Chapter 5: Inter-VLAN Routing

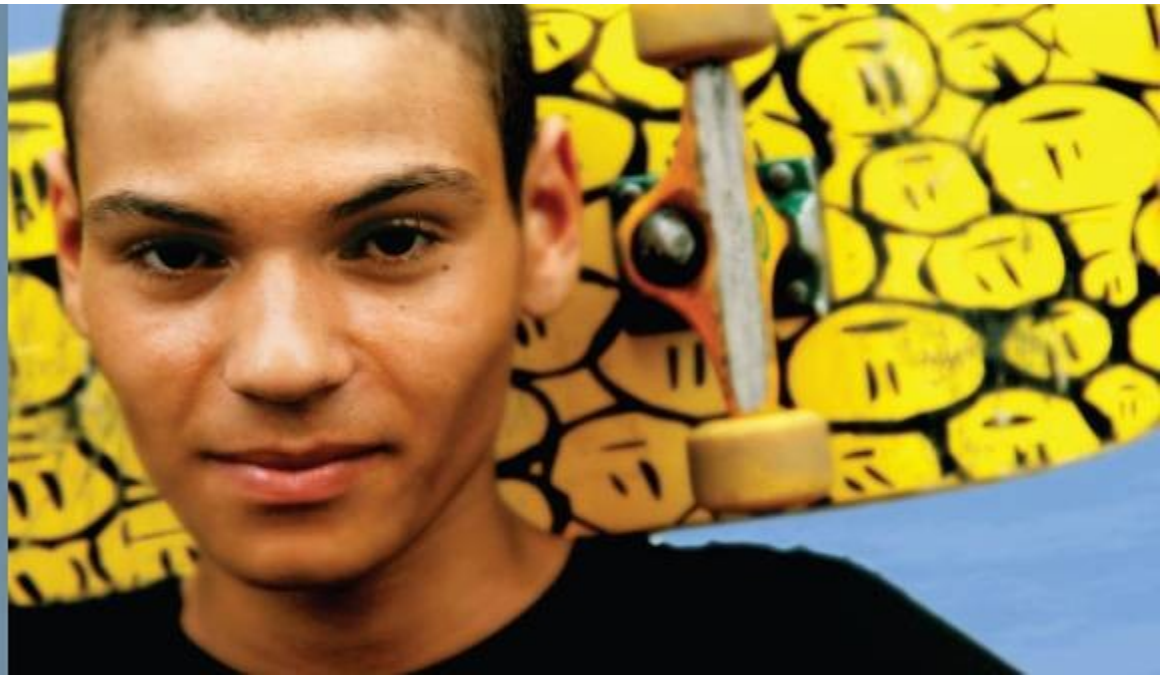
CCNP SWITCH: Implementace Cisco IP přepínaných sítí

Cisco | Networking Academy®
Mind Wide Open™

Cíle kapitoly 5

- Návrh podnikové sítě, a jeho implementace a ověření inter-VLAN směrování pomocí externího směrovače nebo vícevrstvého přepínače pomocí přepínače virtuálních rozhraní nebo směrovaných rozhraní
- Pochopení vrstvy 3 EtherChannelu a jeho konfigurace
- Porozumění provozu DHCP a jeho implementaci, ověřování v dané podnikové síti

