



NAT

Network Address Translation

Mario Baldi

Politecnico di Torino

(Technical University of Turin)

<http://staff.polito.it/mario.baldi>

Nota di Copyright

This set of transparencies, hereinafter referred to as slides, is protected by copyright laws and provisions of International Treaties. The title and copyright regarding the slides (including, but not limited to, each and every image, photography, animation, video, audio, music and text) are property of the authors specified on page 1.

The slides may be reproduced and used freely by research institutes, schools and Universities for non-profit, institutional purposes. In such cases, no authorization is requested.

Any total or partial use or reproduction (including, but not limited to, reproduction on magnetic media, computer networks, and printed reproduction) is forbidden, unless explicitly authorized by the authors by means of written license.

Information included in these slides is deemed as accurate at the date of publication. Such information is supplied for merely educational purposes and may not be used in designing systems, products, networks, etc. In any case, these slides are subject to changes without any previous notice. The authors do not assume any responsibility for the contents of these slides (including, but not limited to, accuracy, completeness, enforceability, updated-ness of information hereinafter provided).

In any case, accordance with information hereinafter included must not be declared.

In any case, this copyright notice must never be removed and must be reported even in partial uses.

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

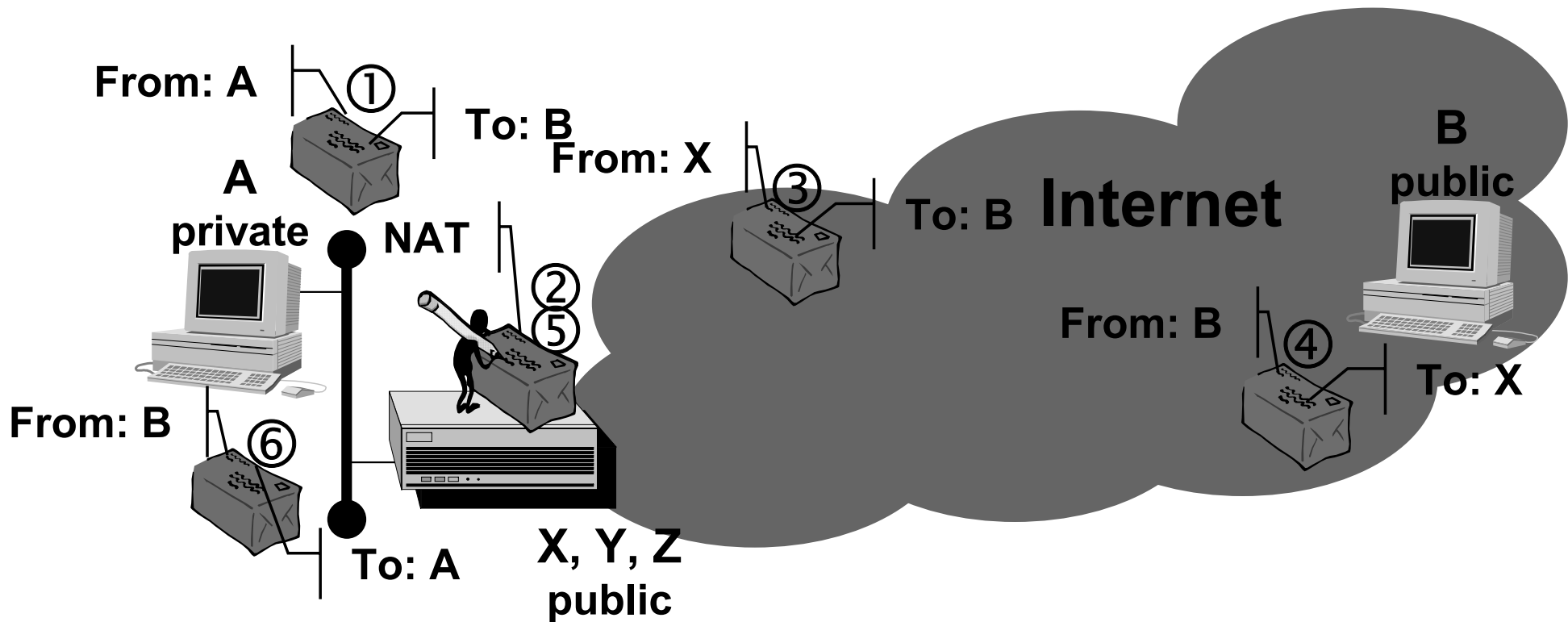
→ **Outbound packet**

→ **Substitute *private* IP source address with *public* one**

→ **Inbound packet**

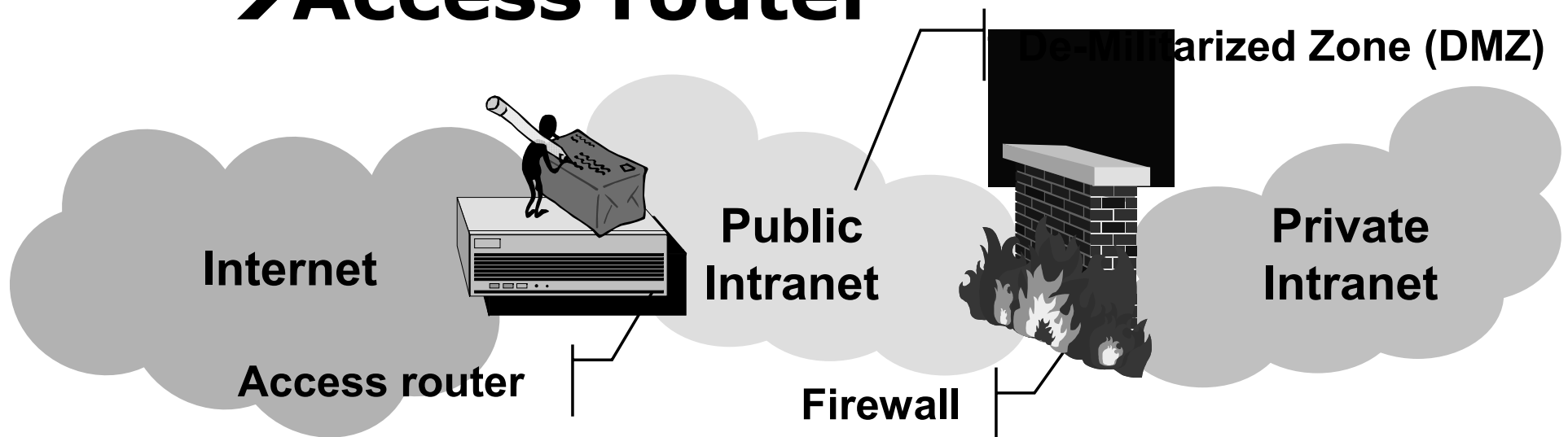
→ **Substitute *public* IP destination address with original *private* one**

