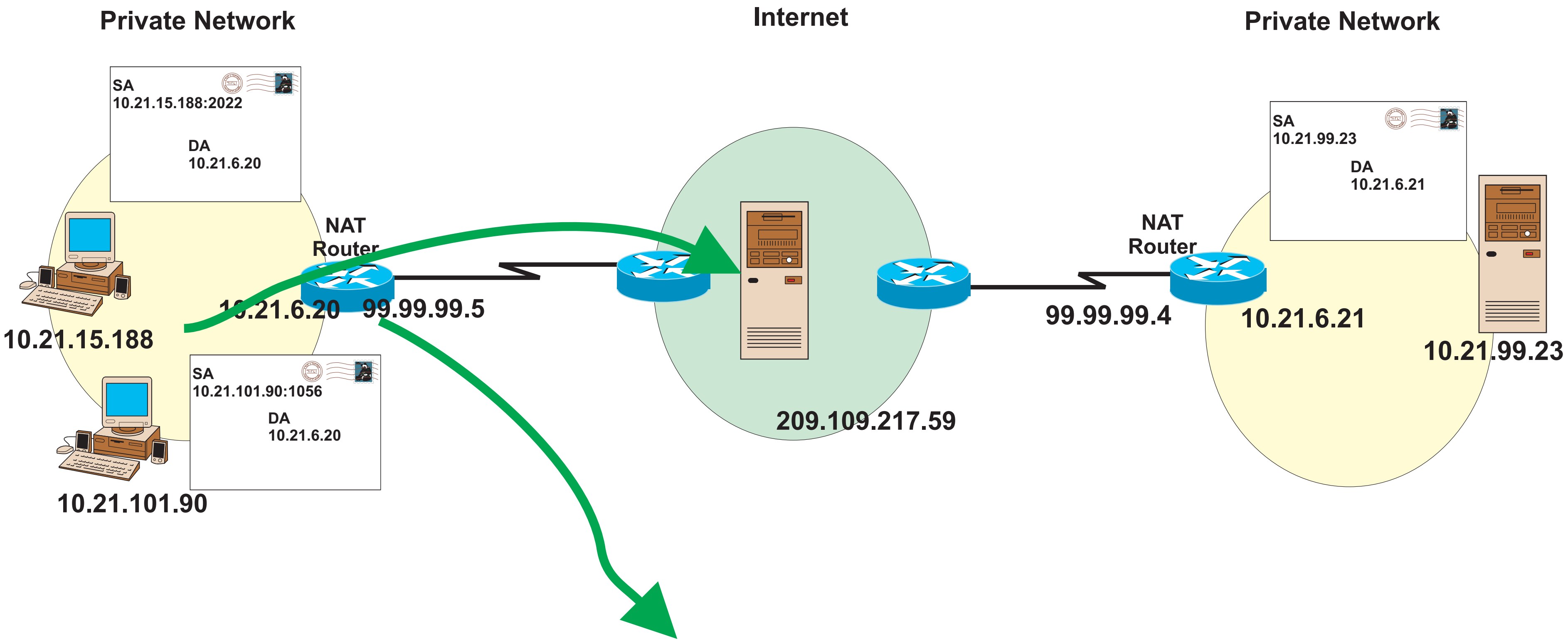
Protocol	Inside Global	Inside Local	Outside Local	Outside Global
Any	99.99.99.4	10.21.99.23		

NAT Configuration Expanded



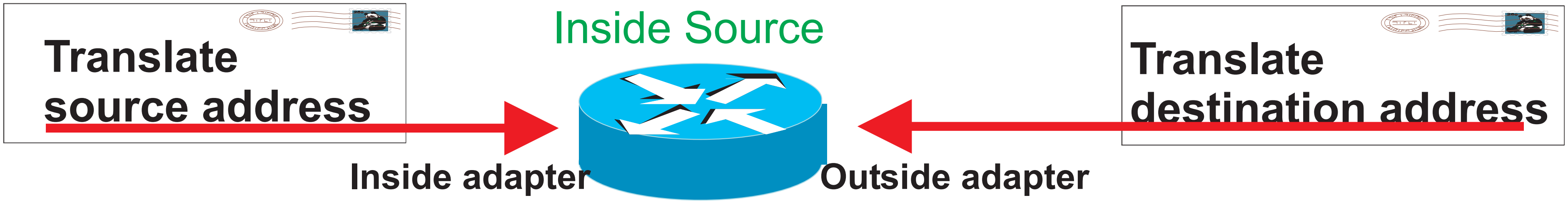
Protocol	Inside Global	Inside Local	Outside Local	Outside Global
Any	99.99.99.4	10.21.99.23	10.21.6.21	209.109.217.59

NAT Configuration Expanded



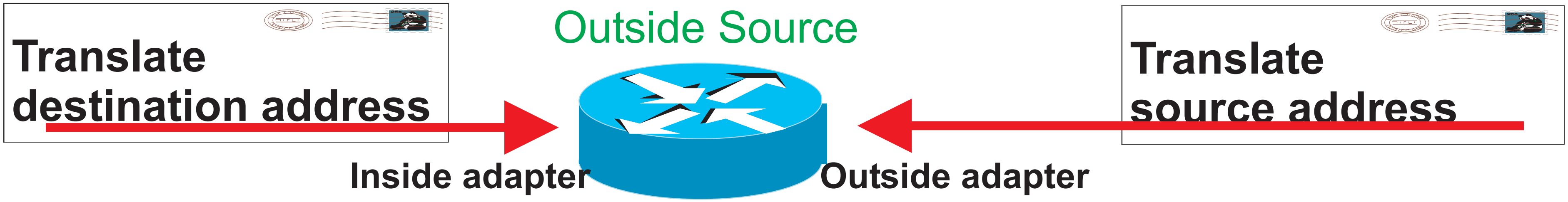
Protocol	Inside Global	Inside Local	Outside Local	Outside Global
TCP	99.99.99.5:1202	10.21.101.90:1056	209.109.217.59:23	209.109.217.59:23
TCP	99.99.99.5:2022	10.21.15.188:2022	209.109.217.59:80	209.109.217.59:80

Outside and Inside Source Addresses



Inside source translation

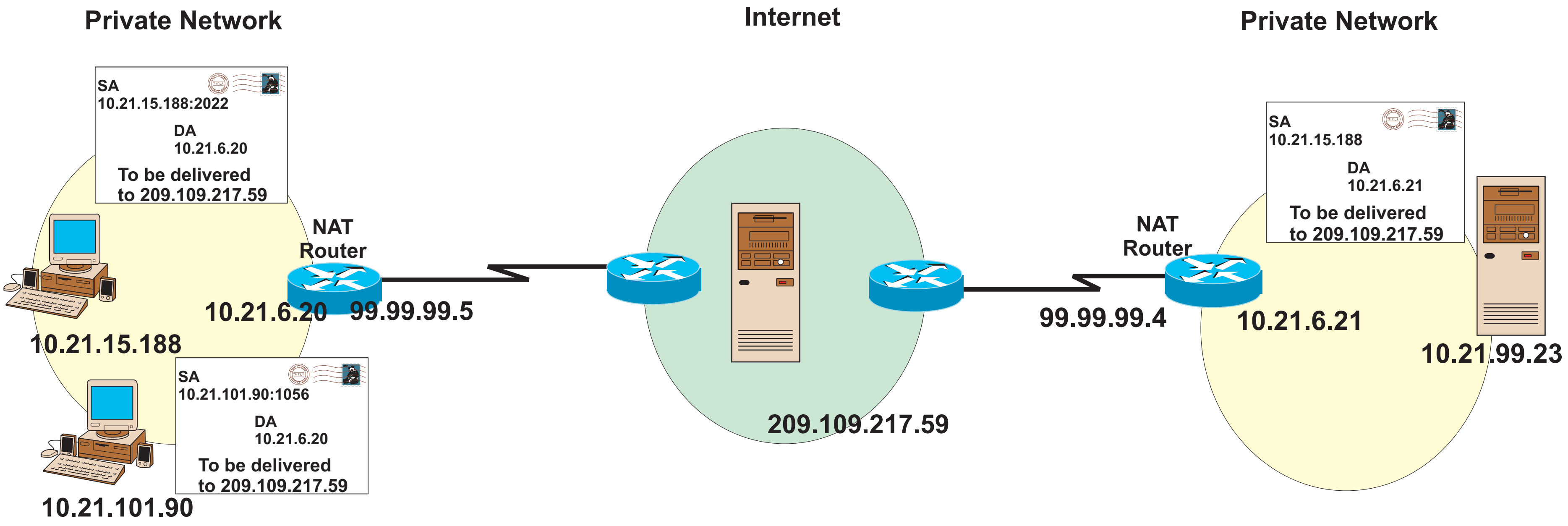
- IP hosts addresses that should not be seen in the public Internet
- Translates source IP address for packets going from inside to outside
- Translates destination IP address for packets going from outside to inside