Popis Inter-VLAN Routingu



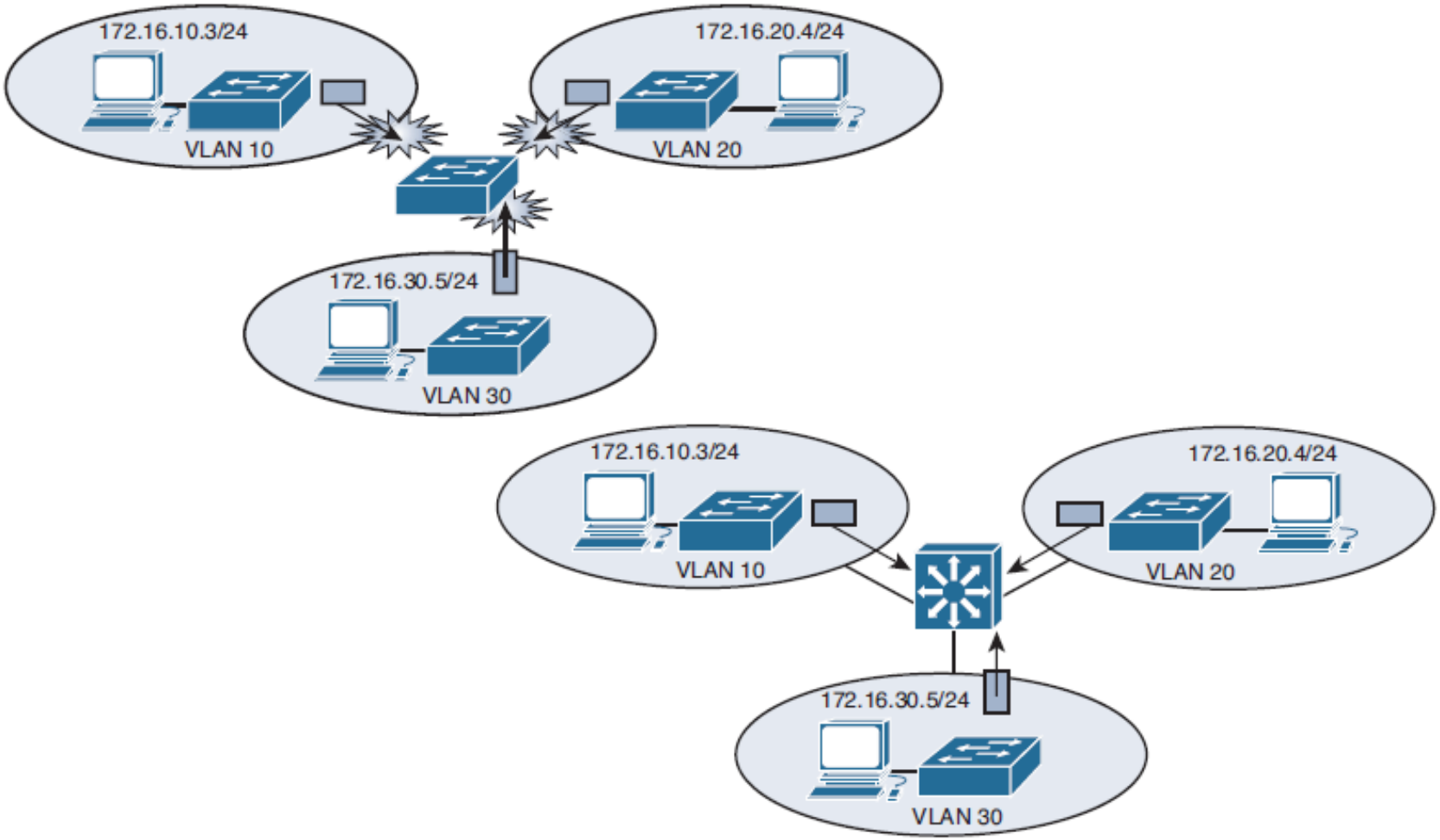
Popis Inter-VLAN Routingu

- Úvod do inter-VLAN routingu
- Inter-VLAN routing používající externí router
- Inter-VLAN routing s virtuálními rozhraními přepínačů
- Routing s routovanými porty
- Konfigurace inter-VLAN routingu za použití SVI (Switch Virtual Interface) a routovaných portů
- Troubleshooting inter-VLAN routingu

Úvod do Inter-VLAN Routingu

- Protože VLAN izolují provoz do definované vysílací domény a podsítě, síťová zařízení v různých VLAN nemohou navzájem komunikovat.
- Zařízení v každé síti VLAN mohou komunikovat se síťovými zařízeními v jiné síti VLAN pouze prostřednictvím směrovacího zařízení vrstvy 3
- Následující zařízení mohou poskytovat směrování mezi sítěmi VLAN:
  - Každý externí směrovač nebo skupina směrovačů s odděleným rozhraním do každé VLAN – CCNA
  - Jakýkoli externí směrovač s rozhraním, které podporuje kanál (router-on-a-stick) – CCNA
  - Jakýkoli přepínač Catalyst vrstvy 3 – **CCNP**