Public Address Expansion

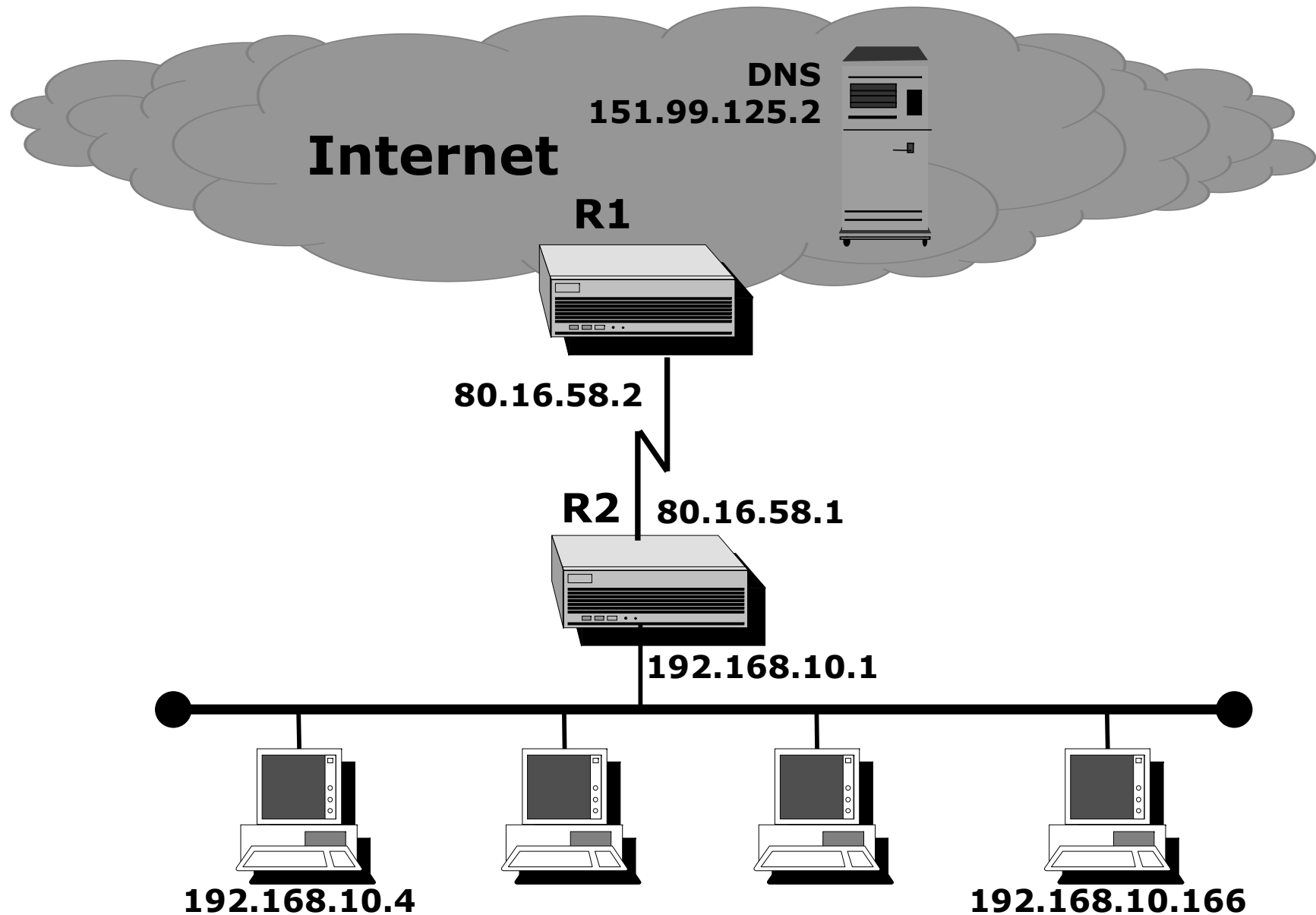


Public Address Expansion

- 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
  !
```

R2 Translation Table

Visualizzazione della tabella delle traduzioni

