

CCNA4, Module1: Network Address Translation – Dynamic Host Configuration protocol

Prednáška 9

Problém ...

- Vďaka flexibilitnosti IP technológie nárast používania → potreba nových metód riadenia adresných rozsahov v snahe riešenia adresnej krízy
- = **Network Address Translation (NAT)**
- Princíp:
 - Vo vnútri siete použitie privátneho adresného priestoru na adresáciu IP zariadení
 - Pri prechode paketu cez okraj do verejného Internetu → preklad zdrojovej privátnej IP do verejného adresného IP priestoru

Private Addressing

■ Verejné IP adresy

■ Riadený priestor

- V Európe prideliuje RIPE (Réseaux IP Européens)
- Zákazník prenajíma od ISP

■ Privátne IP adresy

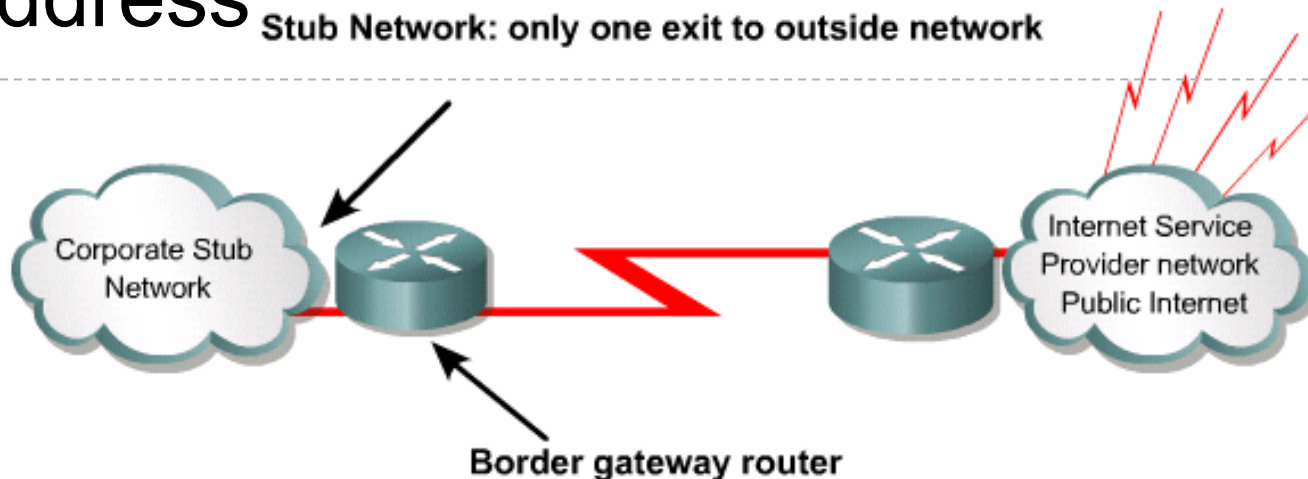
- Môže použiť hocikto
- Neriadené
- Routre nesmú smerovať privátne adresy
 - ACL, Route policy a pod.
- Vyčlenené podľa RFC 1918

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

NAT

- A NAT- enabled device typically operates at the border of a stub network.
- Corporate net = Private addressing
- Packets crossing the border = translation source private IP to public routable IP address

Stub Network: only one exit to outside network



NAT Terms

■ Inside Local Addresses

- An IP address assigned to a host inside a network. This address is likely to be a RFC 1918 private address.

■ Inside Global Address

- A legitimate IP address assigned by the NIC or service provider that represents one or more inside local IP address to the outside world.

■ Outside Local Address

- The IP address of an outside host as it known to the hosts in the inside network.

■ Outside Global Address

- The IP address assigned to a host on the outside network. The owner of the host assigns this address.

Translating network address

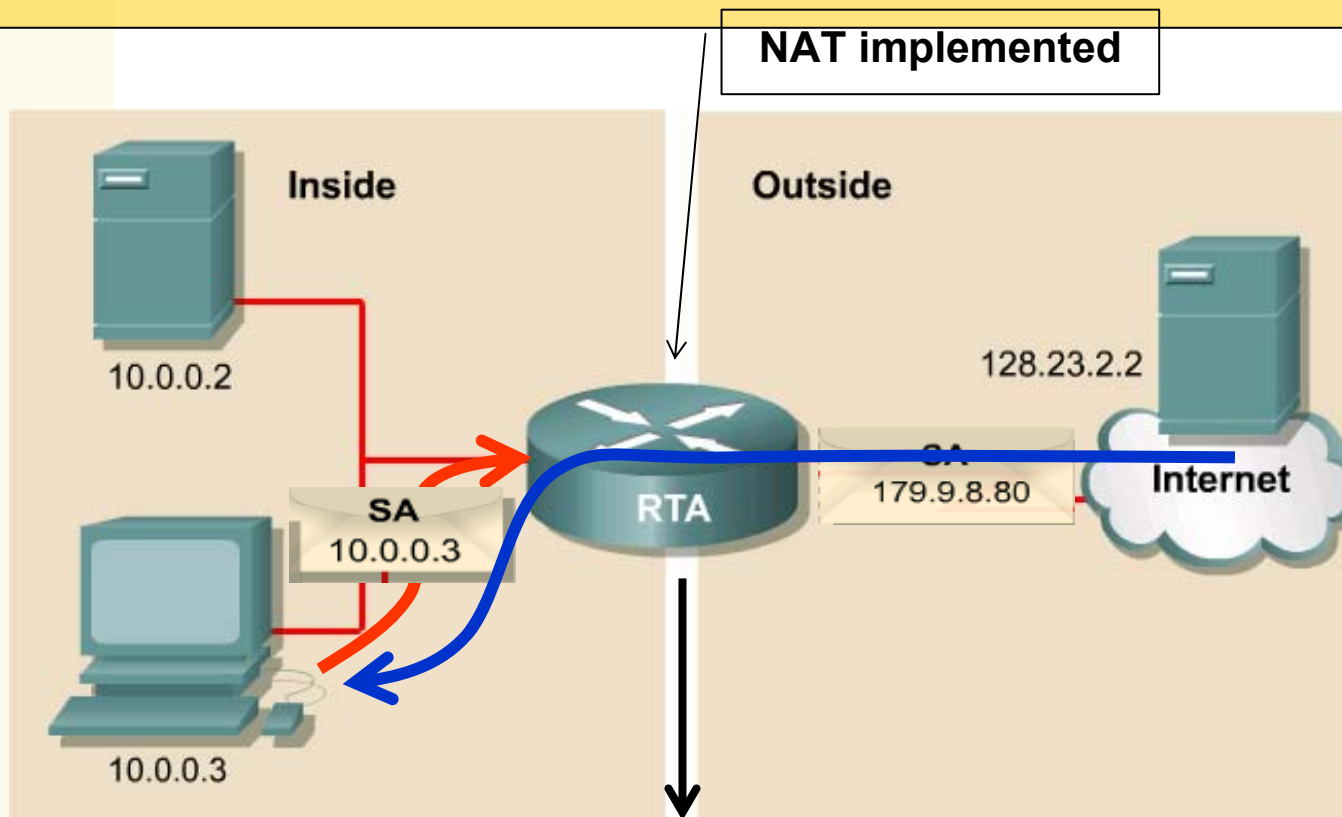
An internal host (10.0.0.3) wants to communicate with an external host (128.23.2.2). The internal host sends a packet to the gateway, RTA.

