



I indirizzamento privato e NAT

Contenuti del corso

- **La progettazione delle reti**
- **Il routing nelle reti IP**
- **Il collegamento agli Internet Service Provider e problematiche di sicurezza**
- **Analisi di traffico e dei protocolli applicativi**
- **Multimedialità in rete**
- **Tecnologie per le reti future**

Contenuti del corso

- La progettazione delle reti
- Il routing nelle reti IP
- Il collegamento agli Internet Service Provider e problematiche di sicurezza
- Analisi di traffico e dei protocolli applicativi
- Multimedialità in rete
- Tecnologie per le reti future

Internet e indirizzi IP

IANA (Internet Assigned Numbers Authority)

**Ente centrale che gestisce
l'assegnazione degli indirizzi IP
su scala mondiale**

Internet e indirizzi IP

Lo IANA:

- Delega altri enti su base continentale (Europa: RIPE)
- Garantisce l'unicità degli indirizzi su Internet
- Assegna gli indirizzi a lotti di interesse sottoreti

Indirizzi IP pubblici

- Un ente potrebbe acquistare dallo IANA una o più sottoreti IP per collegare a Internet la LAN
- La scarsità di indirizzi IP pubblici rende tale acquisto assai oneroso
- Soluzione ormai improponibile per gli utenti finali di Internet

Indirizzi IP pubblici

Necessari per i sistemi che devono essere raggiungibili da tutti gli host di Internet

- **Server Web per e-commerce**
- **Server di posta elettronica (POP3, SMTP)**
- **Server di database e sistemi per applicazioni B2B**

Internet e intranet

Per realizzare una intranet non è necessario disporre di indirizzi ufficiali assegnati dallo IANA

Tecniche per l'internetworking tra Internet e una rete intranet con **indirizzi privati**

Indirizzi IP per uso privato

- **Indirizzi IP validi (RFC 1918)**
- **Possono essere assegnati solamente agli host di una intranet**
- **Indirizzi riutilizzabili, non hanno significato a livello globale**

Indirizzi IP per uso privato

Appartengono alle seguenti reti:

- **Rete 10 (classe A)**
da 10.0.0.0 a 10.255.255.255
- **Parte della rete 172 (classe B)**
da 172.16.0.0 a 172.31.255.255
- **Rete 192 (classe C)**
da 192.168.0.0 a 192.168.255.255

Indirizzi IP di loopback

La rete 127.0.0.0 (di classe A) è usata dai sistemi operativi come rete di "loopback"

Permette di provare il funzionamento del software senza usare realmente la rete

Indirizzi IP di loopback

Esempio
(effettua il ping su se stesso):

```
# ping 127.0.0.1
```

Internetworking

Gli indirizzi delle reti private non possono essere annunciati dai router collegati a Internet

L'accesso ad Internet per una rete intranet con indirizzi IP privati richiede l'uso di tecniche avanzate

NAT

Network Address Translation

RFC 1631, 2663

Offre connettività a Internet per le reti con indirizzamento privato

NAT: vantaggi

- Limita il numero di indirizzi IP pubblici necessari per collegare una LAN a Internet
- Mantiene inalterata la configurazione degli host

NAT: vantaggi

- **Non modifica il funzionamento dei protocolli e delle applicazioni della rete intranet**
- **Flessibilità elevata grazie allo spazio di indirizzi privati molto esteso**

NAT: vantaggi

- **Riduzione dei costi di accesso a Internet**
- **Maggiore sicurezza per i calcolatori della rete locale**

NAT



NAT: funzionalità

- **Corrispondenza biunivoca tra indirizzi esterni e interni (Static NAT)**
- **Traduzione dinamica degli indirizzi di origine (Dynamic NAT)**
- **Traduzione dinamica delle porte di origine (Port Address Translation, o IP masquerading)**

IP masquerading

Caso tipico nelle reti aziendali

- Permette di condividere una singola connessione a Internet per più calcolatori di una intranet
- Utilizza un solo indirizzo IP pubblico
- Traduce in modo dinamico gli indirizzi e le porte di origine del flusso di dati

