Miroslav Michalko

DHCP, NAT, IPv6

Obsah prezentácie

- Úvod do technológií:
  - DHCP
  - NAT
  - IPv6
- Ukážky konfigurácií

Spôsoby priradenia IP adresy

- manuálne *nastavenie*
  - administrátorom
  - používateľom
- statické *pridelenie*
  - na základe MAC adresy stále tú istú IP (automaticky)
- dynamické *pridelenie*
  - pridelenie IP z rozsahu adries danej podsiete

Služby pre *prideľovanie* IP

- **BOOTP**
  - angl. **Bootstrap Protocol**
  - RFC 951
  - nahradený DHCP
- **DHCP**
  - angl. **Dynamic Host Configuration Protocol**
  - RFC 1531 (1993), aktualizovaný RFC 3315 (1997)

BOOTP

- základná IP konfigurácia (IP, GW, SM, DNS, atď.)

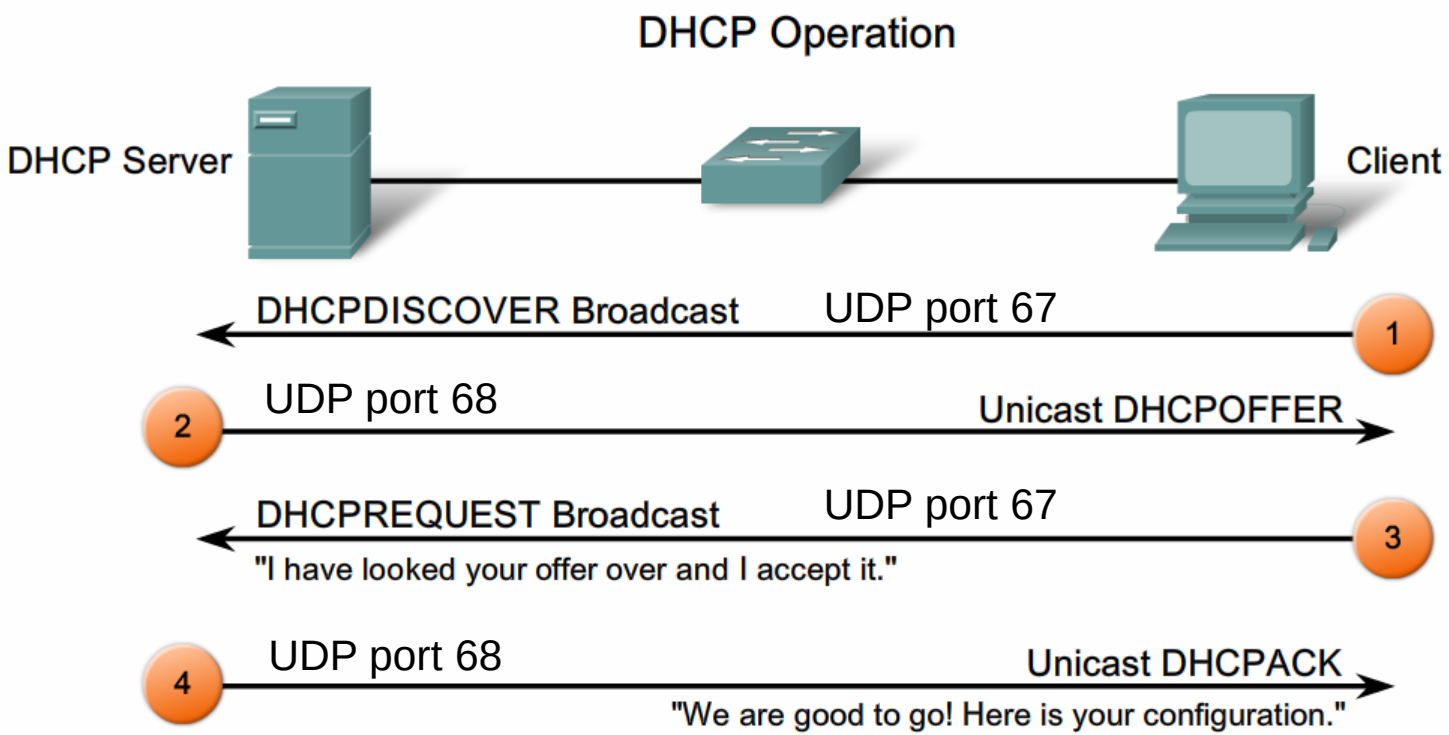
Počet oktetov	Názov poľa	Popis
1	Operation	Kód operacie (BOOTREQUEST alebo BOOTREPLY)
1	Hardware Typ	Typ hardvérovej adresy
1	Hardware Length	Dĺžka hardvérovej adresy
1	Hops	
4	Transaction ID	ID transakcie
2	Seconds	Doba (sek.), ktorá uplynula od začiatku bootovania
2	Flags	
4	Client IP Adress	IP adresa klienta – pokiaľ pozná klient svoju IP adresu
4	Your Client IP Address	IP adresa klienta – na toto miesto ju doplní server
4	Server IP Address	IP adresa servera
4	Gateway IP Address	IP adresa gateway-a
16	Clinet Hardware Adress	Hardvérová adresa klienta
64	Server Host Name	Meno servera
128	File Name	Meno boot-ovacieho súboru
	Vendor Specific Area	Dalšie informacie pre klienta (adresa DNS atď.)

DHCP

- možnosť prenájmu IP adresy
- spätne kompatibilný s BOOTP
- podpora IPv6

- dôvody prechodu z BOOTP na DHCP
  - neobsahoval mechanizmy pre odobratie IP adresy (po odpojení PC, 30 dní lease time)
  - dlhší proces pridelenia IP (požiadavka na ďalšie konfiguračné detaily i po pridelení IP)
  - chýbala dynamická alokácia IP (nedostatok IP adries v súčasnosti)
  - málo priestoru pre vlastné konfiguračné parametre

DHCP pridelenie IP adresy

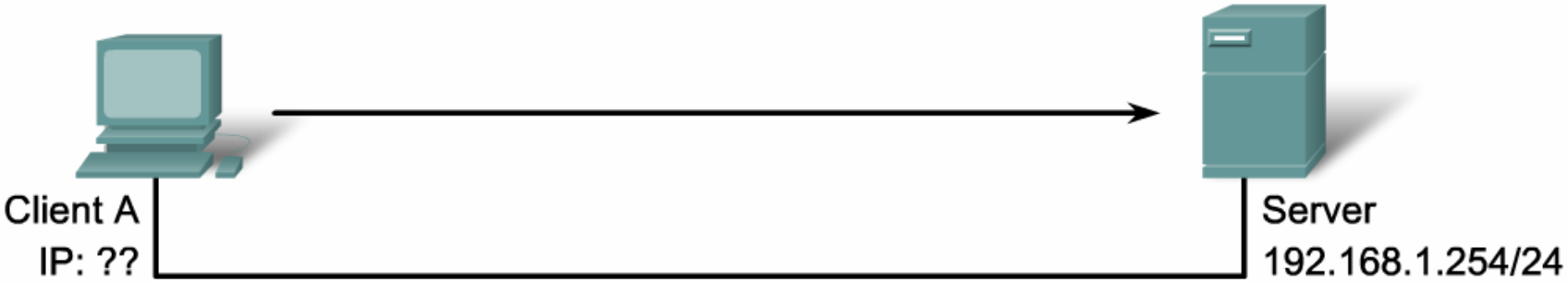



```
IP address: 192.168.10.15
Subnet mask: 255.255.255.0
Default gateway: 192.168.10.1
DNS servers:
Lease Time: 3 days
```

Formát DHCP správy

8	16	24	32
OP Code (1)	Hardware type (1)	Hardware address length (1)	Hops (1)
Transaction Identifier			
Seconds – 2 bytes		Flags – 2 bytes	
Client IP Address (CIADDR) – 4 bytes			
Your IP Address (YIADDR) – 4 bytes			
Server IP Address (SIADDR) – 4 bytes			
Gateway IP Address (GIADDR) – 4 bytes			
Client Hardware Address (CHADDR) – 16 bytes			
Server name (SNAME) – 64 bytes			
Filename – 128 bytes			
DHCP Options – variable			

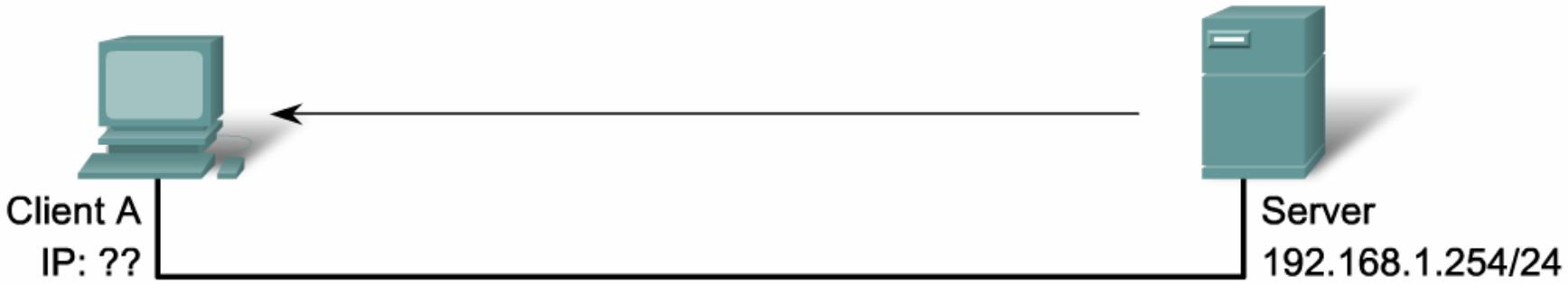
DHCP Discover



Ethernet Frame	IP	UDP	DHCPDISCOVER	
SRC MAC: MAC A DST MAC: FF:FF:FF:FF:FF:FF	IP SRC: 0.0.0.0 IP DST: 255.255.255.255	UDP 67	CIADDR: ? Mask:?	GIADDR: ? CHADDR: MAC A