Úvod do Inter-VLAN Routingu



Router vs MLS pro IVR

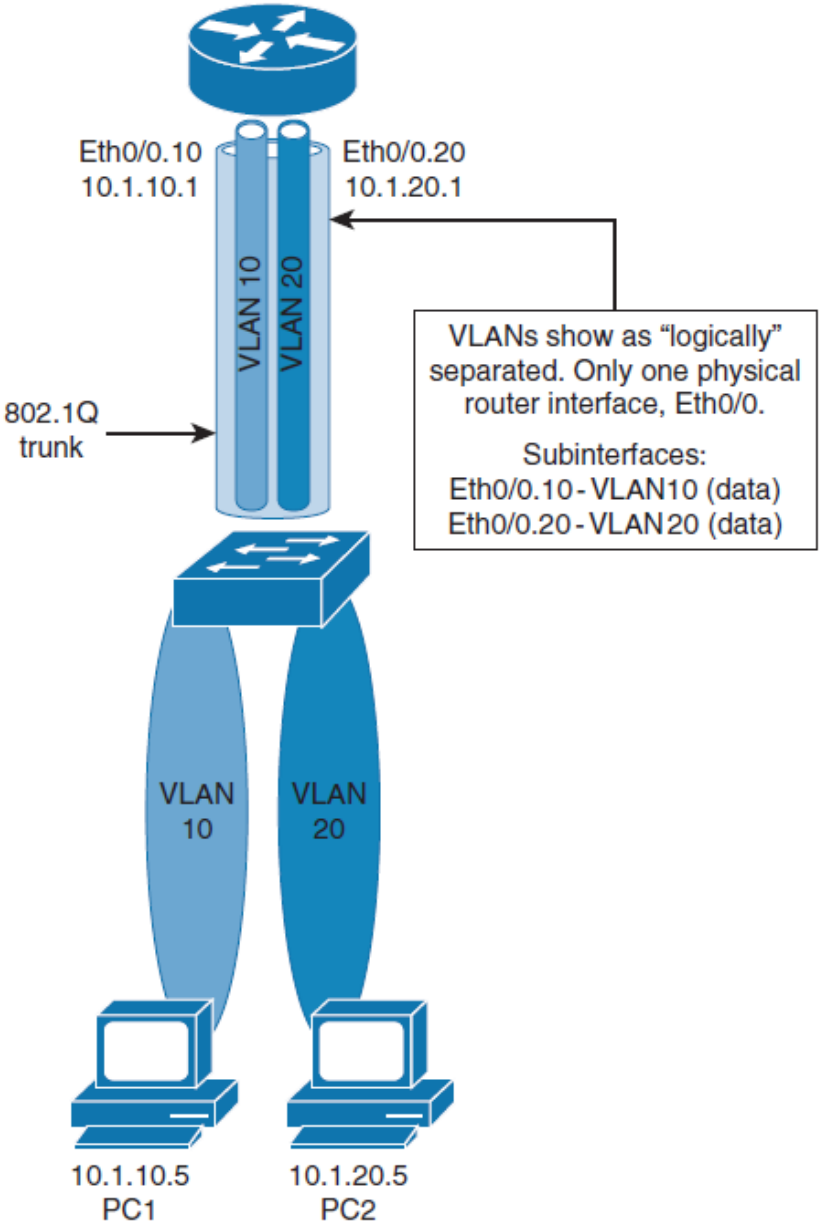
- Přepínače vrstvy 3 mají obvykle propustnost přepínání paketů v **milionech paketů za sekundu** (p/s), zatímco tradiční směrovače obecného určení poskytují přepínání paketů v rozsahu **100 000 p/s až více než 1 milion p/s**.
- Všechny vícevrstvé přepínače Catalyst podporují tři různé typy rozhraní vrstvy 3:

  A) Routed port: Čisté rozhraní vrstvy 3 podobné routovanému portu routeru Cisco IOS.

  B) Switch virtual interface (SVI): Virtuální rozhraní VLAN pro směrování mezi VLAN. Jinými slovy, switch virtual interface (SVI) jsou virtuální směrované VLAN rozhraní.

