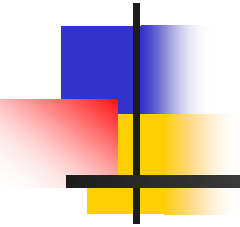
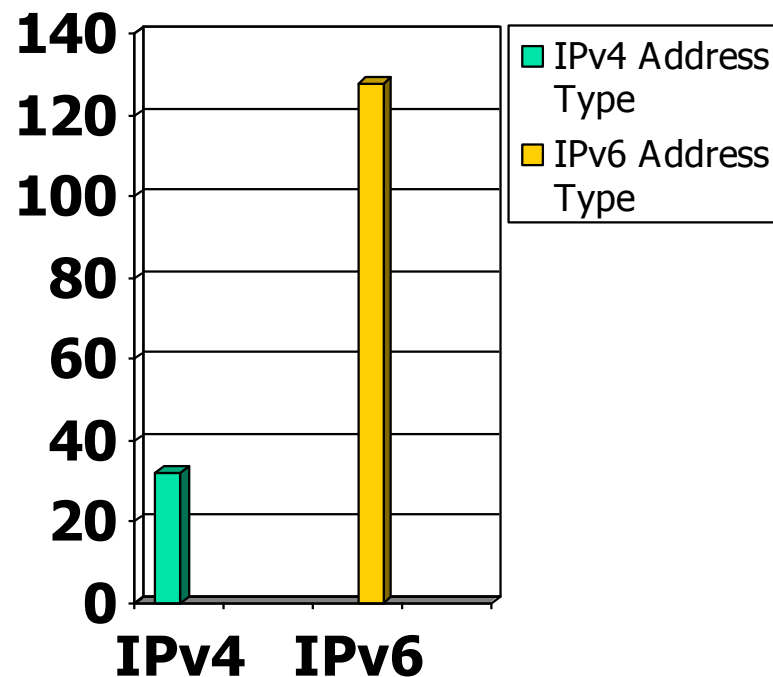


Network Address Translation & Port Address Translation



IP Address Allocation Overview




- IPv4 – address length is 4 bytes long.
- IPv6 – address length is 16 bytes long.
- 2^{32} v.s 2^{128}



Temporary Solutions For Scaling The Internet Address Space

- IPV4 address shortages and expanding Internet routing tables are still problems
- RFC - 1917 is an appeal to return unused address blocks to IANA for redistribution
- Address allocation for private internets RFC - 1918 suggests organizations use private address space with translation performed on a smaller “routable” pool of addresses at edge of network.
- IANA has reserved:
 - 10.0.0.0 - 10.255.255.255 (10.0.0.0/8 prefix)
 - 172.16.0.0 - 172.31.255.255 (172.16.0.0/12 prefix)
 - 192.168.0.0.- 192.168.255.255 (192.168.0.0/16 prefix)

Private addressing



| Class | RFC 1918 Internal Address Range | CIDR Prefix |
|-------|---------------------------------|----------------|
| A | 10.0.0.0 - 10.255.255.255 | 10.0.0.0/8 |
| B | 172.16.0.0 - 172.31.255.255 | 172.16.0.0/12 |
| C | 192.168.0.0 - 192.168.255.255 | 192.168.0.0/16 |

- 172.16.0.0 – 172.31.255.255: 172.16.0.0/12
 - Where does the /12 come from?

12 bits in common

10101100 . 00010000 . 00000000 . 00000000 – 172.16.0.0
10101100 . 00011111 . 11111111 . 11111111 – 172.31.255.255

10101100 . 00010000 . 00000000 . 00000000 – 172.16.0.0/12



Temporary Solutions For Scaling The Internet

Address Space (continued)

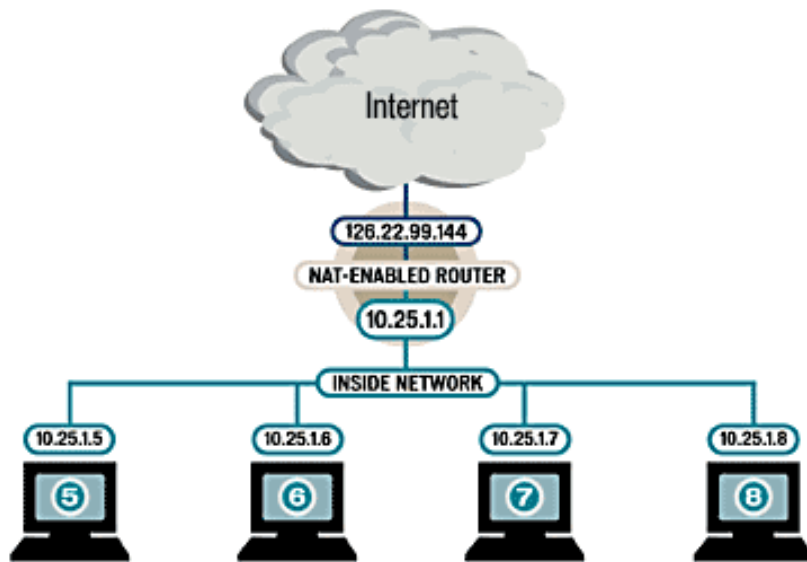
- Private IP not routable on internet
- Can be used simultaneously by many organizations
- Requires a network address translator (NAT) for internet access.
- Easier for customer to change ISP's.
- Address allocation from the reserved class A address space
- RFC-1797 explores allocation of upper half of class A by using CIDR blocks from the 64.0.0.0/2 address space



Why use NAT (RFC 1631)?