```
router#sho ip nat translation
```

Pro	Inside global	Inside local	Outside local	Outside global
tcp	80.16.58.1:1056	192.168.10.4:1056	213.212.128.8:80	213.212.128.8:80
tcp	80.16.58.1:1027	192.168.10.166:1027	195.31.235.39:21	195.31.235.39:21
tcp	80.16.58.1:1028	192.168.10.166:1028	195.31.235.39:20	195.31.235.39:20
tcp	80.16.58.1:1098	192.168.10.4:1098	195.31.235.39:21	195.31.235.39:21
tcp	80.16.58.1:1099	192.168.10.4:1099	195.31.235.39:20	195.31.235.39:20
udp	80.16.58.1:137	192.168.10.166:137	151.99.125.2:53	151.99.125.2:53
tcp	80.16.58.1:1058	192.168.10.4:1058	212.110.36.130:80	212.110.36.130:80
tcp	80.16.58.1:1059	192.168.10.4:1059	212.110.36.130:80	212.110.36.130:80
tcp	80.16.58.1:1060	192.168.10.4:1060	212.110.36.130:80	212.110.36.130:80
udp	80.16.58.1:137	192.168.10.4:137	151.99.125.2:53	151.99.125.2:53

3 pagine HTTP aperte dal client 192.168.10.4
verso il server 212.110.36.130

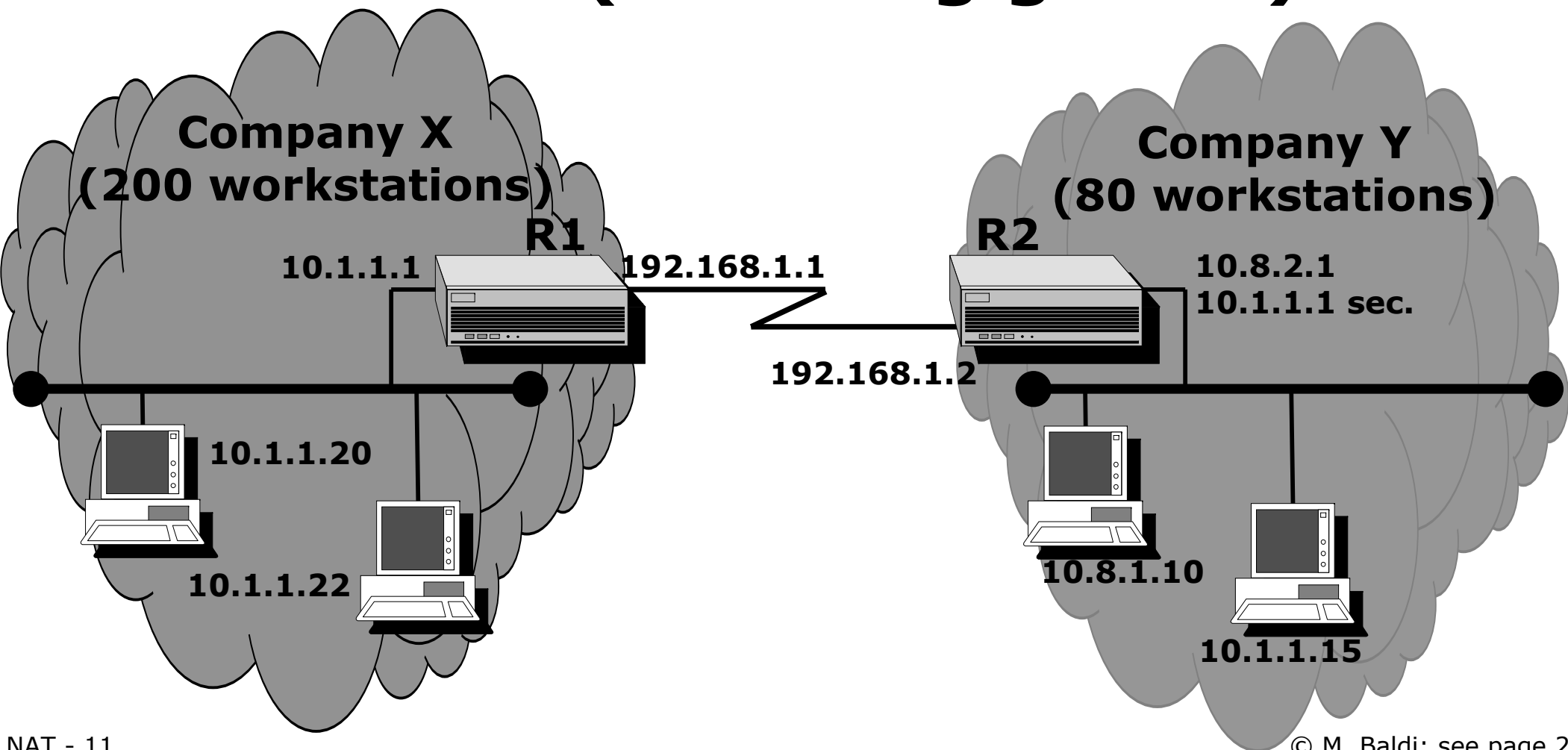
Indirizzo pubblico di traduzione

Risoluzione nomi indirizzi tramite DNS pubblico

Private Address Overlapping

→ Merging and acquisition

→ Extranets (including guests)



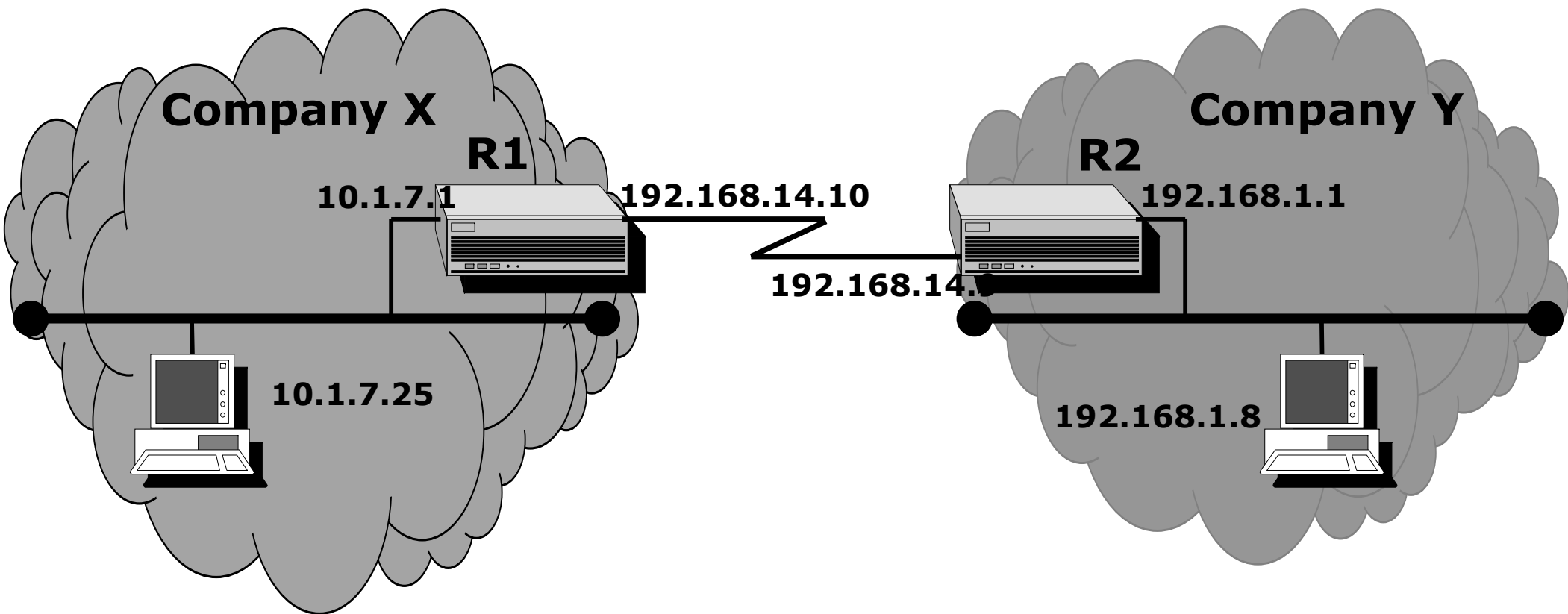
Sample Configuration: R1

