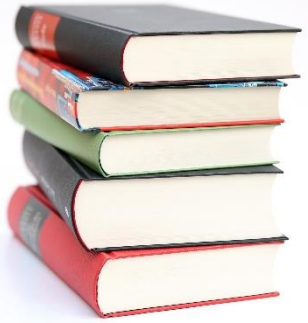
MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

DHCPv4, DHCPv6

Počítačové siete 1

Katedra informačných sietí
Fakulta riadenia a informatiky, ŽU

Vytvorené v rámci projektu KEGA 011STU - 4/2017.



Čo nás dnes čaká

- **Dokončenie z predošlej prednášky:**
  - Komplexné ACL
    - Dynamické (Dynamic) ACL
    - Reflexívne (Reflexive) ACL
    - Časové (Time-Based) ACL
  - IPv6 ACLs
- **DHCPv4**
  - Komponenty, činnosť, správy
  - Konfigurácia
- **Multicastové IPv6 adresy (pripomienka)**
- **DHCPv6**
  - Dynamické prideľovanie IPv6 adries
    - SLAAC
    - Stateless DHCPv6
    - Statefull DHCPv6
  - Konfigurácia

(RSE_08 DHCP)

Reakcia na otázku v ankete k predošlej prednáške - ACL

„Aký je rozdiel medzi ACL a firewall-om ?“

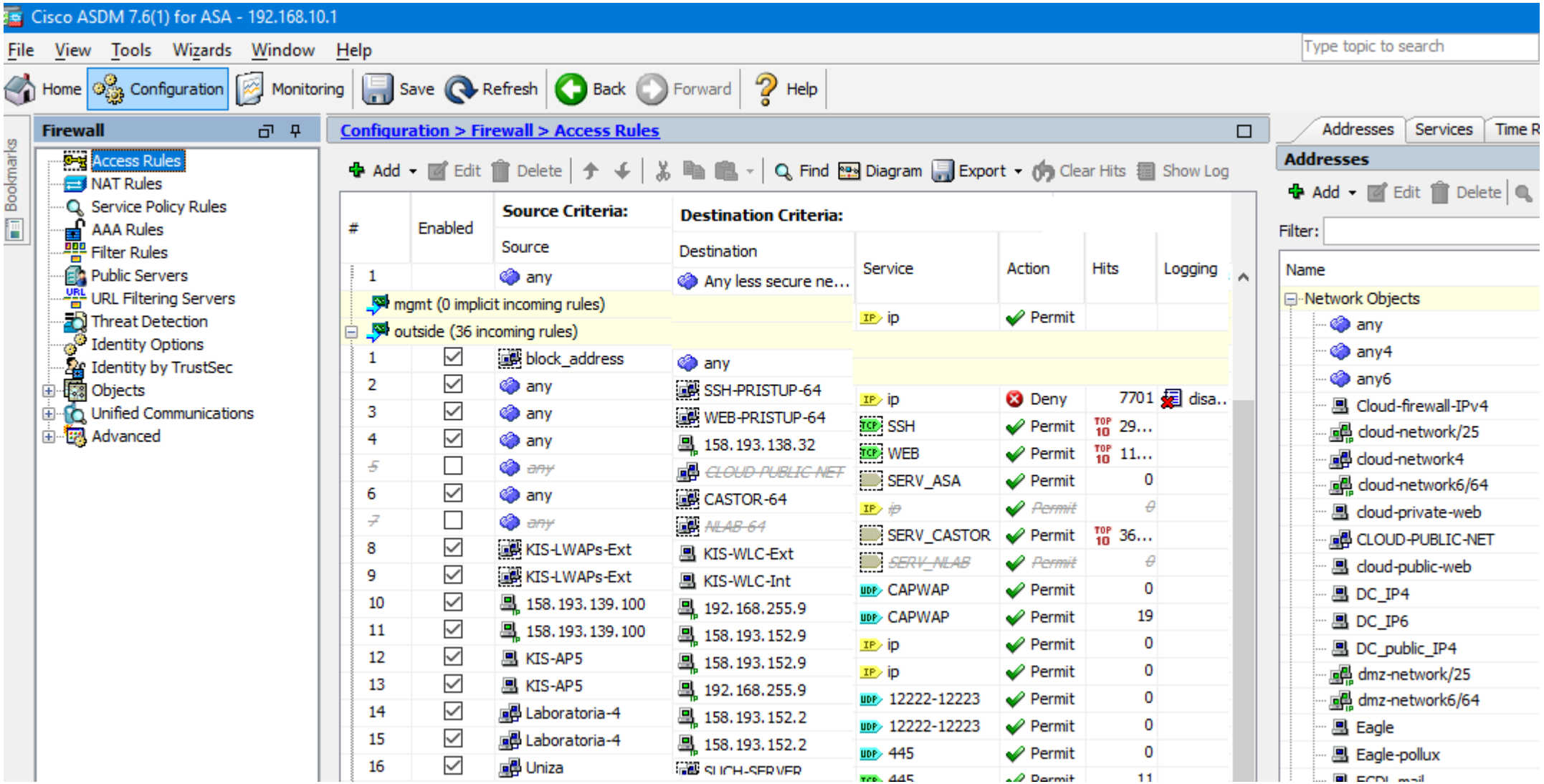
Definovanie objektov na Cisco ASA (KIS sieť)

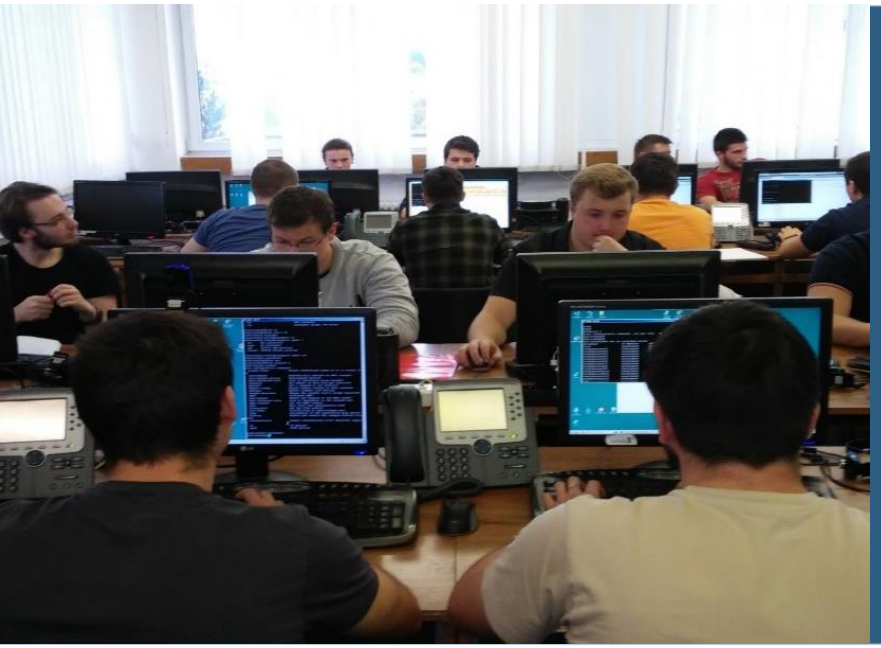
```
object network KIS-VLAN-110-IPv4
 subnet 192.168.110.0 255.255.255.0
 description KIS WIFI VLAN 192.168.110.0/24
object network NAT-POOL-NEW
 range 158.193.152.81 158.193.152.94
 description KIS OUTSIDE NAT POOL 158.193.152.80/28
object network KIS-VLAN-30-IPv4
 subnet 192.168.30.0 255.255.255.0
 description KIS ECDL VLAN 192.168.30.0/24
```

Definovanie ACL na Cisco ASA (KIS sieť)

```
access-list vlan10_multicast standard permit host 233.10.47.10
access-list VLAN10-IN extended permit ip object-group WIFI-APS object
KIS-WLC-Int
access-list VLAN10-IN extended deny ip object KIS-VLAN-10-IPv4 object
KIS-VLAN-255-IPv4
access-list VLAN10-IN extended permit ip object KIS-VLAN-10-IPv4 any
access-list VLAN255-IN extended permit ip any any
access-list VPN-DISABLED-NAT extended permit ip object KIS-VLAN-10-IPv4
object KIS-VPN-NET
access-list VPN-DISABLED-NAT extended permit ip object KIS-VLAN-255-IPv4
object KIS-VPN-NET
access-list VPN-ALLOWED-NETWORKS standard permit 192.168.10.0
255.255.255.0
access-list VPN-ALLOWED-NETWORKS standard permit 192.168.255.0
255.255.255.0
```

Web GUI na Cisco ASA (KIS sieť)

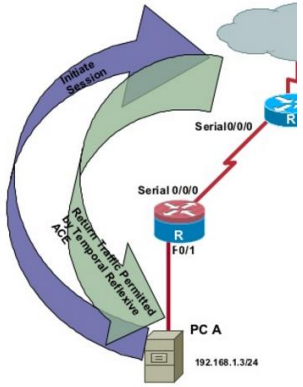


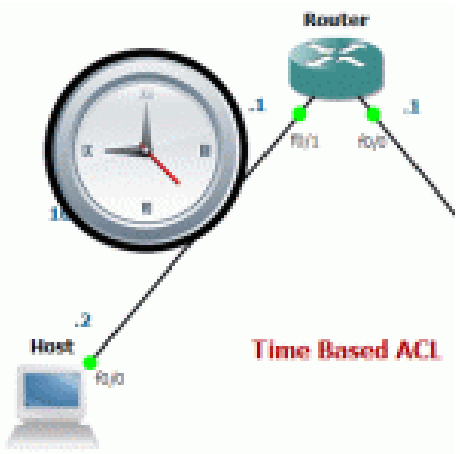


Komplexné ACL

Komplexné ACL

- Máme tri typy komplexných ACL
  - Dynamické (Dynamic) ACL
    - Používatelia, ktorí chcú komunikovať cez router sa musia najskôr naň prihlásiť cez telnet
  - Reflexívne (Reflexive) ACL
    - Umožňuje prevádzke prechádzať smerom z dnu von, v opačnom smere obmedzuje komunikáciu
  - Časové (Time-Based) ACL
    - Riadenie prevádzky podľa času



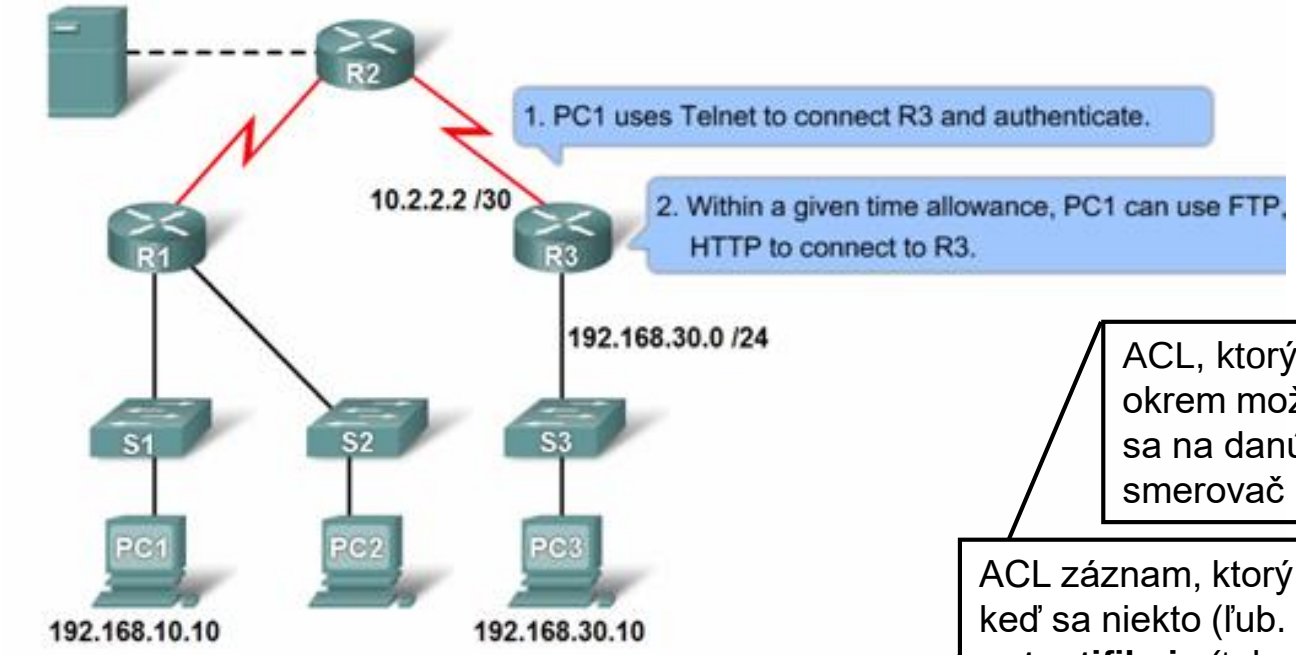


Dynamické ACL

- Princíp **zámka & kľúč** (lock-and-key)
- Dostupné len pre IP prevádzku
  - Využíva extended ACL
- Používateľ, ktorý chce „prechádzať“ cez smerovač, sa musí naň najprv prihlásiť a autentifikovať (telnet)
  - Do extended ACL je pridaná **dočasná** položka, ktorá mu umožní **dočasne** (na určitý čas, napr. 120 min) komunikovať cez smerovač
- Účel
  - Poskytnutie dočasnej konektivity do siete pre vzdialených používateľov
- Výhody
  - Mechanizmus autentifikácie používateľov
  - Zjednodušený manažment prístupu vo veľkých sieťach
  - Obmedzenie prielomov do siete hackermi
  - Vytvorenie dynamických prechodov cez firewall (FW), bez obmedzenia iných bezpečnostných reštrikcií

Dynamické ACL

Príklad



ACL, ktorý blokuje všetko, okrem možnosti telnetnúť sa na danú IP na smerovač

ACL záznam, ktorý sa aplikuje vtedy, keď sa niekto (ľub. užívateľ) úspešne **autentifikuje** (telnet na smerovač). Definuje sa časový interval, počas ktorého je vytvorený dočasný ACL a užívateľ môže komunikovať cez smerovač akokoľvek (ip any any), default 120 min.

```
! Vytvorenie uctu pre telnet
username peter password P$T$T_2018
```

```
! Vytvorenie ACL
access-list 111 permit tcp any host 10.2.2.2 eq telnet
access-list 111 dynamic MY_DYNAMIC timeout 120 permit ip any any
```

```
int s 0/0/0
  ip access-group 111 in
```

```
line vty 0 4
  autocommand access-enable timeout 5
  login local
```

Príkaz **autocommand** vytvorí dočasný ACL záznam (bude na ďalšom slajde) v smere IN pre rozhranie serial 0/0/0, na základe druhého záznamu (MY_DYNAMIC). Tento dočasný záznam expiruje po **5 minútach nečinnosti** usera, čo špecifikuje príkaz timeout.

Príklad - pokračovanie

```
Router#show access-lists
Extended IP access list 111
    10 Dynamic MY_DYNAMIC permit ip any any
    20 permit tcp any host 10.2.2.2 eq telnet (68 matches)
```

PC1 (192.168.10.10) cmd:

telnet 10.2.2.2

```
Trying 10.2.2.2 ...
Connected to 10.2.2.2.
Escape character is '^]'.
User Access Verification

Username: peter
Password: P$T$T_2018
Connection closed by foreign host.
```