Outside source translation

- Same IP addresses are being used on both inside and outside networks (overlapping networks)
- Translates source IP address for packets going from outside to inside
- Translates destination IP address for packets going from inside to outside

NAT Order of Operation



Private Network

Internet

Private Network

SA
10.21.15.188:2022
DA
10.21.6.20
To be delivered
to 209.109.217.59

NAT
Router

10.21.6.20

99.99.99.5

10.21.15.188

SA
10.21.101.90:1056
DA
10.21.6.20
To be delivered
to 209.109.217.59

10.21.101.90

209.109.217.59

SA
10.21.15.188
DA
10.21.6.21
To be delivered
to 209.109.217.59

NAT
Router

99.99.99.4

10.21.6.21

10.21.99.23

NAT always checks translation table before access lists

Check with vendors regarding full NAT order of operation
it varies even in a single vendors product line

Vendors have assigned ‘marketing’ names to PAT

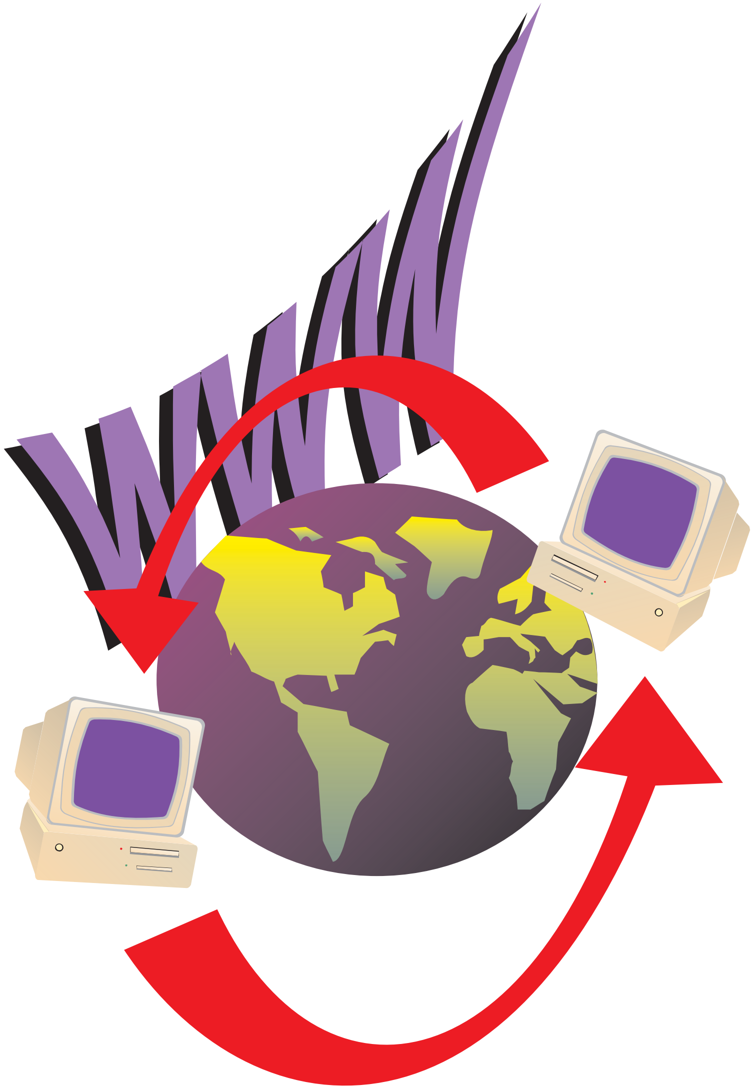
Agenda

Concepts of NAT (Network Address Translation) and
PAT (Port Address Translation)

Virtual Private Networks Considerations

Other Considerations

Summary

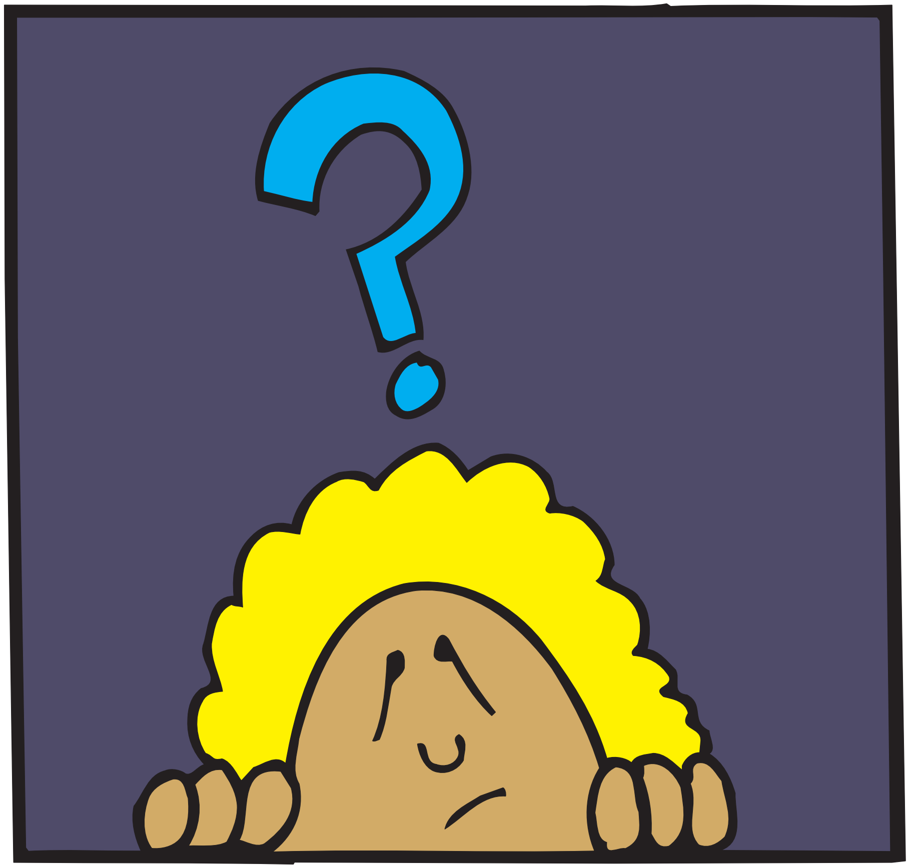


Application Considerations

Is there embedded IP information in the payload?