MAC: Media Access Control Address
CIADDR: Client IP Address
GIADDR: Gateway IP Address
CHADDR: Client Hardware Address

DHCP Offer



Ethernet Frame	IP	UDP	DHCP Offer	
SRC MAC: MAC Serv DST MAC: MAC A	IP SRC: 192.168.1.254 IP DST: 192.168.1.10	UDP 68	CIADDR: 192.168.1.10 Mask: 255.255.255.0	GIADDR: ? CHADDR: MAC A

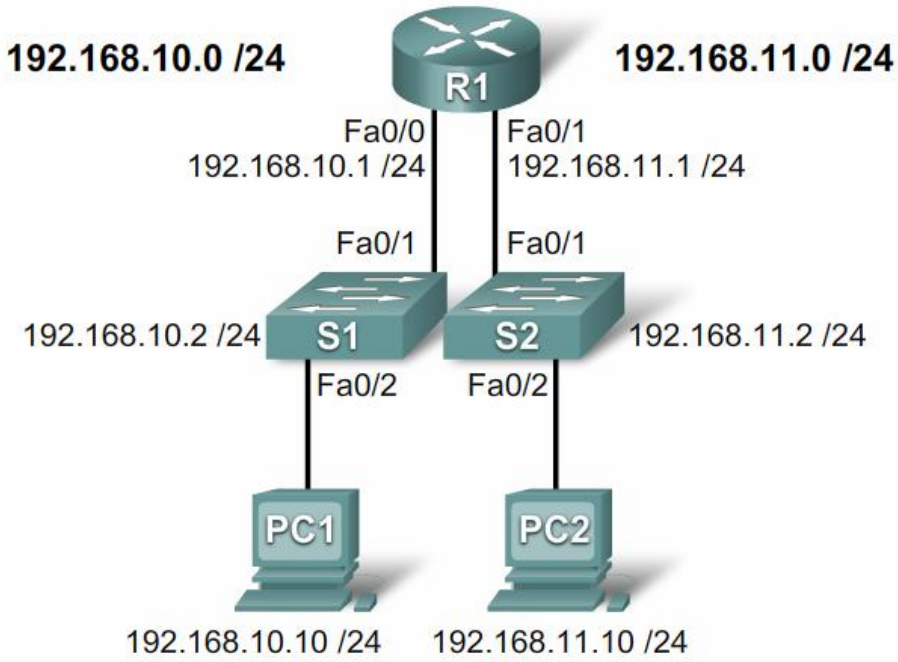
MAC: Media Access Control Address
CIADDR: Client IP Address
GIADDR: Gateway IP Address
CHADDR: Client Hardware Address

Konfigurácia DHCP servera (IOS)

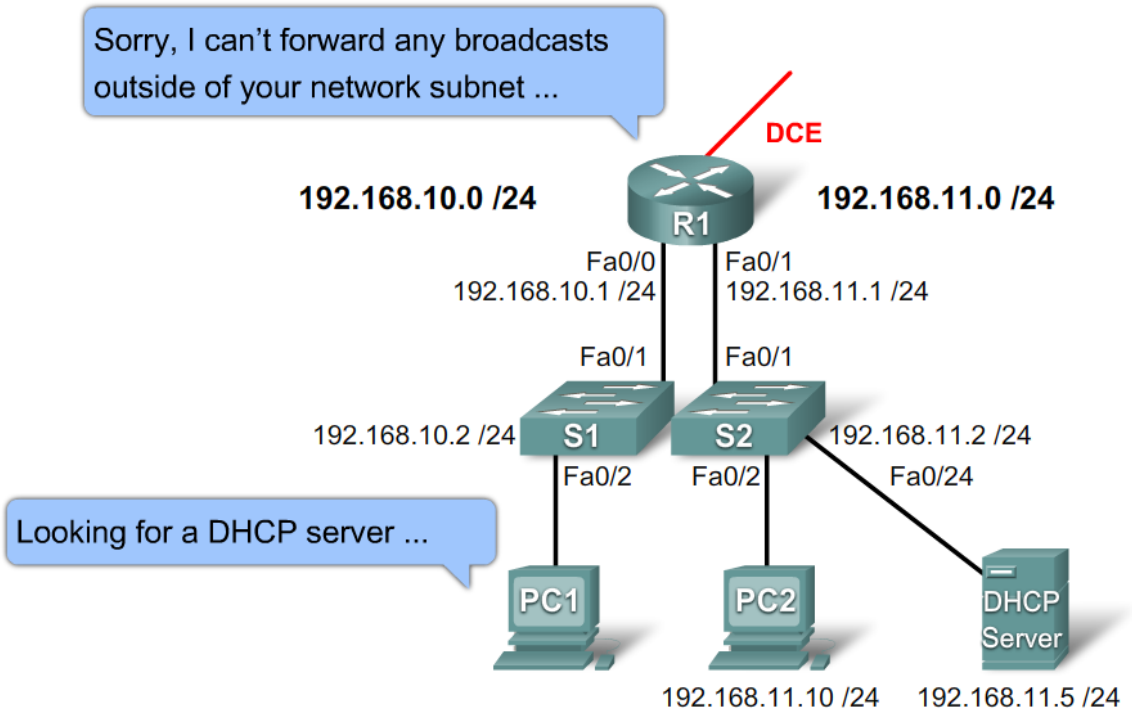

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# domain-name span.com
R1(dhcp-config)# end
```

Verifikácia DHCP


```
R1#sho ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.10.10       0100.e018.5bdd.35       Oct 03 2007 06:14 PM    Automatic
192.168.11.10       0100.b0d0.d817.e6       Oct 03 2007 06:18 PM    Automatic


R1#sho ip dhcp server statistics
Memory usage         25307
Address pools        2
Database agents      0
Automatic bindings   2
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   0

R1#show ip dhcp pool

Pool LAN-POOL-1 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Lease
 192.168.10.11        192.168.10.1     - 192.168.10.254    1

Pool LAN-POOL-2 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
```



DHCP Relay



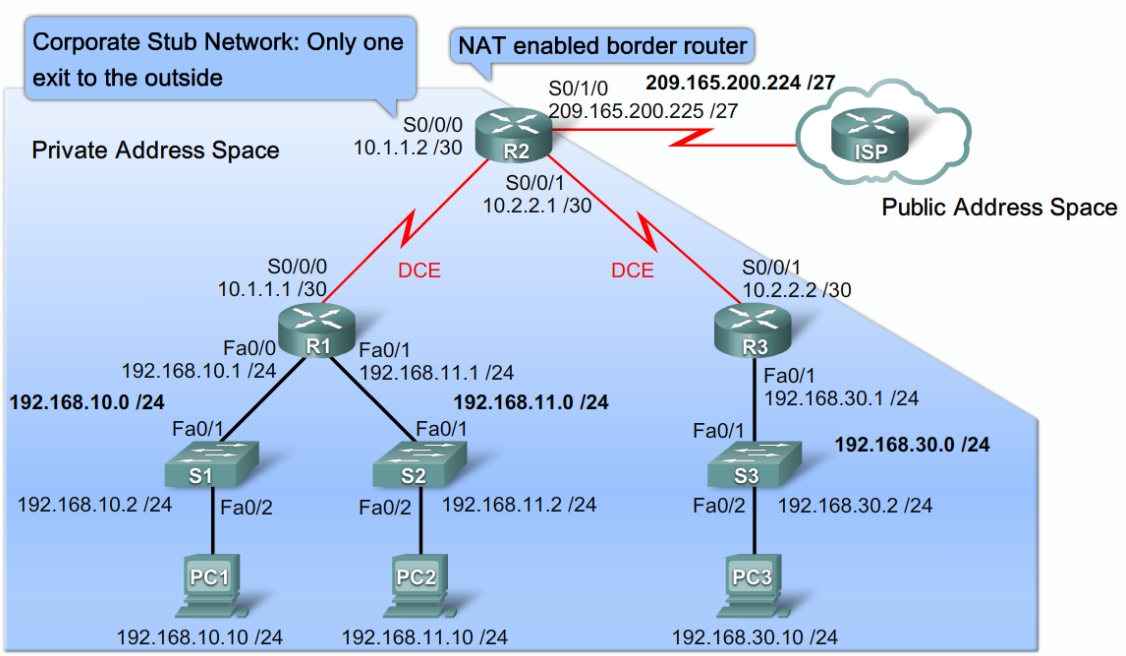

