



**Antonio Cianfrani**

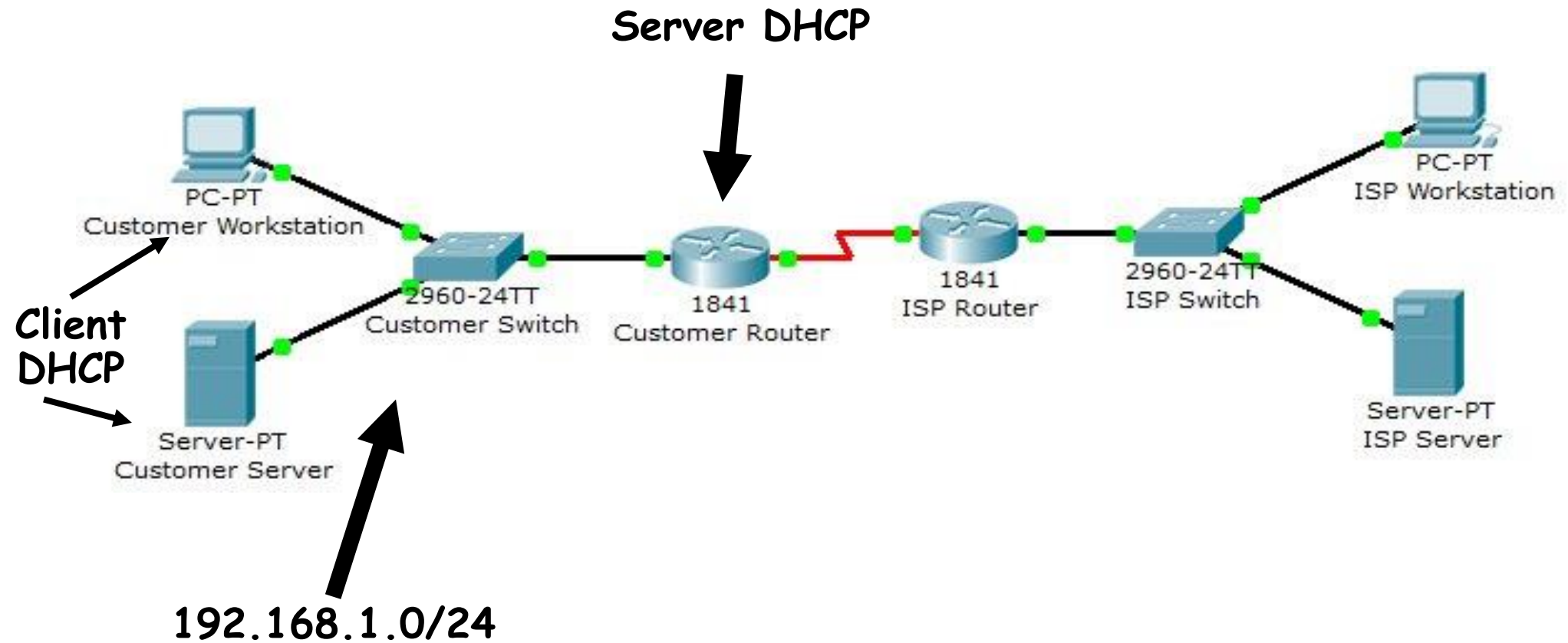
# **Dynamic Host Configuration Protocol (DHCP)**

# DHCP protocol



- The DHCP protocol allows to dynamically configure hosts in a LAN.
- Configuration parameters:
  - ✓ IP address and subnet mask
  - ✓ Default gateway
  - ✓ DNS Server

# Example



# Server DHCP configuration (1/3)

- The command to start DHCP configuration is

```
Router(config)#ip dhcp pool NAME_POOL
```

- NAME\_POOL is the name used to identify the DHCP configuration on the router
- The next step is the definition of the address pool to be assigned dynamically:

```
Router(config-dhcp)# network NET_ADDRESS NETMASK
```

- In the case of 10.0.0.0/8 block:

```
Router(config-dhcp)# network 10.0.0.0 255.0.0.0
```

## Server DHCP configuration (2/3)

- It could happen that the set of available IP addresses to be assigned dynamically is not exactly the pool
- Motivation: a host (usually a server) requires a static (fixed) IP address
- It is possible to exclude IP address from the pool

```
Router(config)#ip dhcp excluded-address IPADDRESS (ES)
```

- If the initial 49 addresses should be excluded:

```
Router(config)#ip dhcp excluded-address 192.168.1.1  
192.168.1.49
```

# Server DHCP configuration (3/3)

- To provide the Internet access, default router (192.168.1.1) and DNS server (192.168.1.10) must be configured

```
Router(config-dhcp)# default-router 192.168.1.1
```

```
Router(config-dhcp)# dns-server 192.168.1.10
```



Antonio Cianfrani

# Network Address Translation (NAT)


# Public and private IP addresses

- Problem: IP addresses are not enough to assign a unique IP address to each network host/device