Well behaved applications

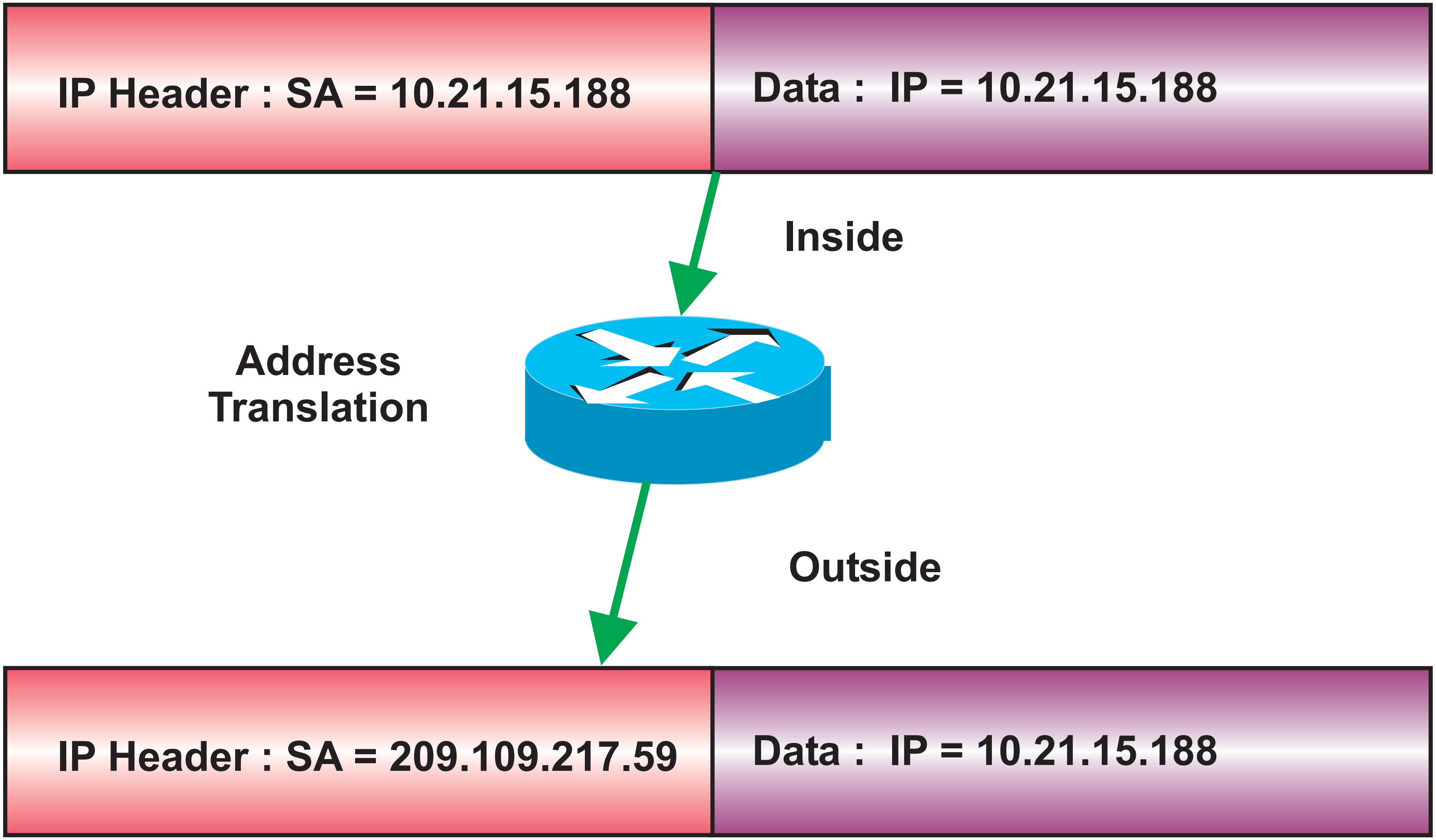
- HTTP
- Telnet
- Archie
- Finger
- NTP
- rlogin
- rsh
- rcp
- NFS
- TFTP



Problem applications

- IP Multicast
- VOIP
- ICMP
- PPTP
- H.323
- SMTP
- FTP
- NetBios over IP
- RealAudio
- CuSeeMe
- DNS “a”
- DNS “ptr”
- Most DVC

Embedded IP



IP Header : SA = 10.21.15.188

Data : IP = 10.21.15.188

Inside

Address
Translation

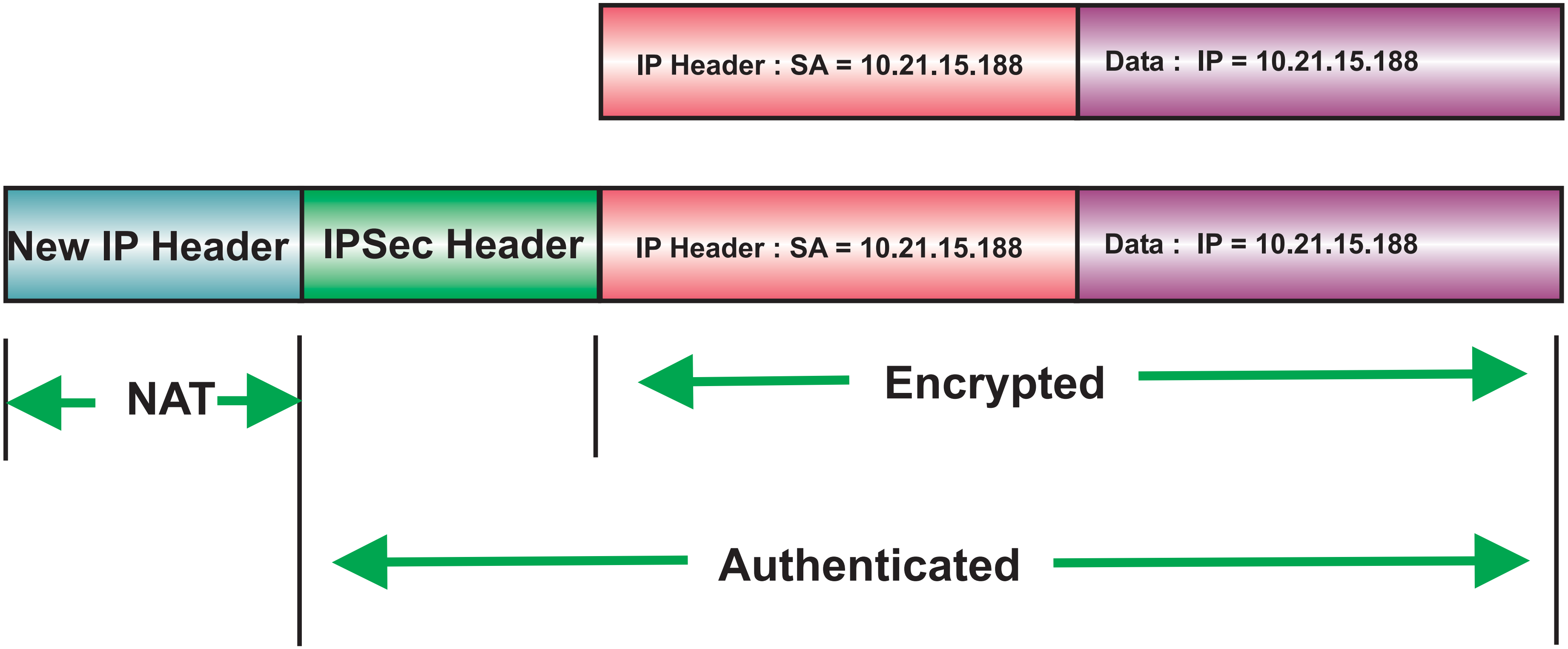
Outside

IP Header : SA = 209.109.217.59

Data : IP = 10.21.15.188

Which address will the end system use for the response?