```
R1# config t
R1(config)# interface Fa0/0
R1(config-if)# ip helper-address 192.168.11.5
R1(config-if)# end
```

- Otázky k DHCP?

Privátne IP adresy

- RFC1918

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

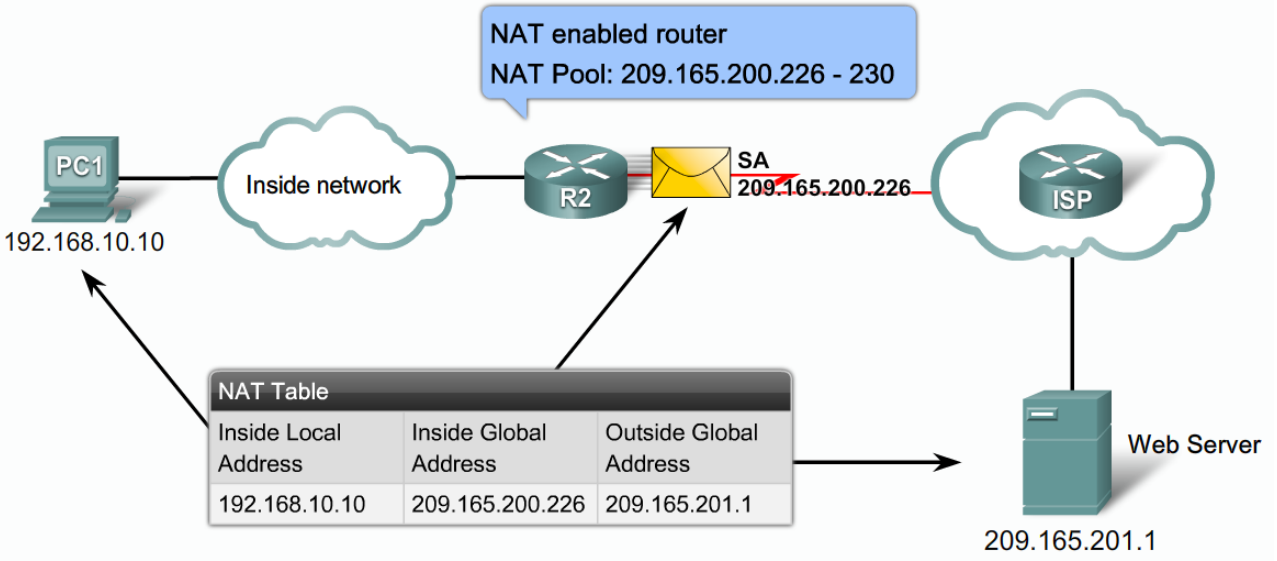
- angl. **Network Address Translation**
- prekladá privátne IP adresy na verejné
- RFC 4008, 3022, 1631, 3489

Výhody:

- umožňuje pripojiť viac počítačov na jednu verejnú IP adresu
- zvyšuje bezpečnosť počítačov pripojených za NATom

NAT terminológia

- **Inside local address** – privátna IP host-u za NAT
- **Inside global address** – verejná IP adresa na ktorú sa privátna IP preložila
- **Outside global address** – verejná IP adresa počítača s ktorým komunikujeme
- **Outside local address** – skutočná IP adresa s ktorým sa komunikuje

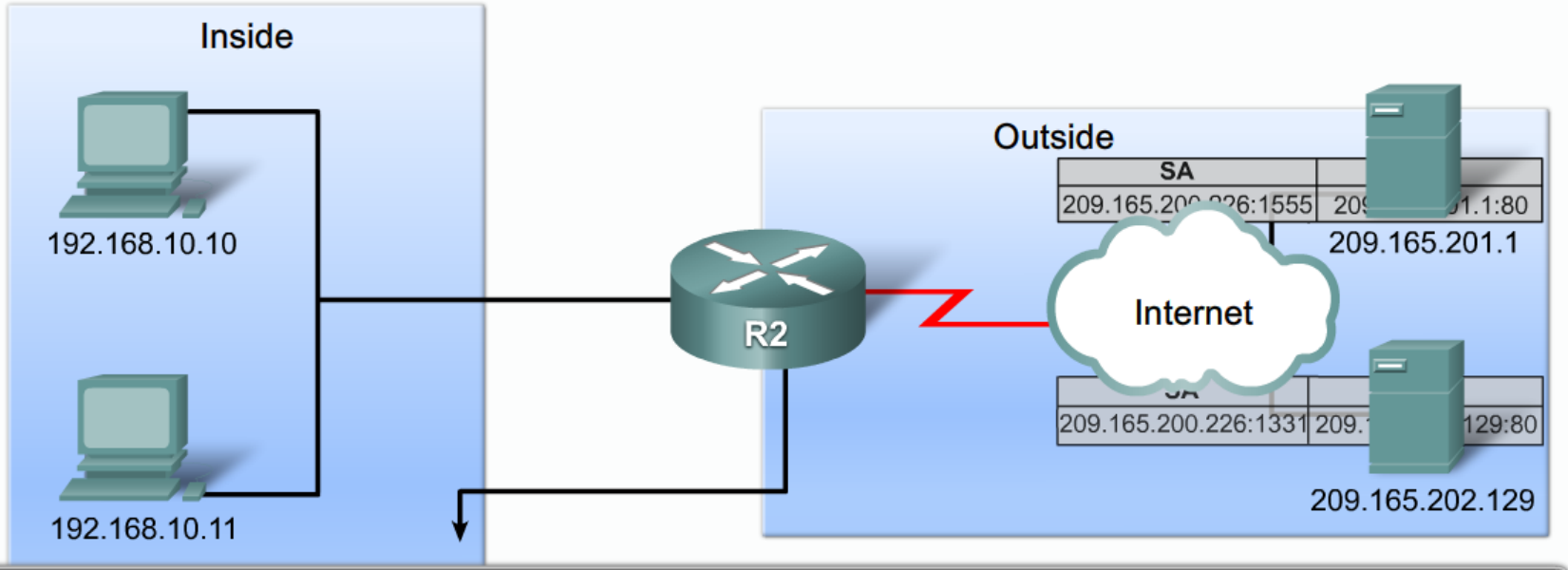


Typy NAT

- dynamické NAT
  - privátne adresy sú prekladané na verejné IP adresy na princípe „first-come, first-served “
- statické NAT
  - mapovanie 1:1
  - spätná dosiahnuteľnosť stanice za NAT

NAT Overload

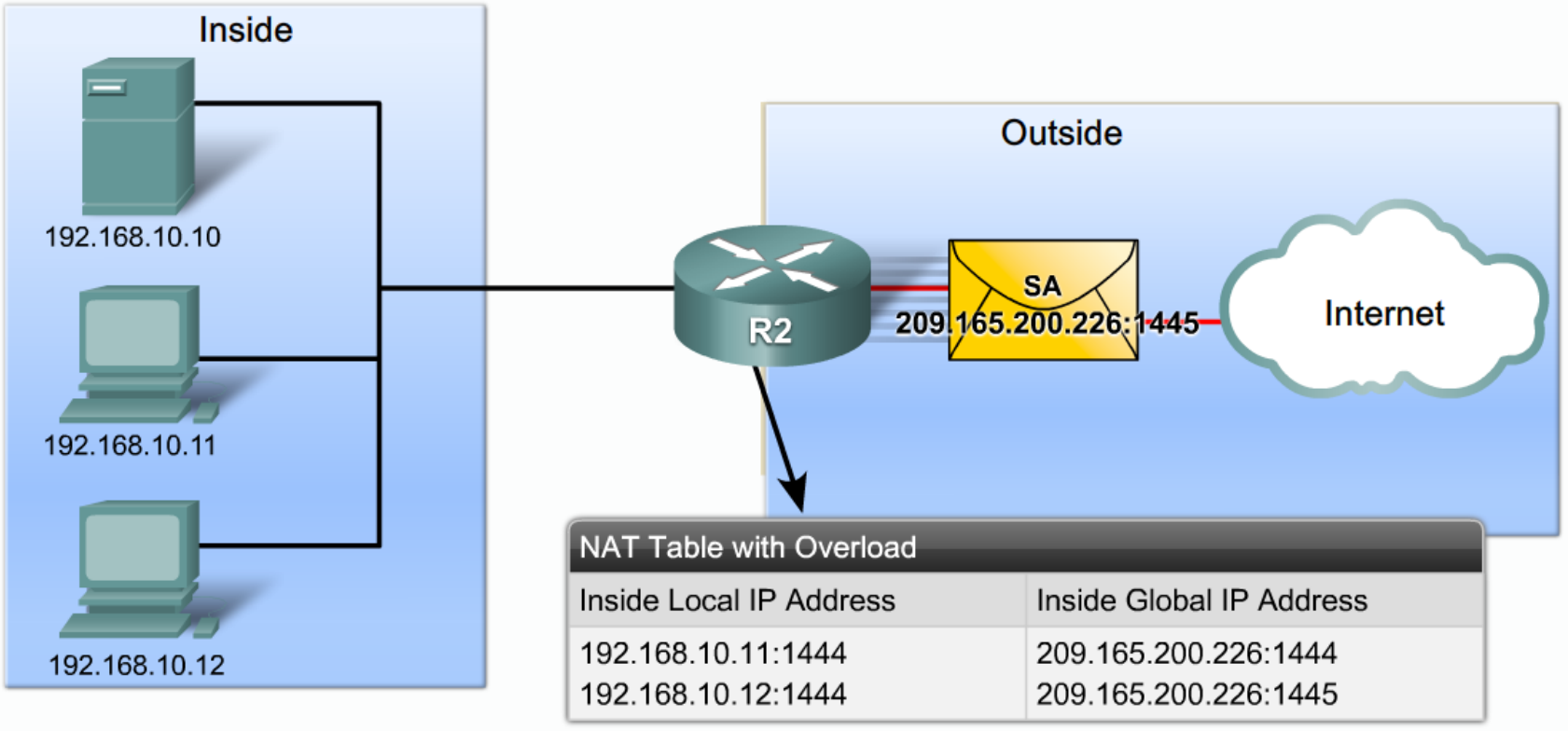
- PAT (Port Address Translation)
- viac privátnych adries na jednu verejnú IP



NAT Table with Overload			
Inside Local IP Address	Inside Global IP Address	Outside Global IP Address	Outside Local IP Address
192.168.10.10:1555 192.168.10.11:1331	209.165.200.226:1555 209.165.200.226:1331	209.165.201.1:80 209.165.202.129:80	209.165.201.1:80 209.165.202.129:80

Rovnaké zdrojové porty

- PAT porty: 0-511, 512-1023, or 1024-65535



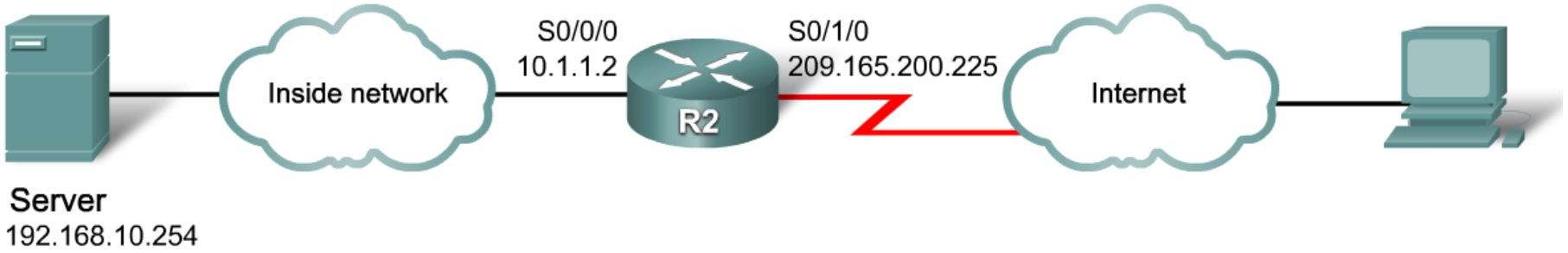
Výhody NAT

- Výhody:
  - šetrenie na verejných IP adresách
  - zvýšenie flexibility pripojenia (viac IP k dispozícii na rôzne záložné riešenia)
  - zmena poskytovateľa nemusí znamenať zmenu IP adresnej schémy organizácie
  - zvýšená bezpečnosť siete – nemožnosť identifikovať skutočnú IP zdroja

Nevýhody NAT

- Nevýhody:
  - zvýšenie požiadavky na výpočtový výkon, vyššie oneskorenie
  - obmedzenie fungovania niektorých end-to-end služieb
  - nemožnosť nadviazať TCP spojenie na PC z vonkajšej siete
  - nemožnosť nasadenia niektorých služieb

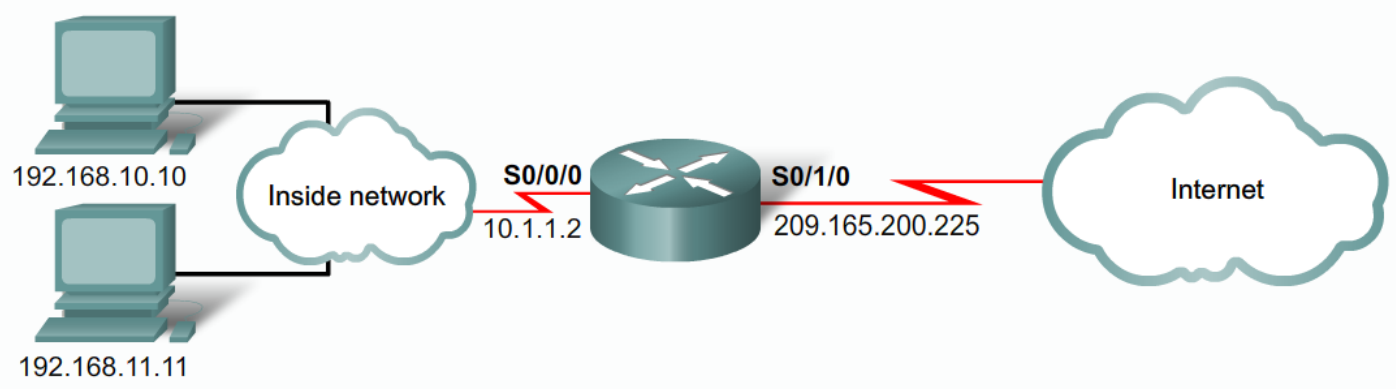
Statické NAT - konfigurácia