  C) Bridge virtual interface (BVI): virtuální přemostění rozhraní vrstvy 3.

Inter-VLAN Routing používající externí router



Konfigurace směrování s externím routerem

Konfigurace subinterface routeru pro směrování provozu mezi VLAN 10 a VLAN 20:

- `R1(config)# interface ethernet 0/0.10`
- `R1(config-subif)# encapsulation dot1q 10`
- `R1(config-subif)# ip address 10.0.10.1 255.255.255.0`
- `R1(config)# interface ethernet 0/0.20`
- `R1(config-subif)# encapsulation dot1q 20`
- `R1(config-subif)# ip address 10.0.20.1 255.255.255.0`

Konfigurace interface pro nativní VLAN provoz.

- `R1(config)# interface ethernet 0/0.1`
- `R1(config-subif)# encapsulation dot1q 1 native`
- `R1(config-subif)# ip address 10.0.1.1 255.255.255.0`

Verifikace konfigurace

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES NVRAM  up                    up
Ethernet0/0.1          10.0.1.1        YES manual up                    up
Ethernet0/0.10         10.0.10.1       YES manual up                    up
Ethernet0/0.20         10.0.20.1       YES manual up                    up
Ethernet0/1            unassigned      YES NVRAM  administratively down down
Ethernet0/2            unassigned      YES NVRAM  administratively down down
Ethernet0/3            unassigned      YES NVRAM  administratively down down
```

Routing s konfigurací externího routeru

Konfigurujme trunk port na přepínači. Povolme provoz VLAN 1, 10, a 20.