IP masquerading

Utilizzato nel caso degli accessi xDSL o ISDN per piccole LAN

Alcuni sistemi operativi offrono tale funzionalità in modo nativo (Windows ME/2000/XP, Linux)

NAT: esempio di funzionamento

NAT

192.168.1.1



intranet

192.168.1.254

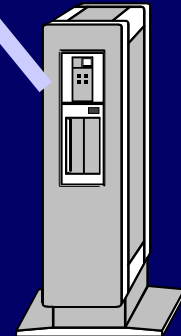
router



158.109.1.253



Internet

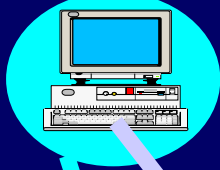


62.41.244.2

L'host 192.168.1.1 (client)
deve contattare un server web
su Internet

NAT

192.168.1.1



192.168.1.254

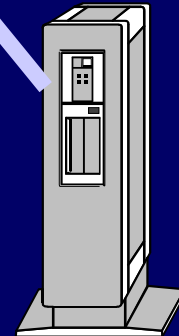
intranet

router



158.109.1.253

Internet



62.41.244.2

Il client invia al default router un pacchetto IP avente:

SIP 192.168.1.1 SPort 30231/TCP

DIP 62.41.244.2 DPort 80/TCP

NAT

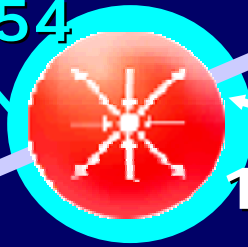
192.168.1.1



intranet

192.168.1.254

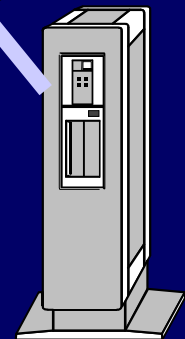
router



158.109.1.253



Internet



62.41.244.2

**Il router, prima di inoltrarlo,
modifica l'indirizzo sorgente:
192.168.1.1 \Rightarrow 158.109.1.253**

NAT

192.168.1.1



intranet

192.168.1.254

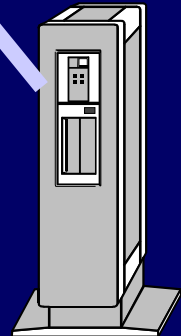
router



158.109.1.253



Internet



62.41.244.2

**Il router, prima di inoltrarlo,
modifica la porta sorgente:
30231/TCP \Rightarrow 1024/TCP**

NAT

192.168.1.1

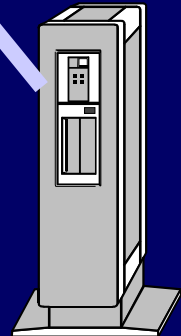


192.168.1.254

router



158.109.1.253



62.41.244.2

Il router inserisce un record nella Dynamic NAT table per tenere traccia del flusso di dati uscente

NAT

192.168.1.1



intranet

192.168.1.254

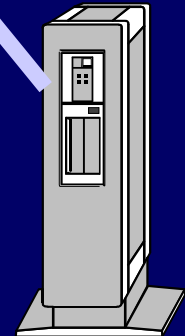
router



158.109.1.253



Internet



62.41.244.2

Dynamic NAT table

<i>Int address</i>	<i>Int port</i>	<i>Ext address</i>	<i>Ext port</i>	<i>Age</i>
192.168.1.1	30231/TCP	158.109.1.253	1024/TCP	

NAT

192.168.1.1



intranet

192.168.1.254

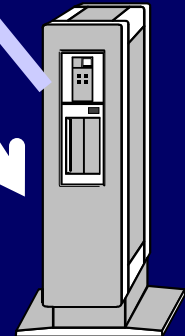
router



158.109.1.253



Internet



62.41.244.2

Il router inoltra il pacchetto modificato al next hop router e quindi al server Web