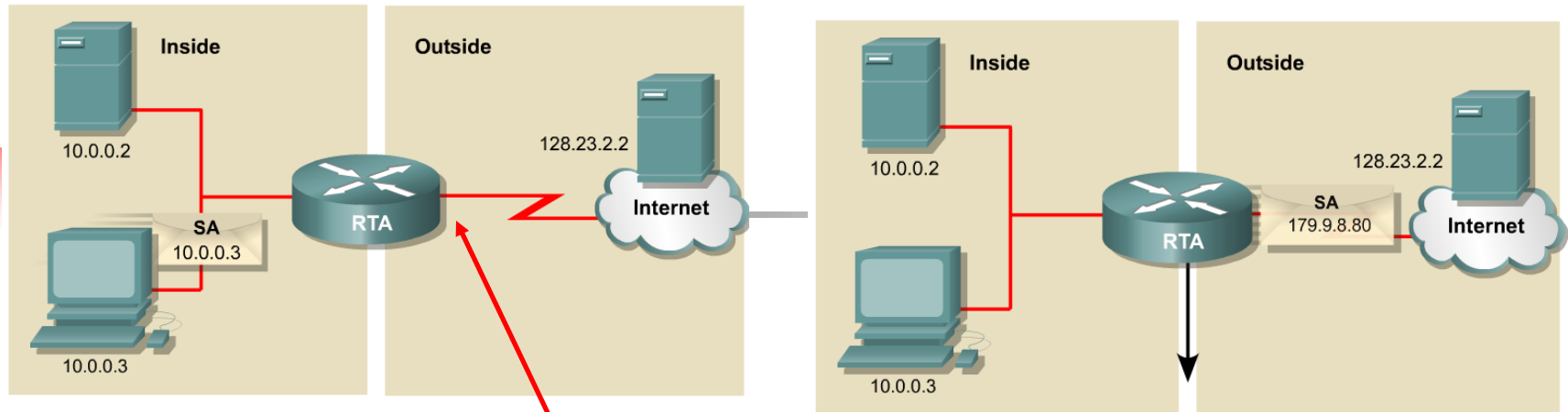
- Ability to use private addresses internally and still access the Internet
 - RFC1918 addresses are not globally unique
- Ability to connect overlapping IP address space
- Not a security cure

Got NAT?!



- NAT operates at the network layer of the OSI reference model
- NAT is a hotel receptionist
- NAT allows for a "one to one", "one to many", or "many to many" mapping