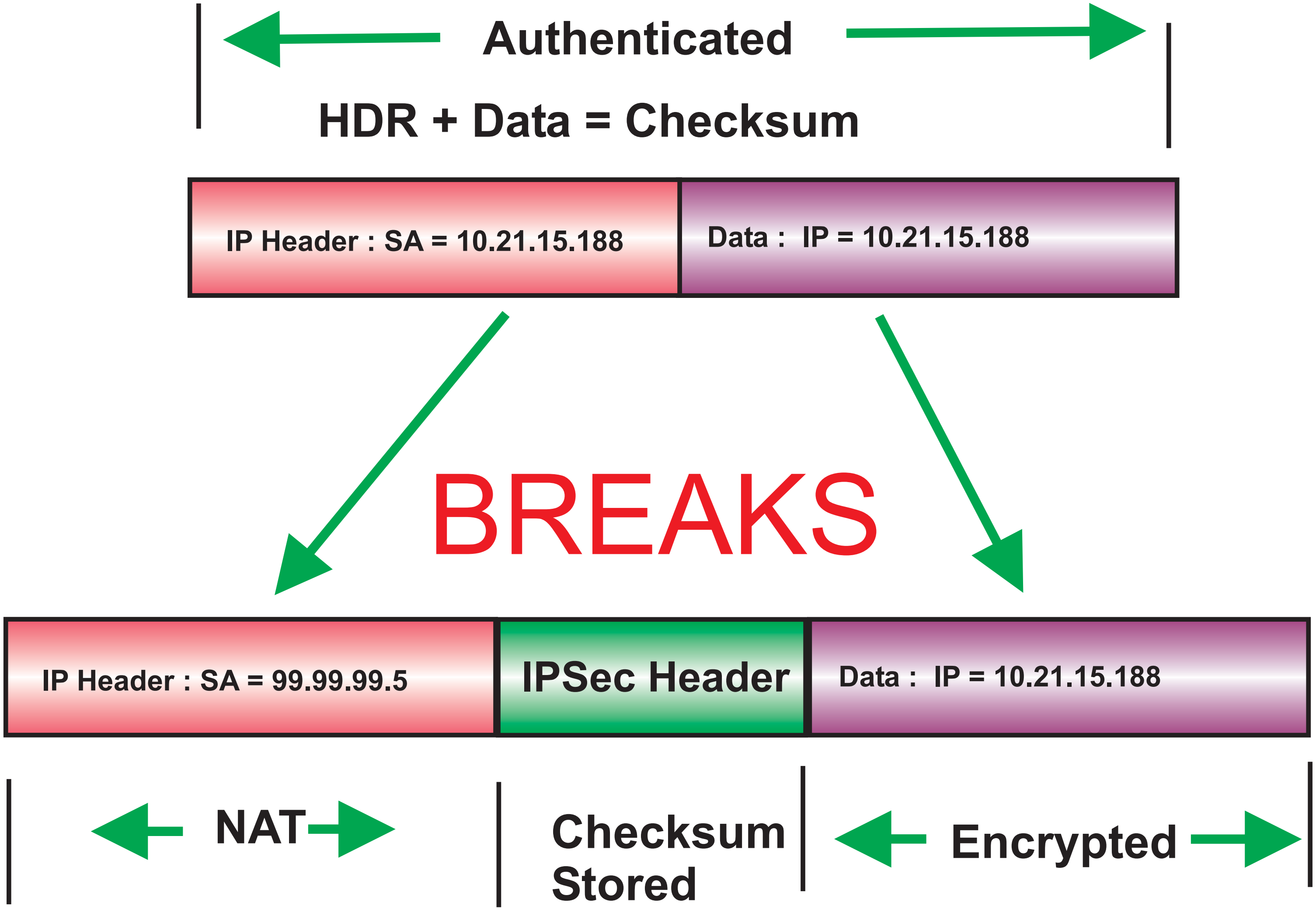
IPSec - ESP Considerations



ESP Tunnel Mode
(host-gateway and gateway-gateway)

Works !!!!!!!!!!

IPSec - AH

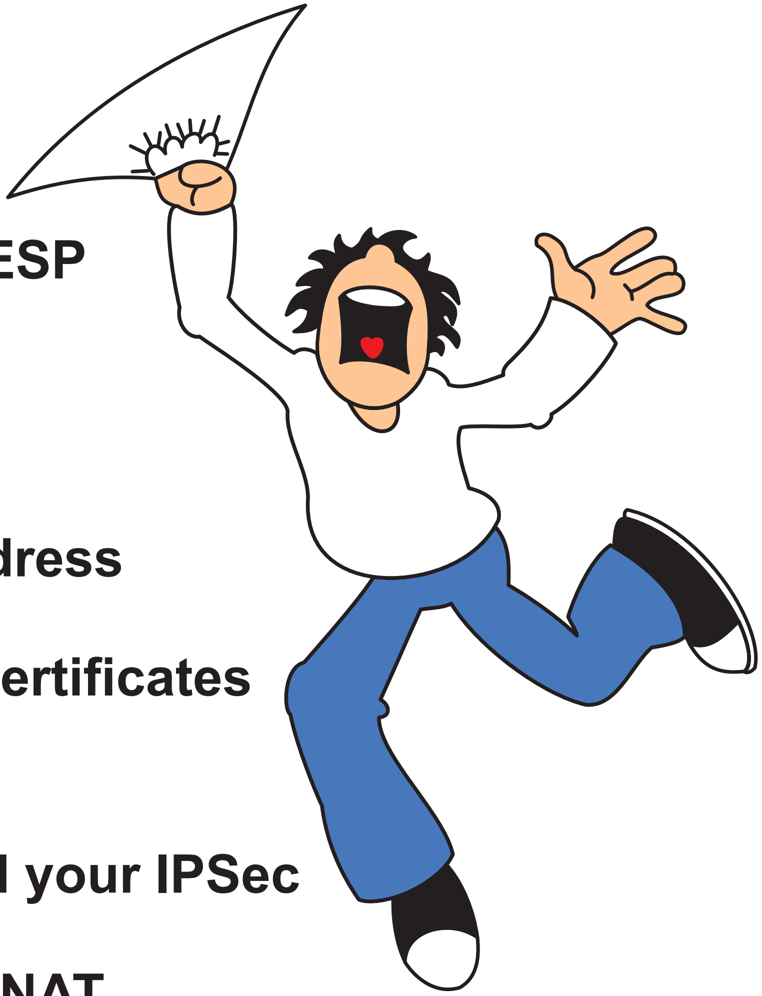


If any field in the in the original header is modified AH will fail. Remember AH was designed to prevent source spoofing, man-in-middle attacks, and unauthorized modifications

IPSec - Catch 22

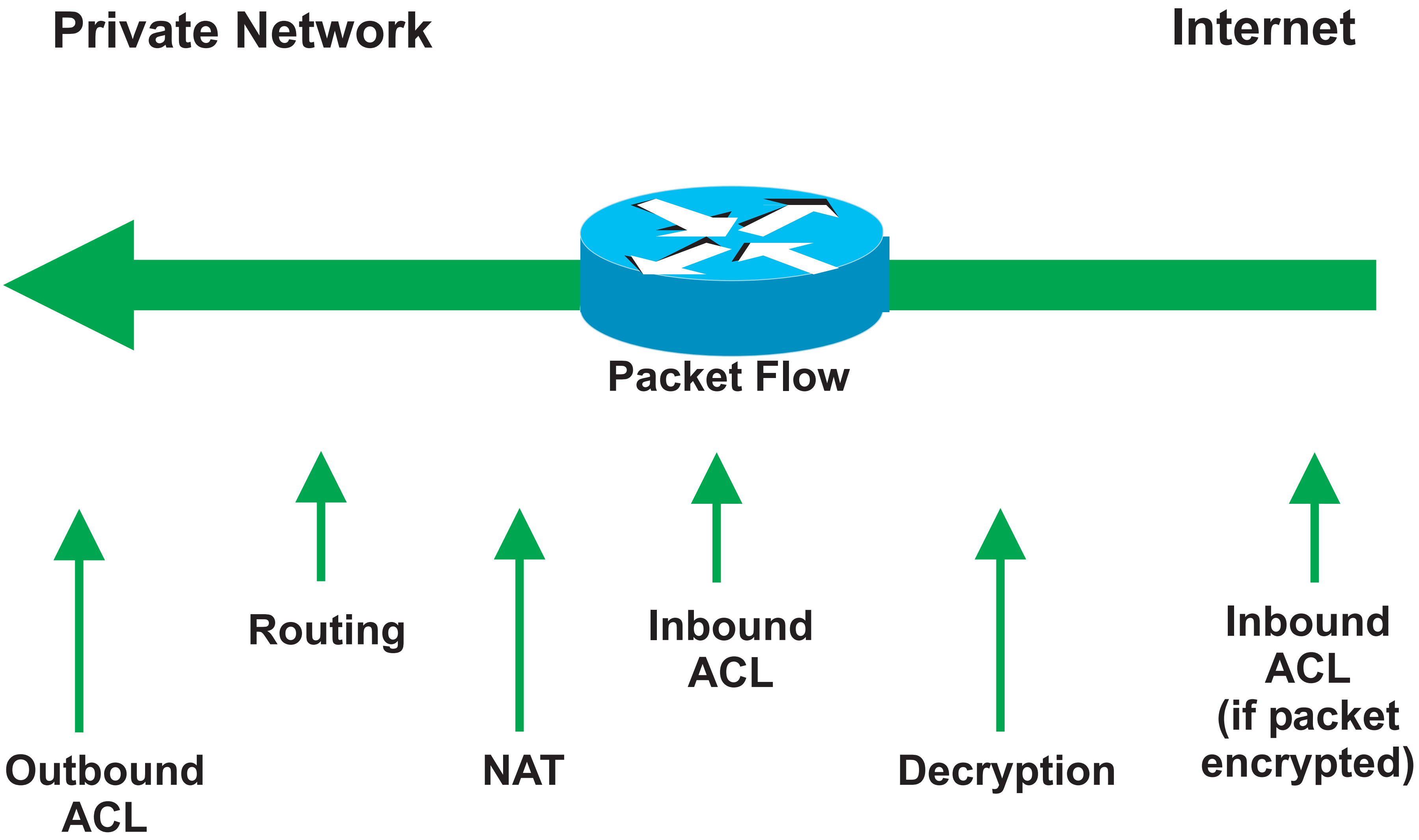
Transport mode ESP (host to host)
- NAT modifies the TCP/UDP packet
- NAT must recalculate the checksum
- If NAT updates the checksum,
  ESP authentication will fail

Turning off checksums in transport mode ESP
- Then we have a IKE issue
- IKE provides security association
  setup between endpoints
- Most often used is pre-shared key
- Pre-shared key relies on the source address
  of the packet
- (Use a VPN solution with X.509 digital certificates
  or public key signature)