NAT

192.168.1.1



intranet

192.168.1.254

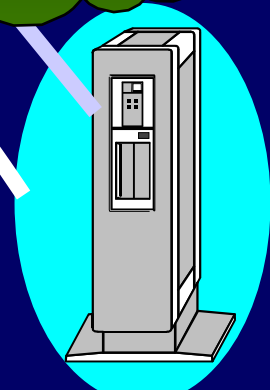
router



158.109.1.253



Internet



62.41.244.2

**Il server risponde al client
con un pacchetto avente:
SIP 62.41.244.2 SPort 80/TCP
DIP 158.109.1.253 DPort 1024/TCP**

NAT

192.168.1.1

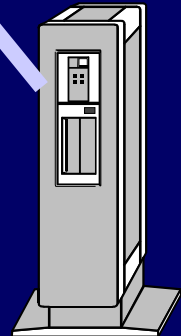


192.168.1.254

router



158.109.1.253



62.41.244.2

**Il router riceve il pacchetto
e consulta la Dynamic NAT
table alla ricerca di eventuali
regole di traduzione da applicare a ritroso**

NAT

192.168.1.1



intranet

192.168.1.254

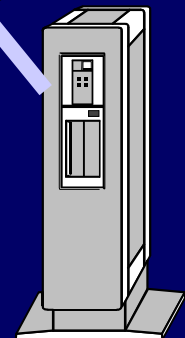
router



158.109.1.253



Internet



Dynamic NAT table

<i>Int address</i>	<i>Int port</i>	<i>Ext address</i>	<i>Ext port</i>	<i>Age</i>
192.168.1.1	30231/TCP	158.109.1.253	1024/TCP	

NAT

192.168.1.1



intranet

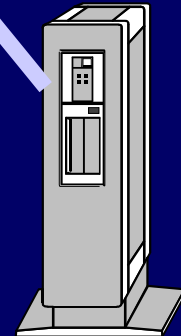
192.168.1.254

router



158.109.1.253

Internet



62.41.244.2

Il router prima di inoltrare
il pacchetto ne modifica
l'indirizzo IP di destinazione:
 $158.109.1.253 \Rightarrow 192.168.1.1$