```
ip nat inside source static 192.168.10.254 209.165.200.254
!Establishes static translation between an inside local address and an inside global address.
interface serial 0/0/0
ip nat inside
!Identifies Serial 0/1/0 as an outside NAT interface.
interface serial 0/1/0
ip nat outside
!Identifies Serial 0/1/0 as an outside NAT interface.
```

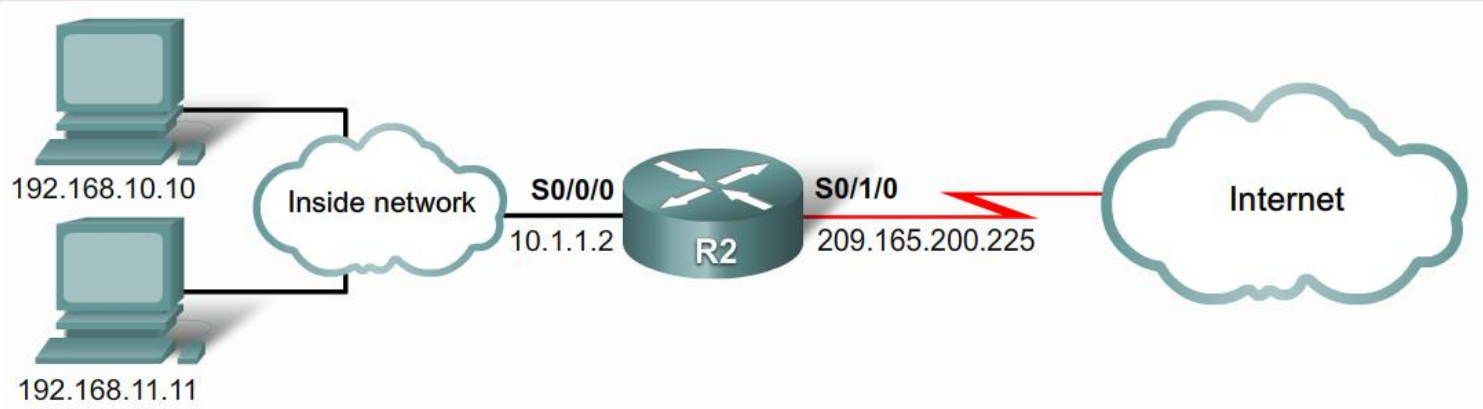
With this configuration, 192.168.10.254 will always translate to 209.165.200.254.

Dynamické NAT - konfigurácia



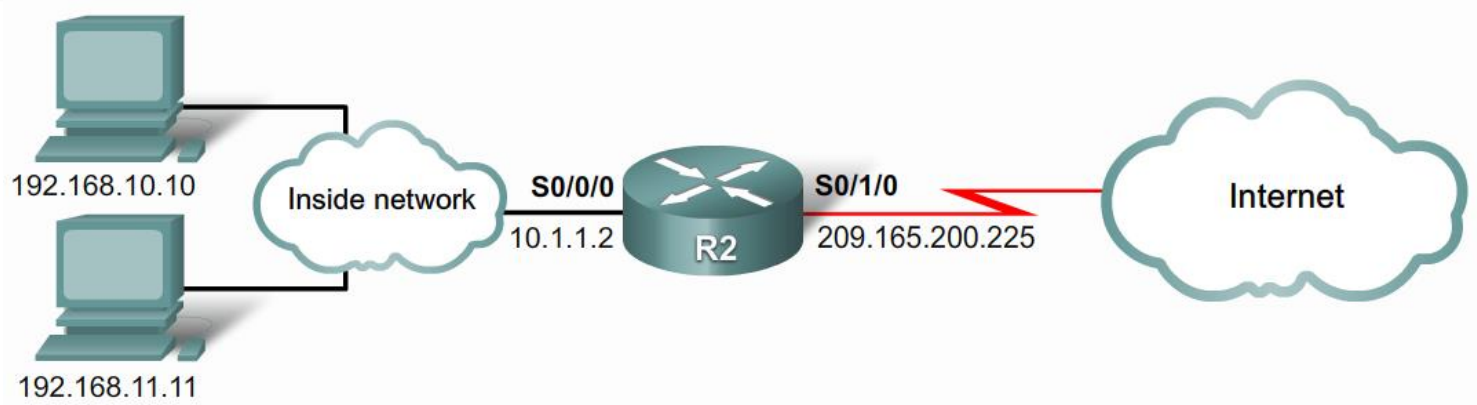

```
ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
```
!Defines a pool of public IP addresses under the pool name NAT-POOL1
```
access-list 1 permit 192.168.0.0 0.0.255.255
```
!Defines which addresses are eligible to be translated
```
ip nat inside source list 1 pool NAT-POOL1
```
!Binds the NAT pool with ACL 1
```
interface serial 0/0/0
  ip nat inside
```
!Identifies interface Serial 0/0/0 as an inside NAT interface
```
interface serial 0/1/0
  ip nat outside
```
!Identifies interface Serial 0/1/0 as the outside NAT interface

NAT Overload - konfigurácia




```
access-list 1 permit 192.168.0.0 0.0.255.255
```
!Defines which addresses are eligible to be translated
```
ip nat inside source list 1 interface serial 0/1/0 overload
```
!Identifies the outside interface Serial 0/1/0 as the inside global address to be overloaded
```
interface serial 0/0/0
  ip nat inside
```
!Identifies Serial 0/0/0 as an inside NAT interface.
```
interface serial 0/1/0
  ip nat outside
```
!Identifies Serial 0/1/0 as an inside NAT interface.

NAT Overload - konfigurácia




```
access-list 1 permit 192.168.0.0 0.0.255.255
```

! – Defines which addresses are eligible to be translated

```
ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240
```

! – Defines a pool of addresses named NAT-POOL2 to be used in NAT translation