- `SW1(config)# interface ethernet 0/0`
- `SW1(config-if)# switchport trunk encapsulation dot1q`
- `SW1(config-if)# switchport mode trunk`
- `SW1(config-if)# switchport trunk allowed vlan 1,10,20`

Externí Routery: výhody

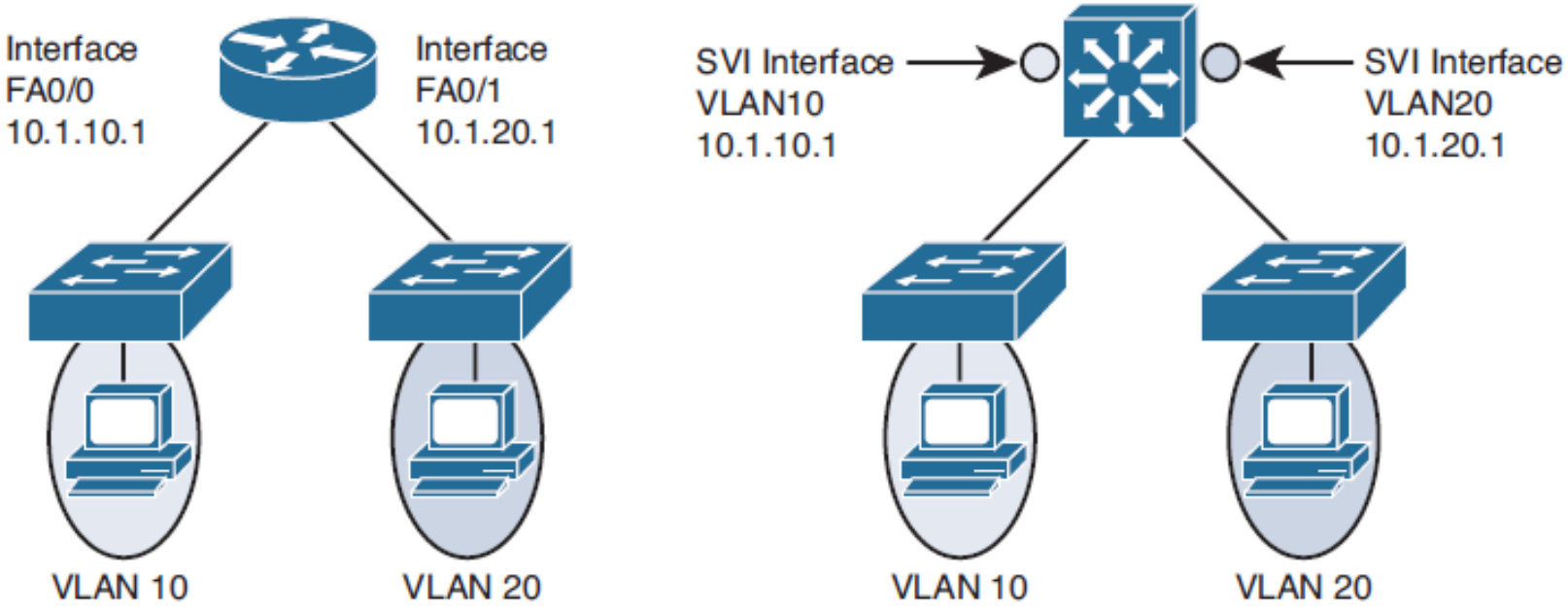
- Externí směrovač pracuje s jakýmkoli přepínačem, protože na přepínači nejsou požadovány služby vrstvy 3. Mnoho přepínačů nemá možnosti předávání vrstvy 3, zejména přepínače, které se používají v přístupové vrstvě hierarchické sítě.
- Implementace je jednoduchá. Konfigurovat je třeba pouze jeden port přepínače a jeden směrovač.
- Pokud návrh sítě obsahuje pouze přepínače vrstvy 2, návrh a proces řešení potíží s tokem paketů jsou velmi jednoduché, protože v síti existuje pouze jedno místo, kde se propojují VLAN.

Externí Routery: nevýhody

- Směrovač je jediným bodem selhání (single point of failure).
- Jediná komunikační cesta může být přetížena. U modelu router-on-a-stick je linka trunku omezena rychlostí rozhraní routeru, protože je sdílena všemi trunky VLANů
- Může dojít ku zpoždění, protože rámce opakovaně opouštějí šasi a router rozhoduje o směrování na bázi softwaru.

Inter-VLAN Routing používající rozhraní SVI (Switch Virtual Interfaces)

- SVI je virtuální rozhraní nakonfigurované v rámci vícevrstvého přepínače.
- SVI může být vytvořeno pro libovolnou VLAN na switchi. Pouze jedna VLAN je spojená s SVI.



Switch Virtual Interfaces