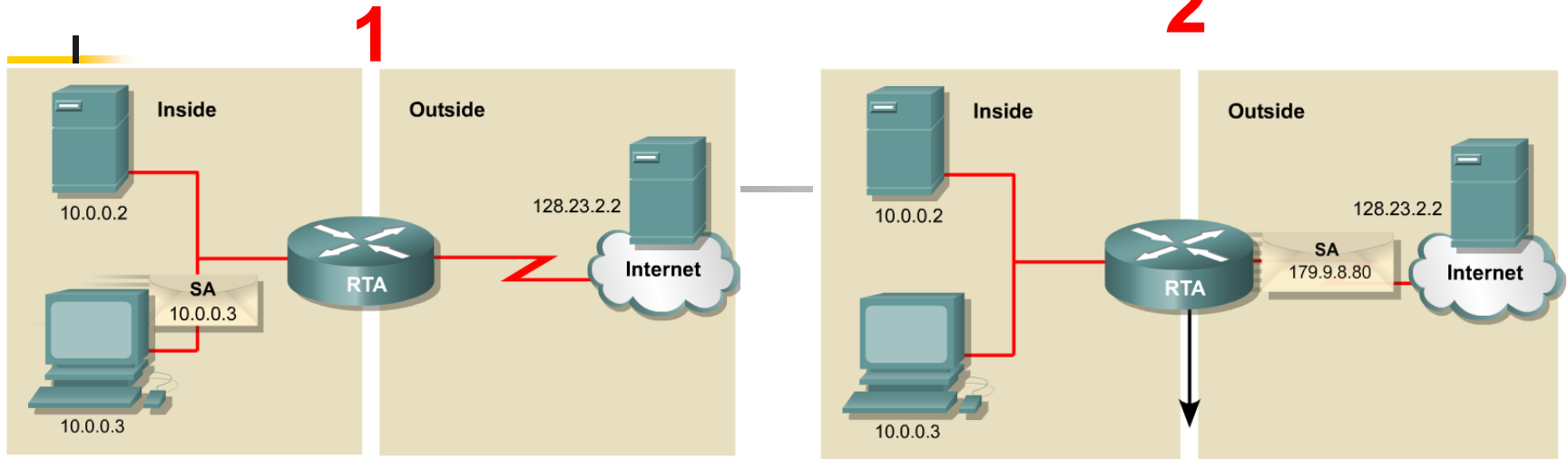
NAT Example



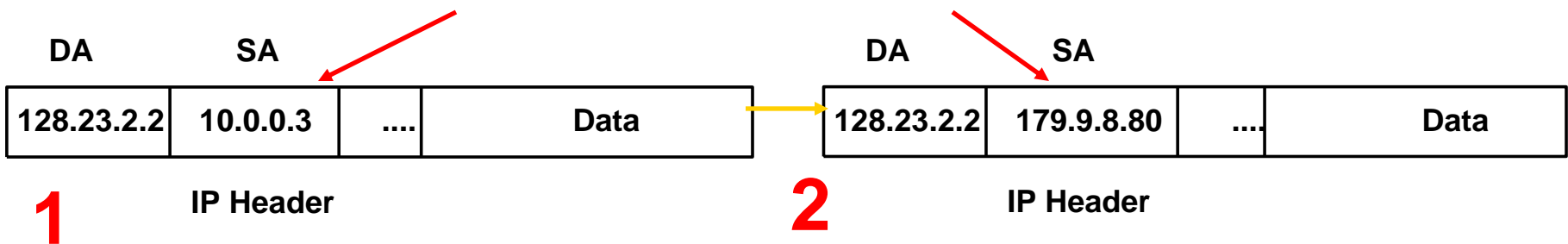
| NAT Table | | |
|-------------------------|--------------------------|---------------------------|
| Inside Local IP Address | Inside Global IP Address | Outside Global IP Address |
| 10.0.0.3 | 179.9.8.80 | 128.23.2.2 |

- **Inside local address** – The IP address assigned to a host on the inside network. This address is likely to be an RFC 1918 private address.
- **Inside global address** – A legitimate (Internet routable or public) IP address assigned by the service provider that represents one or more inside local IP addresses to the outside world.
- **Outside local address** – The IP address of an outside host as it is known to the hosts on the inside network.
- **Outside Global Address**

NAT Example



| NAT Table | | |
|-------------------------|--------------------------|---------------------------|
| Inside Local IP Address | Inside Global IP Address | Outside Global IP Address |
| 10.0.0.3 | 179.9.8.80 | 128.23.2.2 |



- The translation from Private source IP address to Public source IP address.



NAT Characteristics

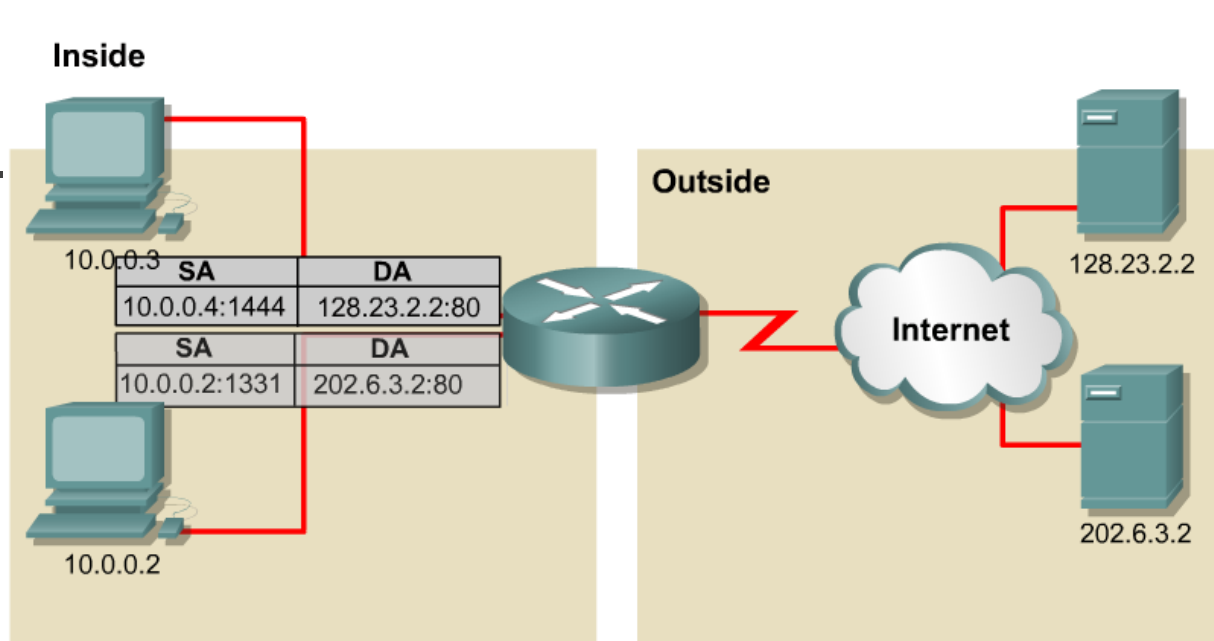
- Converts internal private address to configured public address that is routable
- Performed statically or dynamically
- Creates state table on connection
- Delete state table entry on disconnect
- With use of ACLs to prevent routing, can add to security profile, control traffic