```
ip nat inside source list 1 pool NAT-POOL2 overload
```

! – Binds the NAT pool with ACL 1

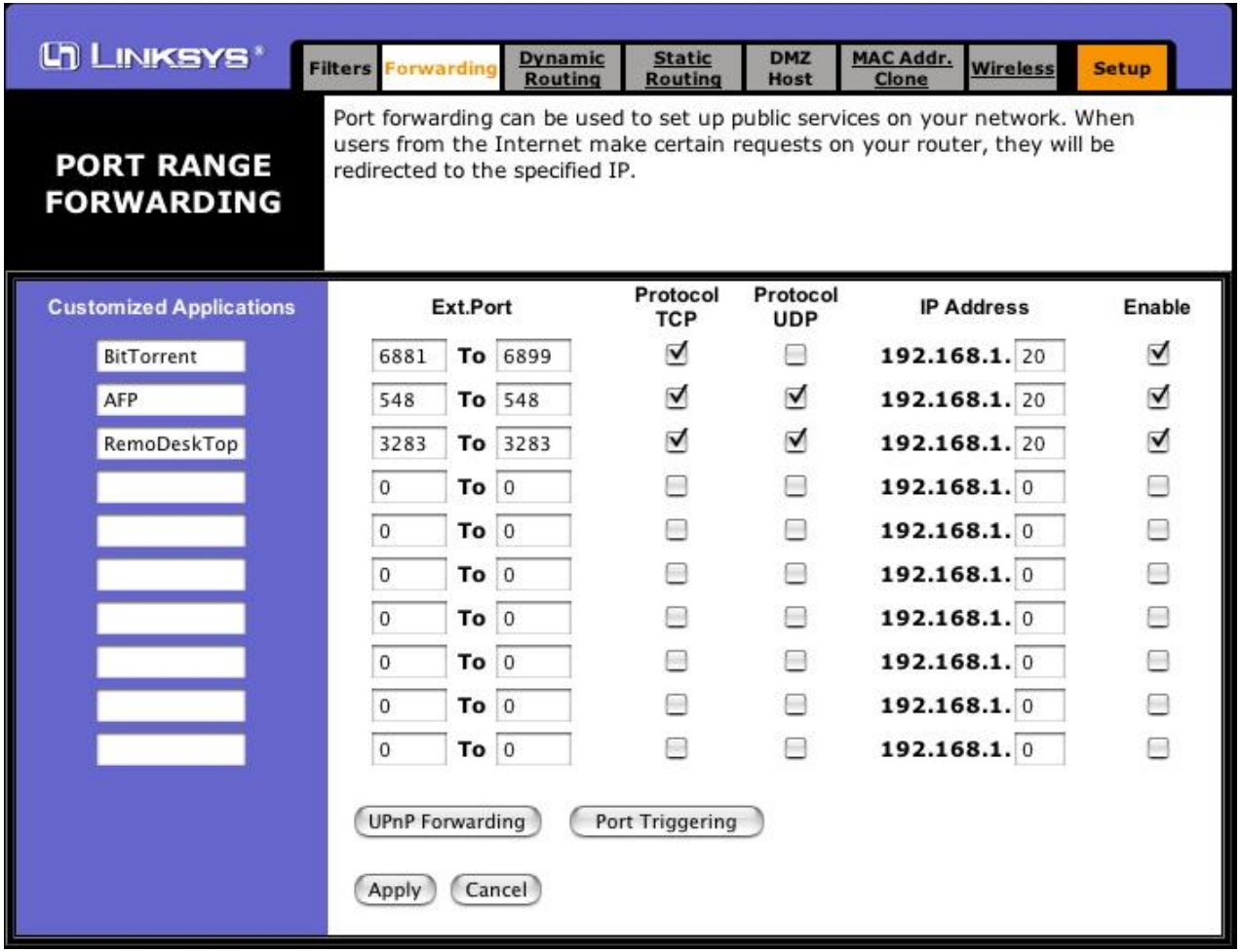
```
interface serial 0/0/0
ip nat inside
```

! – Indentifies interface Serial 0/0/0 as an inside NAT interface

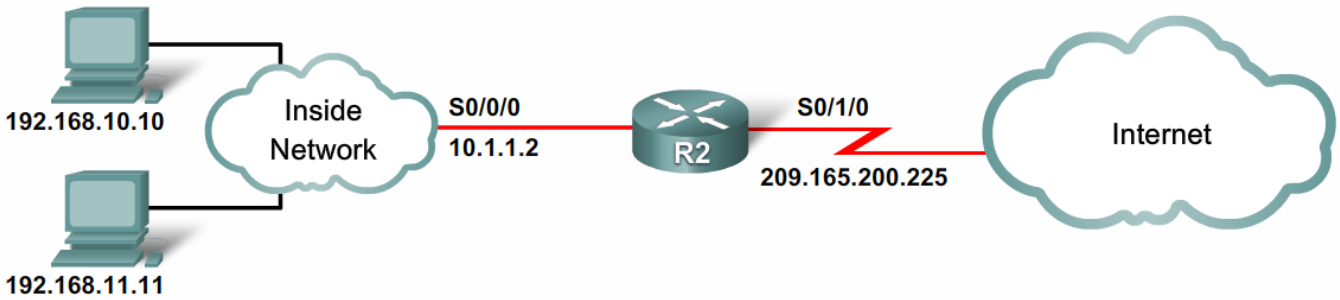
```
interface serial 0/1/0
ip nat outside
```

! – Indentifies interface Serial 0/1/0 as an outside NAT interface

Port forwarding

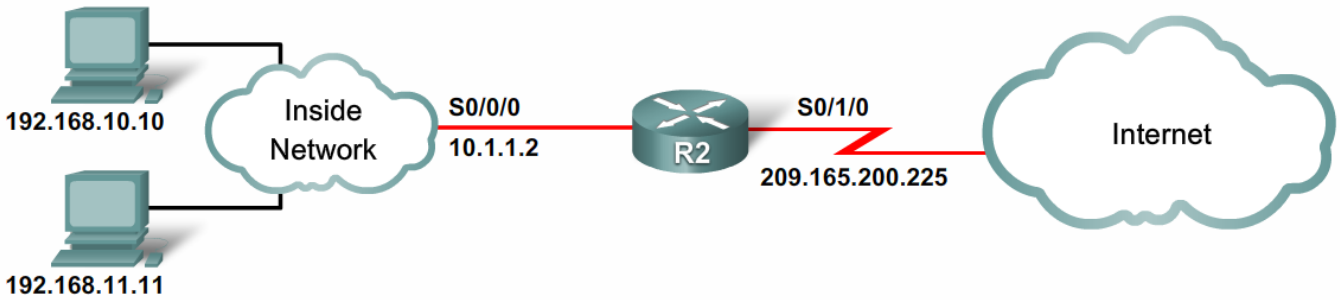


Verifikácia NAT




```
R2#show ip nat translations
Pro Inside global          Inside local          Outside local         Outside global
tcp 209.165.200.225:16642  192.168.10.10:16642   209.165.200.254:80    209.165.200.254:80
tcp 209.165.200.225:62452  192.168.11.10:62452   209.165.200.254:80    209.165.200.254:80

R2#show ip nat translations verbose
Pro Inside global          Inside local          Outside local         Outside global
tcp 209.165.200.225:16642  192.168.10.10:16642   209.165.200.254:80    209.165.200.254:80
    create 00:01:45, use 00:01:43 timeout:86400000, left 23:58:16, Map-Id(In): 1,
    flags:
extended, use_count: 0, entry-id: 4, lc_entries: 0
tcp 209.165.200.225:62452  192.168.11.10:62452   209.165.200.254:80    209.165.200.254:80
    create 00:00:37, use 00:00:35 timeout:86400000, left 23:59:24, Map-Id(In): 1,
    flags:
extended, use_count: 0, entry-id: 5, lc_entries: 0
R2#
```

Verifikácia NAT




```
R2#show ip nat translations
Pro Inside global          Inside local          Outside local         Outside global
icmp 209.165.200.225:3     192.168.10.10:3       209.165.200.254:3     209.165.200.254:3
tcp  209.165.200.225:11679 192.168.10.10:11679   209.165.200.254:80    209.165.200.254:80
icmp 209.165.200.225:0     192.168.11.10:0       209.165.200.254:0     209.165.200.254:0
tcp  209.165.200.225:14462 192.168.11.10:14462   209.165.200.254:80    209.165.200.254:80

R2#show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Outside interfaces:
  Serial0/1/0
Inside interfaces:
  Serial0/0/0, Serial0/0/1
Hits: 173  Misses: 9
CEF Translated packets: 182, CEF Punted packets: 0
Expired translations: 6
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface Serial0/1/0 refcount 3
Queued Packets: 0
R2#
```

Zmazanie NAT prekladov