NAT before IPSec
- Perform NAT on a device located behind your IPSec security gateway
- Use an IPSec device that also performs NAT
- Perform outbound address translation before applying security
- Perform security before address translation for inbound address

Access Lists Inbound



Private Network

Internet

Packet Flow

Outbound ACL

Routing

NAT

Inbound ACL

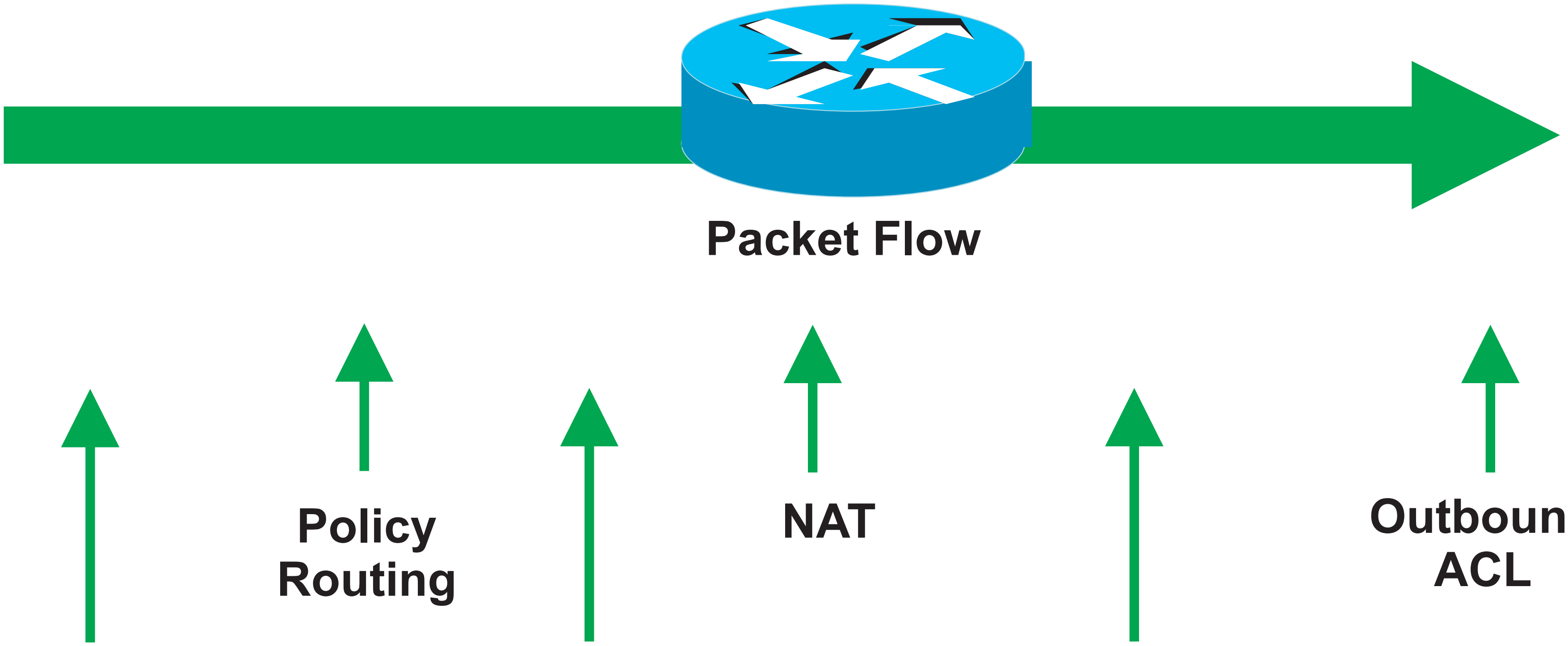
Decryption

Inbound ACL (if packet encrypted)

Access Lists Outbound

Private Network

Internet



Packet Flow

Inbound ACL

Policy Routing

Routing

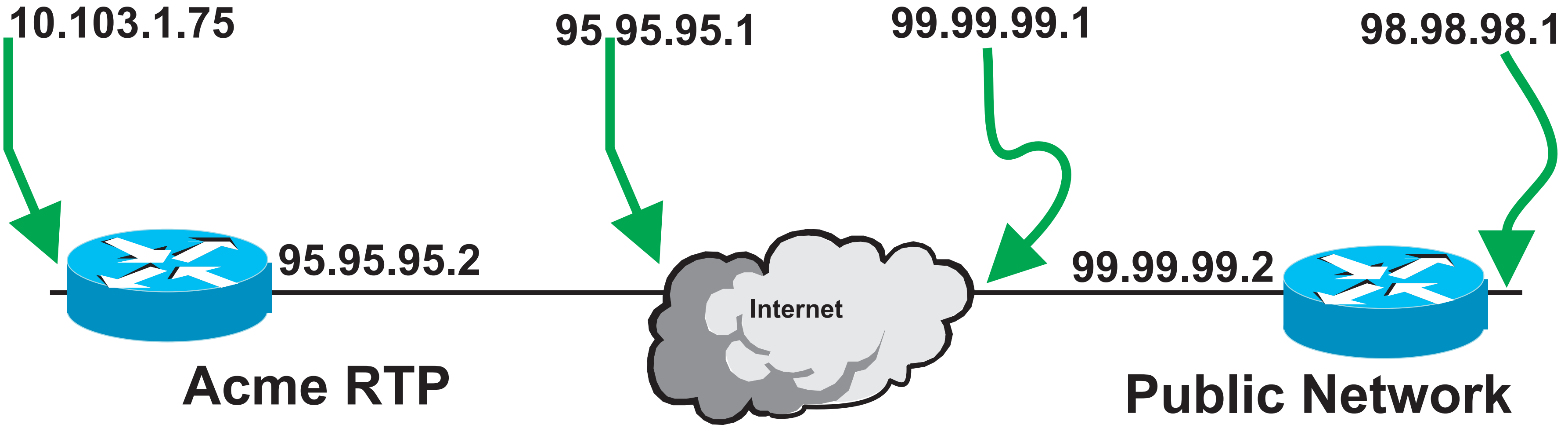
NAT

Encryption

Outbound ACL

Router Configuration
IPSec between Internet and Private Network

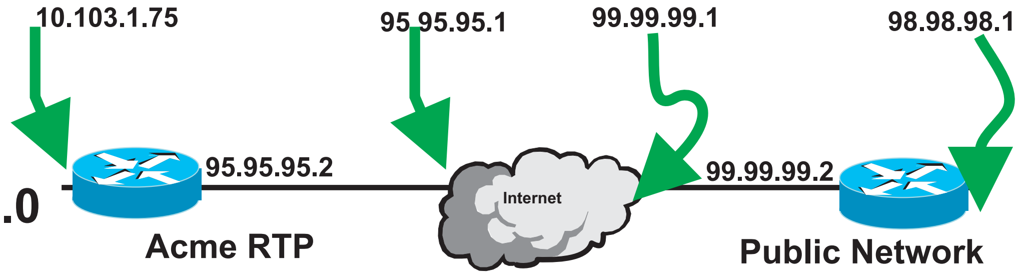
Sample configuration showing how to encrypt traffic between a private network (10.103.1.x) and a public network (98.98.98.x) using IPSec



Router Configuration
IPSec between Internet and Private Network

Public Router

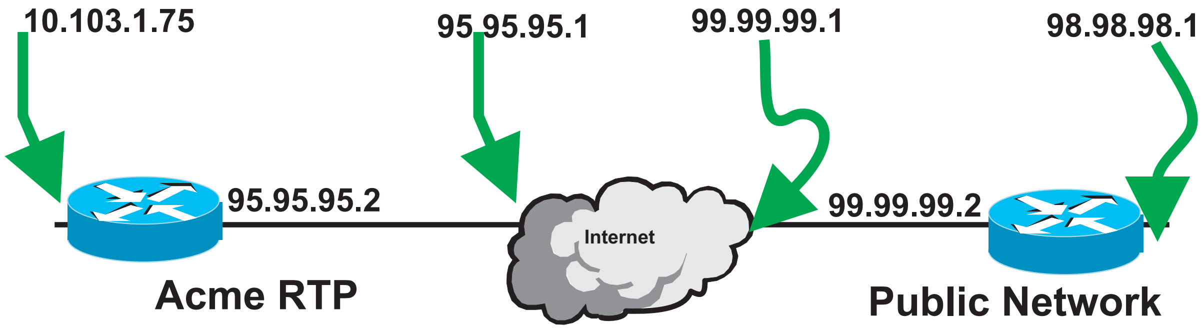
```
Crypto isakamp policy 1
hash md5
authentication pre-share
crypto isakamp key cisco123 address 95.95.95.2
:
crypto map rtp 1 ipsec-isakamp
set peer 95.95.95.2
match address 115
:
interface Ethernet 0/0
ip address 98.98.98.1 255.255.255.0
:
interface Ethernet 0/1
ip address 99.99.99.2 255.255.255.0
:
no ip route cache
:
access list 115 permit ip 98.98.98.0 0.0.0.255 10.103.1.0 0.0.0.255
access list 115 deny ip 98.98.98.0 0.0.0.255 any
```