Definuje dynamický ACL záznam (template), ktorý sa dočasne nainštaloval potom, ako sa užívateľ úspešne nalogoval a vytvoril sa pre neho prístup pomocou autocommand

```
Router#show access-lists
Extended IP access list 111
    10 Dynamic MY_DYNAMIC permit ip any any
    permit ip host 192.168.10.10 any (time left 119)
    20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

Odporúčania

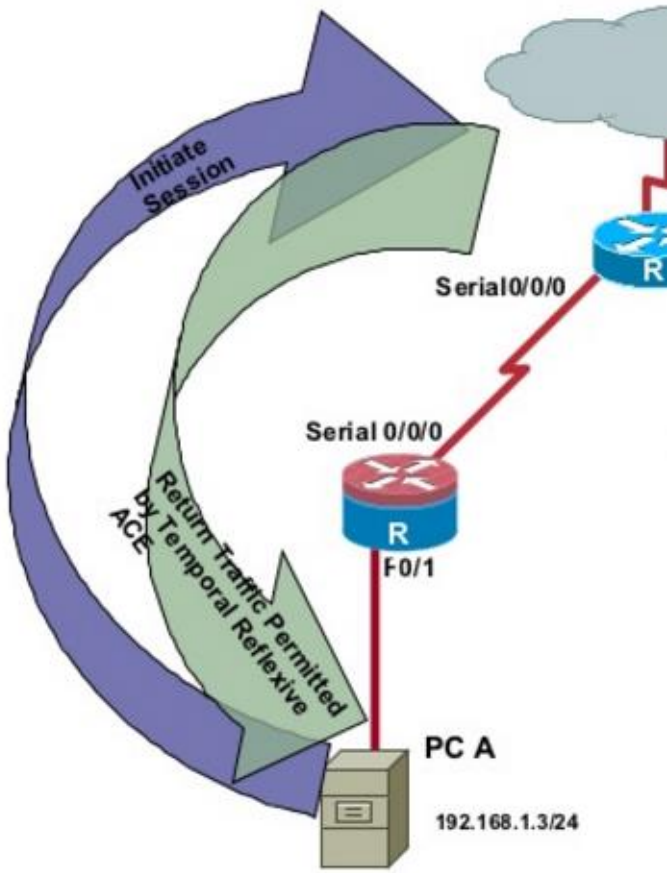
- **Max. 1** dynamický ACL vo vnútri 1 rozšíreného ACL
  - Softvér akceptuje iba prvý definovaný dynamický ACL.
- Neprideľovať rovnaké dynamické meno do iného ACL na 1 smerovači
  - Ak to urobíme, znamená to, že dávame pokyn softvéru, aby znovu použil existujúci ACL.
  - Všetky pomenované položky musia byť globálne jedinečné v rámci konfigurácie.
- Priraďovať atribúty (položky, statements) do dynamického ACL rovnakým spôsobom ako v bežnom ACL.
  - Dočasné ACL položky dedia atribúty priradené tomuto ACL zoznamu.
- Nakonfigurovať Telnet pre autentifikáciu užívateľov na smerovač
  - pre získanie prístupu cez daný smerovač, bude musieť user otvoriť Telnet reláciu do smerovača, aby bol autentifikovaný

Odporúčania – pokrač.

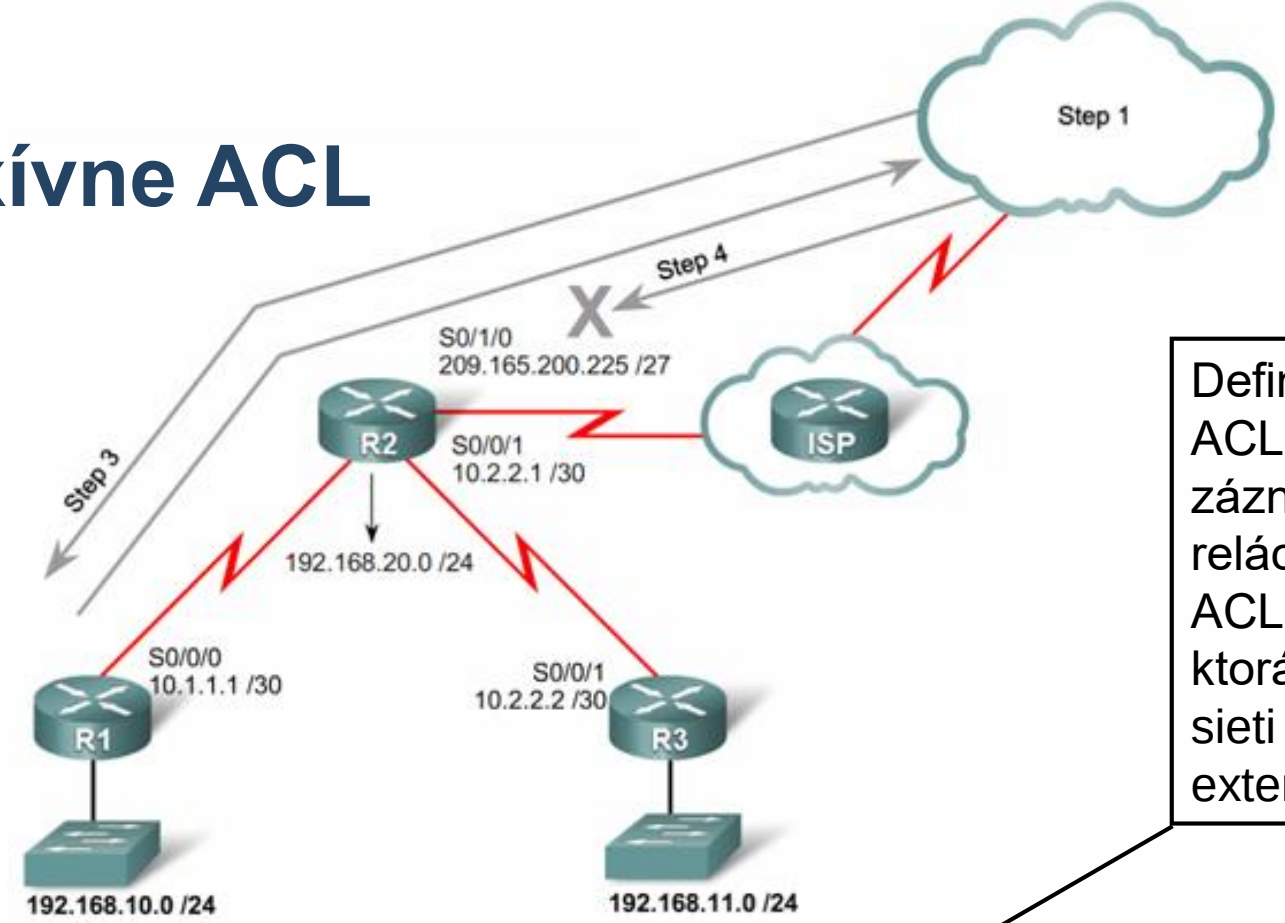
- Idle timeout definovať buď cez autocommand... (timeout 5), alebo definovať absolútnu hodnotu neskôr pri definovaní ACL (timeout 120)
  - Je možné nakonfigurovať oba, potom ale idle timeout musí byť menší ako absolute timeout
- Ak treba natiahnuť čas, možno použiť príkaz **access-list dynamic-extend**
  - Na predĺženie absolute timera dynamického ACL o 6 minút.
  - Príkaz umožní otvoriť novú Telnet reláciu do smerovača na re-autentifikáciu pomocou lock-and-key funkcie.
- Jediné hodnoty, ktoré sa v dočasných záznamoch menia sú zdrojová a cieľová IP adresa, podľa toho, či je daný ACL využívaný ako input alebo output ACL
  - Všetky ďalšie atribúty ako port, sa dedia z hlavného dynamického ACL.
- Každé vloženie doačasnej položky do dynamického ACL sa vždy vloží na začiatok zoznamu
  - Nemožno definovať poradie dočasných ACL položiek.
- Dočasné ACL položky sa nikdy nezapisujú do NVRAM.

Reflexívne ACL (IP Session Filtering)

- Umožňuje otvárať (povoľovať) IP toky (relácie) z vnútra siete dynamicky
  - Zakazuje, resp. nepovoľuje toky z vonku dnu
- Reflexívne ACL obsahuje len dynamické položky
  - Po reštarte nie sú dostupné
  - Dokonalejšie ako `established` parameter v extended ACL
    - Kontrolujú sa aj iné parametre ako TCP Flag bity
  - Použitie len s pomenovanými extended ACL
  - Inštalované pri štarte relácie z vnútra siete
- Výhody nasadenia
  - Nasadenia na routre na rozhraní Internal/External net
  - Lepšia ochrana siete voči útokom.
  - Lepšia ochrana voči DoS a spoofing útokom.
  - Jednoduchšia obsluha, väčšia kontrola nad prevádzkou.



Reflexívne ACL



Definujeme reflexívny ACL, ktorý pridá záznamy dynamickej relácie do rozšíreného ACL pre prevádzku, ktorá vzniká vo vnútornej sieti a smeruje do externej siete

```
! Applied on external interface for outbound direction.
R2(config)#ip access-list extended EXTERNAL_OUT
R2(config-ext-nacl)#permit tcp any any reflect TRAFFIC
R2(config-ext-nacl)#permit udp any any eq domain reflect TRAFFIC
```

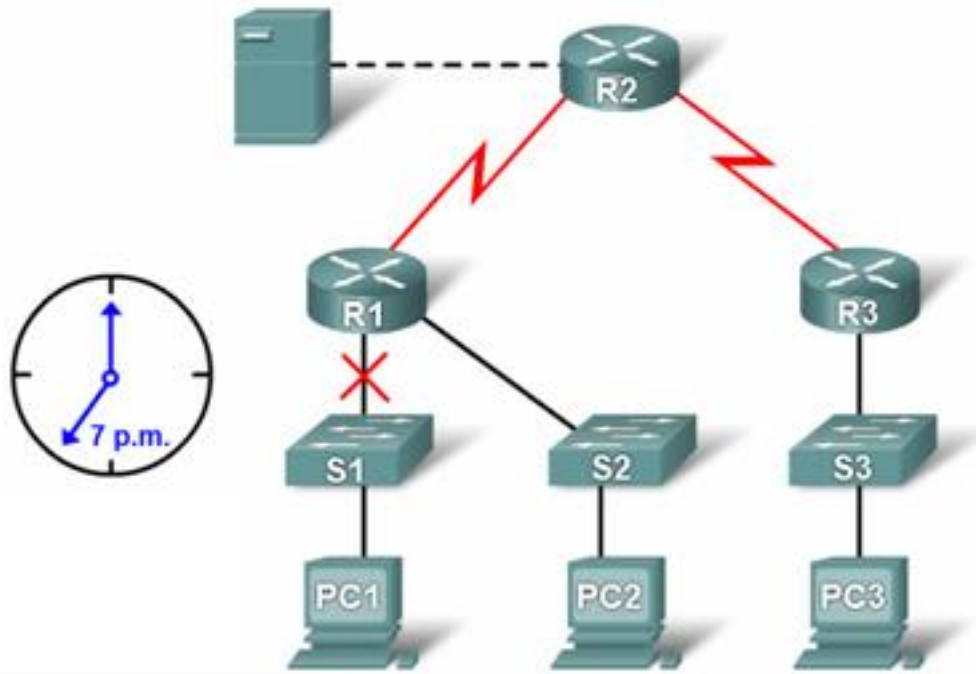
```
! Applied on external interface for inbound direction
R2(config)#ip access-list extended EXTERNAL_IN
R2(config-ext-nacl)#evaluate TRAFFIC
```

Tento ACL porovná vstupnú prevádzku voči záznamom, ktoré sa tvoria pritom ako prevádzka odchádza z vnútornej siete von

```
R2(config)#int se 0/1/0
R2(config-if)#ip access-group EXTERNAL_IN in
R2(config-if)#ip access-group EXTERNAL_OUT out
```

Časové (Time-Based) ACL

- V činnosti podobné extended ACL
  - Len riadenie prístupu môže byť definované časom
    - časť dňa, deň, viacero dní a pod. + nadefinovaná funkcia



Step 1

```
R1(config)#time-range EVERYOTHERDAY
R1(config-time-range)#periodic Monday Wednesday Friday 8:00 to
17:00
```

Step 2

```
R1(config)#access-list 101 permit tcp 192.168.10.0 0.0.0.255
any eq telnet time-range EVERYOTHERDAY
```

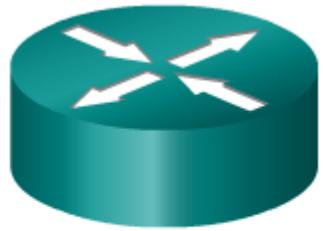
Step 3

```
R1(config)#interface s0/0/0
R1(config-if)#ip access-group 101 out
```

IPv6 ACL

Porovnanie IPv4 a IPv6 ACLs

- Sú podobné, ale tieto 3 veci sú v IPv6 inak:
- Aplikovanie IPv6 ACL príkazom:
  - **`ipv6 traffic-filter`**
- Nepoužíva wildcard masky
  - Používa sa **prefix-length**
- Má niektoré podmienky navyše
  - permit icmp any any **nd-na**
  - permit icmp any any **nd-ns**

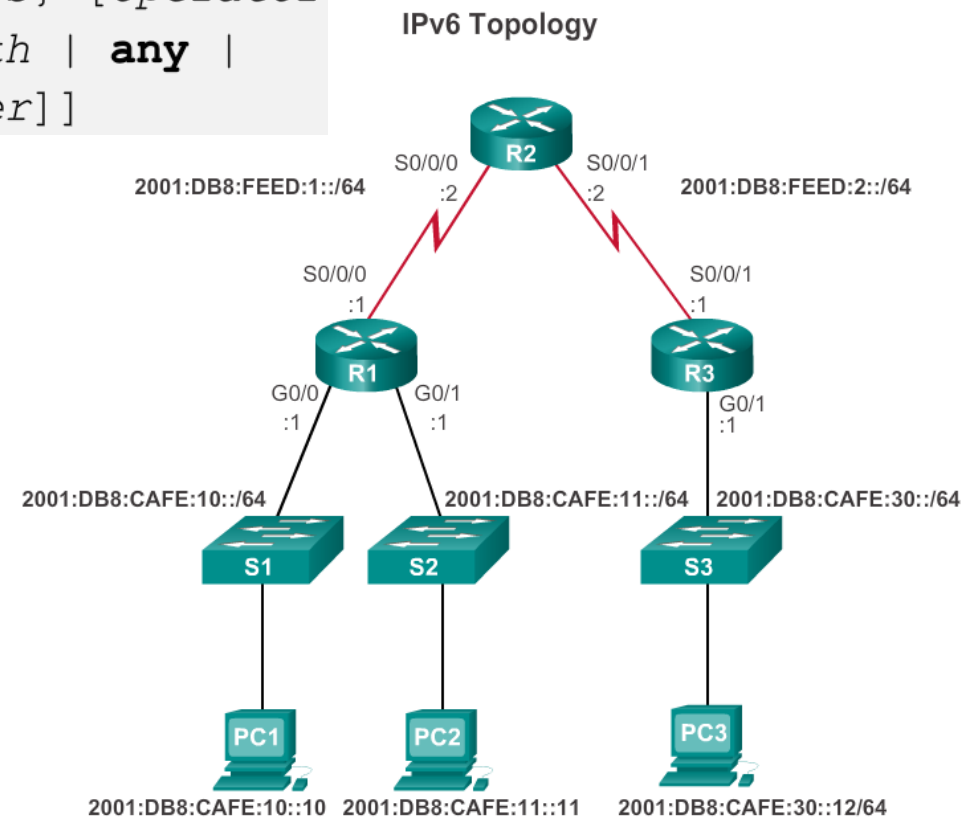


IPv4 ACLs
- Standard
  - Numbered
  - Named
- Extended
  - Numbered
  - Named

IPv6 ACLs
- Named only
- Similar in functionality to IPv4 Extended ACL

Konfigurácia IPv6 ACLs

```
R1(config)# ipv6 access-list access-list-name
R1(config-ipv6-acl)# deny | permit protocol {source-ipv6-
prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any |
host destination-ipv6-address} [operator [port-number]]
```




```
R1(config)# interface s0/0/0
R1(config-if)# ipv6 traffic-filter NO-R3-LAN-ACCESS in
```

IPv6 ACL príklady

```
R1(config)# ipv6 access-list NO-R3-LAN-ACCESS
R1(config-ipv6-acl)# deny ipv6 2001:db8:cafe:30::/64 any
R1(config-ipv6-acl)# permit ipv6 any any
```

```
R1(config)# interface s0/0/0
R1(config-if)# ipv6 traffic-filter NO-R3-LAN-ACCESS in
```

```
R1(config)# ipv6 access-list NO-FTP-TO-11
R1(config-ipv6-acl)# deny tcp any 2001:db8:cafe:11::/64 eq ftp
R1(config-ipv6-acl)# deny tcp any 2001:db8:cafe:11::/64 eq ftp-data
R1(config-ipv6-acl)# permit ipv6 any any
R1(config-ipv6-acl)# exit
R1(config)# interface g0/0
R1(config-if)# ipv6 traffic-filter NO-FTP-TO-11 in
```

IPv6 ACL príklady

```
 ipv6 access-list RESTRICTED-ACCESS
pv6-acl)# remark Permit access only HTTP and HTTPS to Network 10
pv6-acl)# permit tcp any host 2001:db8:cafe:10::10 eq 80
pv6-acl)# permit tcp any host 2001:db8:cafe:10::10 eq 443
pv6-acl)# remark Deny all other traffic to Network 10
pv6-acl)# deny ipv6 any 2001:db8:cafe:10::/64
pv6-acl)# remark Permit PC3 telnet access to PC2
pv6-acl)# permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CAFE:11::11 e
pv6-acl)# remark Deny telnet access to PC2 for all other devices
pv6-acl)# deny tcp any host 2001:db8:cafe:11::11 eq 23
pv6-acl)# remark Permit access to everything else
pv6-acl)# permit ipv6 any any
pv6-acl)# exit
 interface g0/0
f)# ipv6 traffic-filter RESTRICTED-ACCESS in
```

1 2 4 5 6

Overenie IPv6 ACLs

```
R3#show ipv6 interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Global unicast address(es):
    2001:DB8:CAFE:30::1, subnet is 2001:DB8:CAFE:30::/64
  Input features: Access List
  Inbound access list RESTRICTED-ACCESS
```

<some output omitted for brevity>