- SVI je „virtuální“, neboli žádný fyzický port není dedikovaný pro rozhraní, může vykonat stejné funkce, které koná pro VLAN rozhraní routeru.
- Je také konfigurován stejným způsobem, jako rozhraní routeru (IP adresa, ACL, atd.).
- Defaultně, je SVI vytvořeno pro defaultní VLAN (VLAN1) a slouží pro defaultní administraci.

Důvody pro konfiguraci SVI

- Brána pro VLAN – provoz je směrován do ní a z ní.
- Poskytuje fallback bridging pro nesměrovatelné protokoly.
- Poskytuje L3 konektivitu IP pro switch.
- Slouží pro podporu směrovacího protokolu a konfigurace mostu.

SVI: Výhody a nevýhody

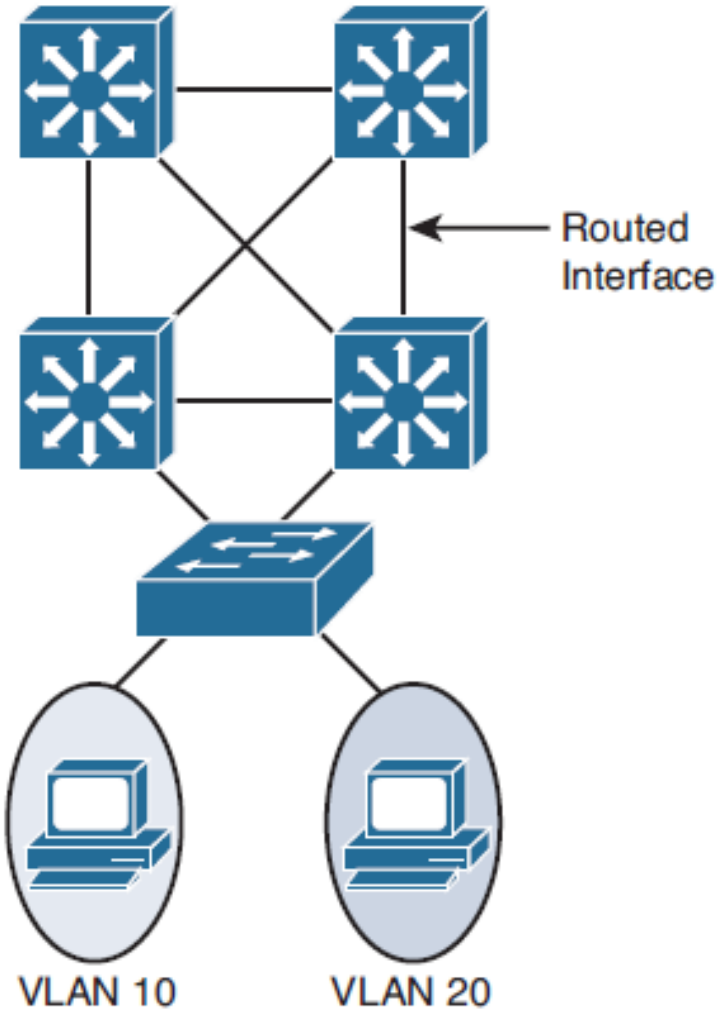
Výhody:

- Rychlejší než router-on-a-stick protože pracuje s hardwarem.
- Pro routing nepotřebuje externí linky.
- Není omezen na jediný link. Mezi switchi mohou být pro navýšení pásma použit L2 EtherChannel.
- Zpoždění je nižší, protože paket nemusí opustit switch.

Nevýhody:

- Pro inter-VLAN routing potřebuje dražší L3 switch.

Routing s Routed Porty

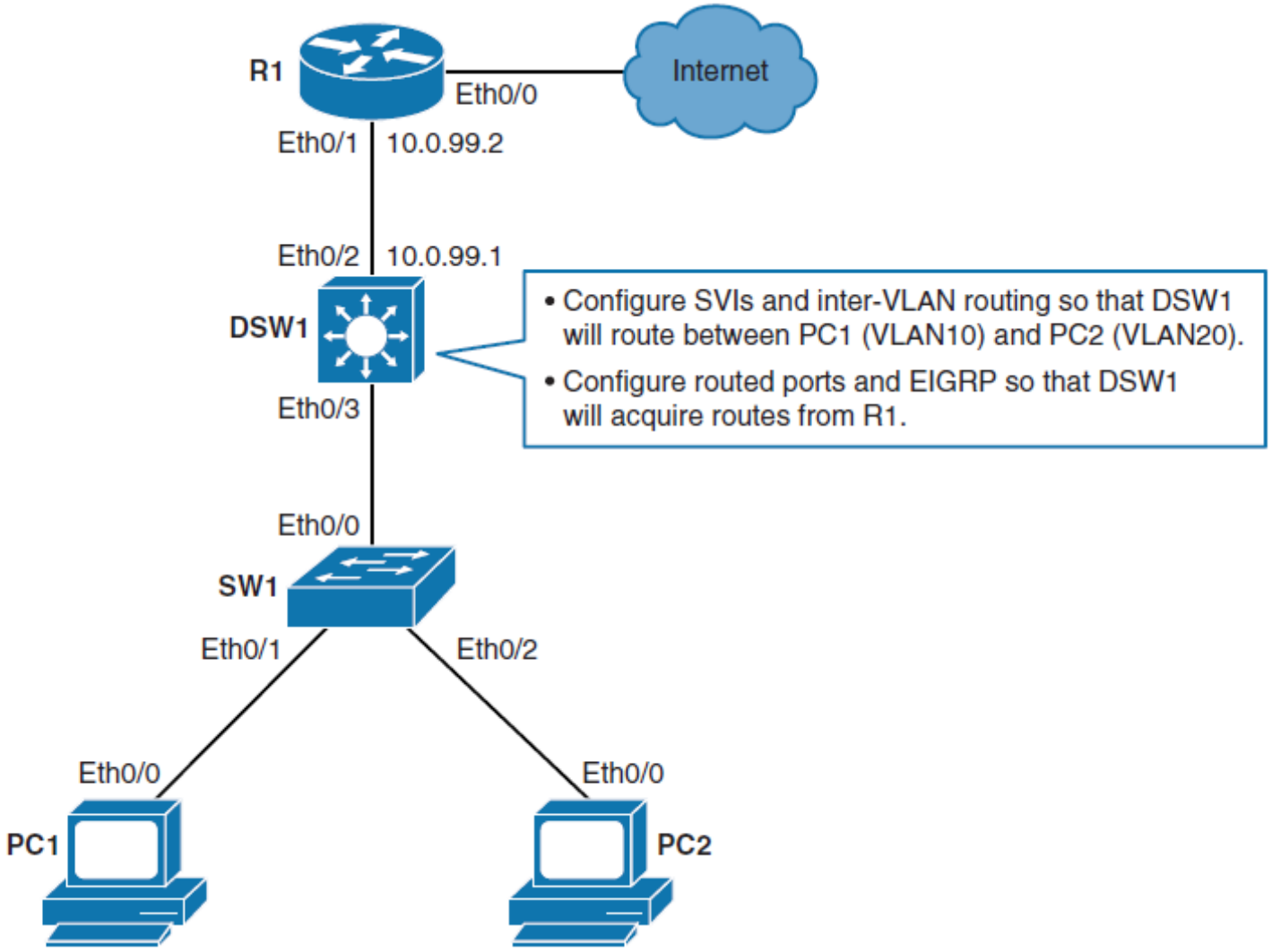


- A routed port je fyzický port, který se chová jako L3 port.
- Není asociován s konkrétní VLAN.
- Je odstraněna L2 funkčnost.
- Link Aggregation Control Protocol (LACP) ale lze použít.
- Slouží pro linky point-to-point.
- Routed rozhraní na rozdíl od routerů nepodporují subinterfaces.
- Je třeba na rozhraní dát příkaz **no switchport**

Routed Ports: Výhody