```
ip nat inside source static 10.1.1.20 10.10.1.20
ip nat inside source static 10.1.1.22 10.10.1.22
!
interface serial 0
ip address 192.168.1.1 255.255.255.252
ip nat outside
!
interface ethernet 0
ip address 10.1.1.1 255.255.255.0
ip nat inside
!
ip route 10.8.1.10 255.255.255.255 192.168.1.2
```

Sample Configuration: R2

```
interface serial 0
ip address 192.168.1.2 255.255.255.252
!
interface ethernet 0
ip address 10.1.8.1 255.255.255.0
ip address 10.1.1.1 255.255.255.0 sec
!
ip route 10.10.1.20 255.255.255.255 192.168.1.1
ip route 10.10.1.22 255.255.255.255 192.168.1.1
!
```

Address Hiding or Adjustment



Policy Compliance: why?

→ **Routing Optimization**

→ **Security/filtering**

→ **Management**

```

!
ip nat inside source static 10.1.7.25 192.168.244.45
!
interface Ethernet0
  ip address 10.1.7.1 255.255.255.252
  ip nat inside
!
!
interface Serial0
  ip address 192.168.14.10 255.255.255.252
  ip nat outside
!
!
ip route 192.168.1.8 255.255.255.255 192.168.14.9
!

```



Traduzione da indirizzo inside a nuovo indirizzo

Definizione dell'interfaccia
inside

Definizione dell'interfaccia outside

Visualizzazione della tabella delle traduzioni

```

*****
**
router#sho ip nat translation
Pro Inside global tradotto Inside local Outside local Outside
global
--- 192.168.244.45          10.1.7.25          ---          ---

```

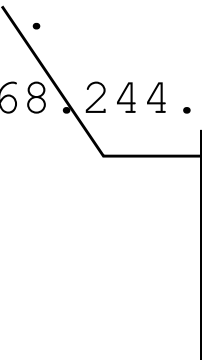


Indirizzo
reale

Indirizzo

tradotto

```
!  
interface Ethernet0  
  ip address 192.168.1.1 255.255.255.0  
!  
interface Serial0  
  ip address 192.168.14.9 255.255.255.252  
!  
ip route . . . .  
ip route 192.168.244.45 255.255.255.255 192.168.14.10  
!
```



**Route esclusiva verso
l'indirizzo IP presunto
(prefisso di rete a 30 bit)**

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

→ Authentication Header (AH)

→ IP addresses are part of AH checksum calculation

→ Received packets are discarded

→ Encapsulation Security Payload (ESP)

→ Ports might be hidden

→ No address expansion

NAT and IPsec

→ Tunnel mode

→ Probably NAT is not needed

→ Translation of tunnel endpoint address is critical

References

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