NAT Applications

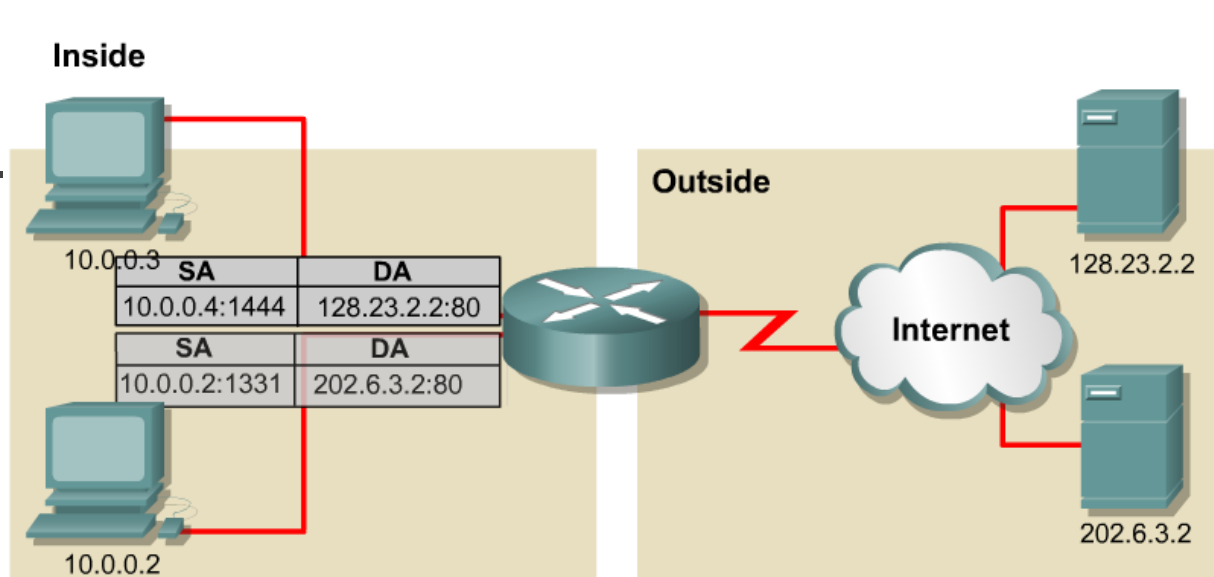
- Hardware and software firewalls
- Routers
- Proxy servers
 - RAS server that is a simple router/firewall

PAT – Port Address Translation



- With PAT a multiple private IP addresses can be translated by a single public address (many-to-one translation).
- This solves the limitation of NAT which is one-to-one translation.