- Jedno multilayer zařízení může mít SVI and routed porty:
  Je to rychlé, protože provoz běží na hardwaru na L2 i L3 úrovni.

Konfigurace Inter-VLAN routingu za použití SVI i Routed Portů



Konfigurace routingu na Multilayer Switchi 1/1

Step 1. Vytvořte VLANs 10 a 20:

- `DSW1(config)# vlan 10`
- `DSW1(config-vlan)# vlan 20`

Step 2. NA DSW1, nastavte IPv4 routing:

- `DSW1(config)# ip routing`

Step 3. Konfigurujte SVI pro VLANy s IP adresami

- `DSW1(config)# interface vlan 10`
- `DSW1(config-if)# ip address 10.0.10.1 255.255.255.0`
- `DSW1(config-if)# no shutdown`
- `DSW1(config)# interface vlan 20`
- `DSW1(config-if)# ip address 10.0.20.1 255.255.255.0`
- `DSW1(config-if)# no shutdown`

Konfigurace routingu na Multilayer Switchi 2/2

Step 4. Zapněte rozhrani k R1 (Ethernet 0/0):

- `DSW1(config)# **interface ethernet 0/2**`
- `DSW1(config-if)# **no switchport**`
- `*Nov 28 15:03:55.138: %LINK-3-UPDOWN: Interface Ethernet0/2, changed state to up`
- `*Nov 28 15:03:56.142: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to up`
- `DSW1(config-if)# **ip address 10.0.99.1 255.255.255.0**`

Step 5. Konfigurujte Routing Protocol

- `DSW1(config)# **router eigrp 1**`
- `DSW1(config-router)# **network 10.0.0.0**`
- `*Nov 28 15:12:22.448: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.99.2 (Ethernet0/2) is up: new adjacency`

Použití příkazu SVI autostate exclude