```
R3#show access-lists
IPv6 access list RESTRICTED-ACCESS
    permit tcp any host 2001:DB8:CAFE:10::10 eq www sequence 20
    permit tcp any host 2001:DB8:CAFE:10::10 eq 443 sequence 30
    deny ipv6 any 2001:DB8:CAFE:10::/64 sequence 50
    permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CAFE:11::11 eq
    telnet sequence 70
    deny tcp any host 2001:DB8:CAFE:11::11 eq telnet sequence 90
    permit ipv6 any any sequence 110
R3#
```

Dynamic Host Configuration Protocol DHCPv4

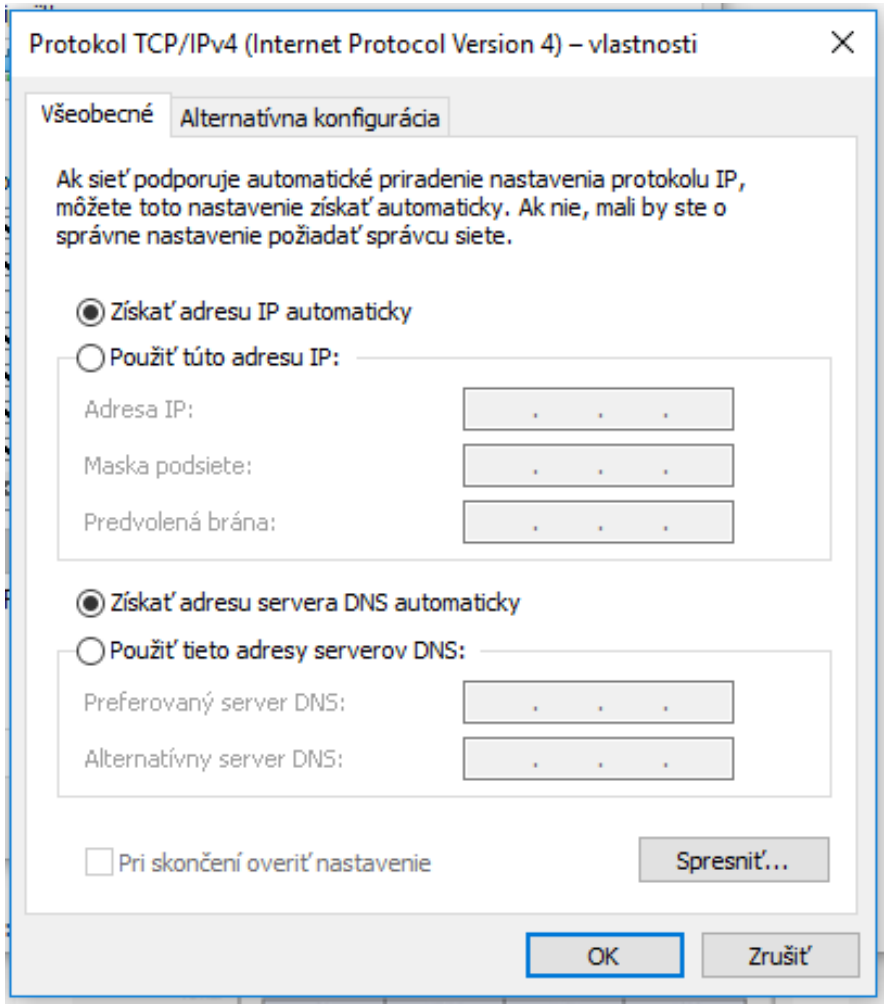
RFC 2131

Dynamická konfigurácia hostov

- Pomocou doplnkovej sieťovej služby
  - Musí byť v sieti nainštalovaná, nakonfigurovaná a spustená
- Historický vývoj:
  - A) Reverse Address Resolution Protocol (**RARP**):
    - Klient/Server dotazovanie, získa len vlastnú adresu; treba nakonfigurovať RARP table
  - B) BOOTstrap Protocol (**BOOTP**):
    - K/S, stanica získa okrem svojej IP adresy aj adresu routra, servera
    - Obmedzený počet konfig. Parametrov (vendor extensions)
    - Používa 2-fázový konfig. Proces
    - klient nerobi rebind/renew konfiguraciu so serverom, okrem restartu
  - C) Dynamic Host Configuration protocol (**DHCP**):
    - K/S, stanici pridelená adresa len kým komunikuje, pri novom prihlásení nová adresa
    - Používa 1-fázový konfig. Proces (negociácia IP aj všetkého ostatného info)
    - Široká množina konfig. Parametrov (options)
    - neptorebuje restart, rebind/renew sa deje automaticky, po istom casovom intervale

Dynamic Host Configuration Protocol

- Klient / Server protokol
- Umožňuje klientom (koncovým staniciam) vyžiadať od DHCP servera konfiguračné parametre
  - Servery a smerovače by mali mať statické IP adresy
    - Vieme prečo?
- Najpoužívanejšie parametre
  - IP adresa, sieťová maska, IP adresa default gateway, IP adresa DNS servera
- **DHCP komponenty**
  - DHCP klient
    - Má ho väčšina moderných OS
  - DHCP Server
  - Relay Agent
    - Prechod DHCP žiadosti cez smerovač



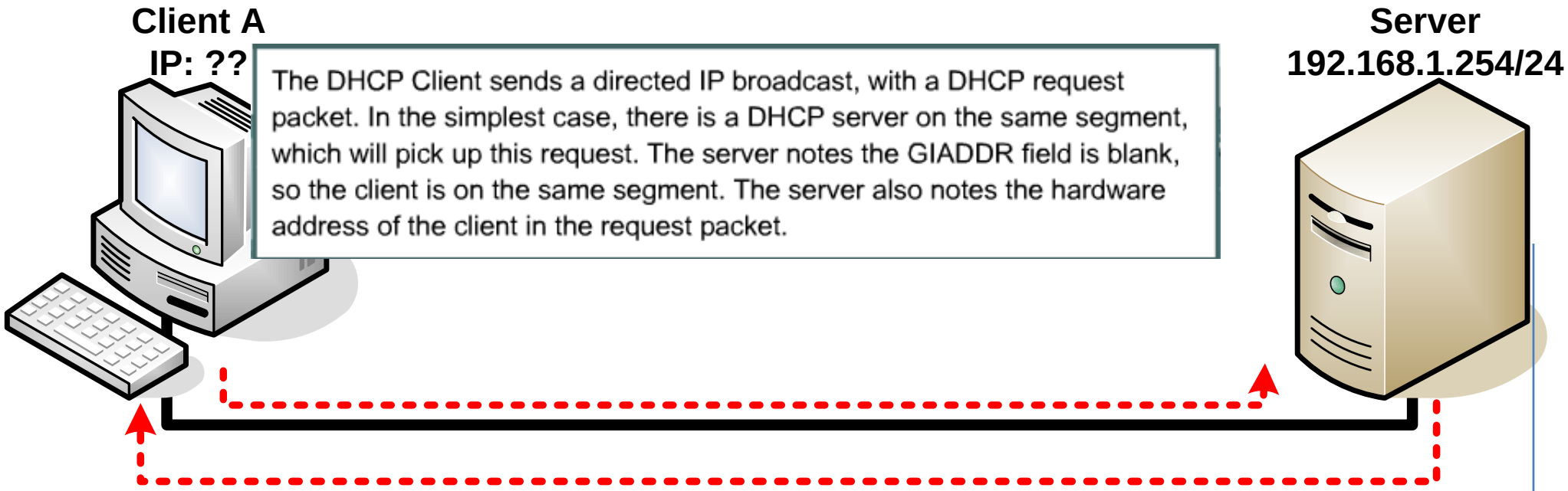
DHCP komponenty

- **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
  - Prideľuje ich na požiadanie DHCP klientom
- **Relay agent**
  - Umožňuje prechod DHCP žiadostí cez L3 zariadenie

Alokácia IP adresy

- **Dynamická** Alokácia
  - Pridelí IP adresu žiadujúcej stanici na špecifikované časové obdobie
  - Potom nastáva uvoľnenie adresy alebo obnovenie prenájmu
- **Automatická** Alokácia
  - DHCP server priradí automaticky stanici permanentnú statickú adresu z rozsahu
- **Manuálna** Alokácia
  - Vyžaduje konfiguráciu DHCP servera
  - Pridelí žiadujúcej stanici vždy rovnakú IP adresu

DHCP činnosť



The DHCP Client sends a directed IP broadcast, with a DHCP request packet. In the simplest case, there is a DHCP server on the same segment, which will pick up this request. The server notes the GIADDR field is blank, so the client is on the same segment. The server also notes the hardware address of the client in the request packet.

Ethernet II Frame	IP	UDP	DHCP Discover
SRC MAC: MAC A DST MAC: FF:FF:FF:FF:FF:FF	SRC IP: ? DST IP: 255.255.255.255	UDP 67	CIADR: ? GIADDR: ? Mask: ? CHADDR: MAC A

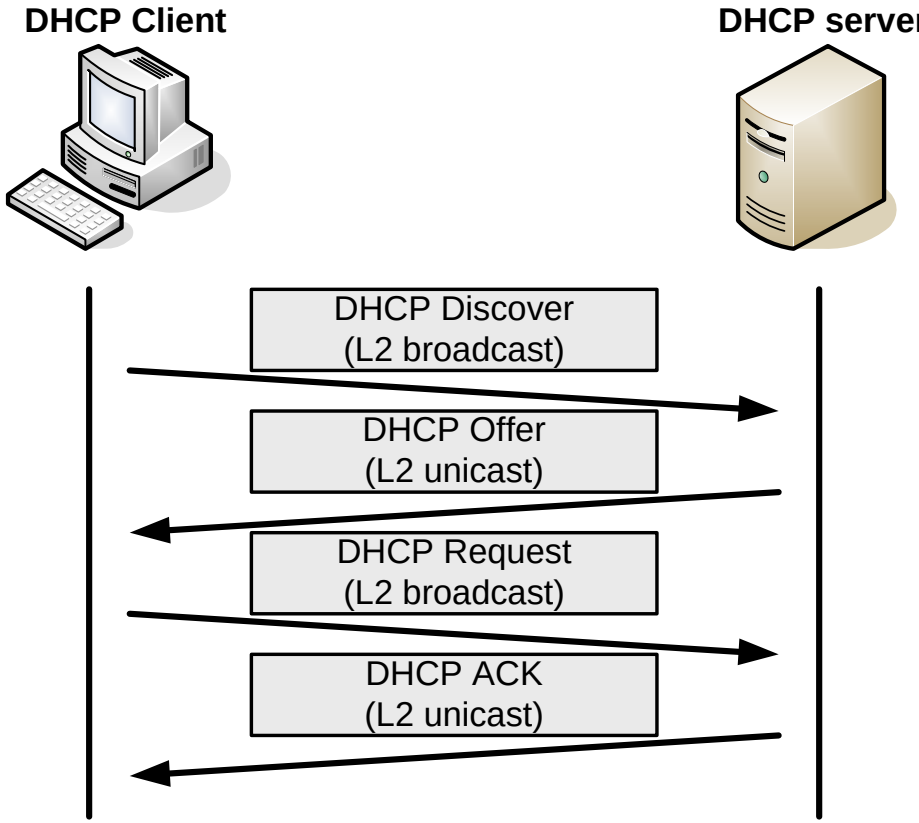
DHCP Offer

SRC MAC: MAC DHCP Serv DST MAC: MAC A	SRC IP: 192.168.1.254 DST IP: 192.168.1.10	UDP 68	CIADR: 192.168.1.10 GIADDR: 192.168.1.1 Mask: 255.255.255.0 CHADDR: MAC A

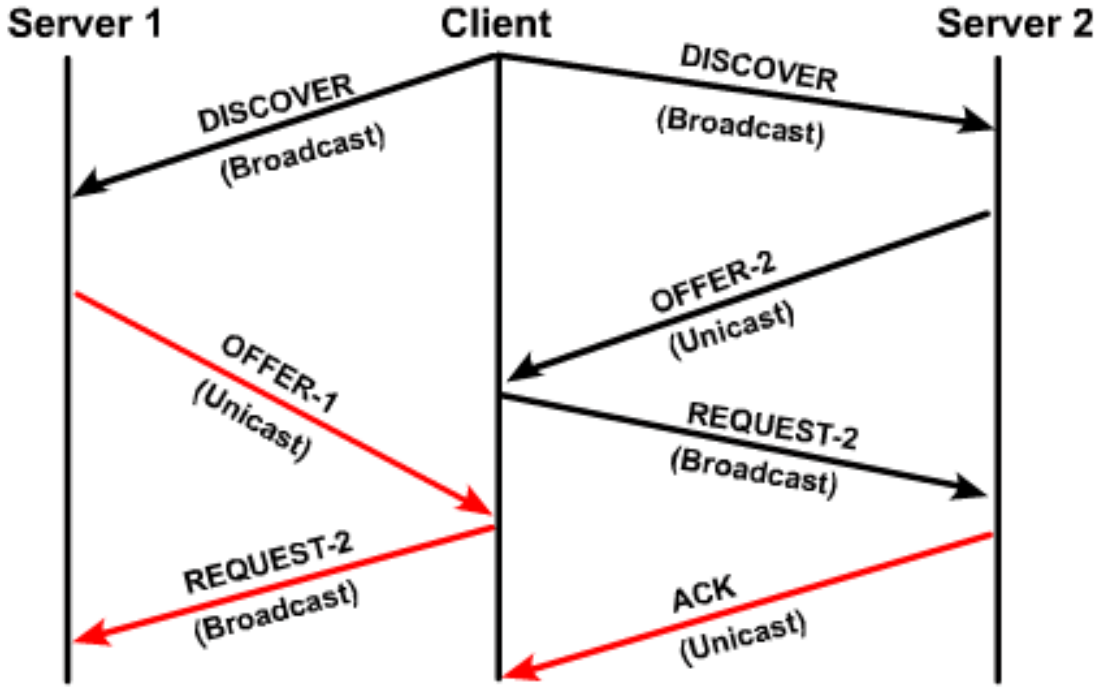
MAC: Media Access Control Address
CIADDR: Client IP Address
GIADDR: Gateway IP Address
CHADDR: Client Harware Address

The DHCP server picks an IP address from the available pool for that segment, as well as the other segment and global parameters. It puts them into the appropriate fields of the DHCP packet. It then uses the hardware address of A (in CHADDR) to construct an appropriate frame to send back to the client.

DHCP činnosť - DORA



- Môže klient dostať viac ponúk?

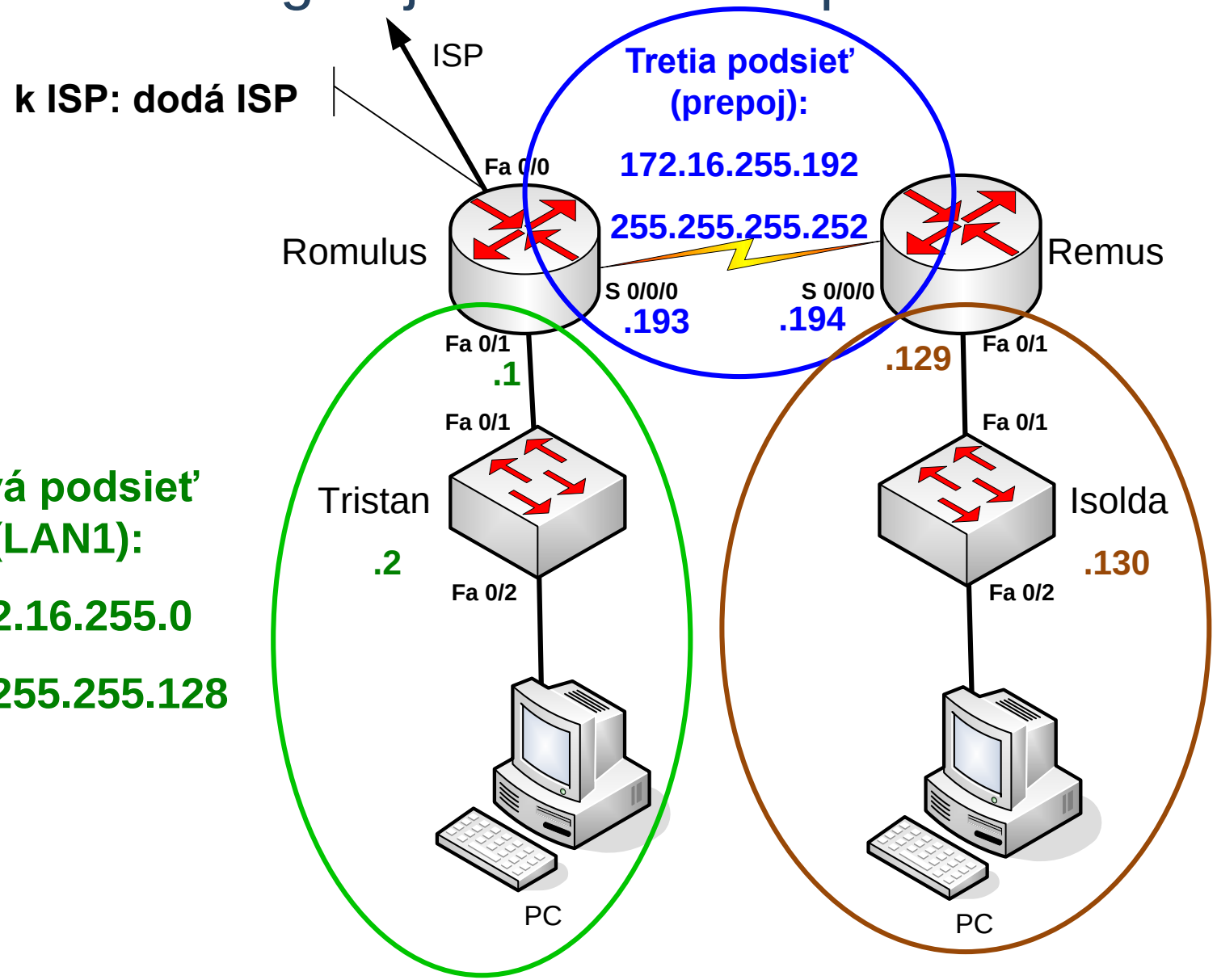


- Discover – niekedy už môže byť s návrhom IP adresy – uvažujme kedy asi?
- Request – uvažujme prečo broadcastom?
- ACK – iba výnimočne server pošle NACK - uvažujme kedy asi?

Konfigurácia DHCP servera na smerovači Cisco

- Konfigurácia DHCP servera sa vykonáva **v GKR**
- Pozostáva z viacerých krokov:
  - **Spustenie** služby a **pomenovanie** konfigurácie
    - Na jednom smerovači môže byť spravovaných viac DHCP rozsahov
  - Nastavenie **parametrov** DHCP služby
    - IP rozsah, z ktorého sa budú prideľovať adresy a sieťové masky
    - Adresa defaultného gateway-a
    - Adresa DNS servera
    - Iných parametrov
      - DHCP parametrov je až okolo 50

Príklad: Nakonfiguruj DHCP server pre LAN1



Prvá podsieť (LAN1):

172.16.255.0

255.255.255.128

Druhá podsieť (LAN2):

172.16.255.128

255.255.255.192

Konfigurácia DHCP servera na smerovači Cisco

```
Romulus(config)#ip dhcp pool Moj_DHCP
```

- Spustenie DHCP služby a pomenovanie adresného rozsahu („pool“)
  - Zmenil sa prompt
  - Som v submóde konfigurácie DHCP služby

