NAT
Network Address Translation

Mario Baldi

Politecnico di Torino

mario.baldi@polito.it

staff.polito.it/mario.baldi

Nota di Copyright

Operating Principle

- Outbound packet
  - Substitute IP source address with another one
- Inbound packet
  - Substitute IP destination address with original one

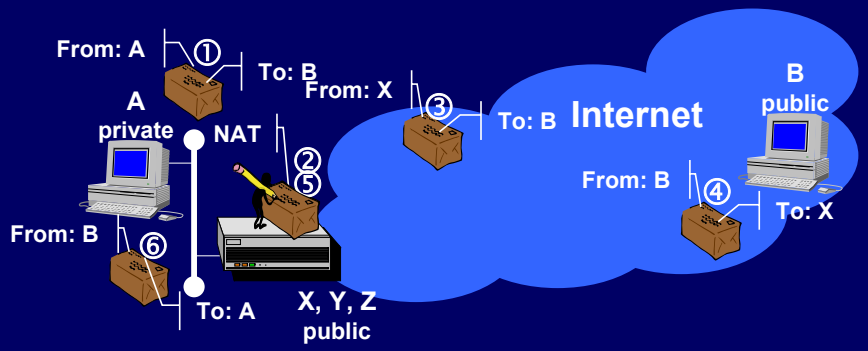
Applications

- Public access with private addressing
  - Public Address Expansion
- (Private) Address Overlapping
- Privacy
  - Address hiding
- Policy compliance

Public Address Expansion

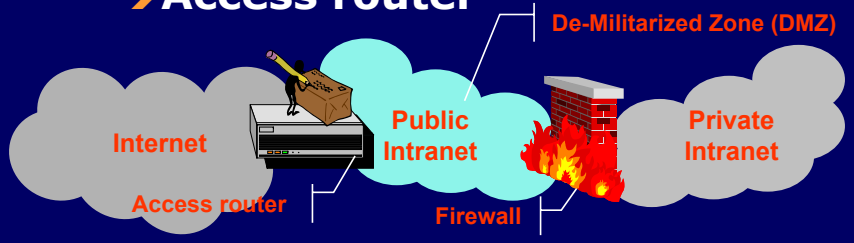
- Outbound packet
  - Substitute *private* IP source address with *public* one
- Inbound packet
  - Substitute *public* IP destination address with original *private* one

Public Address Expansion

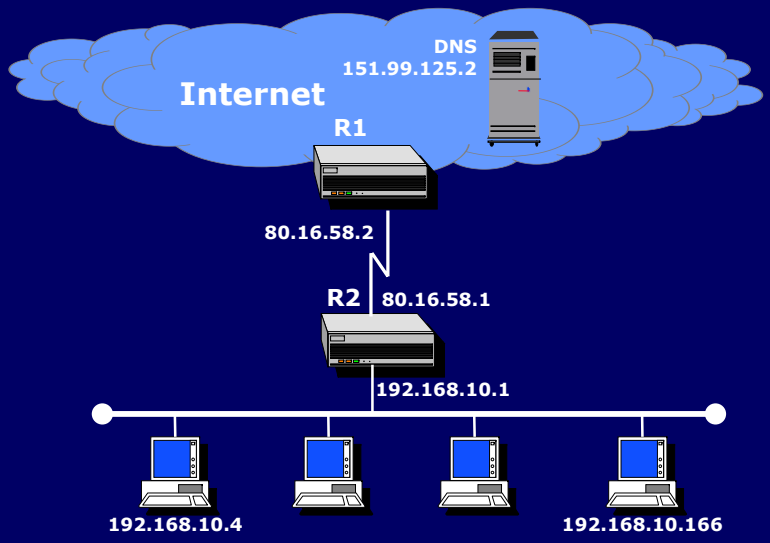


Public Address Expansion

- One IP address dynamically shared by many hosts
- At the edge between enterprise intranet and the Internet
  - Firewall
  - Access router