RTA sees the packet is to be routed to the outside Internet. The NAT process chooses a globally unique IP address (179.9.8.80), and replaces the local address in the source field of the packet with the global address. It stores this mapping of local to global address in the NAT table.

The packet is routed to its destination. In this client-server environment, the server may respond with a packet, which will come back to RTA, addressed to the global address 179.9.8.80.

The NAT process sees a packet that is routed from the outside to the inside and consults the NAT table for a map of this global address into a local address. If a mapping is found, the global address in the destination field of the packet is replaced with the local address and the packet is forwarded internally.

Translating network address



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

NAT

■ Statické mapovanie

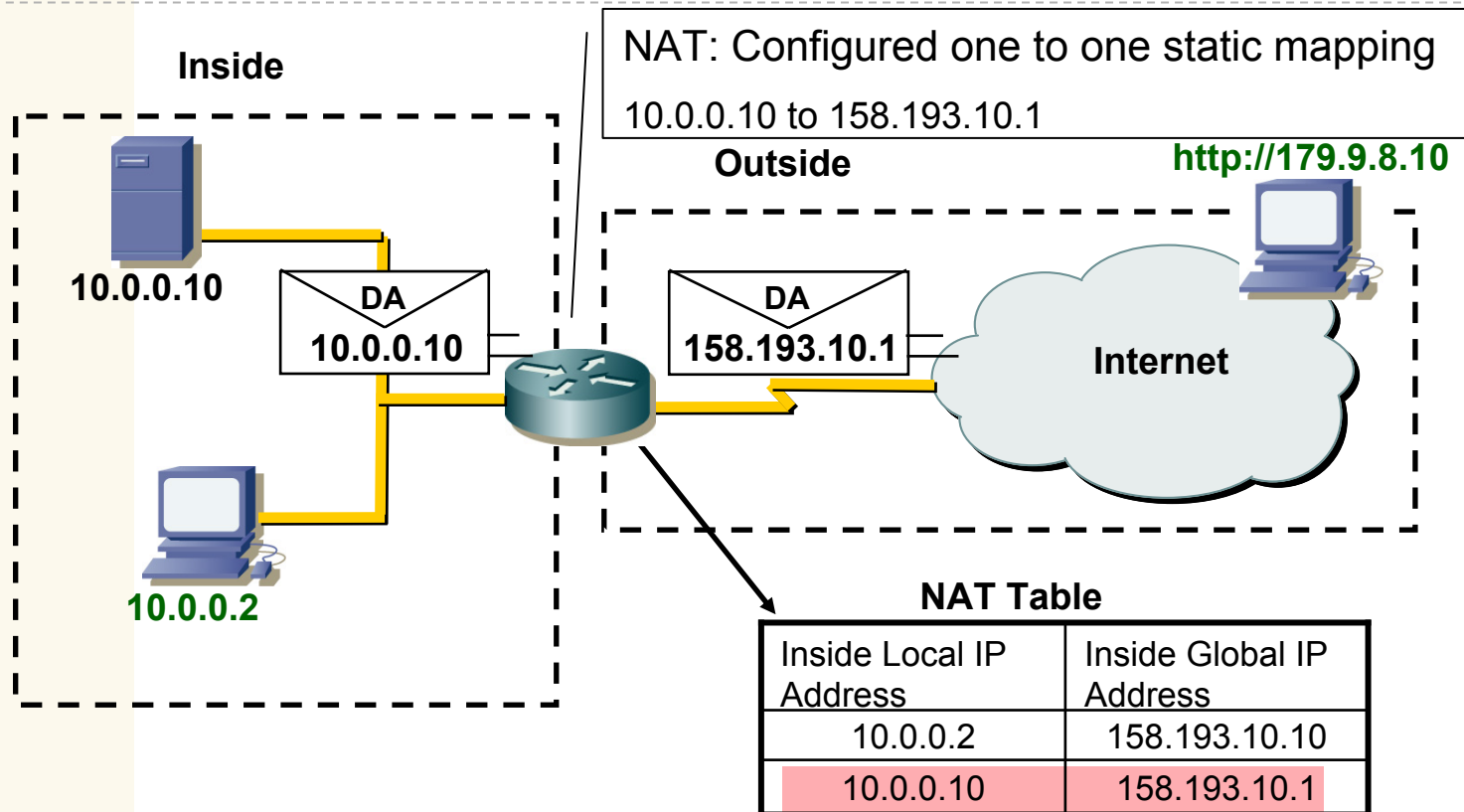
- Tzv. „one-to-one mapping“
- Spárovanie prekladu jednej privátnej adresy (lokálnej) na jednu verejnú adresu (globálnu)
- Výhodné, priam potrebné ak potrebujem zabezpečiť prístup na stanicu (napr. HTTP server) za NAT z Internetu

■ Dynamické mapovanie

- NAT má dostupný rozsah (pool) verejných adries
- NAT riadi preklad pridelovaním neobsadených verejných IP adries z rozsahu