```
Romulus(dhcp-config)#network 172.16.255.0 255.255.255.128
Romulus(dhcp-config)#default-router 172.16.255.1
Romulus(dhcp-config)#dns-server 195.146.132.59
Romulus(dhcp-config)#exit
```

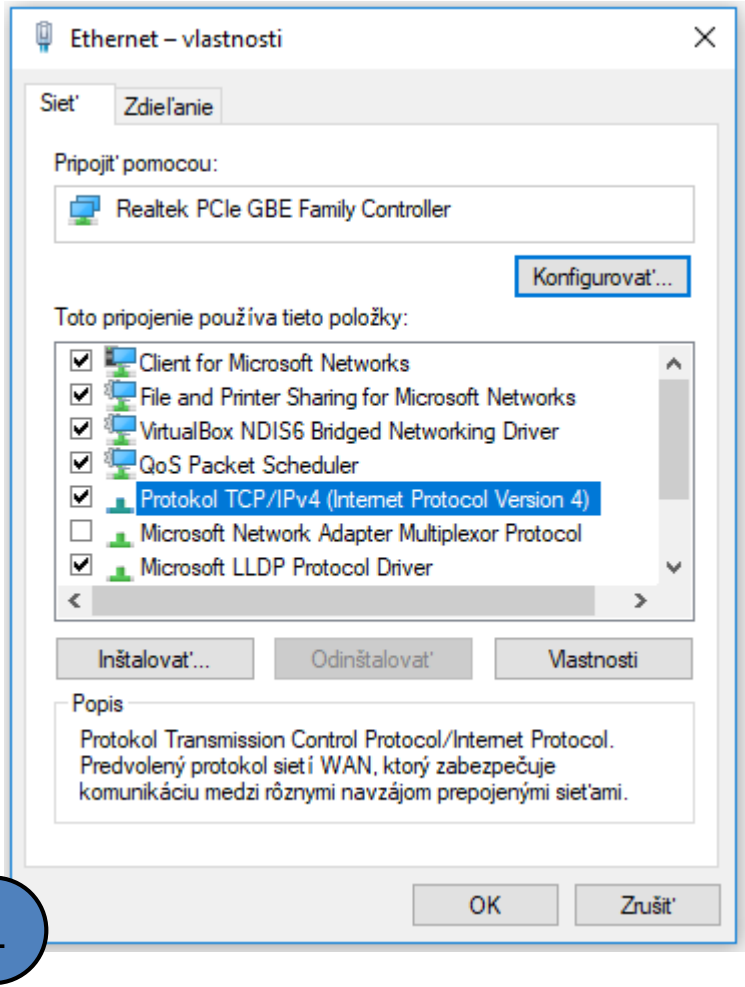
- Nastavenie adresného rozsahu, ktorý bude DHCP služba riadiť pri prideľovaní IP adries
- Nastavenie defaultného gateway-a pre klientov

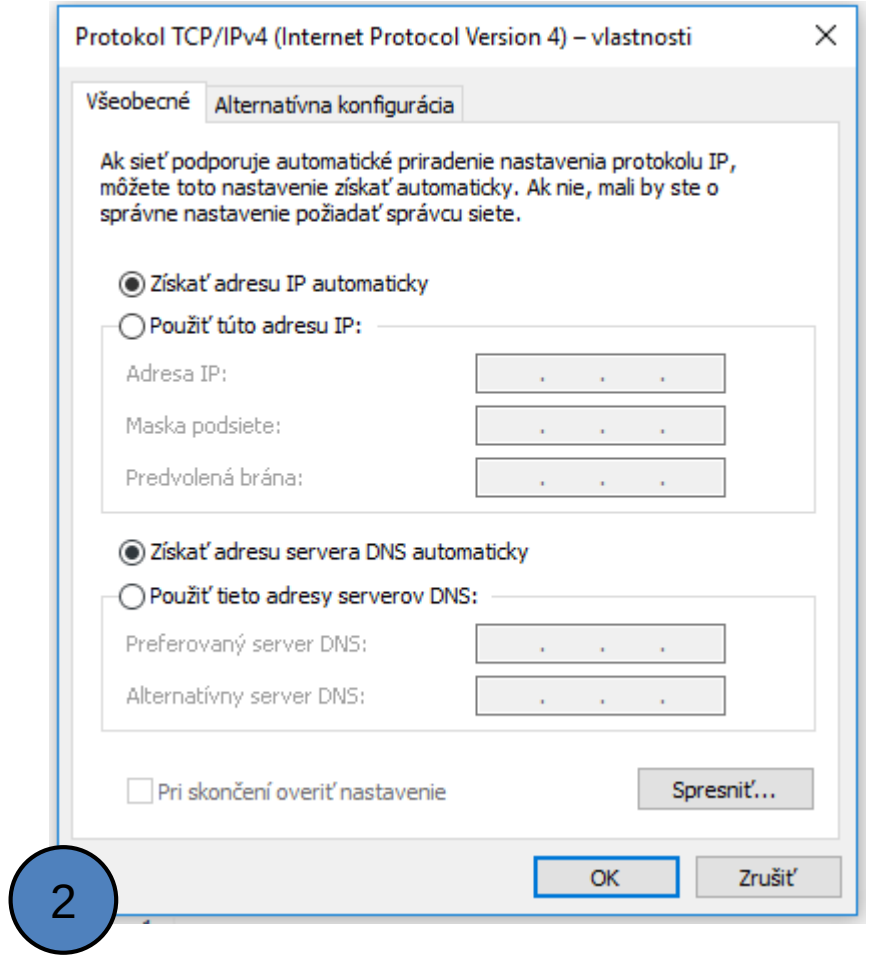
Zoznam iných parametrov

```
Romulus(dhcp-config)#?
DHCP pool configuration commands:
  accounting            Send Accounting Start/Stop messages
  bootfile              Boot file name
  class                 Specify a DHCP class
  client-identifier     Client identifier
  client-name           Client name
  default-router        Default routers
  dns-server            DNS servers
  domain-name           Domain name
  exit                  Exit from DHCP pool configuration mode
  hardware-address      Client hardware address
  host                  Client IP address and mask
  import                Programatically importing DHCP option parameters
  lease                 Address lease time
  netbios-name-server   NetBIOS (WINS) name servers
  netbios-node-type     NetBIOS node type
  network               Network number and mask
  next-server           Next server in boot process
  no                    Negate a command or set its defaults
  option                Raw DHCP options
  origin                Configure the origin of the pool
  relay                 Function as a DHCP relay
--More--
```

Nastavenie DHCP klienta v OS Windows 10

- Start → Control Panel → Network connections → right click on an interface → Choose properties





Ovládanie DHCP klienta

ipconfig

```
C:\Users\janau>ipconfig /?

USAGE:
    ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] |
                                 /showclassid6 adapter |
                                 /setclassid6 adapter [classid] ]

where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
       /release         Release the IPv4 address for the specified adapter.
       /release6        Release the IPv6 address for the specified adapter.
       /renew           Renew the IPv4 address for the specified adapter.
       /renew6          Renew the IPv6 address for the specified adapter.
       /flushdns        Purges the DNS Resolver cache.
       /registerdns     Refreshes all DHCP leases and re-registers DNS names
       /displaydns      Display the contents of the DNS Resolver Cache.
       /showclassid     Displays all the dhcp class IDs allowed for adapter.
       /setclassid      Modifies the dhcp class id.
       /showclassid6    Displays all the IPv6 DHCP class IDs allowed for adapter.
       /setclassid6     Modifies the IPv6 DHCP class id.

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.
```

Overenie získanej IP adresy

ipconfig

```
C:\Users\janau>ipconfig /all

Windows IP Configuration

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 3160
   Physical Address. . . . . . . . . : D0-7E-35-E7-0E-37
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:acad::acad:1(Preferred)
   Link-local IPv6 Address . . . . . : fe80::6ce4:4b68:db81:65ec%8(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.100.6(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, November 10, 2017 8:47:38 AM
   Lease Expires . . . . . . . . . . : Friday, November 17, 2017 3:16:53 AM
   Default Gateway . . . . . . . . . : fe80::1%8
                                       192.168.100.1
   DHCP Server . . . . . . . . . . . : 192.168.100.1
   DHCPv6 IAID . . . . . . . . . . . : 147881525
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-8D-36-AF-F0-76-1C-6C-8A-66
   DNS Servers . . . . . . . . . . . : 192.168.100.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Overenie nastavenia DHCP na smerovači

```
Romulus#sh run
Building configuration...

Current configuration : 859 bytes
!
version 12.4
!
Output omitted
!
!
ip dhcp pool Moj_DHCP
   network 172.16.255.0 255.255.255.128
   default-router 172.16.255.1
   dns-server 195.146.132.59
!
!
Output omitted
!
```

Overenie činnosti DHCP na smerovači

- Výpis zoznamu pridelených IP adries

```
Romulus#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/                  Lease expiration        Type
                    Hardware address/
                    User name
172.16.255.2        0100.1c23.203a.28           Nov 15 2018 09:23 AM    Automatic
```

Vymazanie DHCP štatistík

```
Romulus# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/                  Lease expiration        Type
                    Hardware address/
                    User name
172.16.255.2        0100.1c23.203a.28           Jan 10 2008 09:23 AM    Automatic

Romulus# clear ip dhcp binding
% Incomplete command.

Romulus# clear ip dhcp binding *

Romulus# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/                  Lease expiration        Type
                    Hardware address/
                    User name
```

Vyňatie určitého rozsahu IP adries z DHCP rozsahu

- Konfiguruje sa v GKR móde
- Využitie ak chcem vyčleniť z adresného priestoru DHCP servera časť adries ktoré sa nebudú dynamicky prideľovať
  - Napr. prvých 50 adries

```
Romulus#configure terminal
Romulus(config)#ip dhcp excluded-address 172.16.255.1 172.16.255.50
Romulus(config)#
```

Od: Dolná IP addresa

Do: Horná IP addresa

Uvoľnenie (release) a vyžiadanie novej IP adresy

```
C:\Users\janau>ipconfig /release

Windows IP Configuration

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::dc70:91f4:262f:5e94%4
   Default Gateway . . . . . . . . . : fe80::1%4

C:\Users\Janka>ipconfig /renew

Windows IP Configuration

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::dc70:91f4:262f:5e94%4
   IPv4 Address. . . . . . . . . . . : 192.168.100.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%4
                                       192.168.100.1
```

Diagnostika DHCP

```
Romulus# debug ip dhcp server events
Romulus#
```

```
*Jan  9 10:02:16.063: DHCPD: Sending notification of DISCOVER:
*Jan  9 10:02:16.063:   DHCPD: htype 1 chaddr 001c.2320.3a28
*Jan  9 10:02:16.063:   DHCPD: remote id 020a0000ac10ff0101000000
*Jan  9 10:02:16.063:   DHCPD: circuit id 00000000
*Jan  9 10:02:16.063: DHCPD: Seeing if there is an internally
specified pool class:
*Jan  9 10:02:16.063:   DHCPD: htype 1 chaddr 001c.2320.3a28
*Jan  9 10:02:16.063:   DHCPD: remote id 020a0000ac10ff0101000000
*Jan  9 10:02:16.063:   DHCPD: circuit id 00000000
*Jan  9 10:02:18.063: DHCPD: client requests 172.16.255.51.
*Jan  9 10:02:18.063: DHCPD: Adding binding to radix tree
(172.16.255.51)
*Jan  9 10:02:18.063: DHCPD: Adding binding to hash tree
*Jan  9 10:02:18.063: DHCPD: assigned IP address 172.16.255.51 to
client 0100.1c23.203a.28.
...
Output omitted
```

Štatistiky

```
Remulus# sh ip dhcp server statistics

Memory usage              23340
Address pools             1
Database agents           0
Automatic bindings        1
Manual bindings           0
Expired bindings          0
Malformed messages        0
Secure arp entries        0

Message                   Received
BOOTREQUEST               0
DHCPDISCOVER              1
DHCPREQUEST               2
DHCPDECLINE               0
DHCPRELEASE               0
DHCPINFORM                0

Message                   Sent
BOOTREPLY                 0
DHCPOFFER                 1
DHCPACK                   2
DHCPNAK                   0
```

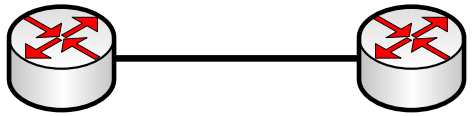
Stav adresného rozsahu

```
Remulus# sh ip dhcp pool

Pool Moj_DHCP :
 Utilization mark (high/low)          : 100 / 0
 Subnet size (first/next)             : 0 / 0
 Total addresses                      : 126
 Leased addresses                     : 1
 Pending event                        : none
 1 subnet is currently in the pool    :

 Current index        IP address range                        Leased addresses
 172.16.255.3         172.16.255.1     - 172.16.255.126       1
```

Konfigurácia dynamickej adresy na smerovači



Remulus
(DHCP client)

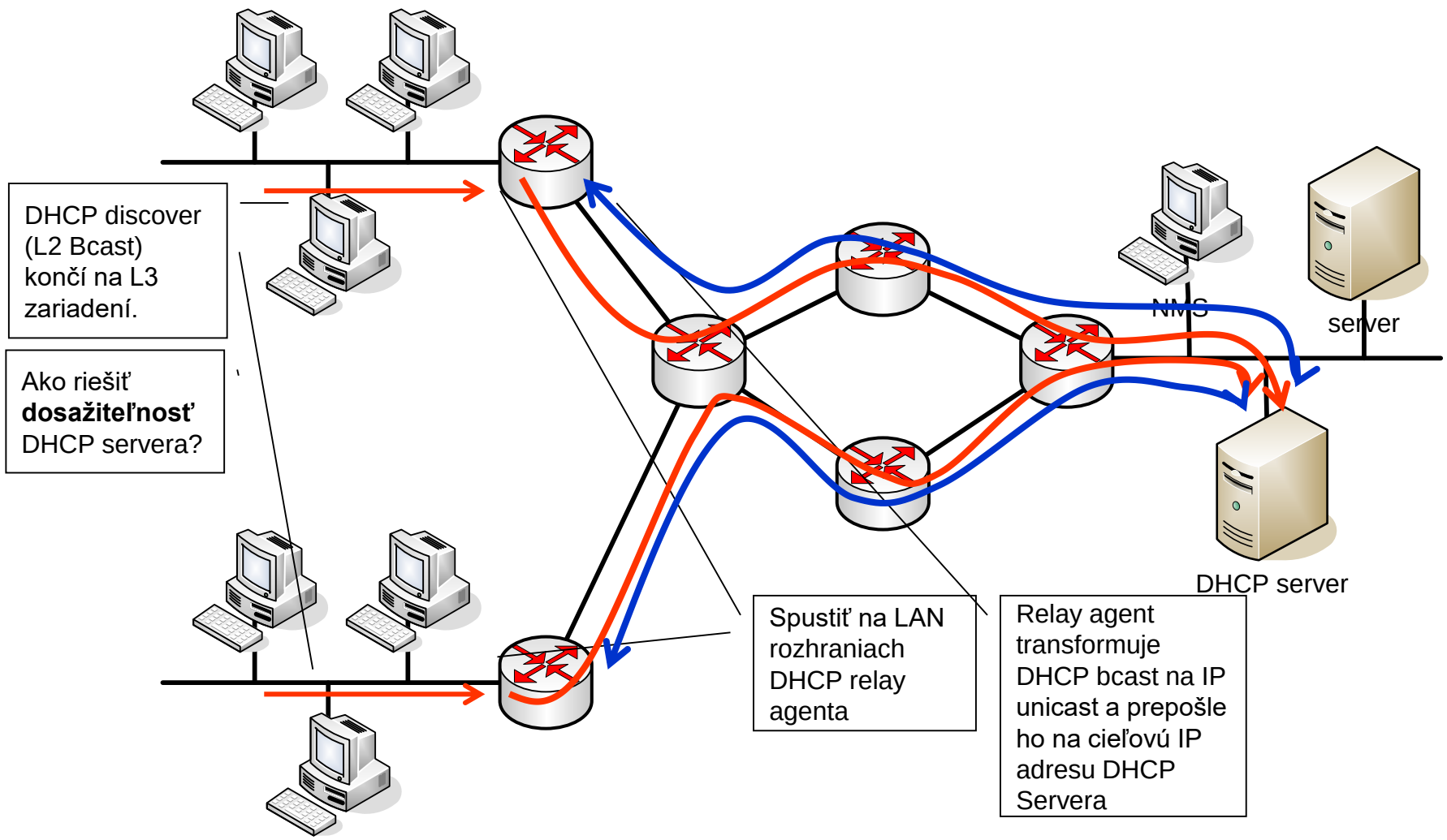
ISP
(DHCP server)

```
ISP#sh run
…
ip dhcp pool DHCP_client
   network 192.168.10.0 /24
   default-router 192.168.10.1
```

```
Remulus(config)#int fa 0/0
Remulus(config-if)#ip address dhcp
Remulus(config-if)#^Z
Remulus#
*Mar  1 00:06:46.927: %SYS-5-CONFIG_I: Configured from console by console
*Mar  1 00:06:57.379: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned
 DHCP address 192.168.10.2, mask 255.255.255.0, hostname Remulus
```

```
Remulus#sh ip int fa 0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.2/24
  Broadcast address is 255.255.255.255
  Address determined by DHCP
```

Relay Agent


DHCP discover (L2 Bcast) končí na L3 zariadení.
Ako riešiť **dosažiteľnosť** DHCP servera?
NMS
server
DHCP server
Spustiť na LAN rozhraniach DHCP relay agenta
Relay agent transformuje DHCP bcast na IP unicast a prepošle ho na cieľovú IP adresu DHCP Servera

Spustenie DHCP relay

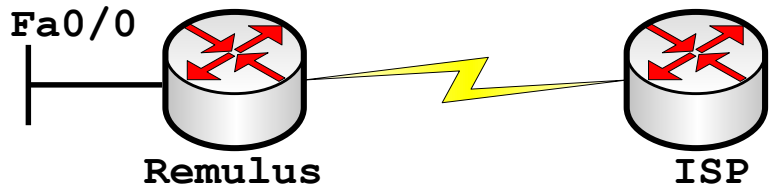
```
Remulus(config-if)# ip helper-address IP_ADRESA
```