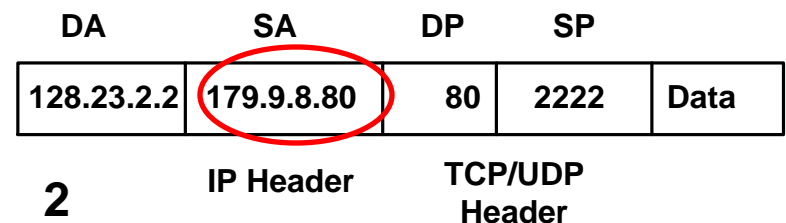
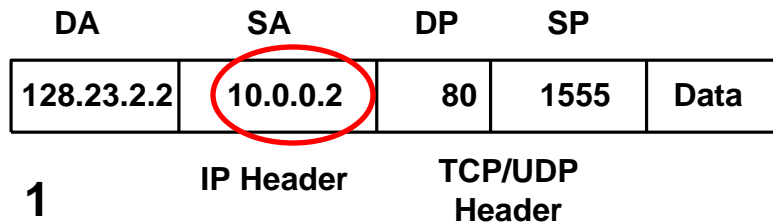
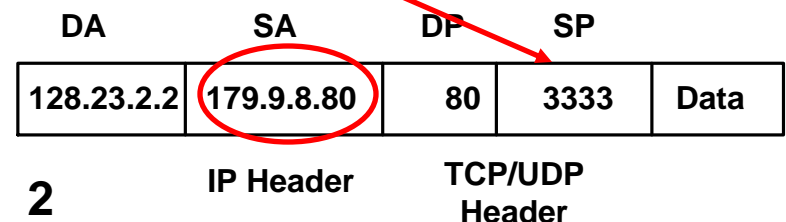
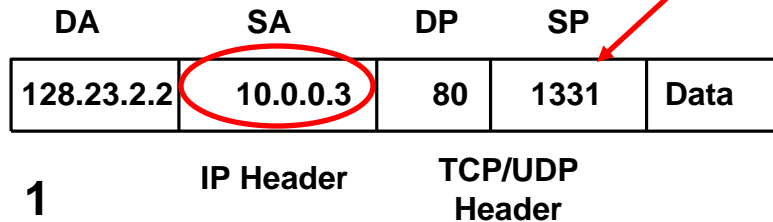
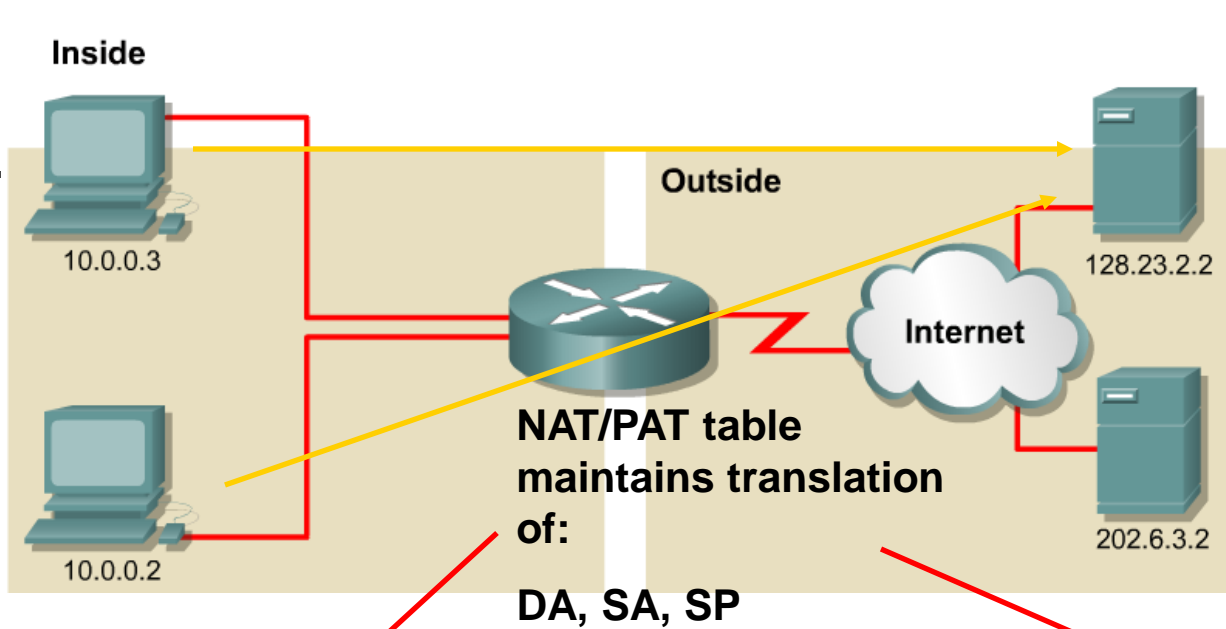
PAT – Port Address Translation



| NAT Table | | | |
|-------------------------|--------------------------|--------------------------|------------------------|
| Inside Local IP Address | Inside Global IP Address | Outside Local IP Address | Outside Global Address |
| 10.0.0.2:1331 | 179.9.8.20:1331 | 202.6.3.2:80 | 202.6.3.2:80 |
| 10.0.0.3:1555 | 179.9.8.20:1555 | 128.23.2.2:80 | 128.23.2.2:80 |