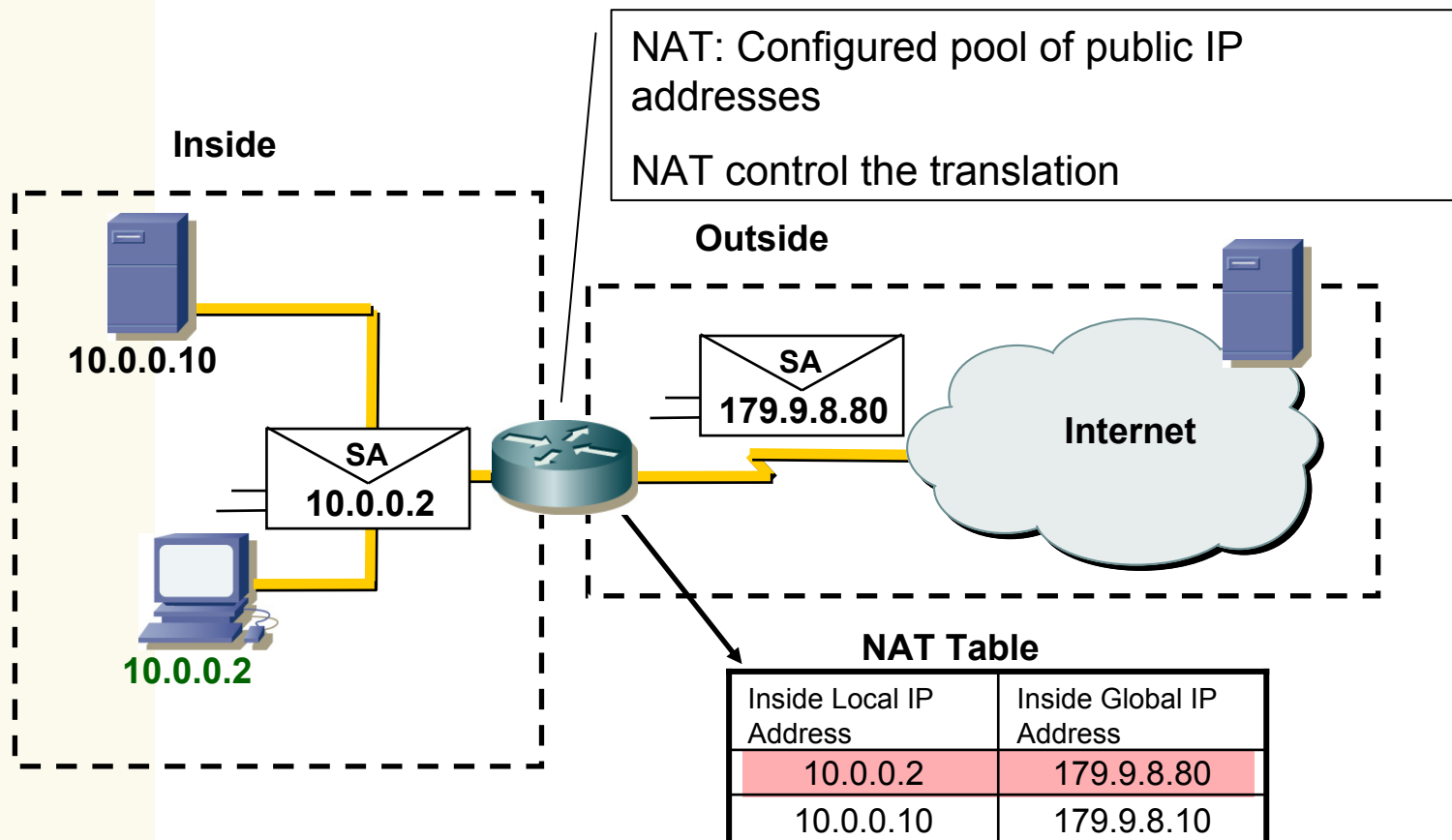
Static NAT

- Static NAT is designed to allow one-to-one mapping of local and global addresses



Dynamic NAT

- Dynamic NAT is designed to map a private IP address to a public address.

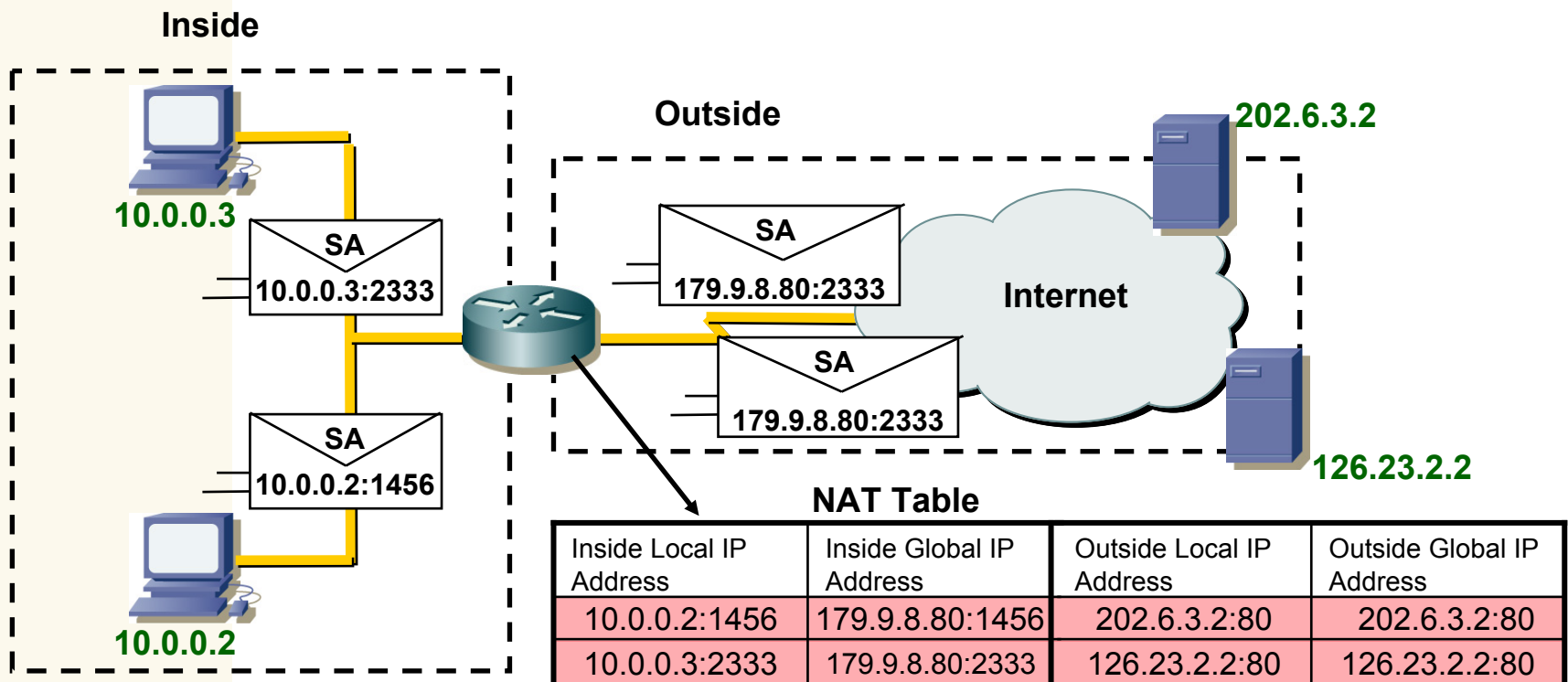


PAT

- Protocol Address Translation
 - NAT overloading
 - Maps multiple private IP addresses to a single public IP address, where each private address is tracked by a port number (16 bit)
 - PAT will attempt to preserve the original source port.
 - If this source port is already used, PAT will assign the first available port number

PAT Features

- PAT uses unique source port numbers on the inside global IP address to distinguish between translations.