Router Configuration
IPSec between Internet and Private Network

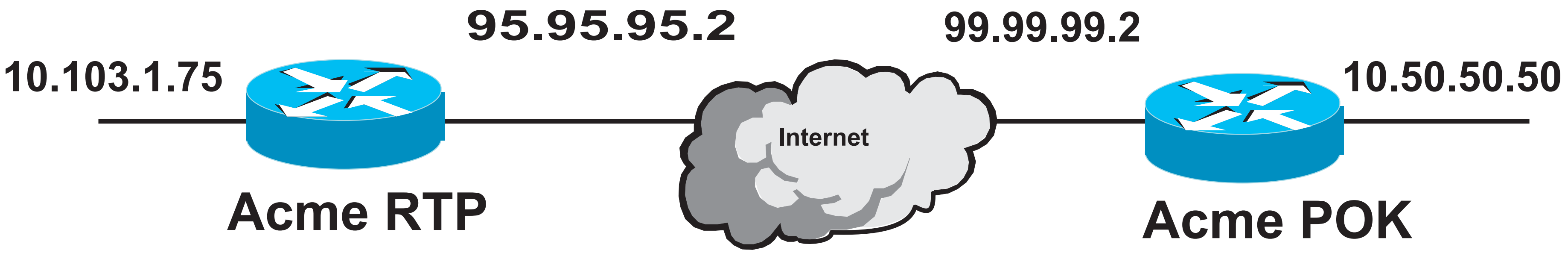
Acme RTP Router

```
Crypto isakamp policy 1
hash md5
authentication pre-share
crypto isakamp key cisco123 address 99.99.99.2
:
crypto map rtp 1 ipsec-isakamp
set peer 99.99.99.2
match address 115
:
interface Ethernet 0/0
ip address 95.95.95.2
ip nat outside
no route-cache
:
interface Ethernet 0/1
ip address 10.103.1.75 255.255.255.0
ip nat inside
:
no ip route cache
:
access list 115 permit ip 10.103.1.0 0.0.0.255 98.98.98.0 0.0.0.255
access list 115 deny ip 10.103.1.0 0.0.0.222 any
```



Router Configuration
IPSec Router-Router

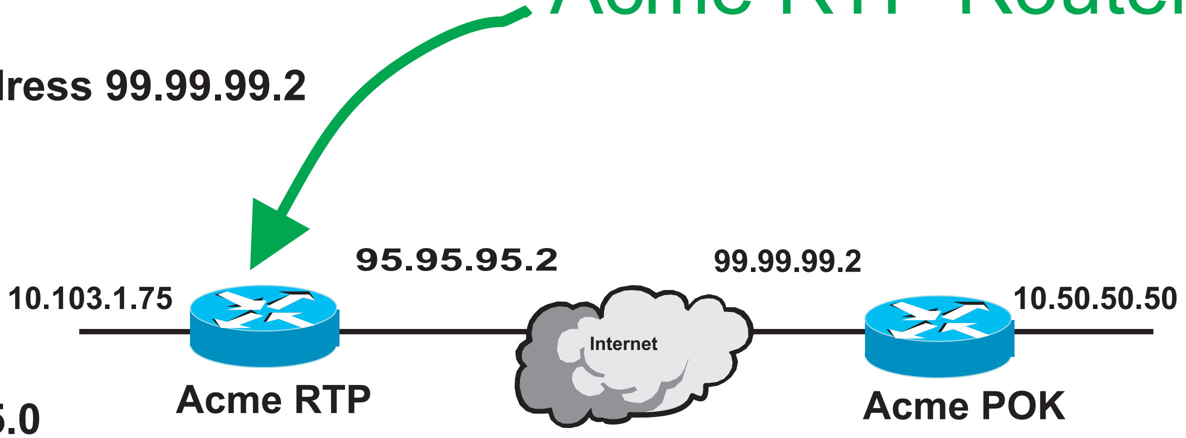
Encrypts traffic from the network behind Acme RTP(10.103.1.x) to the network behind Acme POK (10.50.50.x) and performs PAT. VPN client traffic can flow into Acme RTP. Internet traffic is not encrypted.



Router Configuration
IPSec Router-Router

```
Crypto isakamp policy 1
hash md5
authentication pre-share
crypto isakamp key cisco123 address 99.99.99.2
:
crypto map rtp 1 ipsec-isakamp
set peer 99.99.99.2
match address 115
:
interface Serial0
ip address 95.95.95.2 255.255.255.0
ip nat outside
crypto map rtp
```

Acme RTP Router

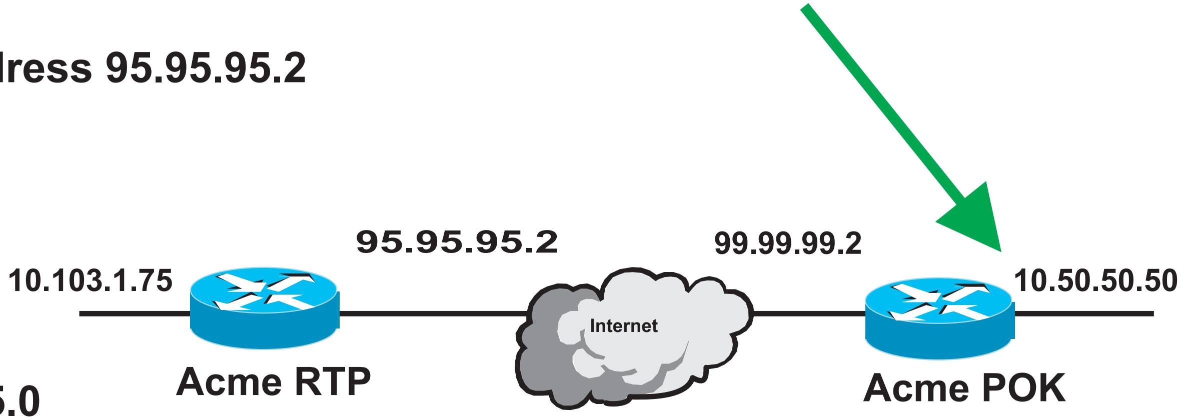


```
interface Ethernet 0/1
ip address 10.103.1.75 255.255.255.0
ip nat inside
:
ip nat inside source route-map nonat pool SER0 overload
:
no ip route cache
:
access list 115 permit ip 10.103.1.0 0.0.0.255 10.50.50.0 0.0.0.255
access list 110 deny ip 10.103.1.0 0.0.0.255 10.50.50.0 0.0.0.255
access list 110 permit 10.103.1.0 0.0.0.255 any
route map nonat permit 10
match ip address 110
```

Router Configuration
IPSec Router-Router

```
Crypto isakamp policy 1
hash md5
authentication pre-share
crypto isakamp key cisco123 address 95.95.95.2
:
crypto map rtp 1 ipsec-isakamp
set peer 95.95.95.2
match address 115
:
interface Ethernet0
ip address 99.99.99.2 255.255.255.0
ip nat outside
crypto map rtp
```

Acme POK Router



```
interface Ethernet 1
ip address 10.50.50.50 255.255.255.0
ip nat inside
:
ip nat inside source route-map nonat pool eth1 overload
:
no ip route cache
:
access list 115 permit ip 10.50.50.0 0.0.0.255 10.103.1.0 0.0.0.255
access list 110 deny ip 10.50.50.0 0.0.0.255 10.103.1.0 0.0.0.255
access list 110 permit 10.50.50.0 0.0.0.255 any
access list 115 deny ip 10.50.50.0 0.0.0.255
route map nonat permit 10
match ip address 110
```