- Preposiela nasledujúce UDP služby:
  - Port 37: Time
  - Port 49: TACACS
  - Port 53: DNS
  - Port 67: DHCP/BOOTP server
  - Port 68: DHCP/BOOTP client
  - Port 69: TFTP
  - Port 137: NetBIOS name service
  - Port 138: NetBIOS datagram service
- Špecifikácia ďalších cez:
  - ip forward-protocol

Konfigurácia IP DHCP relay

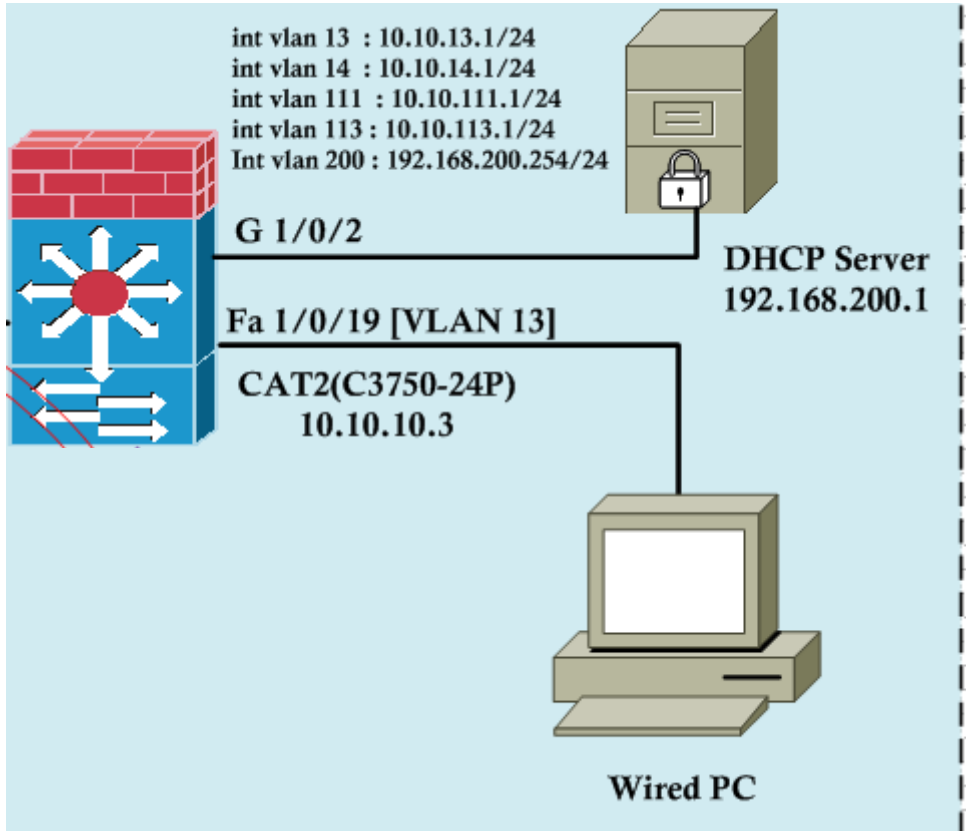
```
ISP#sh run
…
ip dhcp pool LAN_Remus
   network 172.16.255.0 255.255.255.0
   default-router 172.16.255.1
…
```

```
Remulus(config)#int fa 0/0
Remulus(config-if)# ip helper-address 192.168.1.1
Remulus#sh run int fa 0/0
!
interface FastEthernet0/0
 ip address 172.16.255.1 255.255.255.0
 ip helper-address 192.168.1.1
 duplex auto
 speed auto
```




```
Remulus#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/                Lease expiration        Type
                    Hardware address/
                    User name
172.16.255.2        0102.004c.4f4f.50         Mar 02 2002 12:07 AM    Automatic
```

DORA – pohľad na proces z Wiresharku (Relay agent)



No.	Time	Source	Destination	Protocol	Length	RSSI	Info
90	10:13:16.530908	0.0.0.0	255.255.255.255	DHCP	342		DHCP Discover - Transaction ID 0x9f2f9e60
91	10:13:16.535700	10.10.13.3	255.255.255.255	DHCP	342		DHCP Offer - Transaction ID 0x9f2f9e60
92	10:13:16.536504	0.0.0.0	255.255.255.255	DHCP	363		DHCP Request - Transaction ID 0x9f2f9e60
93	10:13:16.540109	10.10.13.3	255.255.255.255	DHCP	342		DHCP ACK - Transaction ID 0x9f2f9e60
94	10:13:16.612576	Dell_65:8f:37	Broadcast	ARP	42		Who has 10.10.13.1? Tell 10.10.13.11
95	10:13:16.617046	All-HSRP-router	Dell_65:8f:37	ARP	60		10.10.13.1 is at 00:00:0c:07:ac:01

Wireshark: DHCP Discover

```
⊞ Frame 19: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
⊟ Ethernet II, Src: Dell_65:8f:37 (5c:26:0a:65:8f:37), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Source: Dell_65:8f:37 (5c:26:0a:65:8f:37)
    Type: IP (0x0800)
⊞ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊟ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
    Source port: bootpc (68)
    Destination port: bootps (67)
    Length: 308
  ⊞ Checksum: 0x0145 [validation disabled]
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x08c0659a
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x8000 (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Dell_65:8f:37 (5c:26:0a:65:8f:37)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Discover
  ⊞ Option: (t=61,l=7) Client identifier
  ⊞ Option: (t=12,l=7) Host Name = "8DWP2Q1"
  ⊞ Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
  ⊞ Option: (t=55,l=12) Parameter Request List
```

Wireshark: DHCP Offer

```
⊞ Frame 20: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
⊟ Ethernet II, Src: Cisco_a7:ff:48 (00:1a:e3:a7:ff:48), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Source: Cisco_a7:ff:48 (00:1a:e3:a7:ff:48)
    Type: IP (0x0800)
⊞ Internet Protocol Version 4, Src: 10.10.13.3 (10.10.13.3), Dst: 255.255.255.255 (255.255.255.255)
⊟ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
    Source port: bootps (67)
    Destination port: bootpc (68)
    Length: 308
  ⊞ Checksum: 0x2a36 [validation disabled]
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x08c0659a
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x8000 (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 10.10.13.10 (10.10.13.10)
    Next server IP address: 192.168.200.1 (192.168.200.1)
    Relay agent IP address: 10.10.13.3 (10.10.13.3)
    Client MAC address: Dell_65:8f:37 (5c:26:0a:65:8f:37)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Offer
  ⊞ Option: (t=1,l=4) Subnet Mask = 255.255.255.0
  ⊞ Option: (t=58,l=4) Renewal Time Value = 12 hours
  ⊞ Option: (t=59,l=4) Rebinding Time Value = 21 hours
  ⊞ Option: (t=51,l=4) IP Address Lease Time = 1 day
  ⊞ Option: (t=54,l=4) DHCP Server Identifier = 192.168.200.1
  ⊞ Option: (t=15,l=8) Domain Name = "mrn.com"
  ⊞ Option: (t=3,l=4) Router = 10.10.13.1
  ⊞ Option: (t=6,l=4) Domain Name Server = 192.168.200.1
```

Wireshark: DHCP Request

```
⊞ Frame 21: 363 bytes on wire (2904 bits), 363 bytes captured (2904 bits)
⊟ Ethernet II, Src: Dell_65:8f:37 (5c:26:0a:65:8f:37), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Source: Dell_65:8f:37 (5c:26:0a:65:8f:37)
    Type: IP (0x0800)
⊞ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊟ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
    Source port: bootpc (68)
    Destination port: bootps (67)
    Length: 329
  ⊞ Checksum: 0x015a [validation disabled]
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x08c0659a
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x8000 (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Dell_65:8f:37 (5c:26:0a:65:8f:37)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Request
  ⊞ Option: (t=61,l=7) Client identifier
  ⊞ Option: (t=50,l=4) Requested IP Address = 10.10.13.10
  ⊞ Option: (t=54,l=4) DHCP Server Identifier = 192.168.200.1
  ⊞ Option: (t=12,l=7) Host Name = "8DWP2Q1"
  ⊞ Option: (t=81,l=21) Client Fully Qualified Domain Name
  ⊞ Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
  ⊞ Option: (t=55,l=12) Parameter Request List
```

Wireshark: DHCP Ack

```
⊞ Frame 22: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
⊟ Ethernet II, Src: Cisco_a7:ff:48 (00:1a:e3:a7:ff:48), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Source: Cisco_a7:ff:48 (00:1a:e3:a7:ff:48)
    Type: IP (0x0800)
⊞ Internet Protocol Version 4, Src: 10.10.13.3 (10.10.13.3), Dst: 255.255.255.255 (255.255.255.255)
⊟ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
    Source port: bootps (67)
    Destination port: bootpc (68)
    Length: 308
  ⊞ Checksum: 0xafe0 [validation disabled]
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x08c0659a
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x8000 (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 10.10.13.10 (10.10.13.10)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 10.10.13.3 (10.10.13.3)
    Client MAC address: Dell_65:8f:37 (5c:26:0a:65:8f:37)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP ACK
  ⊞ Option: (t=58,l=4) Renewal Time Value = 12 hours
  ⊞ Option: (t=59,l=4) Rebinding Time Value = 21 hours
  ⊞ Option: (t=51,l=4) IP Address Lease Time = 1 day
  ⊞ Option: (t=54,l=4) DHCP Server Identifier = 192.168.200.1
  ⊞ Option: (t=1,l=4) Subnet Mask = 255.255.255.0
  ⊞ Option: (t=15,l=8) Domain Name = "mrn.com"
  ⊞ Option: (t=3,l=4) Router = 10.10.13.1
  ⊞ Option: (t=6,l=4) Domain Name Server = 192.168.200.1
```

Overenie činnosti DHCP

- Zisti či nie je vypnutá DHCP služba
  - Hľadaj v running no service dhcp
- Zisti či nie je IP adresný konflikt
  - `sh ip dhcp conflict`
- Overenie fyzickej topológie
  - Či mám priamo dostupný DHCP server
    - Ak je v inej LAN or VLAN: `ip helper-address`
- Testnutie konektivity
  - pridelením statickej adresy a ping
- Zistiť či DHCP prideľuje IP adresu zo správneho rozsahu

Overenie či server prijíma DHCP

```
Remulus#debug ip packet detail
Remulus#undebug all
! Dost obsiahle vypisy, ako to sprehladnit?
```

Overenie či server prijíma DHCP

```
Remulus#debug ip packet detail
Remulus#undebug all
! Dost obsiahle vypisy, ako to sprehladnit?
! Zadefinujeme ACL, ktore bude filtrovat vystup co nas zaujima
Remulus#conf t
Remulus(config)#access-list 100 permit ip host 0.0.0.0 host 255.255.255.255
Remulus(config)#exit
Remulus#debug ip packet detail 100
*Mar  1 00:01:54.623: %SYS-5-CONFIG_I: Configured from console by consoleIP packet
debugging is on (detailed) for access list 100
*Mar  1 00:02:47.795: IP: s=0.0.0.0 (FastEthernet0/0), d=255.255.255.255, len 32 8, rcvd 2
*Mar  1 00:02:47.799:     UDP src=68, dst=67
*Mar  1 00:02:49.863: IP: s=0.0.0.0 (FastEthernet0/0), d=255.255.255.255, len 35 3, rcvd 2
*Mar  1 00:02:49.867:     UDP src=68, dst=67
```

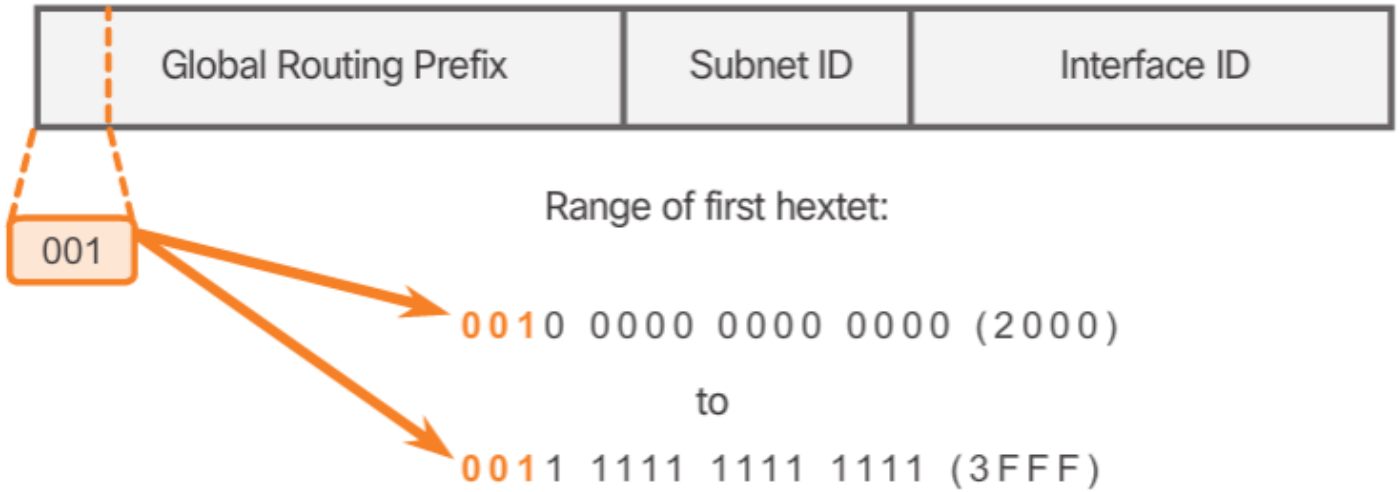
Overenie či server prijíma DHCP

```
Remulus#debug ip dhcp server events
*Mar  1 00:04:22.823: DHCPD: Sending notification of DISCOVER:
*Mar  1 00:04:22.827:   DHCPD: htype 1 chaddr 0200.4c4f.4f50
*Mar  1 00:04:22.827:   DHCPD: remote id 020a0000ac10ff0100000000
*Mar  1 00:04:22.827:   DHCPD: circuit id 00000000
*Mar  1 00:04:22.831: DHCPD: Seeing if there is an internally specified pool class:
*Mar  1 00:04:22.831:   DHCPD: htype 1 chaddr 0200.4c4f.4f50
*Mar  1 00:04:22.835:   DHCPD: remote id 020a0000ac10ff0100000000
*Mar  1 00:04:22.835:   DHCPD: circuit id 00000000
*Mar  1 00:04:24.839: DHCPD: client requests 172.16.255.2.
*Mar  1 00:04:24.839: DHCPD: Adding binding to radix tree (172.16.255.2)
*Mar  1 00:04:24.843: DHCPD: Adding binding to hash tree
*Mar  1 00:04:24.843: DHCPD: assigned IP address 172.16.255.2 to client 0102.004c.4f4f.50.
*Mar  1 00:04:24.863: DHCPD: Sending notification of ASSIGNMENT:
*Mar  1 00:04:24.867:  DHCPD: address 172.16.255.2 mask 255.255.255.0
*Mar  1 00:04:24.867:   DHCPD: htype 1 chaddr 0200.4c4f.4f50
*Mar  1 00:04:24.871:   DHCPD: lease time remaining (secs) = 86400
*Mar  1 00:04:26.907: DHCPD: checking for expired leases.
```

Dynamic Host Configuration Protocol DHCPv6

Unicastové IPv6 adresy

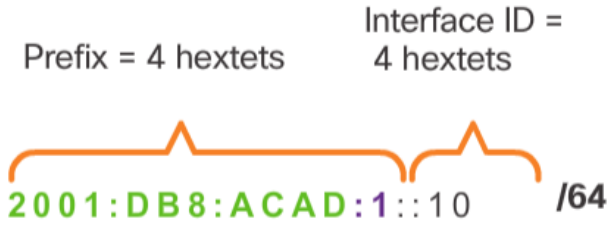
- Musí byť jedninečná v celom Internete (podobne ako verejná adresa v IPv4)
- Je smerovateľná v internete



- Aktuálne sa predeľujú iba rozsahy **2000**::/3
  - t.j. iba 1/8 celého IPv6 priestoru adries
  - na 3 bitoch = 2^3 možností, ale prideľuje sa iba 1 možnosť z nich (001), preto:
  - prvý hextet je v rozsahu od 2000 po 3FFF
  - 2001:0DB8::/32 je vyhradená adresa pre dokumentačné účely

Ako ju čítať a intrepretovať

- **Interface ID** - podobne ako „host portion“ v IPv4, ale volá sa inak, lebo v IPv6 1 host môže mať **viac** IPv6 adries pre každé svoje rozhranie