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
- Protects network security

Configuring Static NAT Translations

- Static translation are entered directly into the configuration and are permanent in the translation table

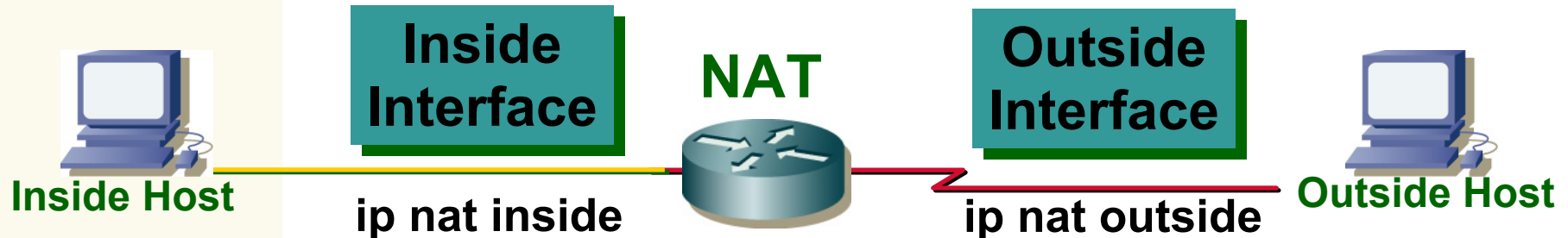
```
Router(config)#ip nat inside source static  
                INSIDE_LOCAL INSIDE_GLOBAL
```

```
Router(config)#ip nat inside source static  
                10.6.1.20 171.69.68.10
```

Inside/Outside interface

Inside Network

Outside Network

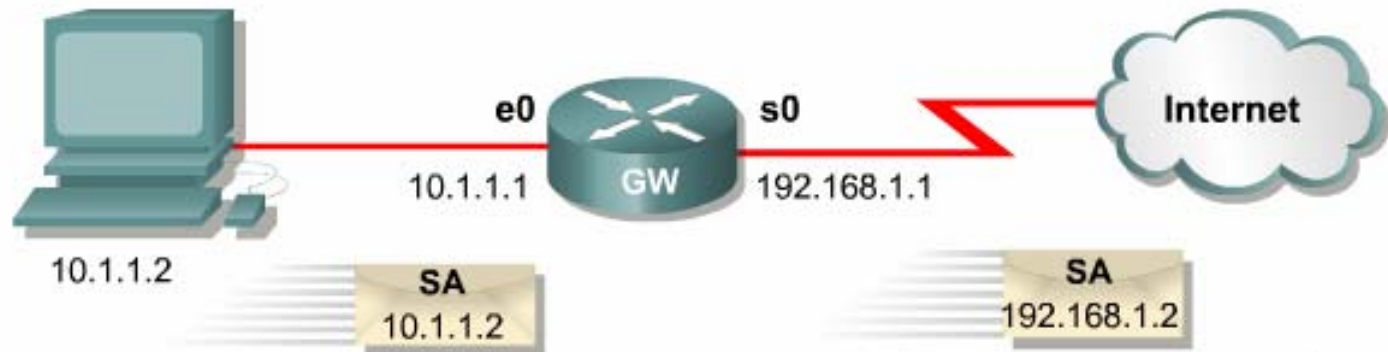


```
Router(config-if)#ip nat inside
```

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

- An interface on the router can be defined as inside or outside
- Translations occur only from inside to outside interfaces or vice versa—never between the same type of interface

Configuring Static NAT

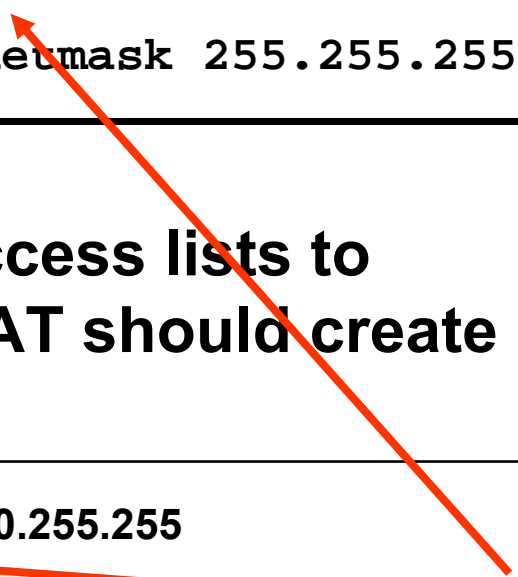


```
hostname GW
!  
ip nat inside source static 10.1.1.2 192.168.1.2  
!  
interface ethernet 0  
  ip address 10.1.1.1 255.255.255.0  
  ip nat inside  
!  
interface serial 0  
  ip address 192.168.1.1 255.255.255.0  
  ip nat outside  
!
```


Dynamic Translations

- Dynamic translation specify the pool of global addresses that inside addresses can be translated into

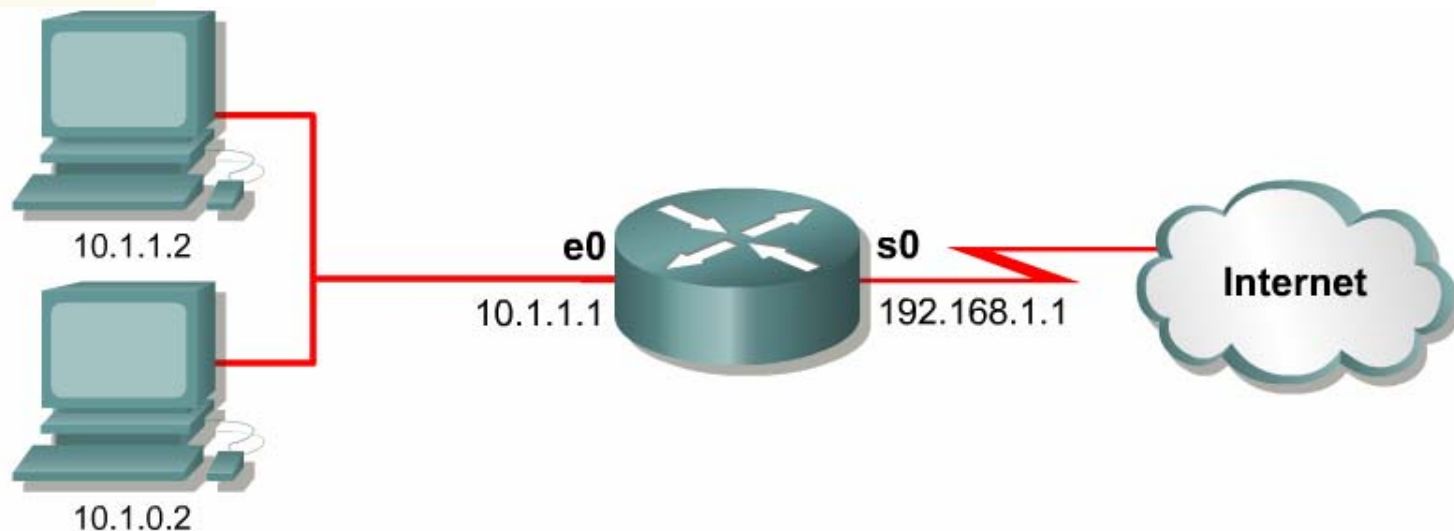
```
Router(config)#ip nat pool nat-pool  
179.9.8.80 179.9.8.95 netmask 255.255.255.240
```