Case Study

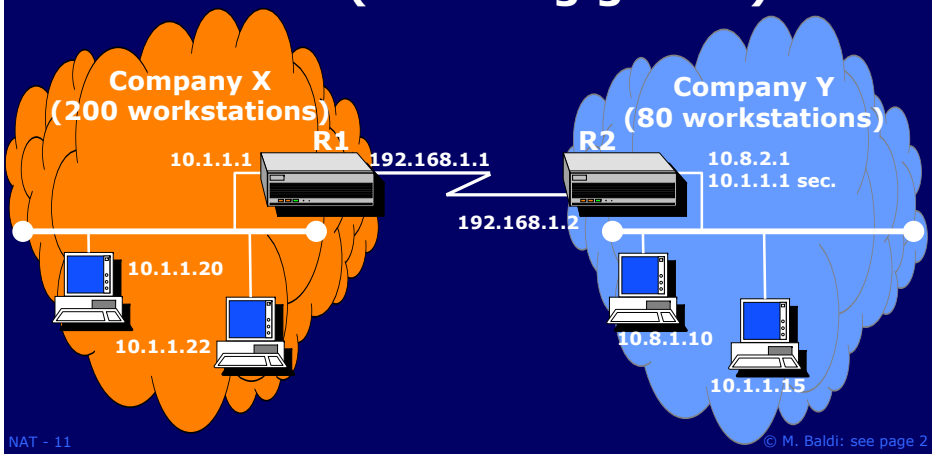


Sample R2 Configuration

```
interface Ethernet0
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
!
interface serial0
 ip address 80.16.58.1 255.255.255.252
 ip nat outside
!
ip nat inside source list 1 interface
     serial0 overload
access-list 1 permit 192.168.10.0 0.0.0.255
!
ip route 0.0.0.0 0.0.0.0 80.16.58.2
!
```


Private Address Overlapping

- Merging and acquisition
- Extranets (including guests)



R2 Translation Table

Visualizzazione della tabella delle traduzioni

```
router#sho ip nat translation
Pro Inside global      Inside local       Outside local      Outside glo
tcp 80.16.58.1:1056 192.168.10.4:1056  213.212.128.8:80   213.212.128.8:
tcp 80.16.58.1:1027 192.168.10.166:1027 195.31.235.39:21  195.31.235.39:
tcp 80.16.58.1:1028 192.168.10.166:1028 195.31.235.39:20  195.31.235.39:
tcp 80.16.58.1:1098 192.168.10.4:1098  195.31.235.39:21   195.31.235.39:
tcp 80.16.58.1:1099 192.168.10.4:1099  195.31.235.39:20   195.31.235.39:
udp 80.16.58.1:137  192.168.10.166:137 151.99.125.2:53    151.99.125.2:5
tcp 80.16.58.1:1058 192.168.10.4:1058  212.110.36.130:80  212.110.36.130
tcp 80.16.58.1:1059 192.168.10.4:1059  212.110.36.130:80  212.110.36.130
tcp 80.16.58.1:1060 192.168.10.4:1060  212.110.36.130:80  212.110.36.130
udp 80.16.58.1:137  192.168.10.4:137   151.99.125.2:53    151.99.125.2:5
```