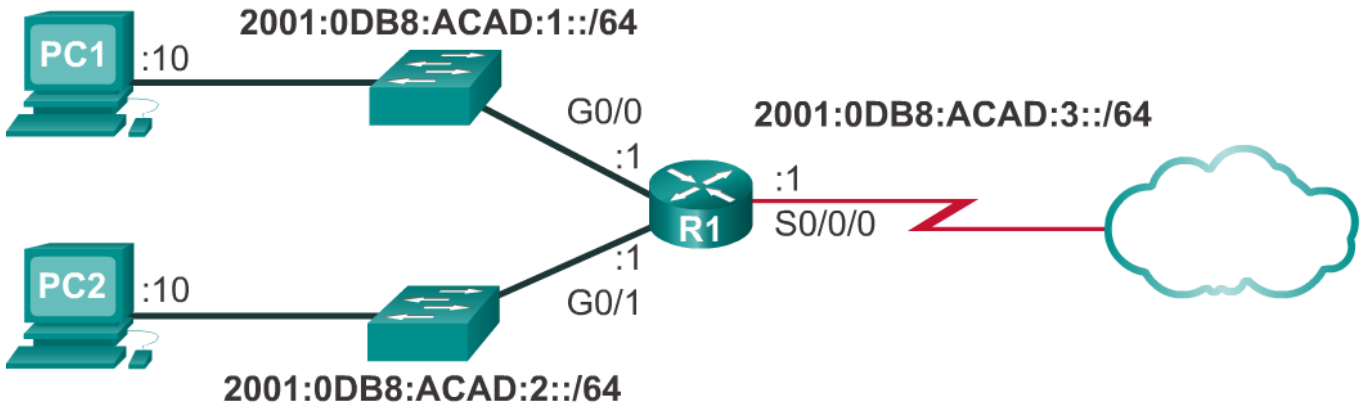
Global Routing Prefix = 2001:0DB8:ACAD

Subnet ID = 0001

Interface ID = 0000:0000:0000:0010

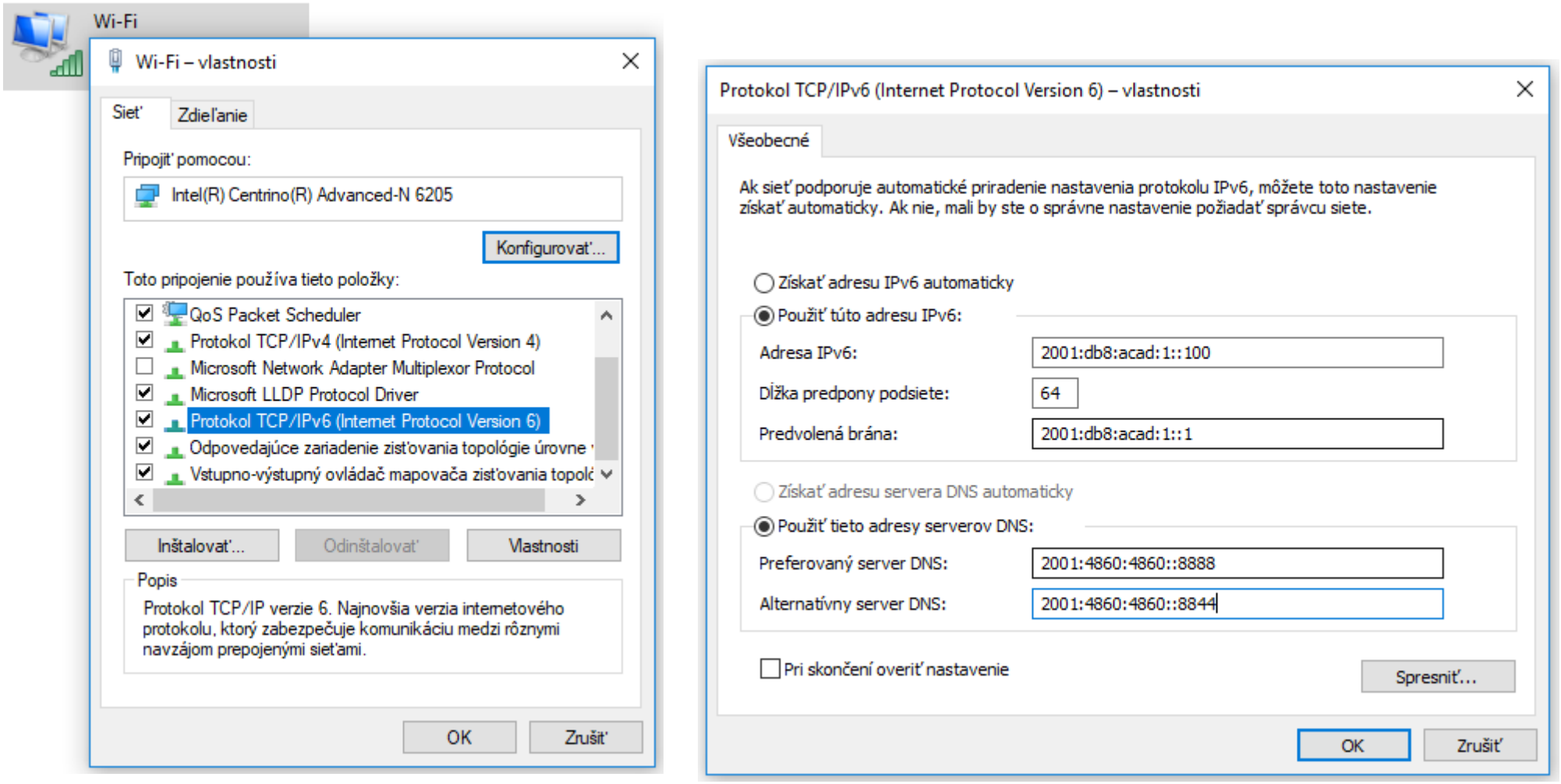
- To čo v IPv4 boli vyhradené adresy vrámci nejakého subnetu (adresa siete a broadcast), už v IPv6 nie sú vyhradené:
  - **Samé 1tky** – možno použiť, lebo v IPv6 nemáme broadcast, ale.. vrchných 128 adries je **rezervovaných** pre adresy: „**Subnet anycast**“)
    - **2001:DB8:ACAD:1::**
      od **FFFF:FFFF:FFFF:FF00**
      do **FFFF:FFFF:FFFF:FFFF**
    - Aktuálne sa využíva iba jedna ....**FE**, pre Mobile IPv6 Home-Agents anycast
  - **Samé 0** – možno použiť, ale... je to **rezervované** pre anycastovú adresu „**Subnet-Router**“, takže sa prideľuje iba smerovačom
    - **2001:DB8:ACAD:1**::

Statická konfigurácia na smerovači




```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address 2001:db8:acad:2::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address 2001:db8:acad:3::1/64
R1(config-if)#clock rate 56000
R1(config-if)#no shutdown
```

Statická konfigurácia na počítači



- Rovnako by to fungovalo, keby sme použili link-local adresu pre GW

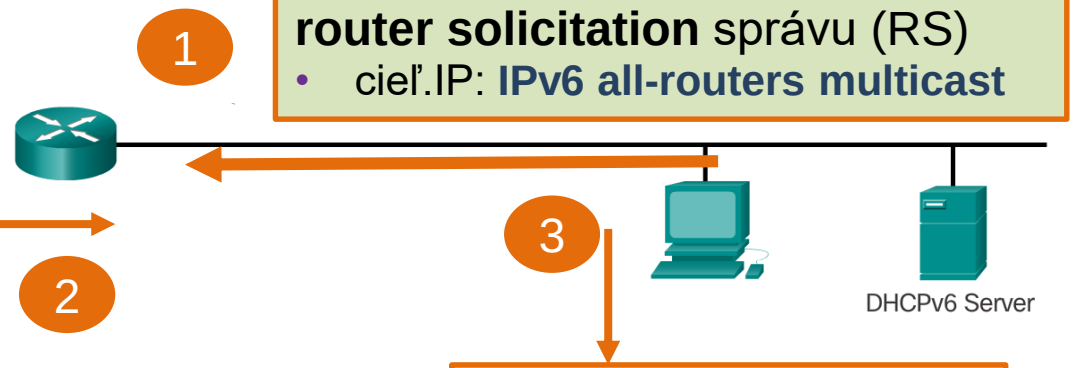
Global Unicast - Dynamická konfigurácia IPv6 adresy

Smerovač posiela rozhraním informácie všetkým IPv6 uzlom na sieti ICMPv6 - tzv. **router advertisement** správy (RA)

- Pravidelne každých 200 s
- Aj ako odpoveď na RS správu
- Aké presne info záleží na danej voľbe v RA (Option 1,2,3)
- cieľ.IP: **IPv6 all-nodes multicast**

Host pošle žiadosť o svoje adresné informácie všetkým IPv6 smerovačom – ICMPv6 tzv. **router solicitation** správu (RS)

- cieľ.IP: **IPv6 all-routers multicast**



Host si pozrie zdrojovú adresu IPv6 paketu, v ktorom prišla zabalená RA správa od routra, a nastaví si na túto (zväčša link-local adresa) ako default gateway vo svojich nastaveniach

Správa router advertisement má tieto možnosti (options):

1. **SLAAC** = Stateless address autoconfiguration
   - RA: Poskytnem ti všetko čo potrebuješ (Prefix, Prefix-length, DNS)
2. **SLAAC + DHCPv6** (stateless)
   - RA: Poskytnem ti niečo (Prefix, Prefix-length), ale pre zvyšné info požiadaj DHCPv6 (DNS)
3. **DHCPv6** (stateful)
   - RA: Neviem ti pomôcť, požiadaj DHCPv6 server o info

Toto sa deje vždy bez ohľadu na option v RA {1, 2, 3}

Global unicast – pripomienka

1. option: SLAAC = Stateless address autoconfiguration

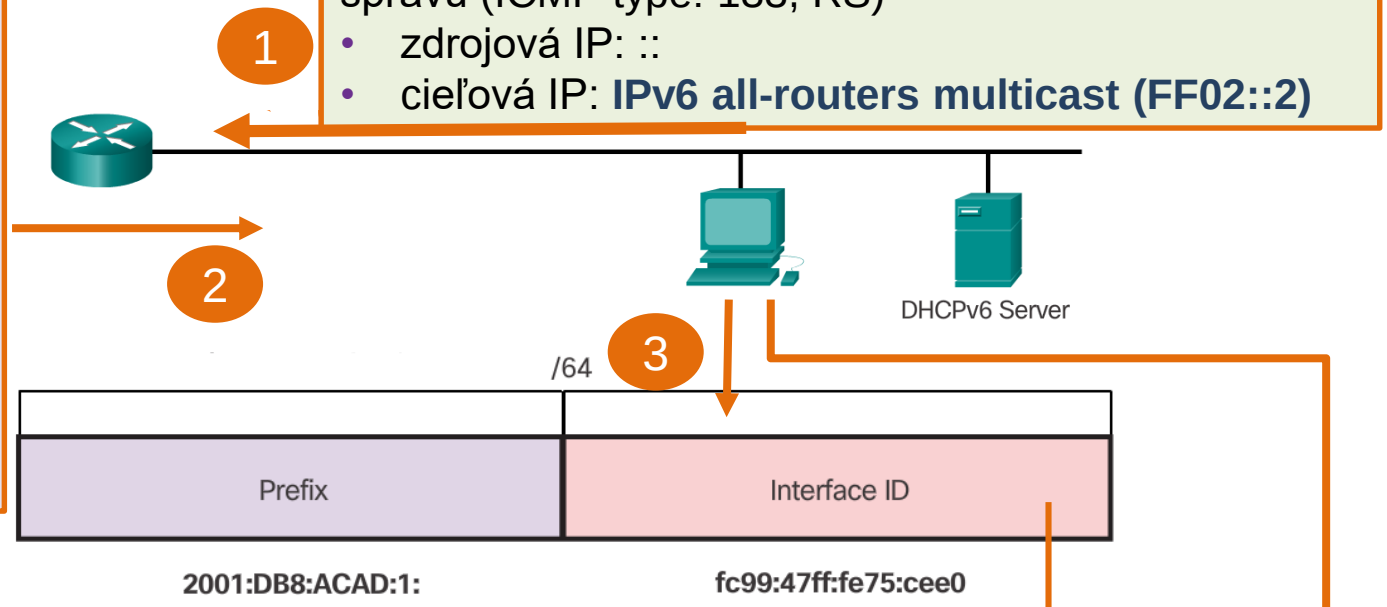
Dynamická konfigurácia

Smerovač pošle rozhraním informácie v správe **RA** s **option 1**:

- **Network prefix** a **prefix length** – do ktorej subsiete patrí host
- **DNS adresy**, doménové meno
- **Default gateway** (IPv6 link-local adresa smerovača) – nie je ako položka v RA, je iba ako zdrojová adresa v hlavičke paketu nesúcom správu RA
- **Lifetime, ...**
- zdroj.IP: R1 link-local adresa
- cieľ.IP: **IPv6 all-nodes multicast (FF02::1)**

Host pošle žiadosť o svoje adresné informácie všetkým IPv6 smerovačom - tzv. **router solicitation** správu (ICMP type: 133, RS)

- zdrojová IP: ::
- cieľová IP: **IPv6 all-routers multicast (FF02::2)**



Host si dokáže sám prideliť adresu tak, že k prefixu siete, ktorý prijal od routra v RA správe, pripojí svoj 64-bitový Interface ID, ktoré môže získať 2 spôsobmi:

- **Modified EUI-64** = modified extended universal identifier (napr. Cisco zariadenia)
- **Náhodné 64bitové číslo** (napr. Windows preferuje tento spôsob) RFC 3041

Výsledok je 128-bitová adresa, ktorá je použiteľná a garantovane globálne unikátna

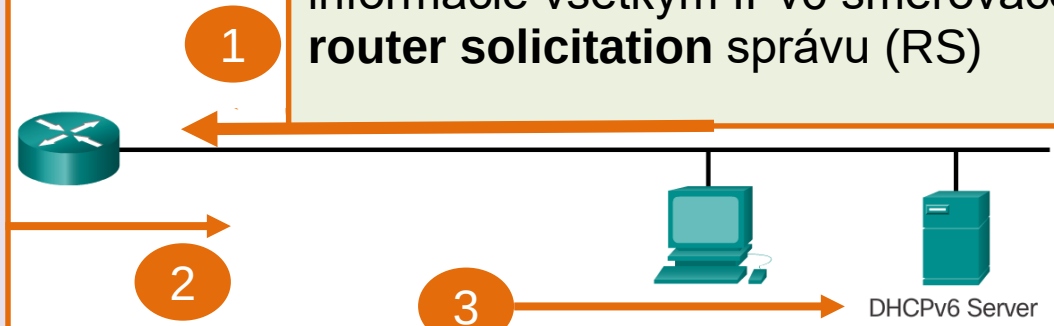
DAD = duplicate address detection: „Nemá náhodou už niekto túto IPv6 adresu?“

- cieľ.IP: **IPv6 solicited-node multicast**

2. option: SLAAC + DHCPv6 - Dynamická konfigurácia

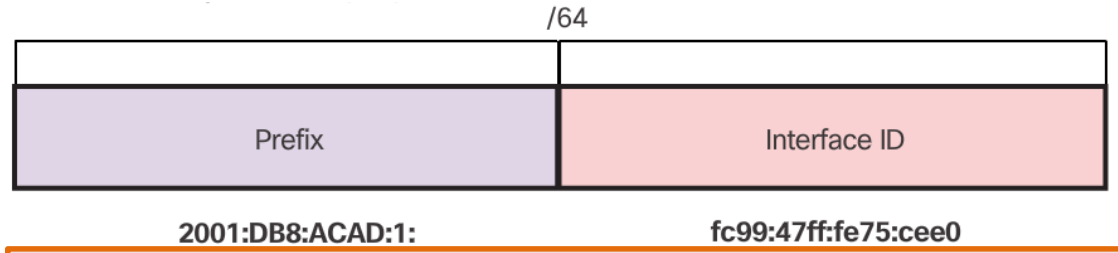
Smerovač pošle rozhraním informácie v správe **RA** s **option 2**:

- **Network prefix** a **prefix length** – do ktorej subsiete patrí host
- **Default gateway** (IPv6 link-local) – nie je ako položka v RA, je iba ako zdrojová adresa v hlavičke paketu nesúcom správu RA
- Neposiela DNS (treba požiadať DHCPv6 server)



Host pošle žiadosť o svoje adresné informácie všetkým IPv6 smerovačom - tzv. **router solicitation** správu (RS)

Host požiada DHCPv6 server o zvyšné info (DNS, doménové mená) – tzv. **DHCPv6 solicitation** správa s **option 2**



Host si sám pridelí adresu (prefix z RA od smerovača + interface ID), interfaced ID môže získať:

- **Modified EUI-64** = modified extended universal identifier (napr. Cisco zariadenia)
- **Náhodné 64bitové číslo** (napr. Windows preferuje tento spôsob) RFC 3041

Výsledok je 128-bitová adresa, ktorá je použiteľná a garantovane globálne unikátna

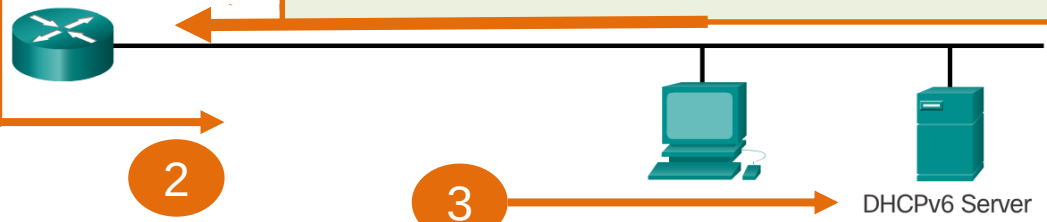
3. option: DHCPv6 - Dynamická konfigurácia

Host pošle žiadosť o svoje adresné informácie všetkým IPv6 smerovačom - tzv. **router solicitation** správu (RS)

1

Smerovač nepošle rozhraním žiadne užitočné info v správe **RA** s **option 3**, iba odkáže hosta na DHCPv6.

2

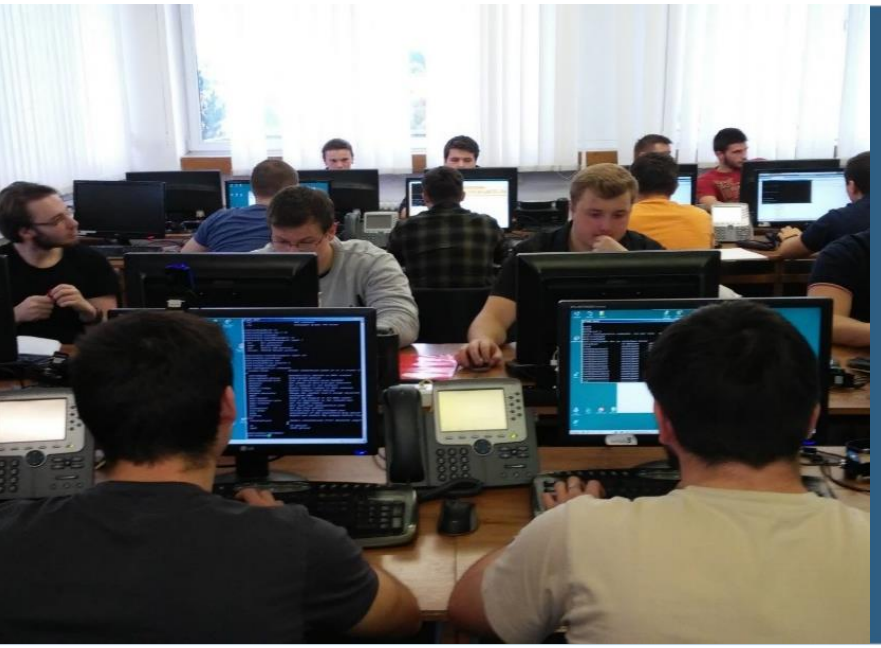


3

Host požiada DHCPv6 server o adresné info – tzv. **DHCPv6 solicitation** správa s option 3

Host si nastaví **default GW** podľa zdrojovej adresy z IPv6 paketu, ktorý mu prišiel od smerovača, a ktorý niesol ICMPv6 RA správu s option 3.