- Dynamic translations use access lists to identify IP addresses that NAT should create translations for

```
Router(config)#access-list 1 permit 10.0.0.0 0.0.255.255  
Router(config)#ip nat inside source list 1 pool nat-pool
```

Configuring Dynamic NAT



```
ip nat pool nat-pool1 179.9.8.80 179.9.8.95 netmask 255.255.255.0
ip nat inside source list 1 pool nat-pool1
!
interface ethernet 0
  ip address 10.1.1.1 255.255.0.0
  ip nat inside
!
interface serial 0
  ip address 192.168.1.1 255.255.255.0
  ip nat outside
!
access-list 1 permit 10.1.0.0 0.0.0.255
```

Configuring PAT

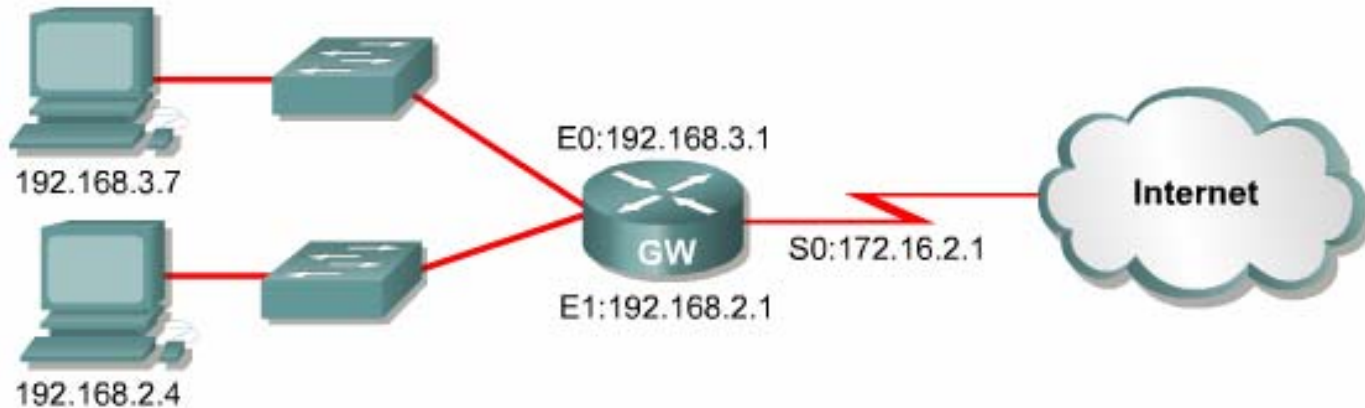
- Establishes overload translation, specifying the IP address to be overloaded as that assigned to an outside interface

```
Router(config)#ip nat inside source list 1  
                interface serial0/0 overload
```

- Establishes overload translation, specifying the IP address to be overloaded as that assigned to a pool name

```
Router(config)# ip nat pool nat-pool2 179.9.8.20  
                netmask 255.255.255.240  
Router(config)#ip nat inside source list 1  
                pool nat-pool2 overload
```

Configuring PAT



```
interface ethernet 0
  ip address 192.168.3.1 255.255.255.0
  ip nat inside
!
interface ethernet 1
  ip address 192.168.2.1 255.255.255.0
  ip nat inside
!
interface serial 0
  ip address 172.16.2.1 255.255.255.0
  ip nat outside
!
ip nat inside source list 1 interface serial 0 overload
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
```

Clearing the NAT Translation Table

```
Router#clear ip nat translation *
```

- **Clears all dynamic address translation entries**

Verifying NAT and PAT Configuration

```
Router#show ip nat translations [verbose]
```

- Displays active translation

```
Router#show ip nat translation
```

Pro	Inside global	Inside local	Outside local	Outside global
172.16.131.1		10.10.10.1	---	---

```
Router#show ip nat statistics
```

- Displays translation statistics

```
Router#show ip nat statistics
```

```
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
```

```
Outside interfaces:
```

```
Serial0
```

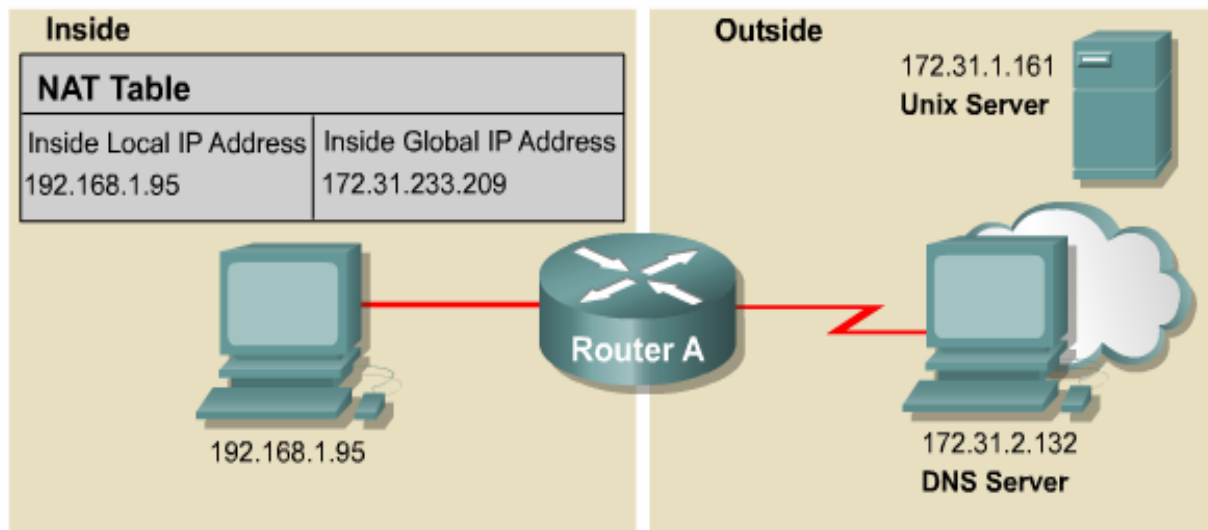
```
Inside interfaces:
```

```
Ethernet0, Ethernet1
```

```
Hits: 5 Misses:0
```