Indirizzo pubblico di traduzione

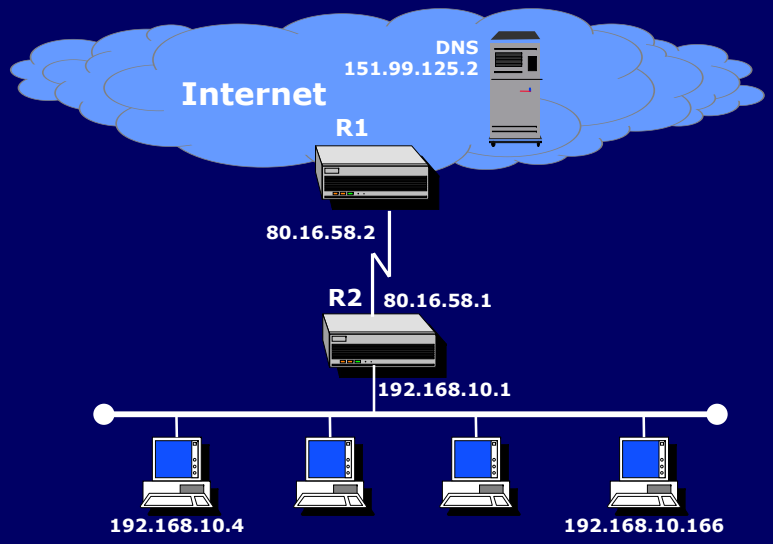
Risoluzione nomi indirizzi tramite DNS pubblico

3 pagine HTTP aperte dal client 192.168.10
verso il server 212.110.36.1

Sample R2 Configuration

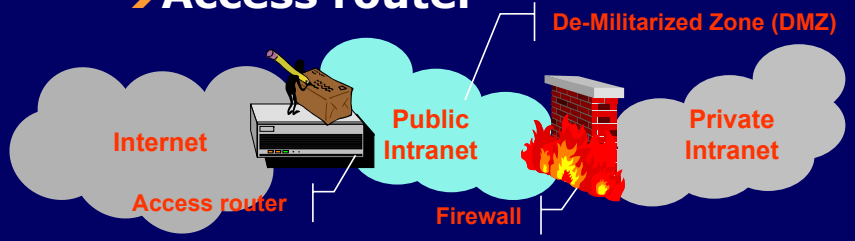
```
interface Ethernet0
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
!
interface serial0
 ip address 80.16.58.1 255.255.255.252
 ip nat outside
!
ip nat inside source list 1 interface
     serial0 overload
access-list 1 permit 192.168.10.0 0.0.0.255
!
ip route 0.0.0.0 0.0.0.0 80.16.58.2
!
```

Case Study

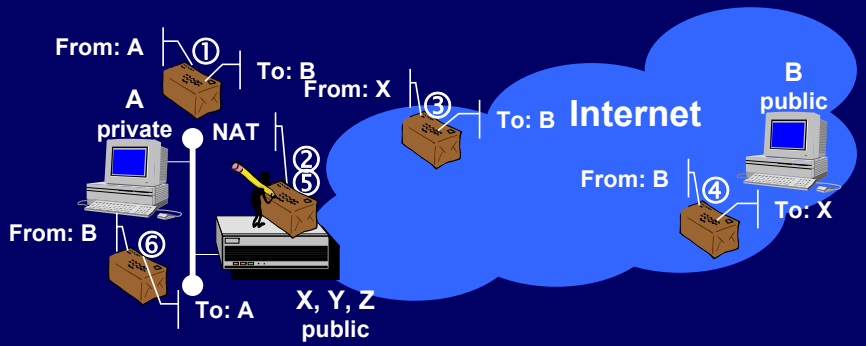


Public Address Expansion

- One IP address dynamically shared by many hosts
- At the edge between enterprise intranet and the Internet
  - Firewall
  - Access router



Public Address Expansion



Public Address Expansion

- Outbound packet
  - Substitute *private* IP source address with *public* one
- Inbound packet
  - Substitute *public* IP destination address with original *private* one

PAT: Port Address Translation

- AKA NAT overload
- Multiple (private) addresses mapped onto the same (public) address
- Source port is mapped onto random unique port
- It does not work when a specific port is needed
  - IPSec (IP Security), DNS, etc.

NAT and IPSec

- Transport mode
  - No problem without key exchange
- Authentication Header (AH)
  - IP addresses are part of AH checksum calculation
  - Received packets are discarded

NAT and IPsec

- Tunnel mode
  - Probably NAT is not needed
  - Translation of tunnel end-point address is critical

References

- K. Egevang, P. Francis, "The IP Network Address Translator (NAT)," RFC 1631, May 1994