Address Class	Number of Network Numbers Reserved	Network Addresses
A	1	10.0.0.0
B	16	172.16.0.0 - 172.31.0.0
C	256	192.168.0.0 - 192.168.255.0



# NAT (1/4)



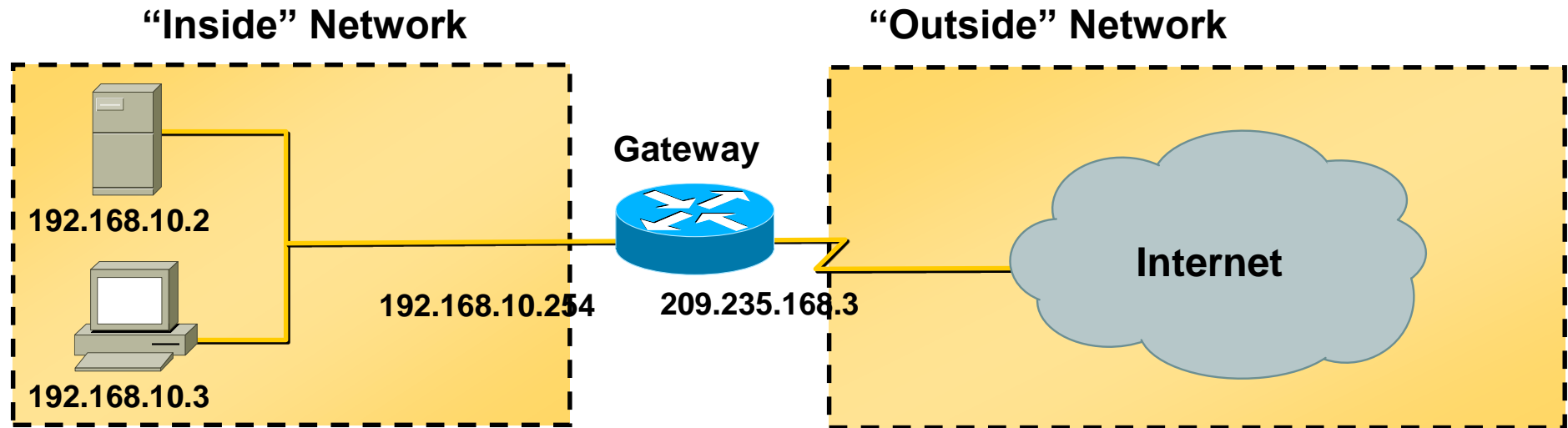
## ➤ **Advantages**

- No need to request public IP addresses for all the devices
- Reduction of public IP addresses
- Security improvement: real devices IP addresses hidden

## ➤ **Drawbacks:**

- Extra-load for access routers
- Breaking of the layers separation rule

# NAT (2/4)



# NAT (3/4)

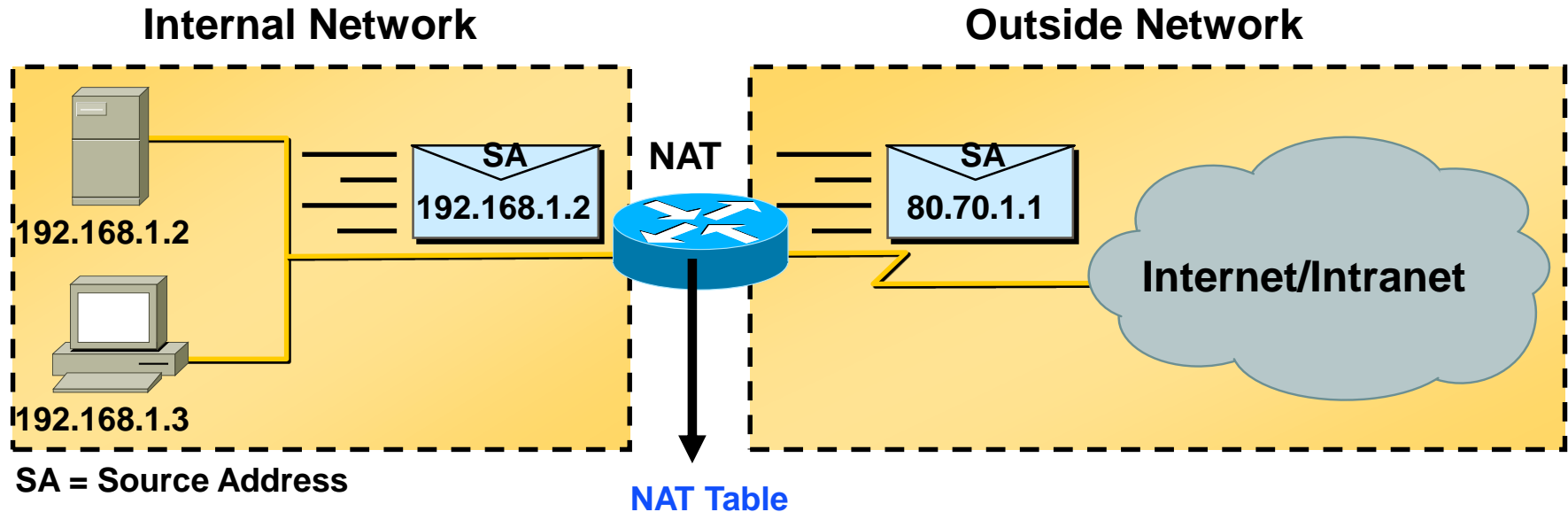


- The IP addresses of the local network (192.168.10.X) are not “visible” from outside.
- The router (Gateway) has two network interfaces, one on the local (inside) network and one on the public (outside) network.
- The router is connected to the Internet Service Provider (ISP), that will assign the public IP address to the outside interface