Command	Description
show ip nat translations	Displays active translations
show ip nat statistics	Displays translation statistics

Troubleshooting NAT and PAT



```
RouterA#debug ip nat
NAT: s= 192.168.1.95    -> 172.31.233.209,      d=172.31.2.132 [6825]
NAT: s= 172.31.2.132,   d=172.31.233.209,      -> 192.168.1.95 [21852]
NAT: s= 192.168.1.95    -> 172.31.233.209,      d=172.31.1.161 [6826]
NAT*: s= 172.31.1.161,   d=172.31.233.209,      -> 192.168.1.95 [23311]
NAT*: s= 192.168.1.95    -> 172.31.233.209,      d=172.31.1.161 [6827]
NAT*: s= 192.168.1.95    -> 172.31.233.209,      d=172.31.1.161 [6828]
NAT*: s= 172.31.1.161    d=172.31.233.209,      -> 192.168.1.95 [23313]
NAT*: s= 172.31.1.161,   d=172.31.233.209,      -> 192.168.1.95 [23313]
```

Issues With NAT

NAT has several advantages, including the following:

- NAT conserves the legally registered addressing scheme by allowing the privatization of intranets.
- NAT allows the existing scheme to remain, and it still supports the new assigned addressing scheme outside the private network.

Cisco IOS NAT does support the following traffic types although they carry IP addresses in the application data stream:

- ICMP
- File Transfer Protocol (FTP), including PORT and PASV commands
- NetBIOS over TCP/IP, datagram, name, and session services
- Progressive Networks' RealAudio
- White Pines' CuSeeMe
- DNS "A" and "PTR" queries
- H.323/NetMeeting, versions 12.0(1)/12.0(1)T and later
- VDOLive, version 11.3(4)11.3(4)T and later
- Vxtreme, versions 11.3(4)11.3(4)T and later
- IP multicast, version 12.0(1)T, the source address translation only

Cisco IOS NAT does not support the following traffic types:

- Routing table updates
- DNS zone transfers
- BOOTP
- talk, ntalk
- Simple Network Management Protocol (SNMP)

■ **Disadvantages:**

- Delay
- HW requirements
- Problem with multilayer IP address process

Dynamické pridelovanie IP adries

■ Dynamické:

■ Pomocou doplnkovej sieťovej služby

- Musí byť v sieti nainštalovaná, nakonfigurovaná a spustená

■ A) **Reverse Address Resolution Protocol (RARP):**

- Klient server dotazovanie, získa len vlastnú adresu

■ B) **BOOTstrp Protocol (BOOTP):**

- K/S, permanentné pridelenie IP adresy (staticky), okrem IP adresy aj adresu routera, ...4 parametre

■ C) **Dynamic Host Configuration protocol (DHCP):**

- K/S, stanici pridelená adresa len kým komunikuje, pri novom prihlásení nová adresa

Dynamic Host Configuration Protocol

RFC 2131

Dynamic Host Configuration Protocol

- Dynamic Host Configuration Protocol (DHCP)
 - Klient / Server protokol
 - Umožňuje klientom (koncovým staniciam) vyžiadať od servera konfiguračné parametre
 - Servery a smerovače by mali mať statické IP adresy
 - Najpoužívanéjšie parametre
 - IP adresa, subsieťová maska, IP adresa default gateway, IP adresa DNS
- DHCP komponenty
 - DHCP klient
 - Má ho väčšina moderných OS
 - DHCP Server
 - Relay Agent
 - Prechod DHCP žiadosti cez smerovač

DHCP

■ DHCP klient

- Žiada o konfiguračné parametre DHCP server
 - L2 Broadcast
- OS Windows:
 - Môžeme riadiť príkazom ipconfig

■ DHCP Server

- Serverovská entita
 - Proces môže byť spustený na smerovači alebo na dedikovanom serveri
- Spravuje IP adresnú množinu
 - a iné konfiguračné parametre
- Prideluje ich na požiadanie DHCP klientom