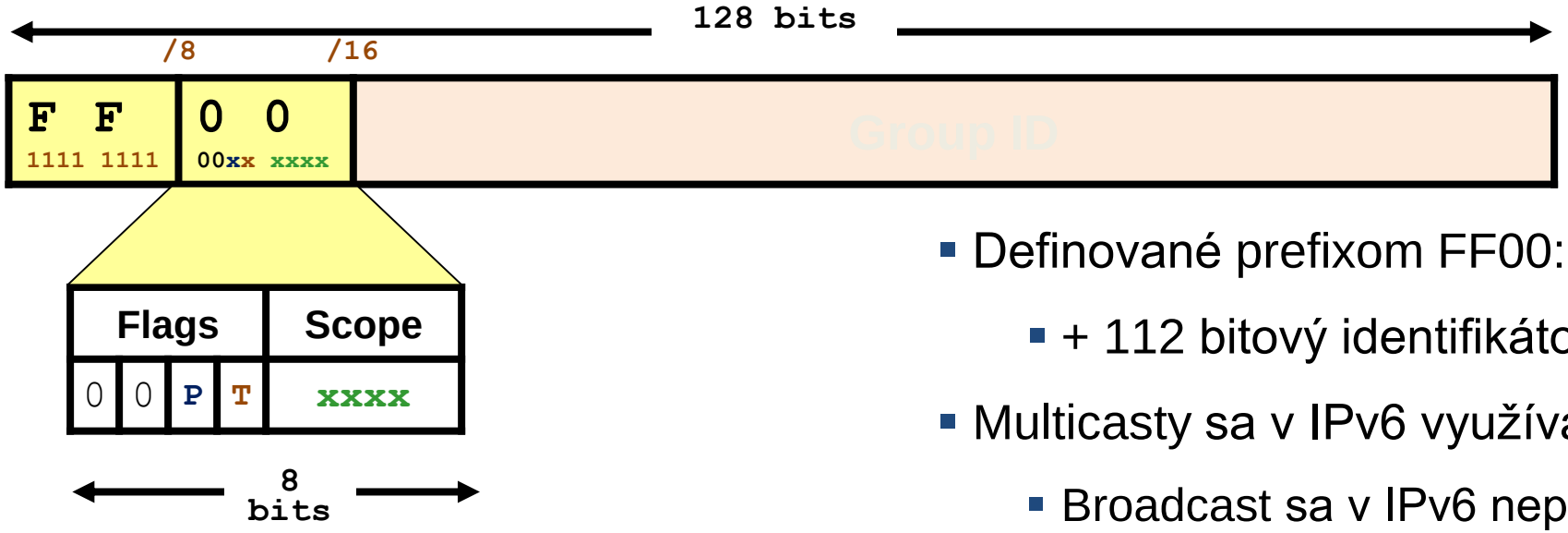
Toto sa deje vždy bez ohľadu na option v RA {1, 2, 3}



Krátka vsuvka o IPv6 multicast adresách

Využívané aj v DHCPv6

IPv6 multicastové adresy



Flags:

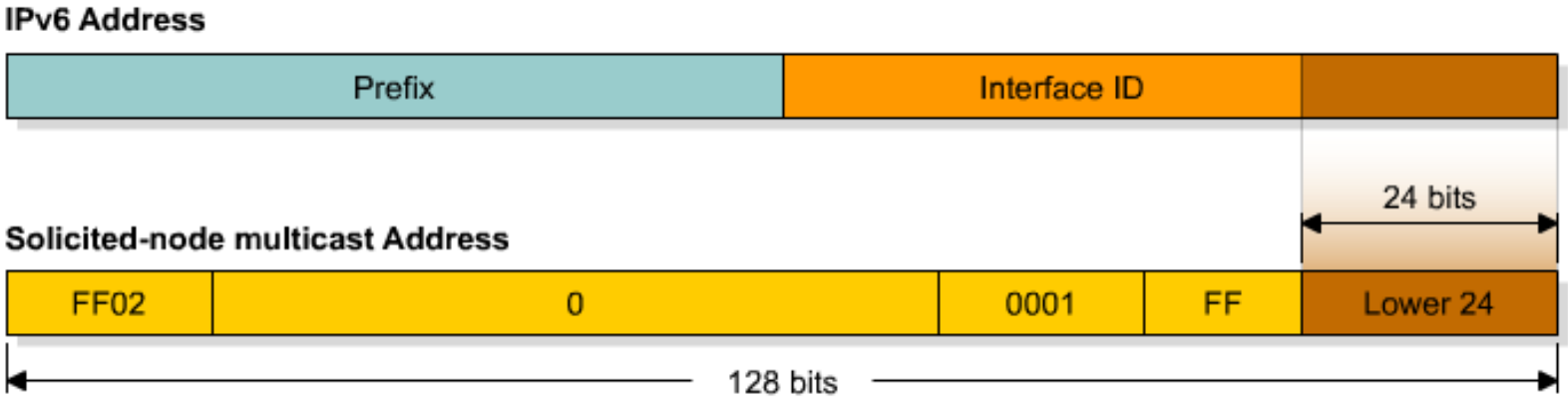
- P = Prefix for unicast-based assignments
- T = 0 if permanent, 1 if temporary

Scope:

- 1 (0001) = Node (interface local)
- 2 (0010) = Link local
- 5 (0101) = Site local
- 8 (1000) = Organization
- E (1110) = Global

- Definované prefixom FF00::/8
  - + 112 bitový identifikátor mcast skupiny
- Multicasty sa v IPv6 využívajú veľmi často
  - Broadcast sa v IPv6 nepoužíva
- Prvý oktet: FF
- Druhý oktet obsahuje:
  - Prefix, platnosť a rozšírenie
  - Adresy `FF00::` to `FF0F::` sú rezervované, napr:
    - **FF02::/16** – všeobecne známe, link local
      - **FF02::1** (IPv6 all-nodes multicast, cieľ.IP v RA)
      - **FF02::2** (IPv6 all-routers multicast, cieľ.IP v RS)

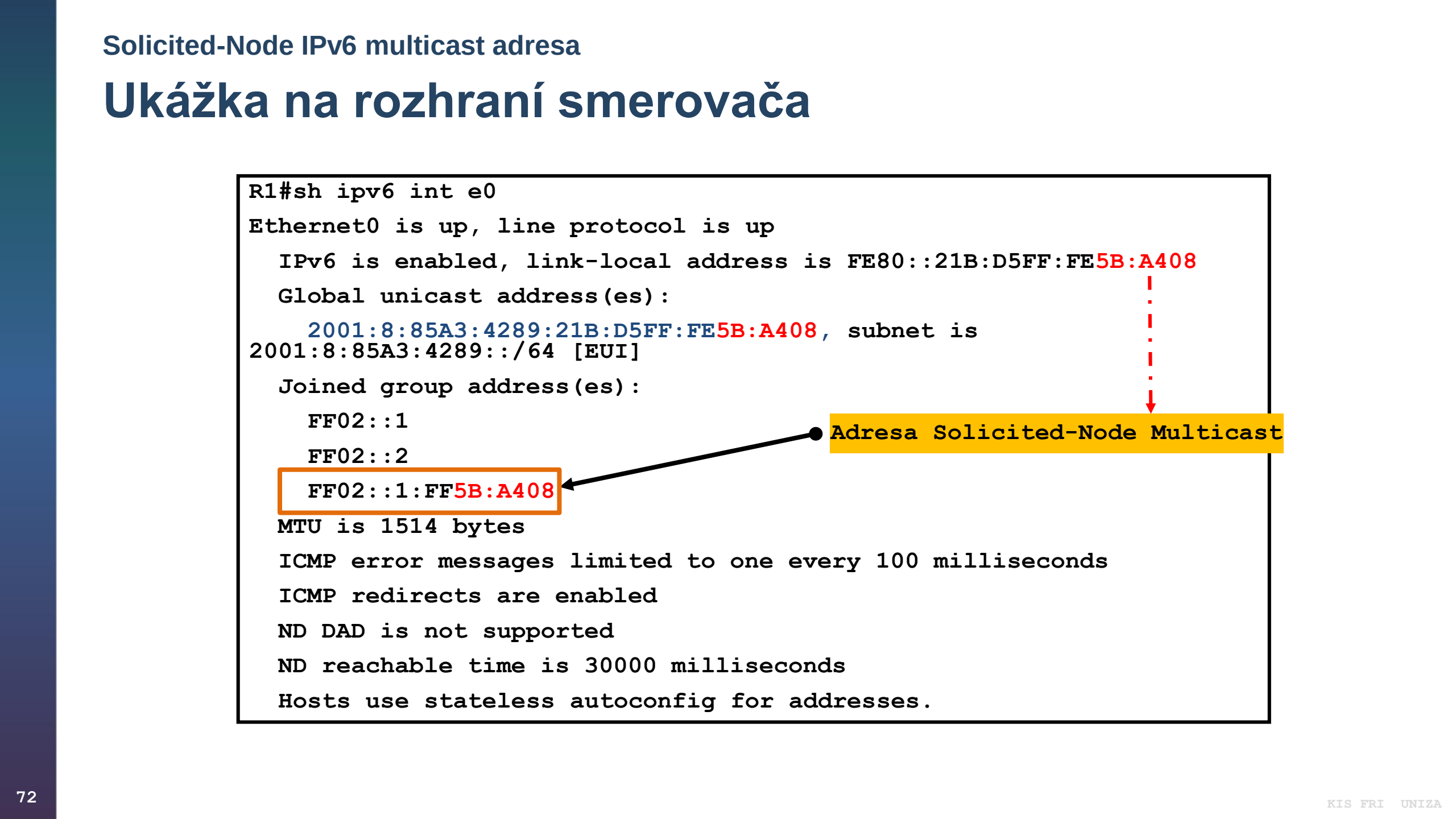
Multicastové adresy Solicited-Node



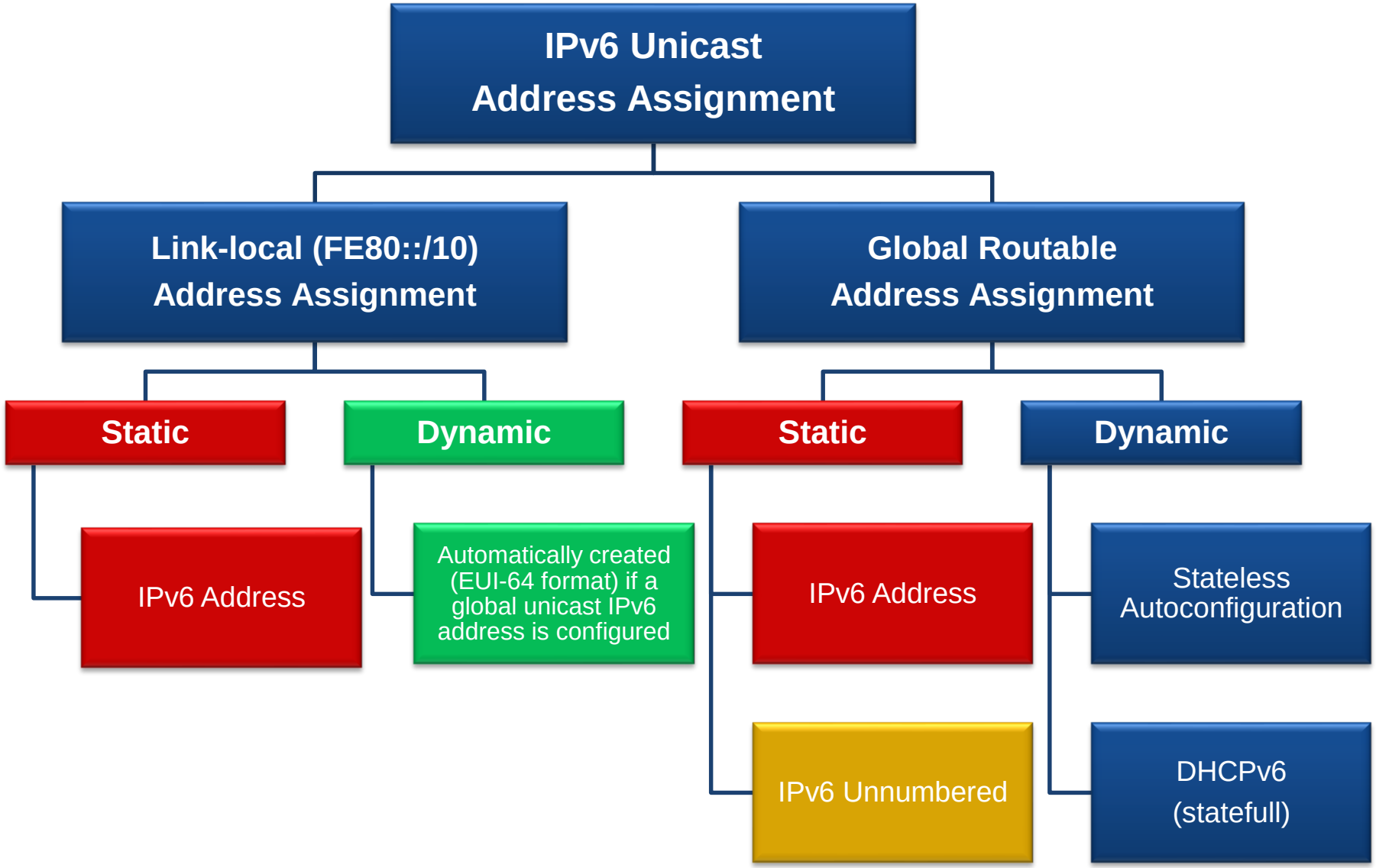
- Solicited-node multicast adresa pozostáva z prefixu **FF02::1:FF:** /104
  - Adresa má rozsah link-local
  - Má ju každý IPv6 host (ukážka na ďalšom slajde)
- Nasadenie
  - Neighbor discovery (ND)
    - Zistenie link-local adresy suseda, zistenie defaut route, zistenie smerovača na linke
  - Bezstavová autokonfigurácia, DAD
- Typické použitie je v ICMPv6, ktoré nahrádza ARP (viem susedovu IPv6 adr. a zisťujem jeho MAC)
  - Spodných 24 bitov IPv6 adresy je 24 bitov z IPv6 adresy hľadaného suseda
  - ICMPv6 je vo vnútri IPv6 paketu, takže paket musí mať adresu príjemcu, v tomto prípade práve Solicited-Node multicast

Ukážka na rozhraní smerovača

```
R1#sh ipv6 int e0
Ethernet0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::21B:D5FF:FE5B:A408
  Global unicast address(es):
    2001:8:85A3:4289:21B:D5FF:FE5B:A408, subnet is
2001:8:85A3:4289::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF5B:A408
  MTU is 1514 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is not supported
  ND reachable time is 30000 milliseconds
  Hosts use stateless autoconfig for addresses.
```