# NAT (4/4)

- The router must implement NAT (Network Address Translator - RFC 1631)
- The NAT idea is to modify (translate) the IP addresses (and other header fields) of outgoing and incoming packets.
- Two main types of NAT operations exist:
  - Static NAT: one-to-one translation;
  - Dynamic NAT: N-to-one translation.

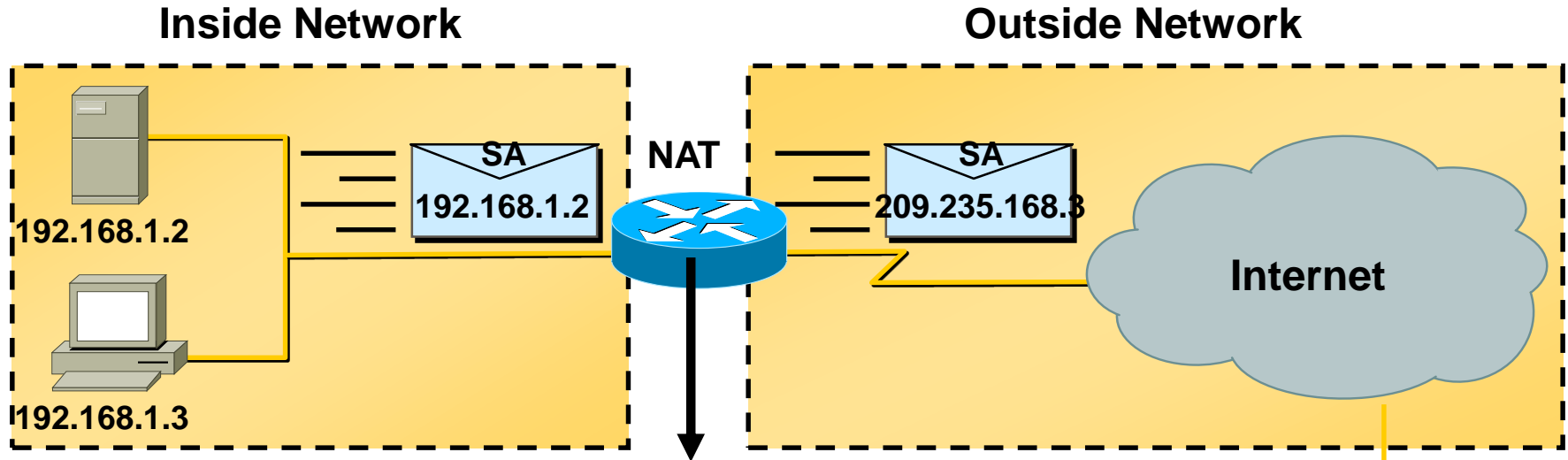
# Static NAT



Inside Local IP Address	Inside Global IP Address
192.168.1.2	80.70.1.1
192.168.1.3	80.70.1.2

The translation is performed also for the incoming packets (acting on the IP destination address field)

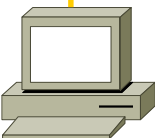
# Dynamic NAT



SA = Source Address

Tabella NAT

Inside Local IP Address & port	Inside Global IP Address & port
192.168.1.2:1024 192.168.1.3:1723	209.235.168.3:55001 209.235.168.3:55002



**151.100.37.12:80**  
**SERVER HTTP**

# NAT Configuration

- The first step in NAT configuration is the setting of inside (local) and outside (global) interfaces

```
Router(config-if)#ip nat inside
```

```
Router(config-if)#ip nat outside
```

# Static NAT configuration

- One-to-one translation among a private and a public IP address.
- Used for servers.
- Translation rule:

```
Router(config)# ip nat inside source static  
                private_address public_address
```



# Dynamic NAT configuration (1/2)

- The number of available public IP addresses is lower than the number of hosts (private IP addresses) requiring Internet access
- Private IP addresses definition:  
`Router(config)# access-list access-list-number  
permit source_address wildcard`
- Pool of public IP addresses:  
`Router(config)# ip nat pool name start-ip end-ip  
netmask netmask`
- Translation rule  
`Router(config)# ip nat inside source list acl-  
number pool name`

## Dynamic NAT configuration (2/2)

- It is also possible to use a single public IP address for all the LAN hosts: the public IP address of the router
- In this case the pool of public IP addresses is not required
- Translation rule:

```
Router(config)# ip nat inside source list acl-  
number interface interface overload
```