```
R2#clear ip nat translation *
R2#show ip nat translations

R2#
```

Command	Description
clear ip nat translation *	Clears all dynamic address translation entries from the NAT translation table
clear ip nat translation inside *global-ip local-ip* [**outside** *local-ip global-ip*]	Clears a simple dynamic translation entry containing an inside translation or both inside and outside translation
clear ip nat translation *protocol* **inside** *global-ip global-port local-ip local-port* [**outside** *local-ip local-port global-ip global-port*]	Clears an extended dynamic translation entry

- Otázky k NAT?

IPv4

- 4,294,967,296 unikátnych adries

Porovnanie počtu IP – v4 a v6

IPv4: 4 octets
11000000.10101000.00001010.01100101
192.168.10.101
4,294,467,295 (2^32) IP addresses

IPv6: 16 octets
11010001.11011100.11001001.01110001.11011100. 11001100.01110001.11010001.11011100.11001001. 11010001.11011100.11001001.01110001.00000010.11011110
A524:72D3:2C80:DD02:0029:EC7A:002B:EA73
3.4 x 10^38 IP addresses

340,282,366,920,938,463,463,374,607,431,768,211,456

- There are so many IPv6 addresses available that many trillions of addresses could be assigned to every human being on the planet.
- There are approximately 665,570,793,348,866,943,898,599 addresses per square meter of the surface of the planet Earth!

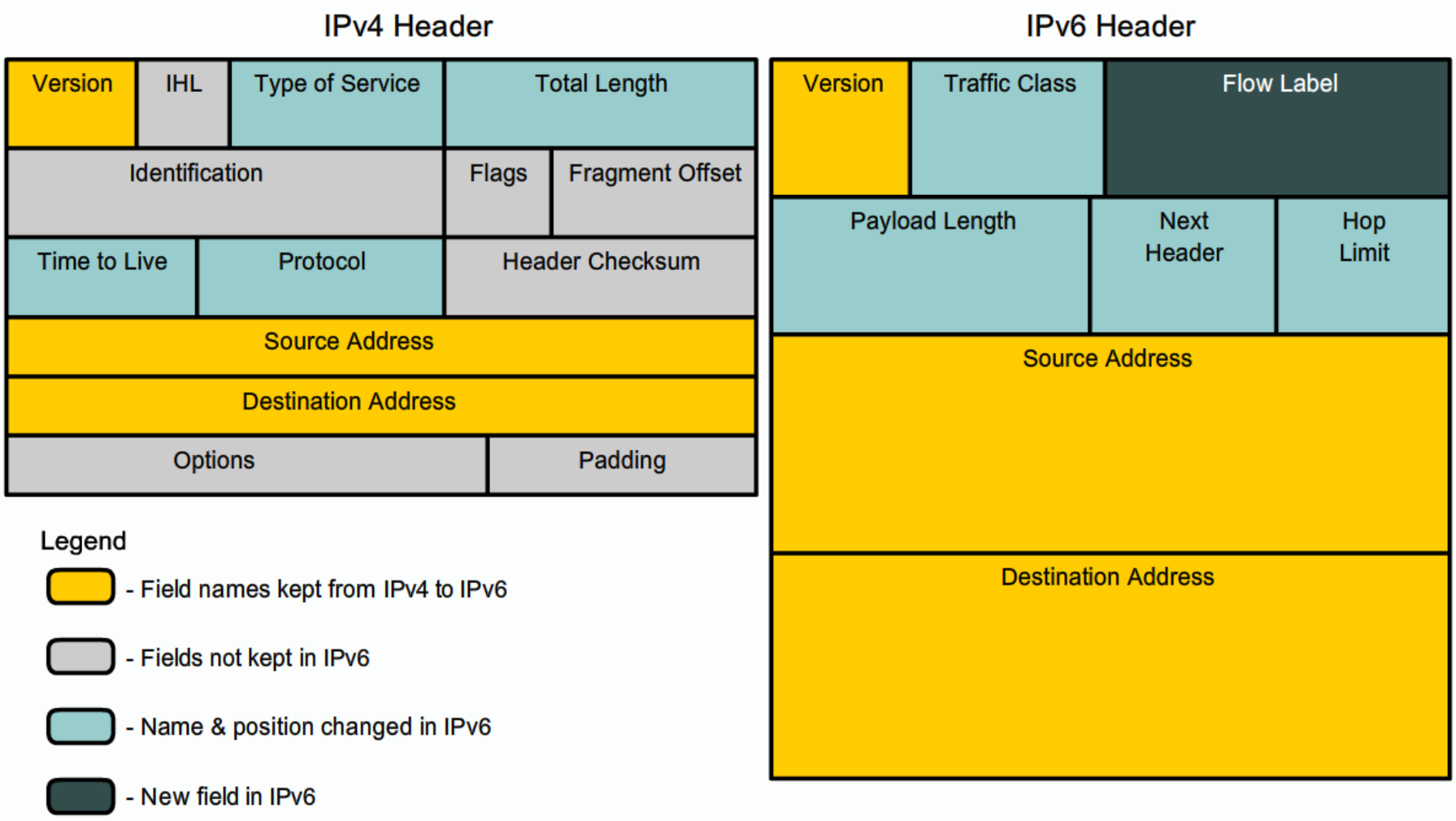
Výhody IPv6

- zlepšená globálna dostupnosť a flexibilita
- lepšia agregácia IP prefixov obsiahnutých v routovacích tabuľkách
- multihoming - technika k zvýšeniu spoľahlivosti internetového pripojenia v IP sieti. Použitím IPv6 môže mať zariadenie niekoľko IP adries cez jednu fyzickú upstream linku, napr. zariadenie môže byť pripojené k niekoľkým poskytovateľom pripojenia (ISP)
- autokonfiguracia, ktorá môže obsahovať adresy spojové vrstvy v adresnom priestore. Viac plug-and-play možností pre viac zariadení.
- adresovanie koniec-koniec bez použitia prekladu adries (NAT), čo umožňuje funkčnú P2P sieť. IP telefónia.
- jednoduchší mechanizmus pre prečíslovanie a zmenu adries.
- jednoduchšia hlavička

Výhody IPv6

- lepšie možnosti smerovania - zlepšujúce výkon
- žiadne Broadcast(y) teda žiadne potenciálne nebezpečenstvo broadcastové búrka
- jednoduchší a efektívnejší mechanizmus rozšírenia hlavičky
- identifikátor toku (flow label) na označenie typu toku dát (zaistenie QoS)

IPv6 hlavička



IPv6 formát

IPv6 Formats

Format:

- **x:x:x:x:x:x:x:x**, where x is a 16-bit hexadecimal field
  - Case-insensitive for hexadecimal A, B, C, D, E, and F
- Leading zeros in a field are optional
- Successive fields of zeros can be represented as **::** only once per address

Examples:

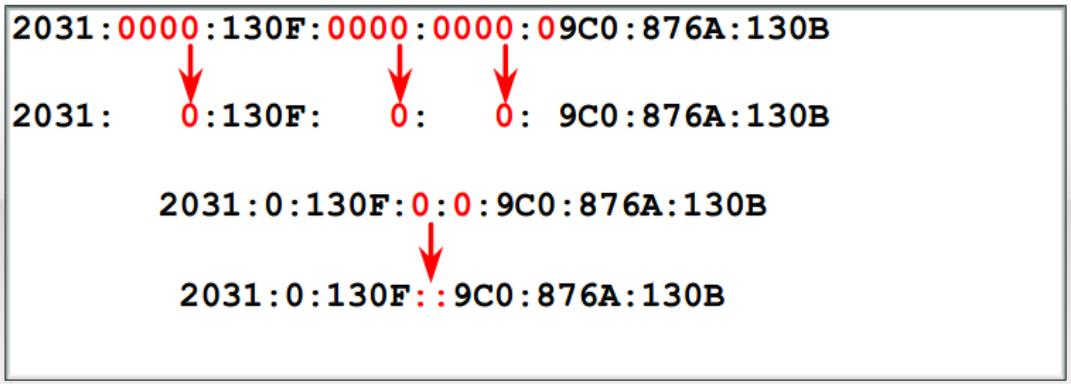
- **2031:0000:130F:0000:0000:09C0:876A:130B**
  - Can be represented as **2031:0:130f::9c0:876a:130b**
  - Cannot be represented as **2031::130f::9c0:876a:130b**
- **FF01:0:0:0:0:0:0:1** **FF01::1**
- **0:0:0:0:0:0:0:1** **::1**
- **0:0:0:0:0:0:0:0** **::**

IPv6 reprezentácia

Representation

2031:0000:130F:0000:0000:09C0:876A:130B

- Can be represented as 2031:0:130f::9c0:876a:130b
- But cannot be represented as 2031::130f::9c0:876a:130b

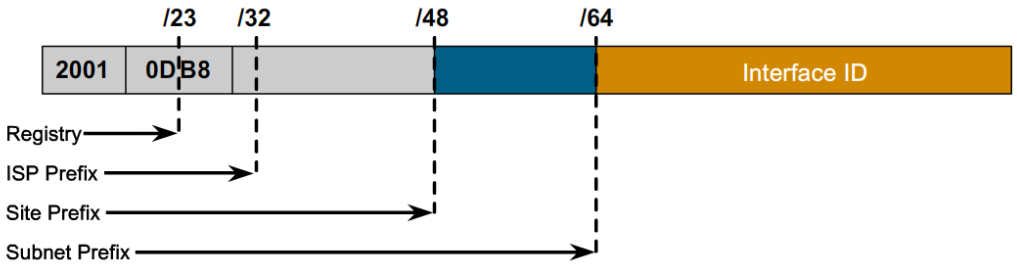