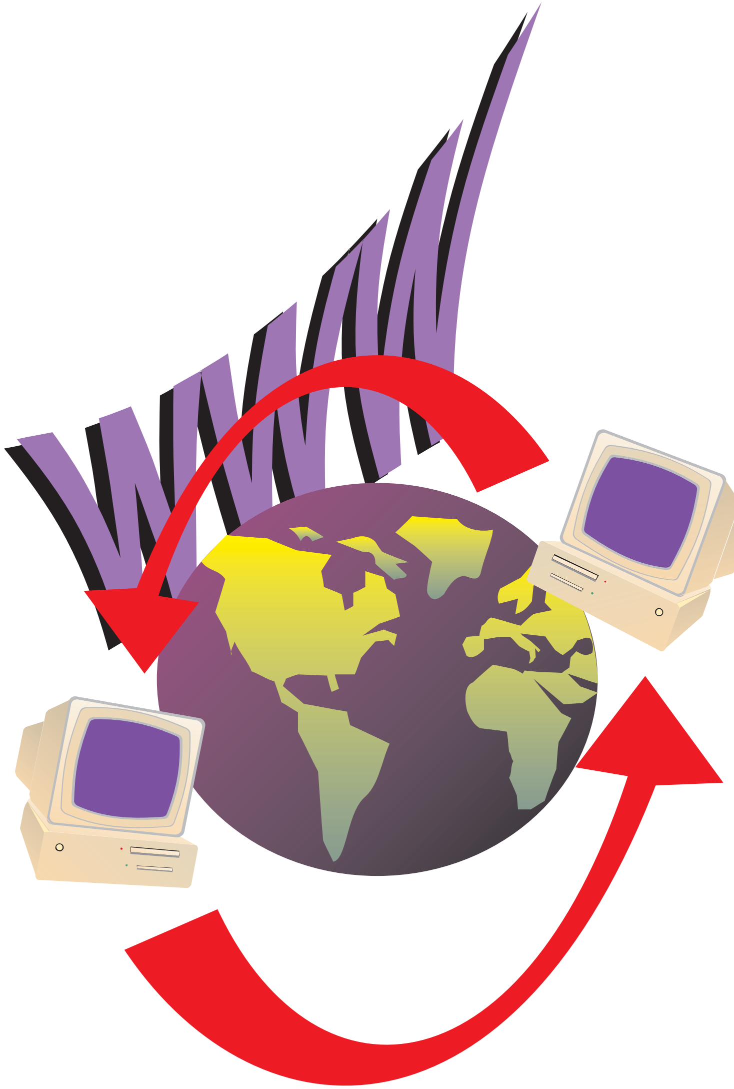
Agenda

Concepts of NAT (Network Address Translation) and PAT (Port Address Translation)