NAT

192.168.1.1

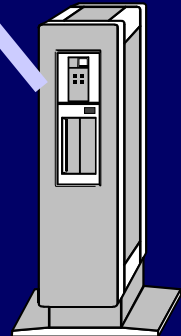


192.168.1.254

router



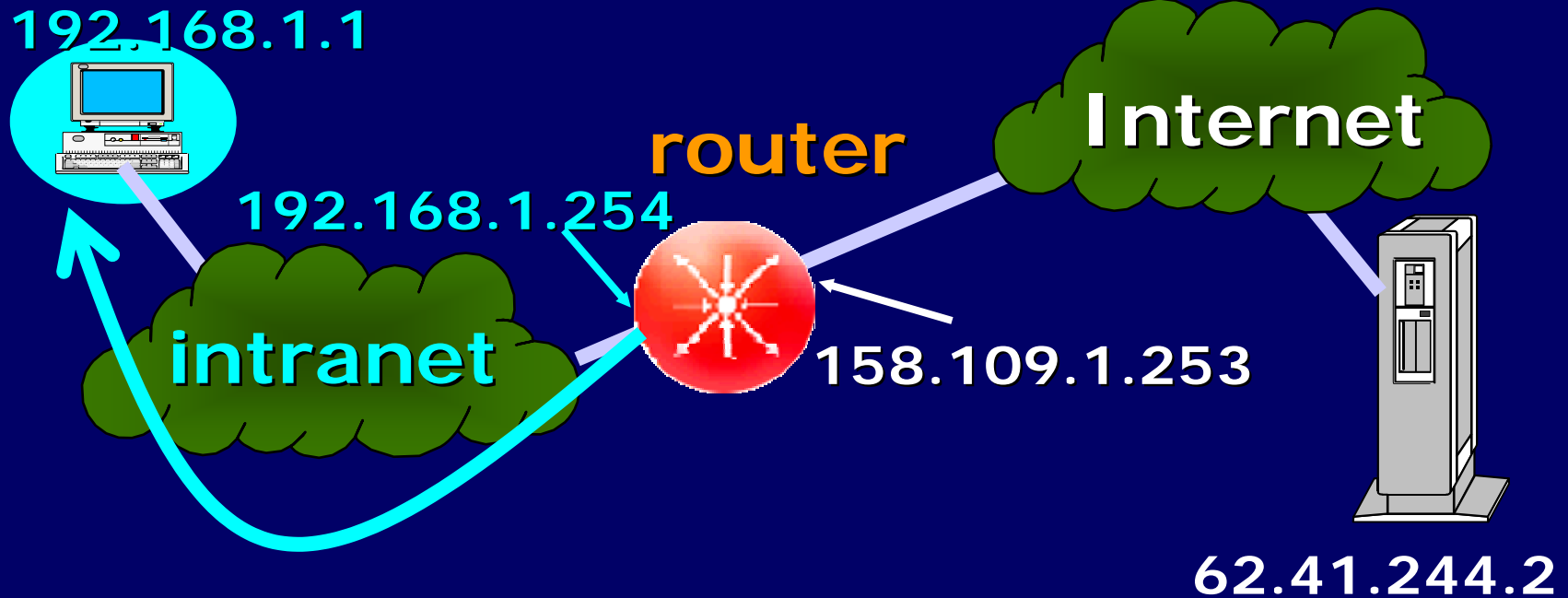
158.109.1.253



62.41.244.2

**Il router prima di inoltrare
il pacchetto ne modifica
la porta TCP di destinazione:
1024/TCP \Rightarrow 30231/TCP**

NAT



Il client riceve il pacchetto correttamente!

NAT: funzionalità

Ogni flusso TCP o UDP uscente dalla rete intranet genererà una nuova entry nella Dynamic NAT table del router

Porte TCP e UDP esterne usate dal router per la Port Address Translation (PAT): 1024 ÷ 4999
(RFC 2663)

NAT: funzionalità

Un client della rete interna:

Può connettersi a qualunque server della rete Internet

Non risente dalla traduzione di indirizzo e di porta effettuati dal default router

NAT e sicurezza

La traduzione non può aver luogo se il flusso ha origine dall'esterno verso un nodo interno

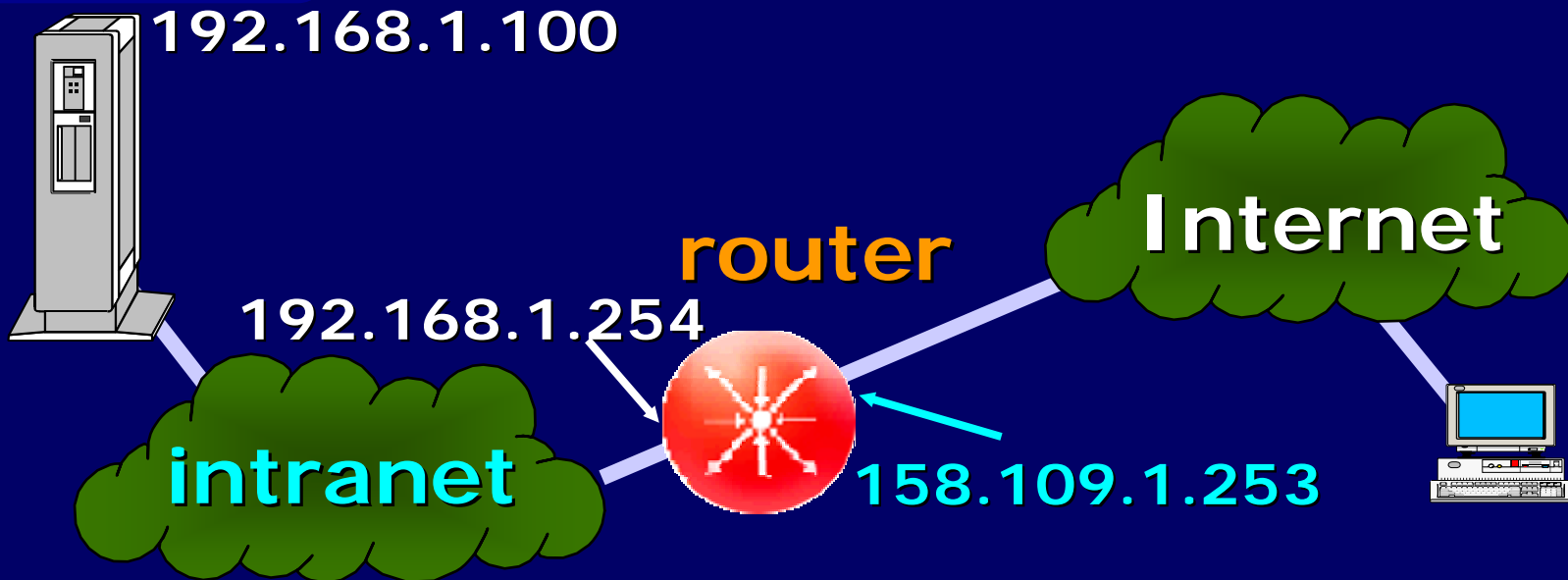
La sicurezza dei nodi interni è perciò intrinsecamente garantita