■ Relay agent

- Umožňuje prechod DHCP žiadostí cez L3 zariadenie

Alokácia IP adresy

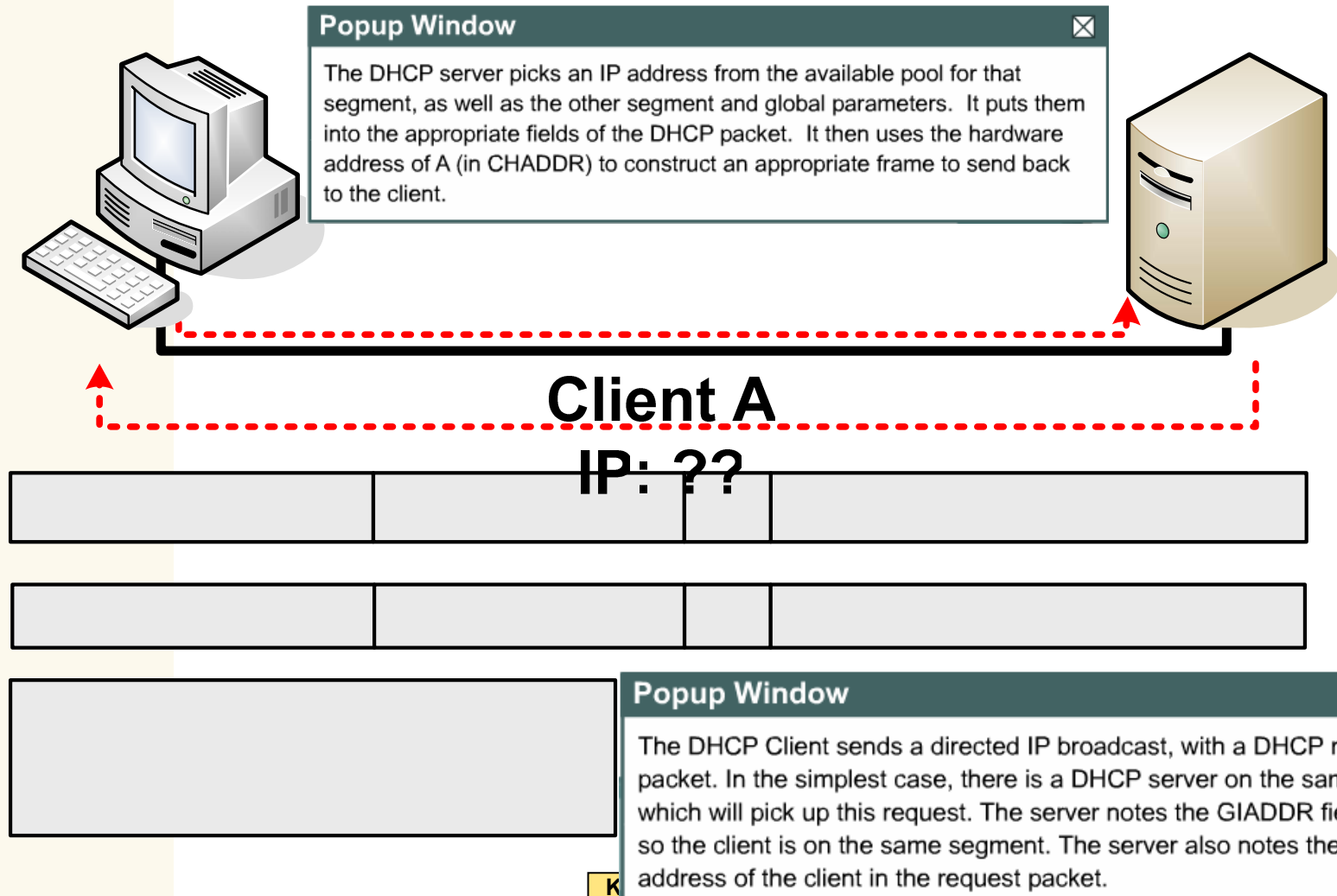
■ Dynamická Alokácia

- Pridelí IP adresu požadujúcej stanici na špecifikované časové obdobie
- Potom nastáva uvoľnenie adresy alebo obnovenie prenájmu

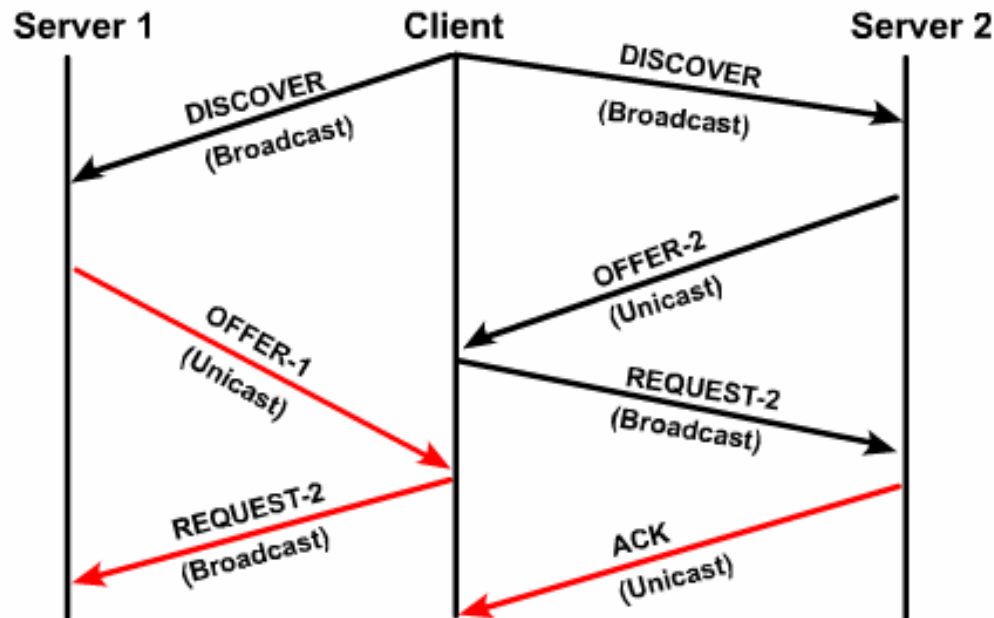
■ Manuálna Alokácia

- Vyžaduje konfiguráciu DHCP servera
- Pridelí požadujúcej stanici vždy rovnakú IP adresu

DHCP činnost'

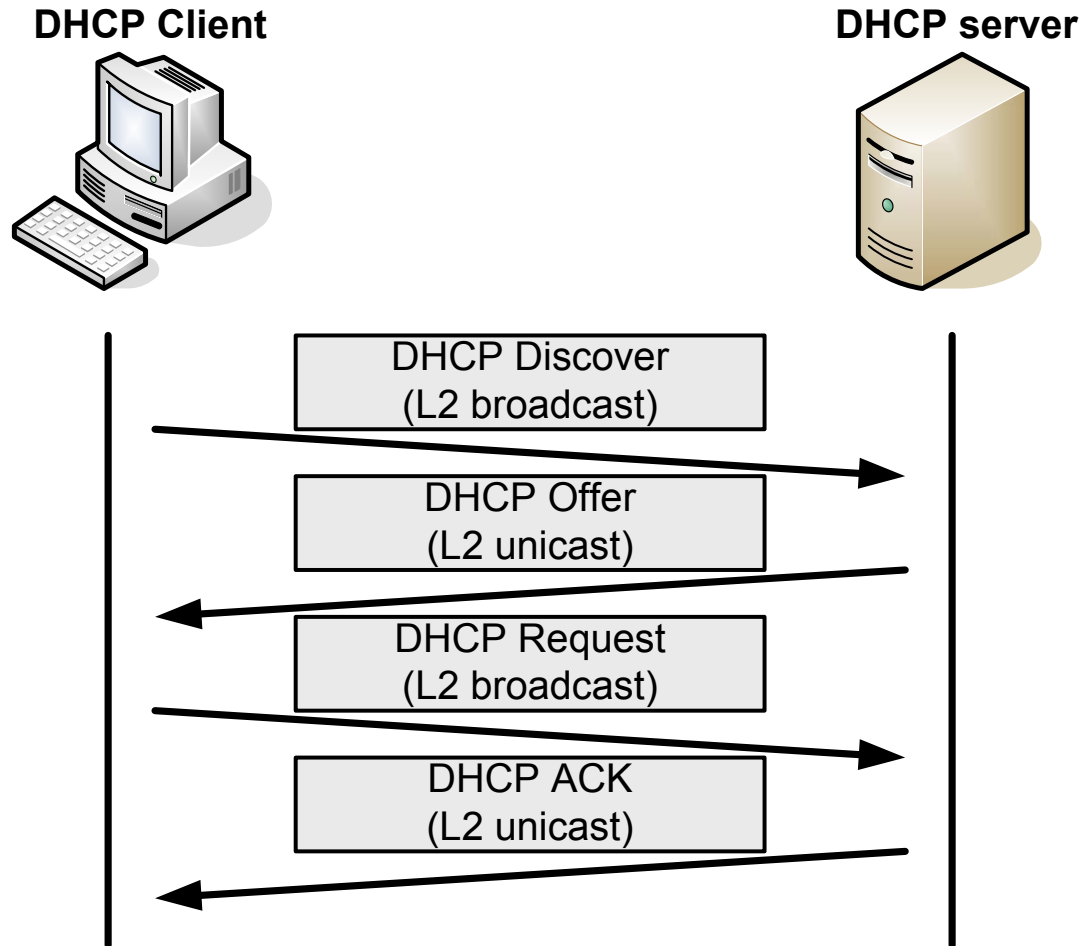


DHCP Operation



- DHCP client broadcasts DHCP DISCOVER packet on local subnet
- DHCP servers send OFFER packet with lease information
- DHCP client selects lease and broadcasts DHCP REQUEST packet
- Selected DHCP server sends DHCP ACK packet