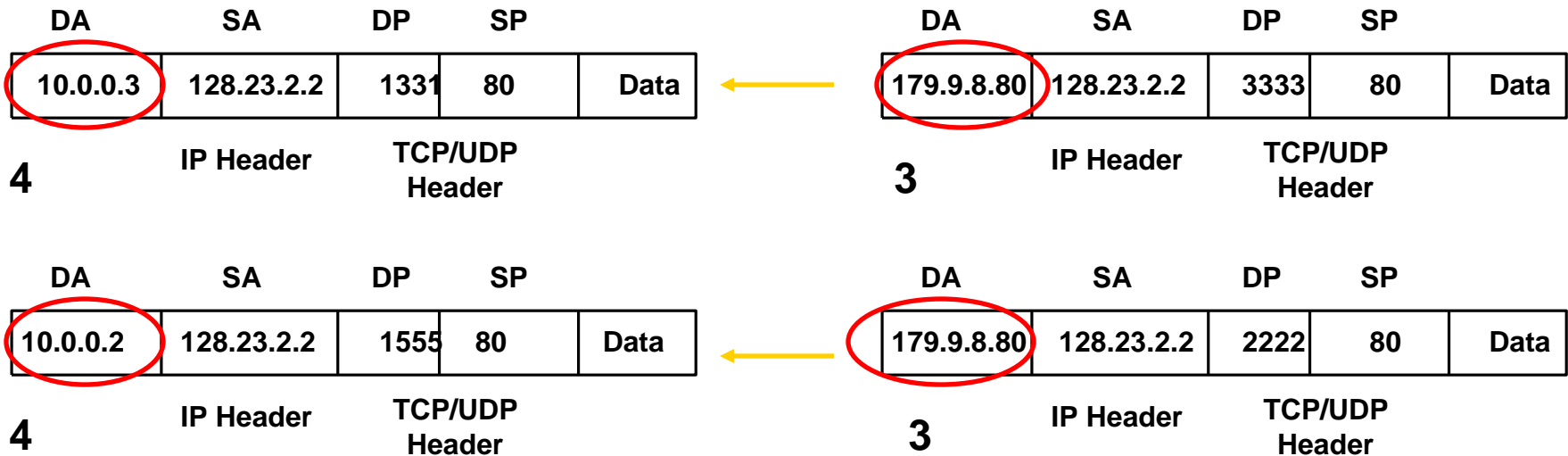
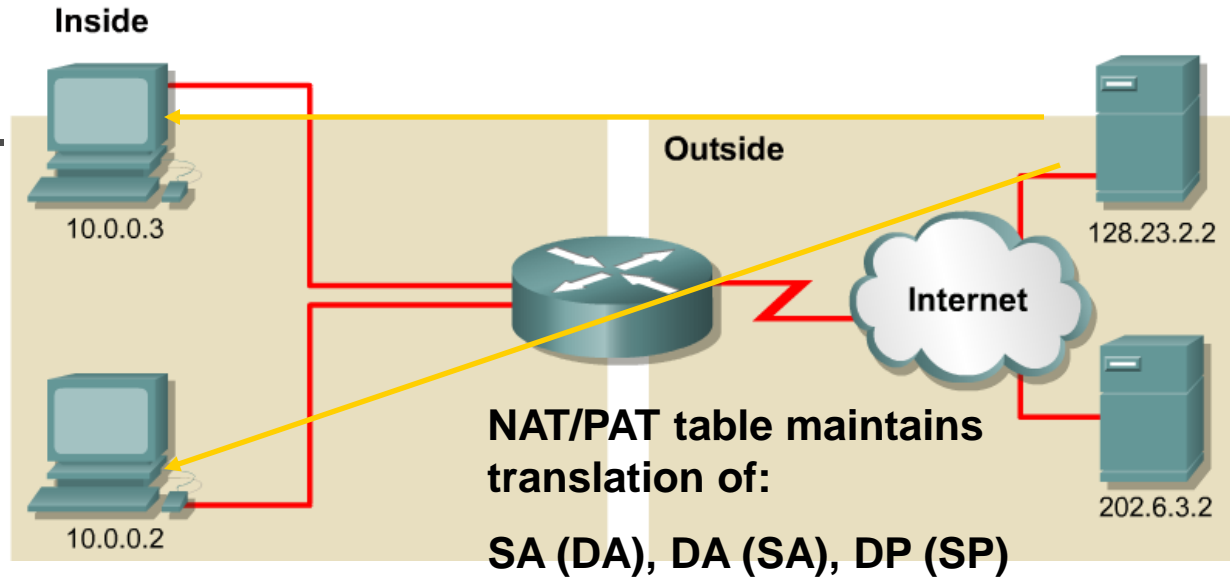
- PAT (Port Address Translation) allows you to use a single Public IP address and assign it up to 65,536 inside hosts (4,000 is more realistic).
- PAT translates and records the TCP/UDP source port address to track inside Host addresses.

PAT Example



PAT Example

How Would the NAT Table Look





Translation Modes

- Static Translation
 - a block of external addresses are translated to a same size block of internal addresses
- Dynamic Translation (IP Masquerading, PAT)
 - large number of internal users share a single external address
- Load Balancing Translation
 - a single incoming IP address is distributed across a number of internal servers
- Network Redundancy Translation
 - multiple internet connections are attached to a NAT Firewall that it chooses and uses based on bandwidth, congestion and availability.