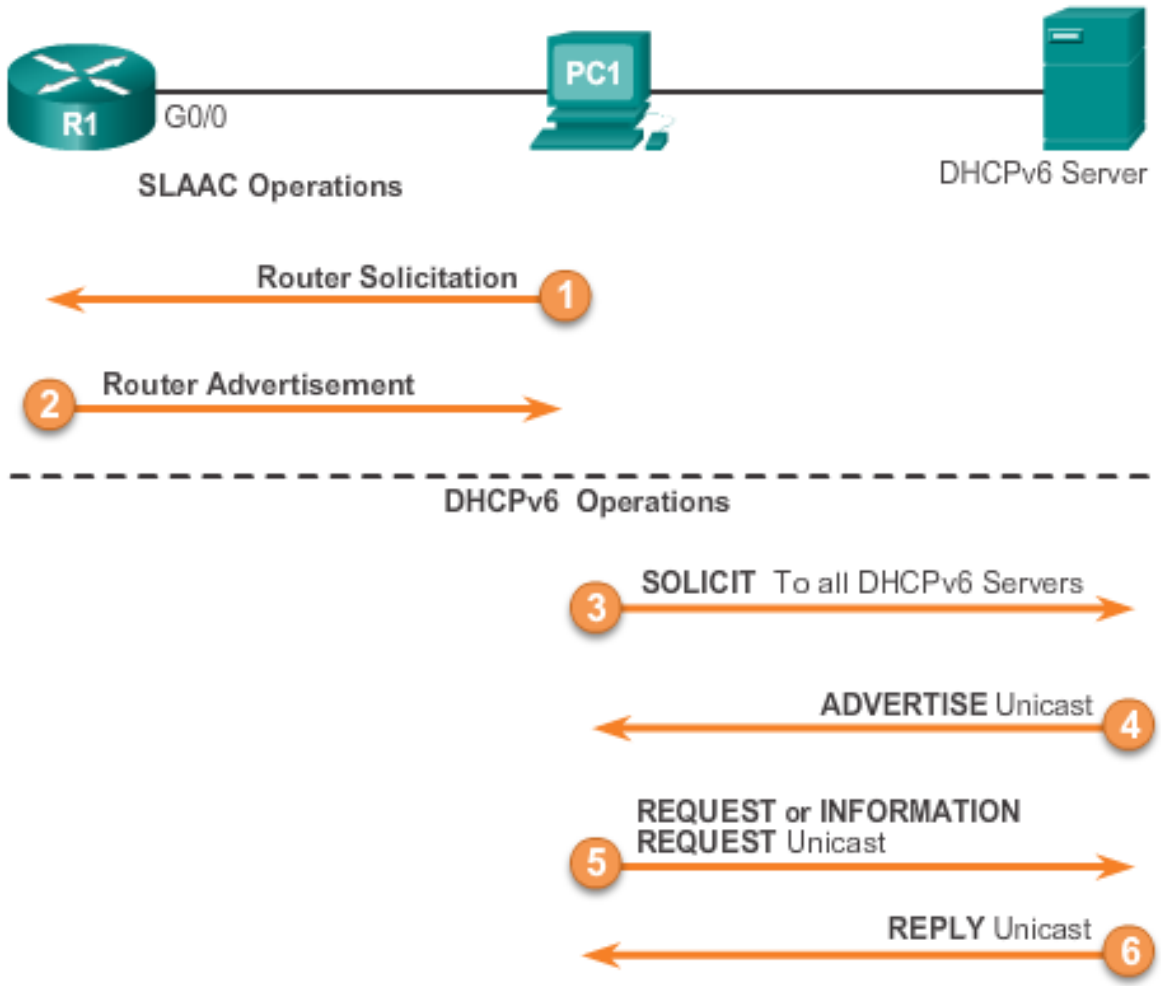


Možnosti konfigurácie unicast IPv6 adries



Konfigurácia DHCPv6

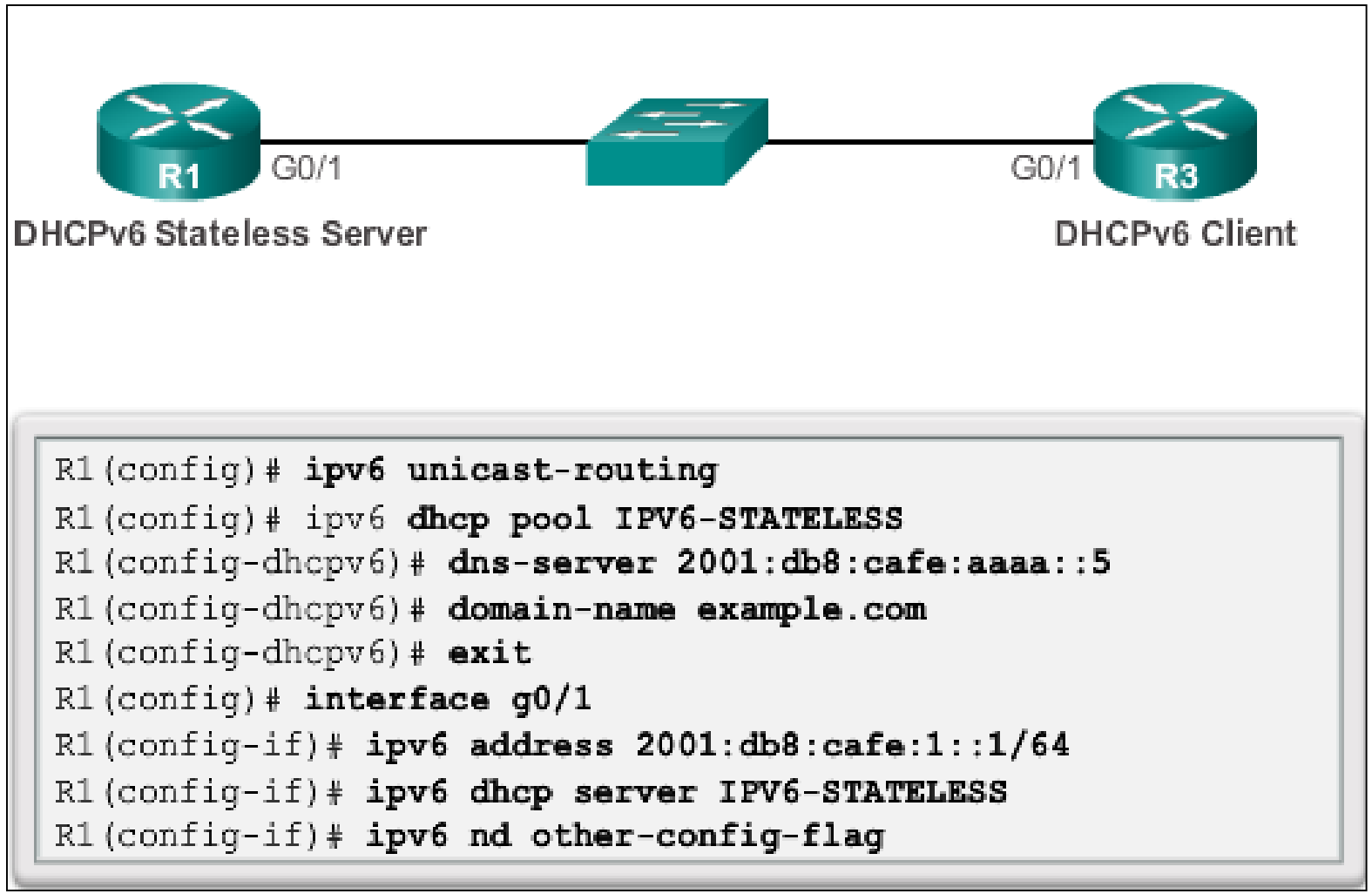
Fungovanie DHCPv6



- Smerovač (default GW) má v správe RA (Router Advertisement) dve konfigurovateľné bity (ktoré rozhodujú o Option: 1,2,3) :
  - **‘M’ bit** - "Managed address configuration" flag.
    - 1 = klientovi povie, aby požiadal DHCPv6 pre získanie IPv6 adresy a ostatných info.
  - **‘O’ bit** - "**Other** configuration" flag
    - 1 = klientovi povie, aby o **ostatné** informácie (okrem prefixu a default GW) požiadal DHCPv6 server (DNS, ..)
  - Možné kombinácie:
    - MO=**00** (SLAAC)
    - MO=**01** (stateless DHCPv6)
    - MO=**10** (statefull DHCPv6)

Stateless DHCPv6 servera

- M = 0
  - Klient získa stateless adresu z RA správy od smerovača
- O = 1
  - DHCPv6 server dodá klientovi iba ostatné info (DNS, ..)



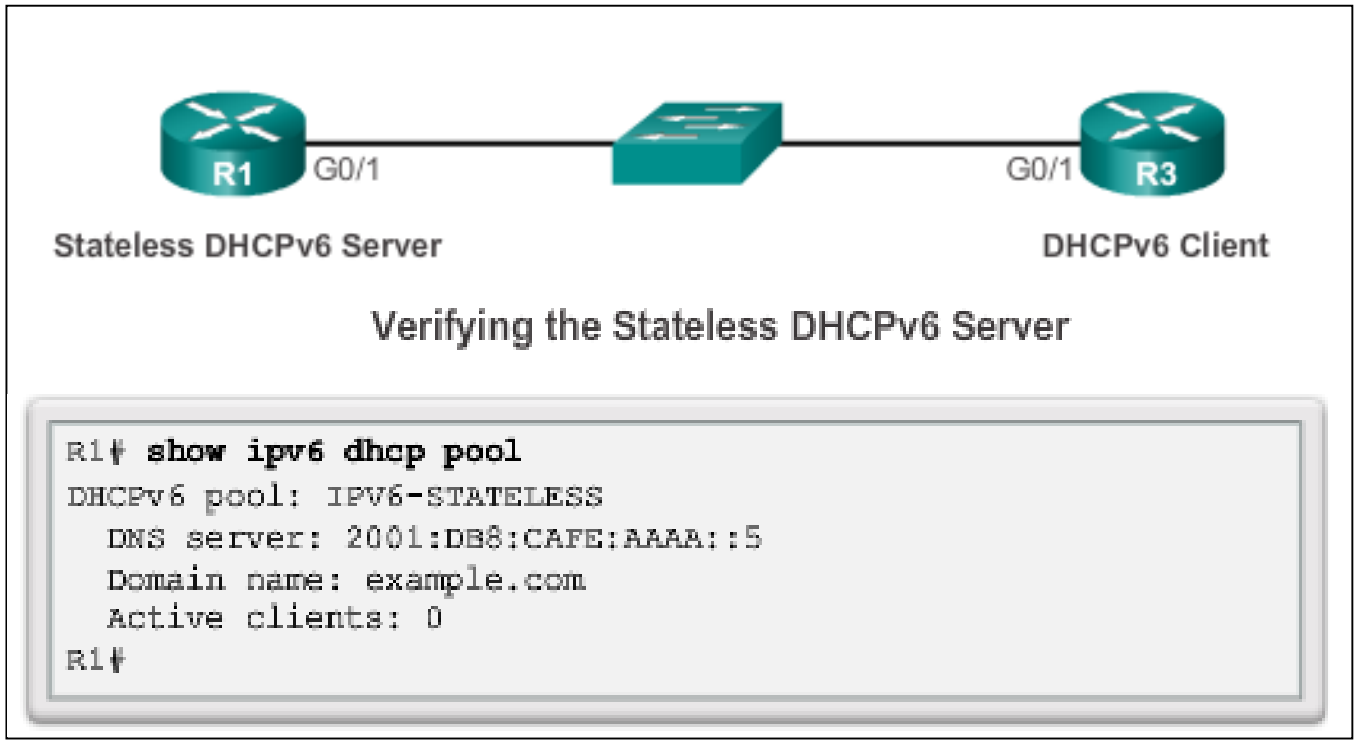

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATELESS
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATELESS
R1(config-if)# ipv6 nd other-config-flag
```

Stateless DHCPv6 klienta

Configuring a Router as Stateless DHCPv6 Client

```
R3(config)# interface g0/1
R3(config-if)# ipv6 enable
R3(config-if)# ipv6 address autoconfig
R3(config-if)#
```

Diagnostika Stateless DHCPv6

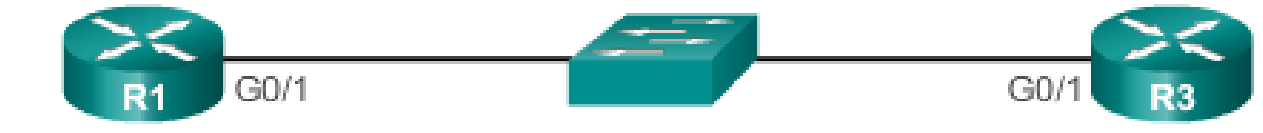


- **show IPv6 interface**
- **debug ipv6 dhcp detail**

Statefull DHCPv6 servera

- M = 1
  - DHCPv6 dodá klientovi IPv6 adresu
- O = 0
  - Hodnotu tohto flagu je v tomto variante nepodstatná

Configuring a Router as a Stateful DHCPv6 Server




```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATEFUL
R1(config-dhcpv6)# address prefix 2001:DB8:CAFE:1::/64
                    lifetime infinite infinite
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATEFUL
R1(config-if)# ipv6 nd managed-config-flag
```

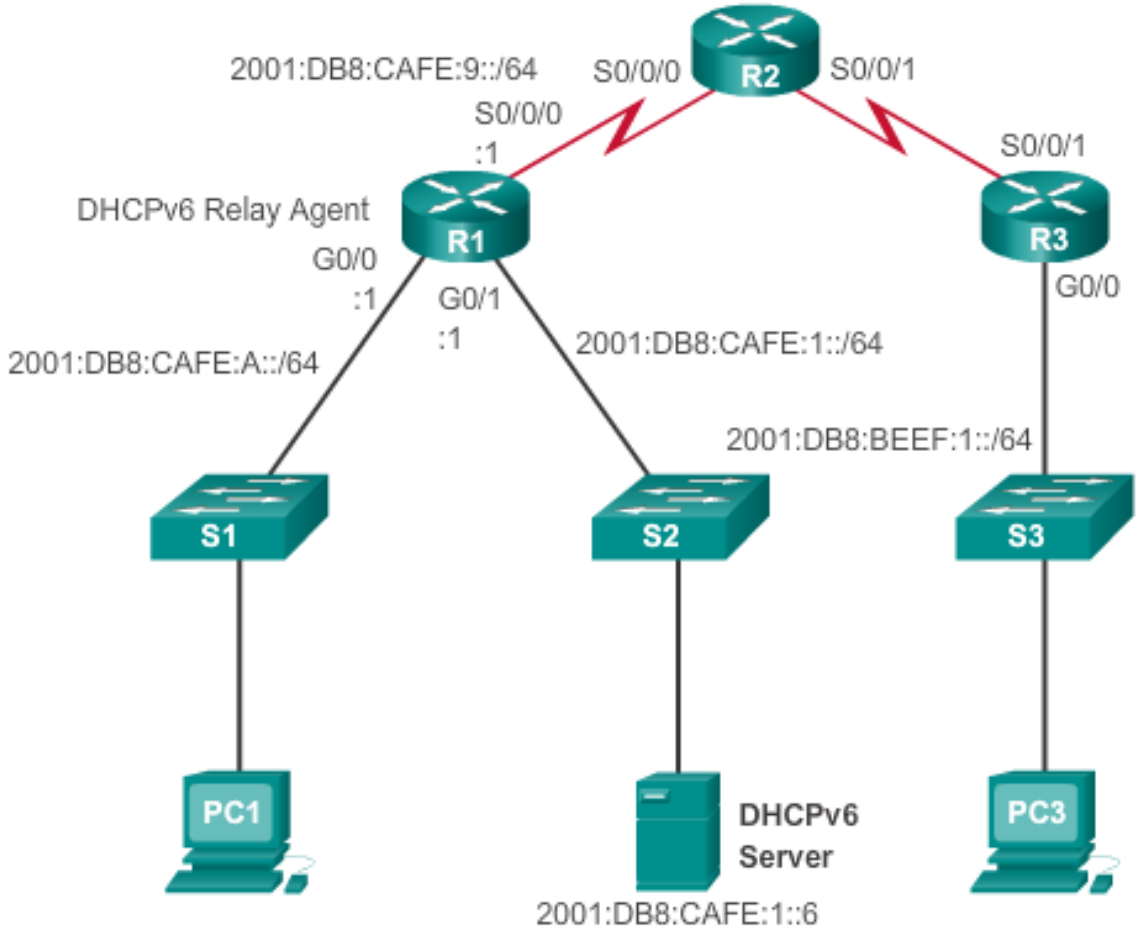
Diagnostika Stateful DHCPv6

- Diagnostika pre stateful DHCPv6 server:
  - show ipv6 dhcp pool
  - show ipv6 dhcp binding
- Diagnostika pre stateful DHCPv6 klienta:
  - show ipv6 interface

```
R3# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is
FE80::32F7:DFF:FE25:2DE1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:CAFE:1:5844:47B2:2603:C171, subnet is
2001:DB8:CAFE:1:5844:47B2:2603:C171/128
  Joined group address(es):
    FF02::1
    FF02::1:FF03:C171
    FF02::1:FF25:2DE1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND NS retransmit interval is 1000 milliseconds
  Default router is FE80::D68C:B5FF:FECE:A0C1 on
```

Konfigurácia smerovača ako

Stateful DHCPv6 Relay Agent




```
R1(config)# interface g0/0
R1(config-if)# ipv6 dhcp relay destination 2001:db8:cafe:1::6
R1(config-if)# end
R1# show ipv6 dhcp interface g0/0
GigabitEthernet0/0 is in relay mode
  Relay destinations:
    2001:DB8:CAFE:1::6
```

Kroky v diagnostike

Troubleshooting Task 1:	Resolve conflicts.
Troubleshooting Task 2:	Verify allocation method.
Troubleshooting Task 3:	Test with a static IPv6 address.
Troubleshooting Task 4:	Verify switch port configuration.
Troubleshooting Task 5:	Test from the same subnet or VLAN.

DHCPv6 konfigurácia na smerovači – stateless / statefull

Statefull DHCPv6 Services

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATEFUL
R1(config-dhcpv6)# address prefix 2001:DB8:CAFE:1::/64 lifetime
infinite infinite
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATEFUL
R1(config-if)# ipv6 nd managed-config-flag
```

Stateless DHCPv6 Services

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATELESS
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATELESS
R1(config-if)# ipv6 nd other-config-flag
```

Debugging DHCPv6

```
R1# debug ipv6 dhcp detail
   IPv6 DHCP debugging is on (detailed)
R1#
*Feb  3 21:27:41.123: IPv6 DHCP: Received SOLICIT from
FE80::32F7:DFF:FE25:2DE1 on GigabitEthernet0/1
*Feb  3 21:27:41.123: IPv6 DHCP: detailed packet contents
*Feb  3 21:27:41.123:   src FE80::32F7:DFF:FE25:2DE1
(GigabitEthernet0/1)
*Feb  3 21:27:41.127:   dst FF02::1:2
*Feb  3 21:27:41.127:   type SOLICIT(1), xid 13190645
*Feb  3 21:27:41.127:   option ELAPSED-TIME(8), len 2
*Feb  3 21:27:41.127:     elapsed-time 0
*Feb  3 21:27:41.127:   option CLIENTID(1), len 10
*Feb  3 21:27:41.127:     000
*Feb  3 21:27:41.127: IPv6 DHCP: Using interface pool IPV6-
STATEFUL
*Feb  3 21:27:41.127: IPv6 DHCP: Creating binding for
FE80::32F7:DFF:FE25:2DE1 in pool IPV6-STATEFUL
```

<Output omitted>

MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť!

Ohodnoť našu CNA na google:

- https://goo.gl/maps/BAnFvQKYCBpffcEX7

Vytvorené v rámci projektu KEGA 011STU - 4/2017.