NAT: entry statiche

NAT e servizi interni

- Per rendere raggiungibile un server della rete interna occorre "forzare" la traduzione
- Si fa inserendo un'entry statica nella tabella del router (Static NAT)
- Può abbassare il livello di sicurezza della rete interna!

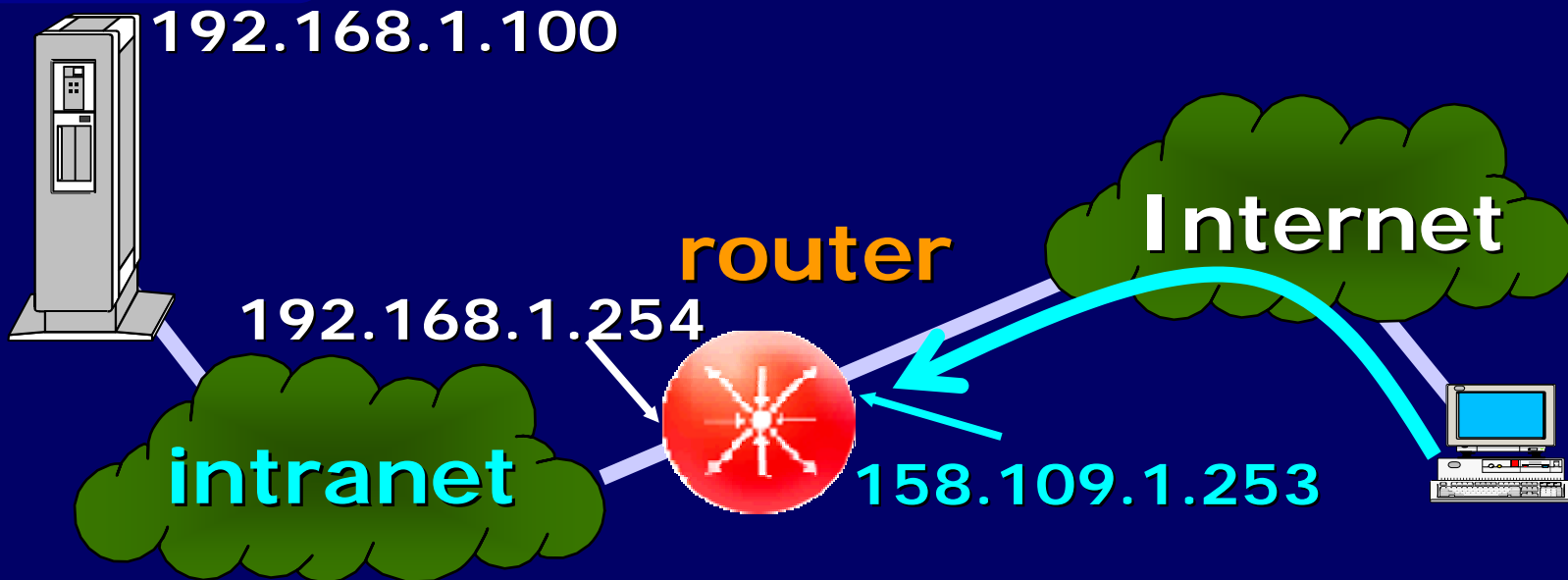
NAT



Static NAT table

<i>Ext address</i>	<i>Ext port</i>	<i>Int address</i>	<i>Int port</i>
158.109.1.253	80/TCP	192.168.1.100	80/TCP