Static Translation

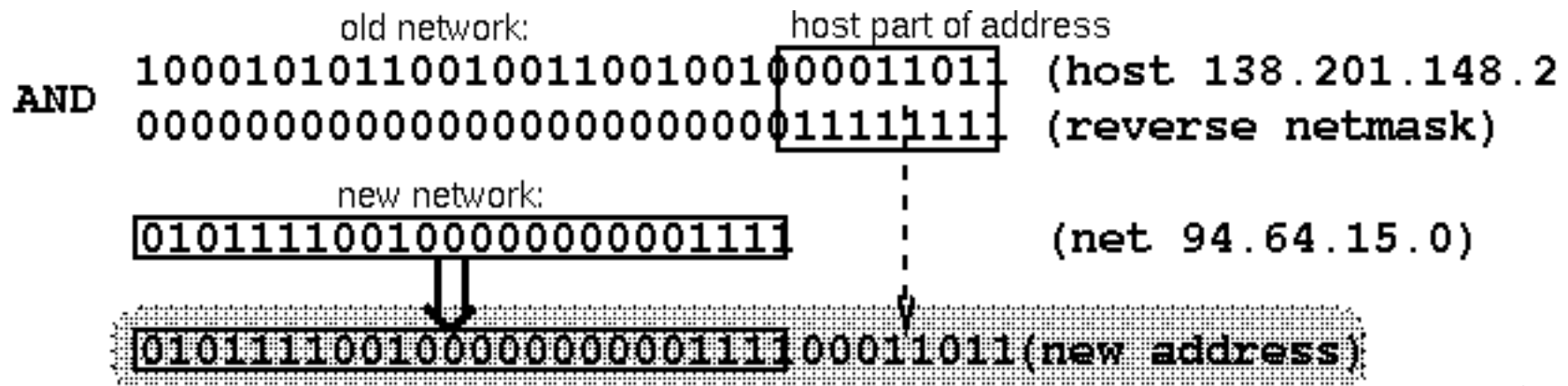
- Map a range of external address to the same size block of internal addresses
 - Firewall just does a simple translation of each address
- Port forwarding - map a specific port to come through the Firewall rather than all ports; useful to expose a specific service on the internal network to the public network

Static Translation Example

- Simple pseudo-code:

new-address = new-network OR (old-address AND (NOT netmask))

Example: NAT rule: translate all IPs in network 138.201.148 to IPs in network 94.64.15, netmask is 255.255.255.0 for both now 138.201.148.27 is translated to 94.64.15.27, and so on





Dynamic Translation

- Also called Network Address and Port Translation (NAPT) or PAT
- Individual hosts inside the firewall are identified based on each connection flowing through the firewall.
 - Since a connection doesn't exist until an internal host requests a connection through the firewall to an external host, and most firewalls only open ports only for the addressed host, only that host can route back into the internal network
- IP Source routing could route back in; but, most firewalls block incoming source routed packets
- NAT only prevents external hosts from making connections to internal hosts.
- Some protocols won't work (FTP); protocols that rely on separate connections back into the local network
- Theoretical max of 2^{16} connections per address, actual is much less

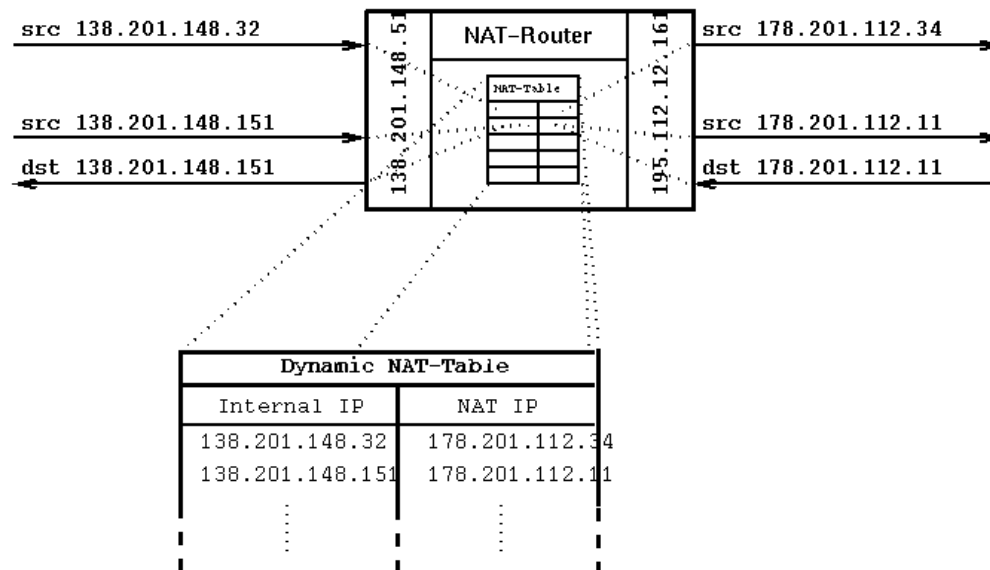


Dynamic Translation (Continued)

- Necessary when the number of IPs to translate does not equal the number of IPs to translate to
- The number of hosts communicating is generally limited by the number of NAT IPs available
- Dynamic NAT is more complex than static NAT, since we must keep track of communicating hosts and possibly even of connections which requires looking at TCP information in packets.