Examples

- FF01:0:0:0:0:0:0:1 becomes FF01::1
- 0:0:0:0:0:0:0:1 becomes ::1
- 0:0:0:0:0:0:0:0 becomes ::
- FF01:0000:0000:0000:0000:0000:0000:1 becomes FF01:0:0:0:0:0:0:1 becomes FF01::1
- E3D7:0000:0000:0000:51F4:00C8:C0A8:6420 becomes E3D7::51F4:C8:C0A8:6420
- 3FFE:0501:0008:0000:0260:97FF:FE40:EFAB becomes 3FFE:501:8:0:260:97FF:FE40:EFAB becomes 3FFE:501:8::260:97FF:FE40:EFAB

Typy adries v IPv6

- **globálna unicast adresa**
  - aktuálne prefix 2000::/3 (snaha o agregáciu)
- **rezervované adresy**
  - 1/256 adries
- **privátne adresy**
  - prvý oktet: FE, ďalšia hex číslica od 8 do F
    - lokálne sieťové adresy
    - lokálne linkové adresy
- **loopback adresa**
  - 0:0:0:0:0:0:0:1 (resp. ::1)
- **nešpecifikovaná adresa**
  - 0:0:0:0:0:0:0:0



Triedy adries IPv6

- **unicast** adresa je pridelená práve jednému sieťovému rozhraniu a teda je úplne jednoznačné, ktoré rozhranie prijíma dáta.
- **anycast** adresy sú formátom nerozlíšiteľné od unicastových, môže ich však mať pridelených viacero sieťových rozhraní. To, ku ktorému sieťovému rozhraniu sa dostanú, je zvyčajne určené routovacou vzdialenosťou.
- **multicast** je doručovaný všetkým sieťovým rozhraniam, ktoré sú zapojené do multicast skupiny.

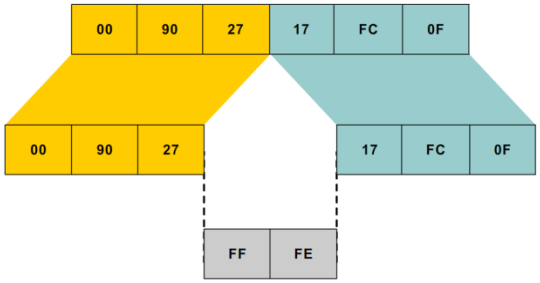
Rozsahy adries

Rozsahy adries *(address scopes)* (RFC 4291) určujú, nakoľko bude možné komunikovať s určitou IPv6 adresou. Konkrétny rozsah, ktorý používa nejaká adresa, je určený pomocou prvých niekoľko bitov.

- **interface-local** -- dosah iba v rámci sieťového rozhrania
- **link-local** adresy je možné používať iba na adresovanie v rámci jednej linkovej vrstvy, nie sú routovateľné
- **site-local** -- dostupnosť v rámci organizácie
- **global** -- globálne dostupné

Prideľovanie IP adries

- **statické pridelenie prostredníctvom interface ID**
  - ipv6 address *ipv6-address/prefix-length*
  - RouterX(config-if)#ipv6 address 2001:DB8:2222:7272::72/64
- **statické pridelenie prostredn EUI-64 interface ID**
  - ipv6 address *ipv6-address/prefix-length eui-64*
  - RouterX(config-if)#ipv6 address 2001:DB8:2222:7272::/64 eui-64



- **stateless autokonfigurácia (SLAAC)**
- **DHCP pre IPv6 (DHCPv6)**

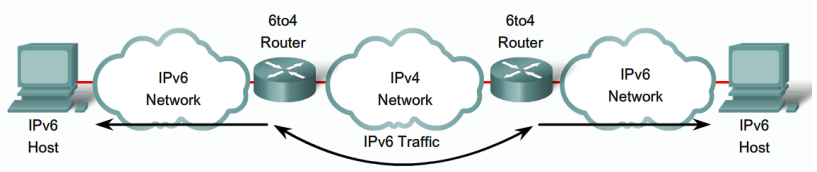
Neighbor Discovery

IPv6 preniesol funkcie, ktoré pre IPv4 plnil protokol ARP, do Neighbor Discovery protokolu, ktorý funguje nad ICMP. Definuje 5 nových ICMP správ:

- **Neighbor solicitation** - požiadavka na zistenie linkovej adresy suseda
- **Neighbor advertisment** - oznámenie linkovej adresy suseda
- **Router solicitation** - požiadavka na zistenie informácií o routeroch
- **Router advertisment** - oznam o dostupných routeroch
- **Redirect** - presmerovanie a informácie o lepších cestách

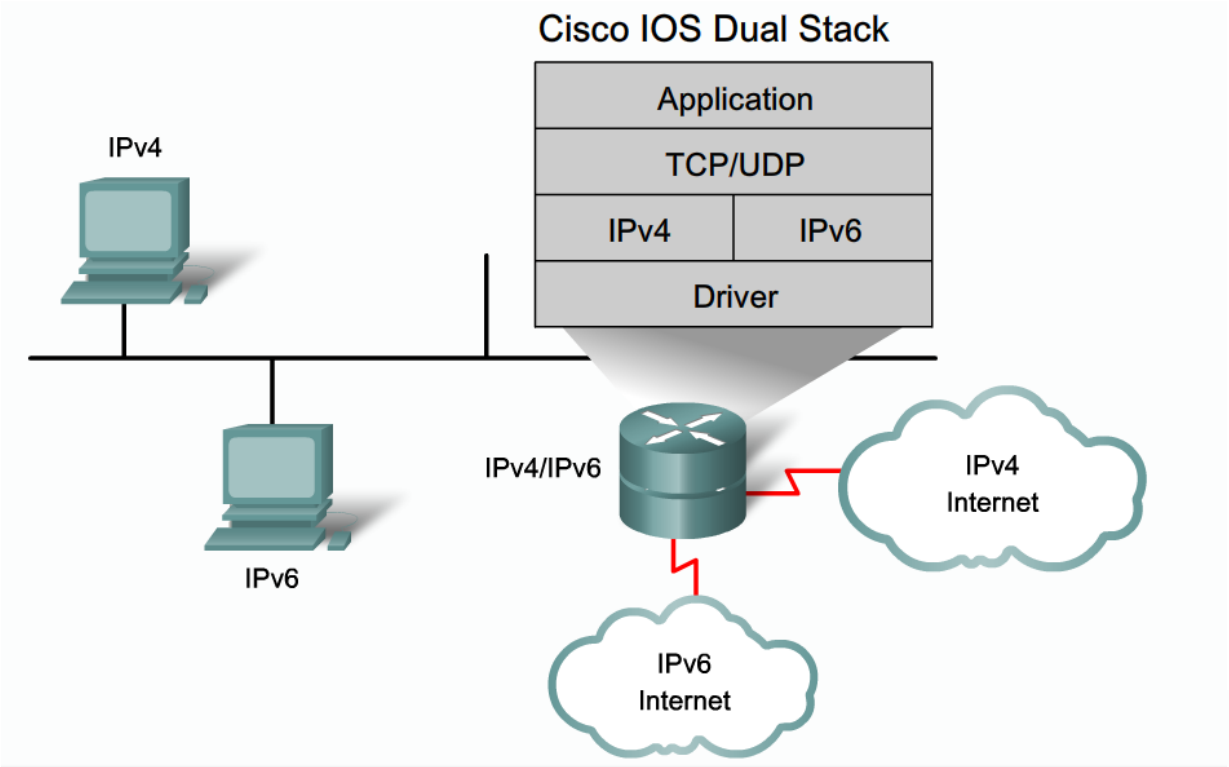
Prechod z IPv4 na IPv6

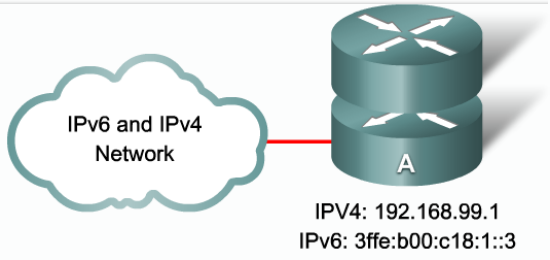
- Dual Stacking
  - koncová stanica ma obe verzie IP adresy
  - preferencia na IPv6
- Tunneling
  - Manual IPv6-over-IPv4 tunneling (IPv6 paket je enkapsulovaný do IPv4 – vyžaduje si to dual-stack router)
  - Dynamic 6to4 tunneling



- NAT-Protocol Translation (IPv6 <-> IPv4)

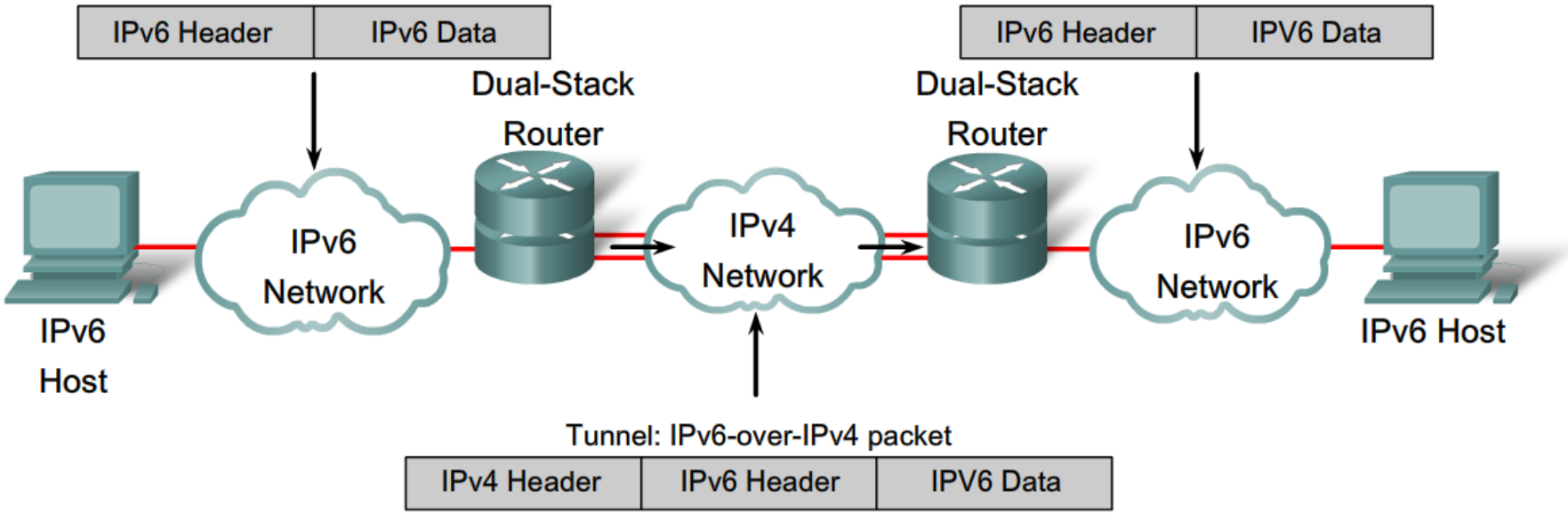
Cisco IOS Dual Stack