DHCP činnosť - správy



Configuring DHCP

```
Router(config)#ip dhcp pool pool-name1
```

Specify the DHCP pool

```
Router(dhcp-config)#network ip-address mask
```

Specify the range of addresses in the pool

- Creates an IP DHCP pool, and gives it a name
- Up to multiple DHCP pools can be created on one server
- Specify the IP range of addresses using an IP network address and mask

Configuring DHCP While Excluding IP

```
Router(config)#ip dhcp excluded-address  
ip-address [end-ip-address]
```

```
Router(config)#ip dhcp excluded-address 172.16.1.1 172.16.1.10  
Router(config)#ip dhcp excluded-address 172.16.1.254
```

```
Router(config)#ip dhcp pool subnet12  
Router(dhcp-config)#network 172.16.12.0 255.255.255.0  
Router(dhcp-config)#default-router 172.16.12.254  
Router(dhcp-config)#dns-server 172.16.1.2  
Router(dhcp-config)#netbios-name-server 172.16.1.3  
Router(dhcp-config)#domain-name foo.com
```

Verifying DHCP

```
Router#show ip dhcp binding
```

```
Router#show ip dhcp binding
```

IP address	Hardware address	Lease expiration	Type
172.16.12.11	0100.10a4.97f4.6d	Mar 02 1993 12:38 AM	Automatic

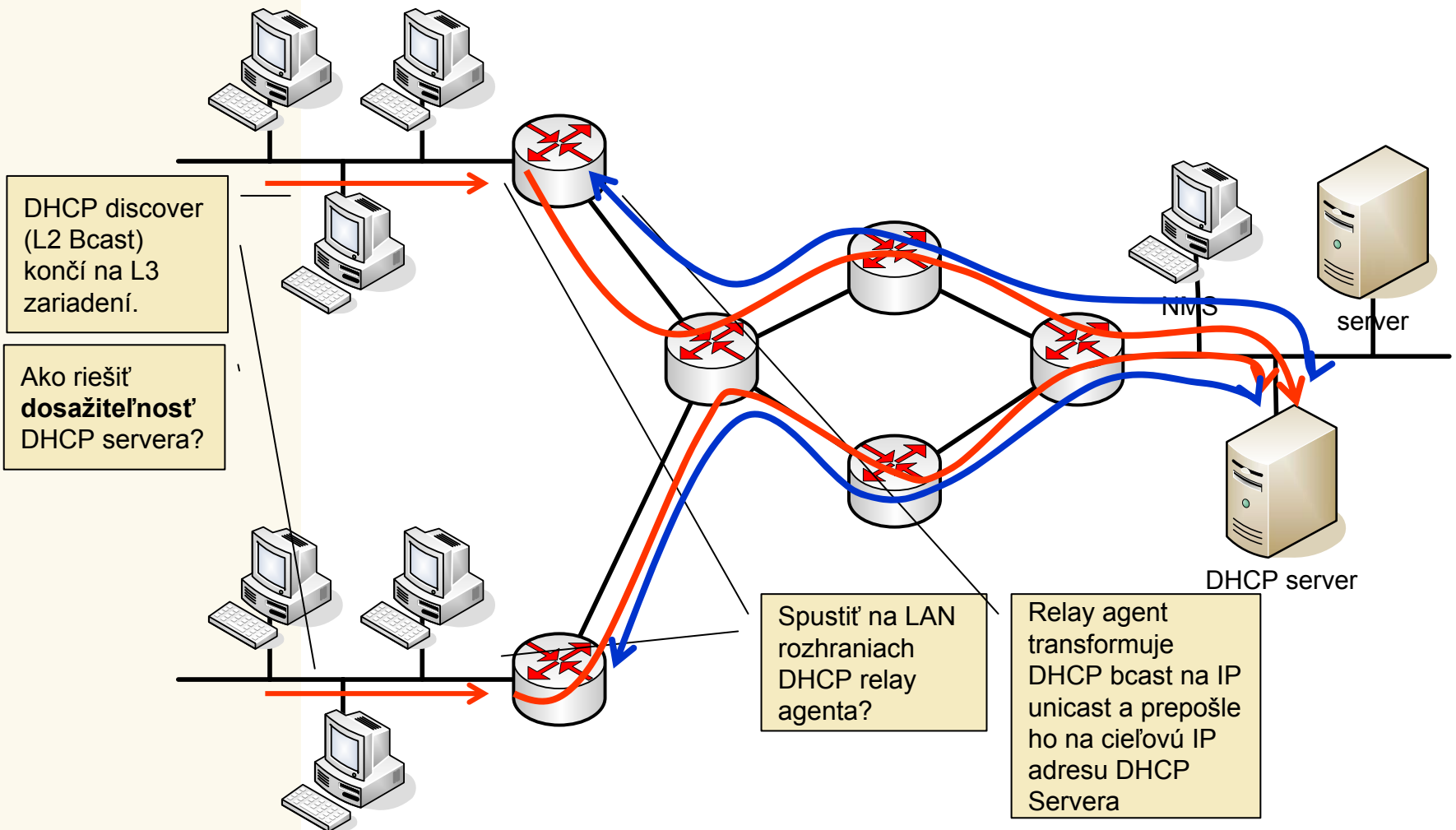
```
Router#
```

Troubleshooting DHCP

```
Router#debug ip dhcp server events
```

```
Router#debug ip dhcp server events
Router#
00:22:53: DHCPD:checking for expired leases.
00:22:23: DHCPD: assigned IP address 172.16.13.11 to client
0100.10a4.97f4.6d
00:22:49: DHCPD:retured 172.16.13.11 to address pool remote.
00:22:59: DHCPD: assigned IP address 172.16.13.11 to client
0100.10a497f4.6d.
```

Relay Agent



DHCP Relay