Dynamic Translation Example

- **Example: NAT rule: dynamically translate all IPs in (class B) network 138.201 to IPs in (class C) network 178.201.112**
- **Each new connection from the inside gets assigned an IP from the pool of class C addresses, as long as there are unused addresses left**
- **If a mapping already exists for the internal host this one is used instead**
- **As long as the mapping exists the internal host can be reached via the IP that has been (temporarily) assigned to it**



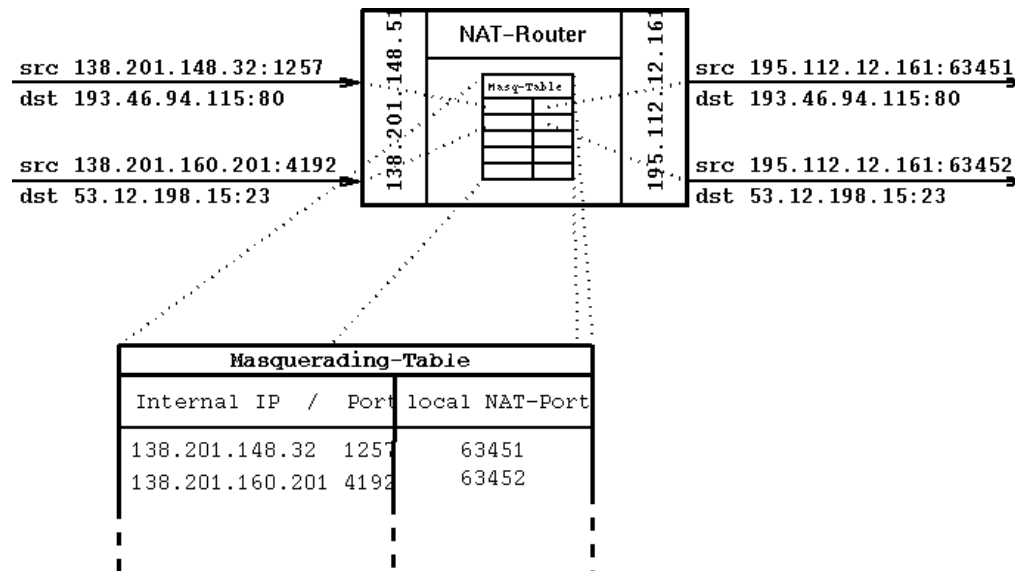


Masquerading (NAPT)

- A very special case of dynamic NAT is m:1-translation
- Probably the kind of NAT-technique that is used most often these days

Masquerading (NAPT) Example

- NAT rule: masquerade the internal network 138.201 using the NAT routers own address
- For each outgoing packet the source IP is replaced by the routers (external) IP, and the source port is exchanged against an unused port from the range reserved exclusively for masquerading on the router
- If the destination IP of an incoming packet is the local router IP and the destination port is inside the range of ports used for masquerading on the router, the NAT router checks its masquerading table if the packet belongs to a masqueraded session; if this is the case, the destination IP and port of the internal host is inserted and the packet is sent to the internal host





Load Balancing

- A firewall that will dynamically map a request to a pool of identical clone machines
 - often done for really busy web sites
 - each clone must have a way to notify the Firewall of its current load so the Firewall can choose a target machine
 - or the firewall just uses a dispatching algorithm like round robin
- Only works for stateless protocols (like HTTP)



Network Redundancy

- Can be used to provide automatic fail-over of servers or load balancing
- Firewall is connected to multiple ISP with a masquerade for each ISP and chooses which ISP to use based on client load
 - kind of like reverse load balancing
 - a dead ISP will be treated as a fully loaded one and the client will be routed through another ISP



NAT Benefits

- Eliminates re-assigning each host a new IP address when changing to a new ISP
- Eliminates the need to re-address all hosts that require external access, saving time and money
- Conserves addresses through application port-level multiplexing
- Provides basic network security



Problems with NAT

- Hides the internal network structure
 - Some consider this an advantage
- Some protocols carry addresses
 - E.g., ICMP carries addresses in text
 - What is the problem?
- Must update transport protocol headers (port number & checksum)
- Encryption
- No inbound connections



Problems with NAT

- Can't be used with:
 - protocols that require a separate back-channel
 - protocols that encrypt TCP headers
 - embed TCP address info
 - specifically use original IP for some security reason



Services that NAT has problems with

- H.323, CUSeeMe, VDO Live – video teleconferencing applications
- Xing – Requires a back channel
- Rshell – used to execute command on remote Unix machine – back channel
- IRC – Internet Relay Chat – requires a back channel
- PPTP – Point-to-Point Tunneling Protocol
- SQLNet2 – Oracle Database Networking Services
- FTP – Must be RFC-1631 compliant to work
- ICMP – sometimes embeds the packed address info in the ICMP message
- IPSec – used for many VPNs
- IKE – Internet Key Exchange Protocol
- ESP – IP Encapsulating Security Payload



Conclusion

- NAT can be static or dynamic
- Uses a set of predefined private addresses
- Conserves legal IPv4 addresses
- NAT plus PAT often used
- PAT uses unique source port numbers on the inside global IP address to distinguish between translations
- Provides a level of security