```
conf t
ipv6 unicast-routing

interface ethernet0
  ip address 192.168.99.1 255.255.255.0
  ipv6 address 3ffe:b00:c18:1::3/127
```

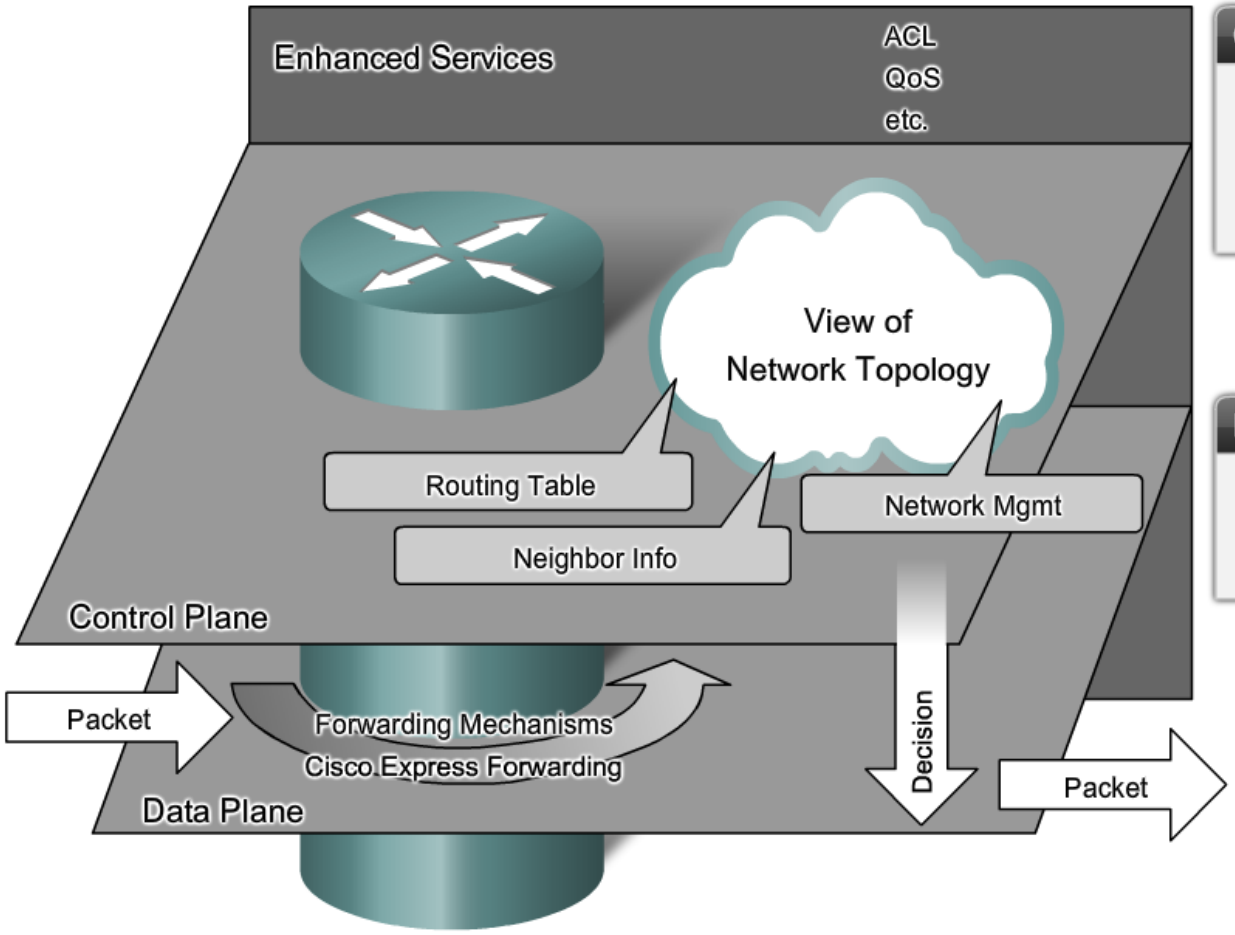
IPv6 Tunelling



Tunneling is an integration method in which an IPv6 packet is encapsulated within another protocol, such as IPv4. This method of encapsulation is IPv4:

- Includes a 20-byte IPv4 header with no options and an IPv6 header and payload
- Requires dual-stack routers

IPv6 routing



Control Plane Considerations:

- IPv6 Address Size
- Multiple IPv6 Node Addresses
- IPv6 Routing Protocols
- Routing Table Size

Forwarding Plane Considerations:

- Parsing IPv6 Extension Headers
- IPv6 Address Lookup

RIPNg

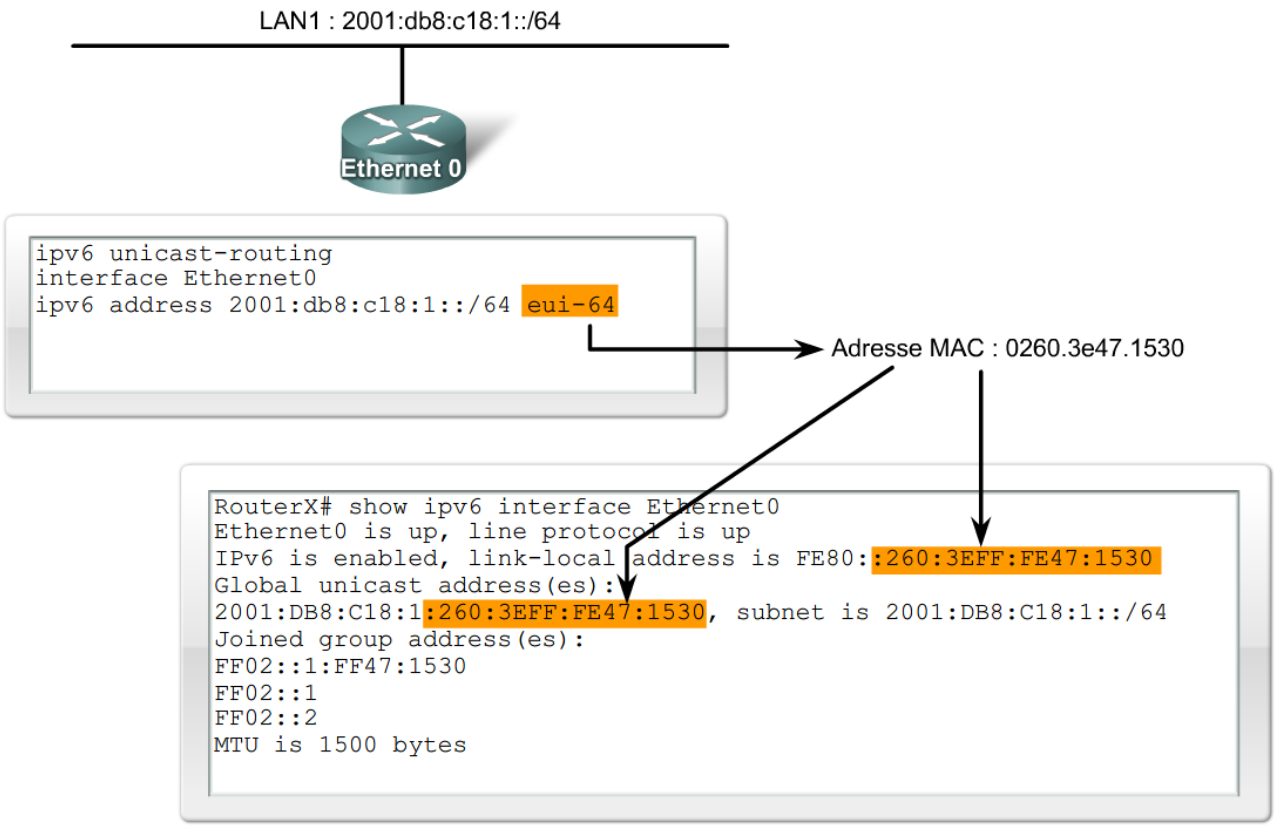
- rozšírenie RIPv2 pre IPv4
- RFC 2080

- distance vector (15 hops)
  - split horizon
  - poison reverse
- multicast group FF02::9 pre RIP updates

- Cisco IOS 12.2(2)T a vyšší

Konfigurácia IPv6

Command	Purpose
RouterX(config)#ipv6 unicast-routing	Enables IPv6 traffic forwarding
RouterX(config-if)# ipv6 address ipv6prefix/prefix-length eui-64	Configures the interface IPv6 addresses

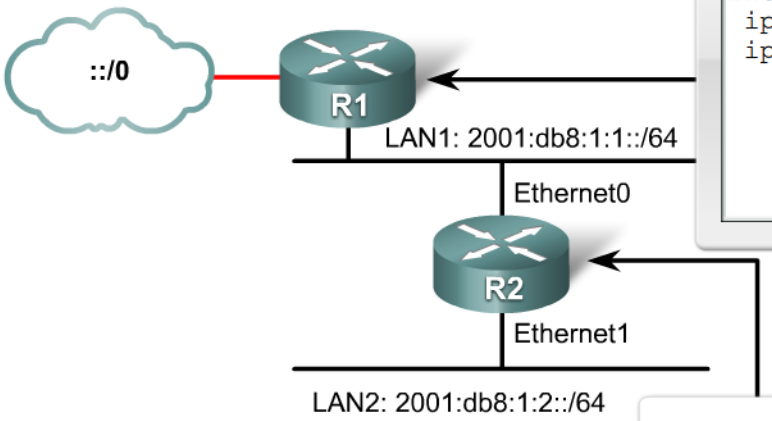


IPv6 Name Resolution

Command	Purpose
RouterX(config)# **ipv6 host** *name* [*port*] *ipv6addr* [{*ipv6addr*} ...] RouterX(config)# **ipv6 host router1 3ffe:b00:ffff:b::1**	Define a static name for IPv6 addresses
RouterX(config)#**ip name-server** *address* RouterX(config)#**ip name-server 3ffe:b00:ffff:1::10**	Configure a DNS server or servers to query

RIPNg - konfigurácia

Command	Purpose
`RouterX(config)#ipv6 router rip name`	Creates and enters RIP router configuration mode.
`RouterX(config-if)#ipv6 rip name enable`	Configures RIP on an interface.




```
ipv6 unicast-routing
ipv6 router rip RT0

interface Ethernet0
 ipv6 address 2001:db8:1:1::/64 eui-64
 ipv6 rip RT0 enable
```

```
ipv6 unicast-routing
ipv6 router rip RT0

interface Ethernet0
 ipv6 address 2001:db8:1:1::/64 eui-64
 ipv6 rip RT0 enable

interface Ethernet1
 ipv6 address 2001:db8:1:2::/64 eui-64
 ipv6 rip RT0 enable
```

Verifikácia RIPNg

Command	Purpose
`show ipv6 interface`	Displays the status of interfaces configured for IPv6.
`show ipv6 interface brief`	Displays a summarized status of interfaces configured for IPv6.
`show ipv6 neighbors`	Displays IPv6 neighbor discovery cache information.
`show ipv6 protocols`	Displays the parameters and current state of the active IPv6 routing protocol processes.
`show ipv6 rip`	Displays information about current IPv6 Routing Information Protocol (RIP) processes.
`show ipv6 route`	Displays the current IPv6 routing table.
`show ipv6 route summary`	Displays a summarized form of the current IPv6 routing table.
`show ipv6 routers`	Displays IPv6 router advertisement information received from other routers.
`show ipv6 static`	Displays only static IPv6 routes installed in the routing table.
`show ipv6 static 2001:db8:5555:0/16`	Displays only static route information about the specific address given.
`show ipv6 static interface serial 0/0`	Displays only static route information with the specified interface as

Otázky?

Zdroj

- oficiálne kurikulá k CCNA3 v4
- Wikipedia – BOOTP, DHCP
- http://netlab.dcs.fmph.uniba.sk/siete/cviko7/

- neprešlo jazykovou úpravou
- prezentácia môže obsahovať chyby