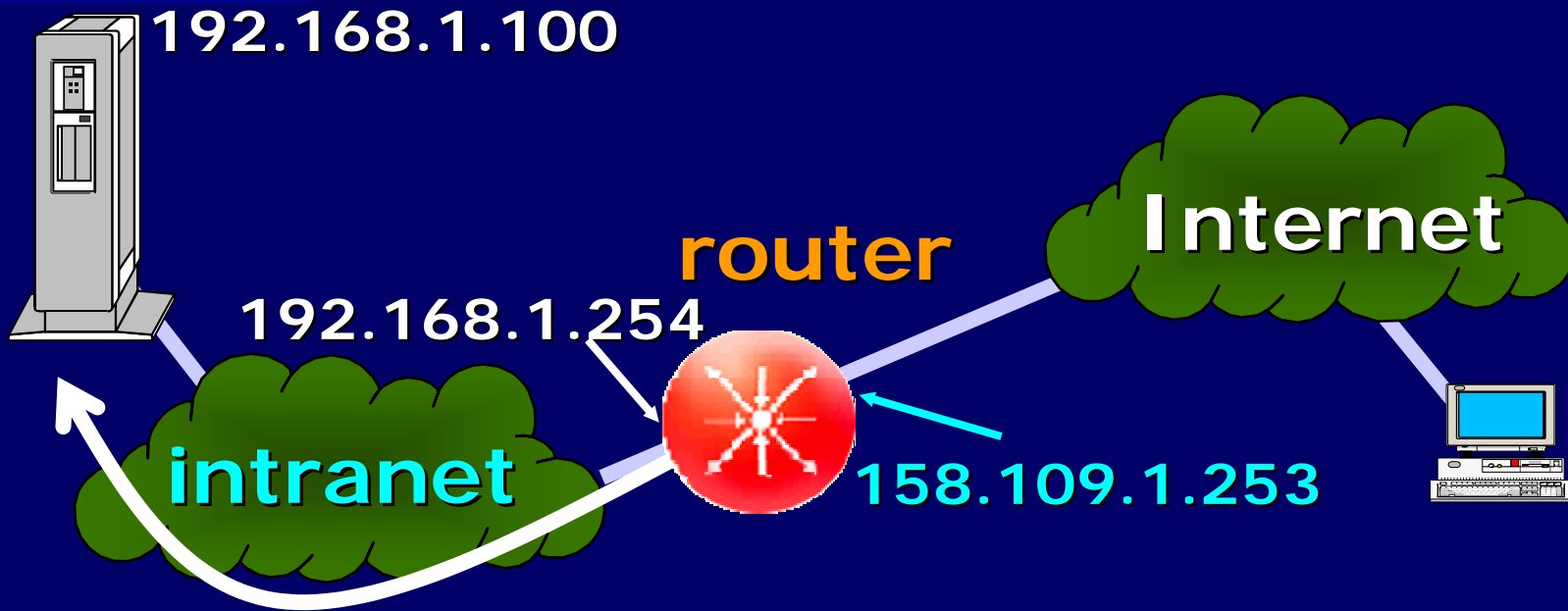
NAT



Static NAT table

<i>Ext address</i>	<i>Ext port</i>	<i>Int address</i>	<i>Int port</i>
158.109.1.253	80/TCP	192.168.1.100	80/TCP

NAT



Static NAT table

<i>Ext address</i>	<i>Ext port</i>	<i>Int address</i>	<i>Int port</i>
158.109.1.253	80/TCP	192.168.1.100	80/TCP



I indirizzamento privato e NAT