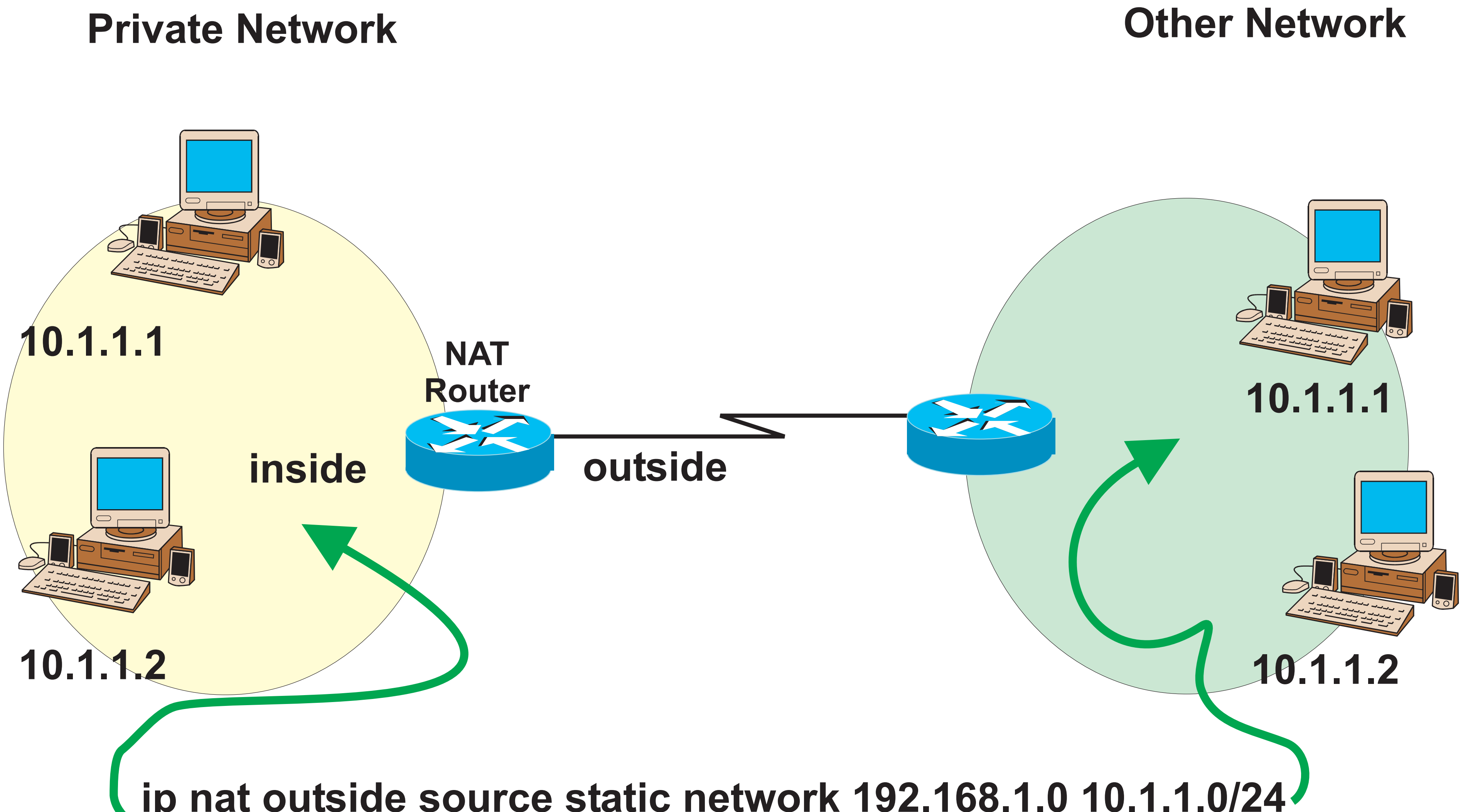
Virtual Private Networks Considerations

Other Considerations

Summary

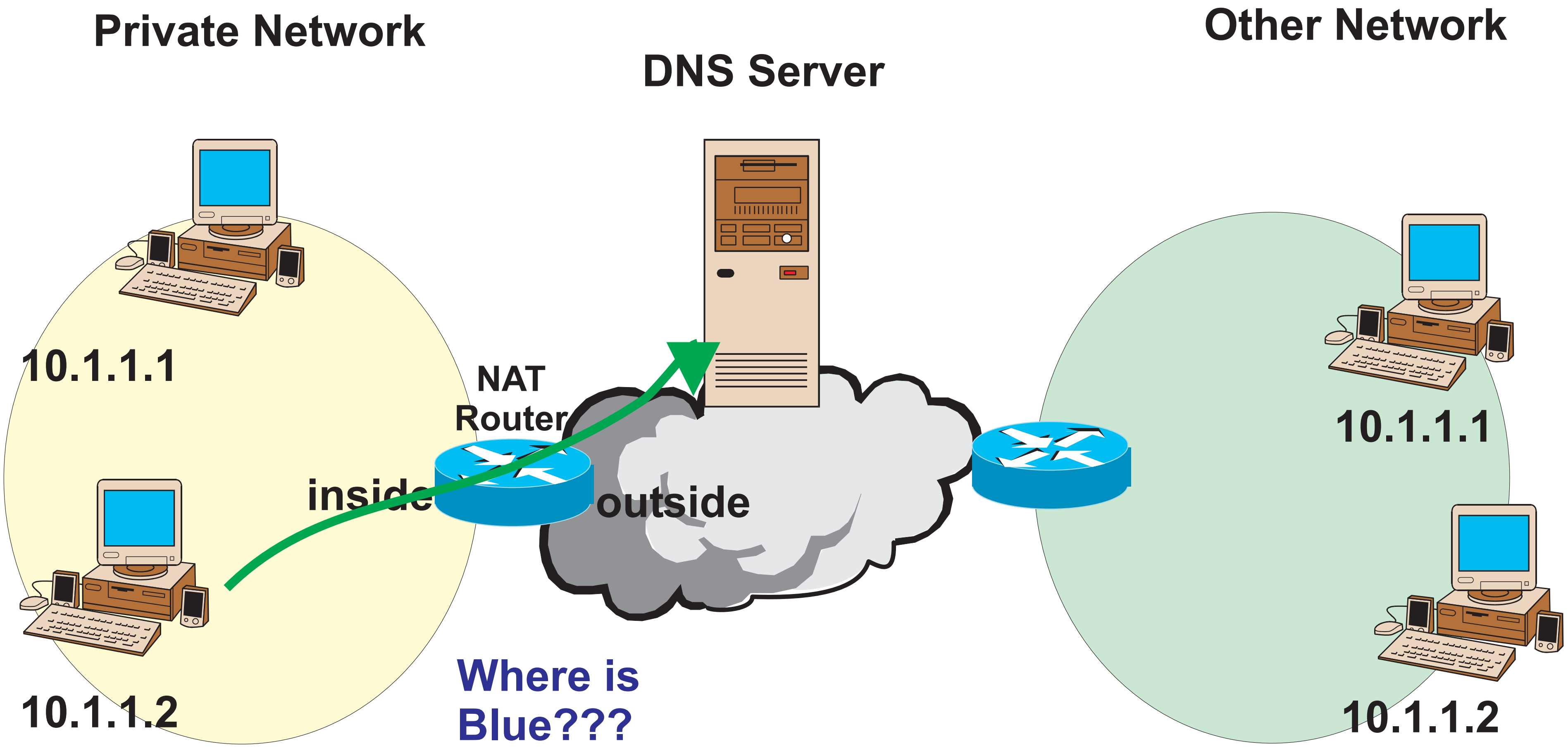


NAT in Overlapping Networks



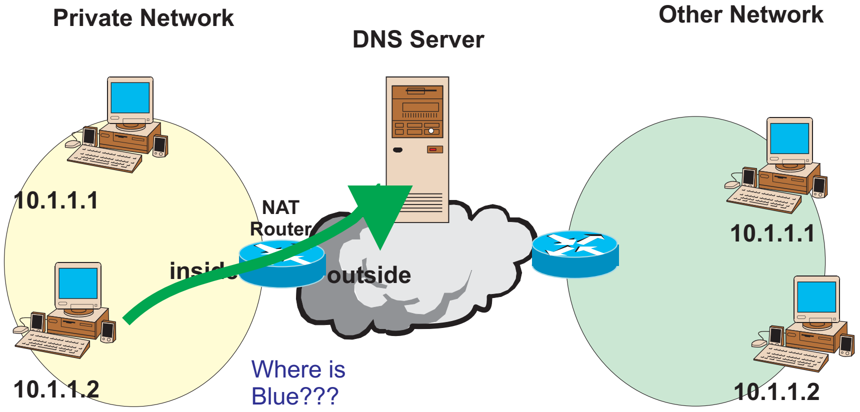
ip nat outside source static network 192.168.1.0 10.1.1.0/24
ip nat inside source static network 10.1.1.0 172.16.1.0/24

NAT in Overlapping Networks



DNS server responds with 10.1.1.2 which is modified in the NAT router to 192.168.1.2

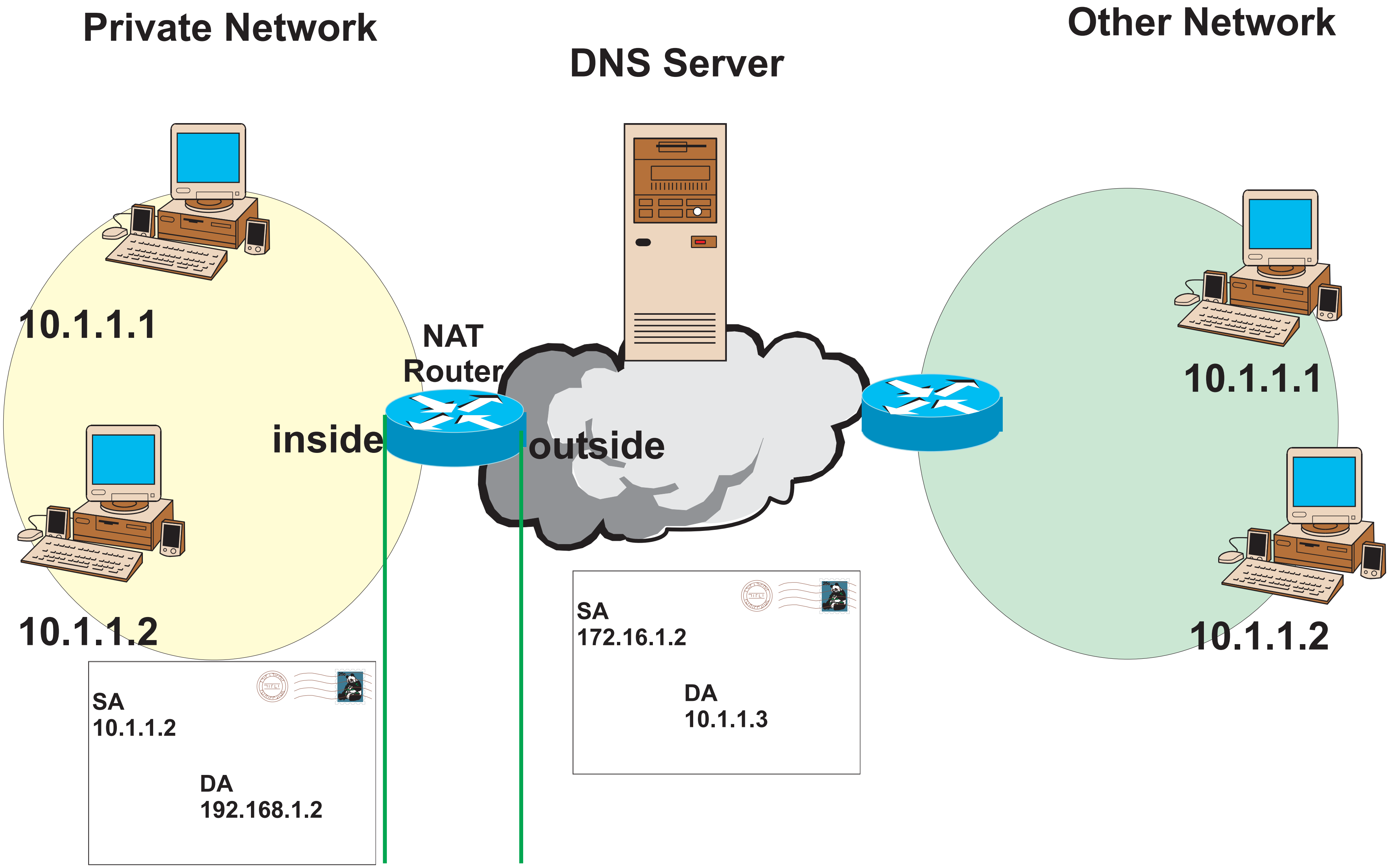
NAT in Overlapping Networks



Inside Global	Inside Local	Outside Local	Outside Global
192.168.1.2	10.1.1.2		
		172.16.1.2	10.1.1.2
192.168.1.2	10.1.1.2	172.16.1.2	10.1.1.2

Inside global and local addresses came from the IP header
Outside global and local addresses came from the DNS payload
The summary was derived from the ping between the two devices

NAT in Overlapping Networks



NAT Summary

NAT provides transparent connectivity

Networks can have arbitrary addressing schemes

NAT needs to consider applications in order to work

NAT enhances network privacy

NAT can be complex to configure, maintain, and understand

Does NAT really solve our addressing problems or just cover them up for a short time?

References

CISCO NAT order of operation : http://www.cisco.com/warp/public/556/5.html

RFC 1631 : The IP Network Address Translator

RFC 2663 : IP Network Address Translator Terminology and Considerations

IETF : http://www.ietf.org/html.charters/nat-charter.html

Cisco NAT technical tips : http://www.cisco.com/warp/public/556/index.shtml

NAT and VPN : http://www.isp-planet.com/technology/nat_ipsec.html

NAT and LINUX : http://www.suse.de/~mha/linux-ip-nat/diplom/nat.html

NAT usage : http://www.nbama.com/network/docs/natrfc.htm

NAT Home Page : http://www.uq.net.au/~zzdmacka/the-nat-page/

Technical Paper : http://www.vicomsoft.com/knowledge/reference/nat.html