- SVI je výhodné, pokud má L2 port ve VLAN čas na konvergenci (změna ze stavu STP listening-learning na stav forwarding).
- Defaultní akce v případě vícenásobných portů je, že SVI spadne, pokud spadnou všechny porty ve VLAN.
- Lze řešit problémy typu „černá díra směrování“:

  R1(config)# **ip route 1.1.1.1 255.255.255.0 null0**

  R2(config)# **int null0**
  R2(config-if)# **no ip unreachables**

- Můžete použít příkaz SVI **autostate exclude, kdy nakonfigurujete port tak, aby nebyl zahrnut do** SVI line-state up-and-down kalkulace.

vlan (UP, forwarding a neblokovaná) + + port (trunk/access) = protocol up

Switch(config)# vlan 100

Switch(config-vlan)# interface **vlan100**

Switch(config-if)# ip address 192.168.100.1 255.255.255.0
Switch(config-if)# end

Switch# show ip interface brief | exclude unassigned

Interface	*IP-Address*	*OK?*	*Method*	*Status*	*Protocol*
Vlan100	*192.168.100.1*	*YES*	*manual*	*up*	***down***

Switch(config)# interface fa0/1

Switch(config-if)# switchport **access** vlan 100

Switch(config-if)#

*LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to **up***

Konfigurace autostate exclude

- `Switch(config)# **interface interface** *slot/number*`
- `Switch(config-if)# **switchport autostate exclude**`

- Vypne SVI autostate a učiní konkrétní rozhraní SVI permanentně aktivní
- Autostate lze celkově vypnout příkazem no **autostate**.

Jak konfigurovat SVI

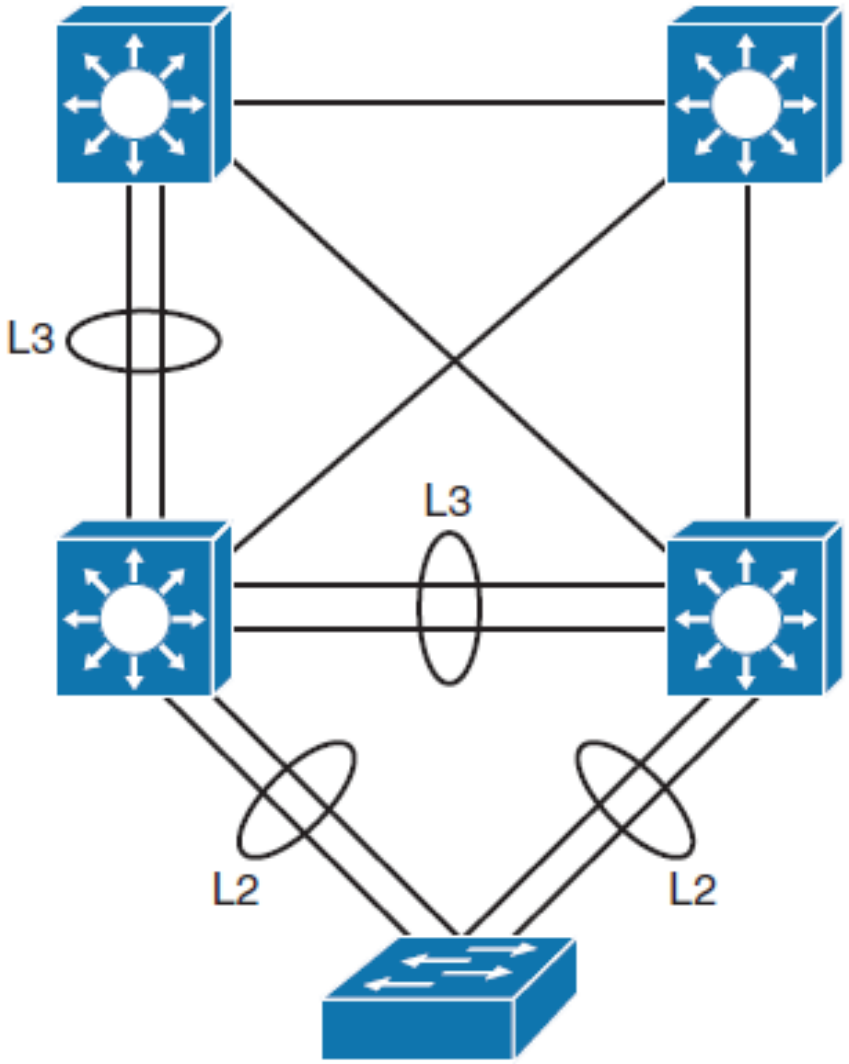
- Identifikovat, kdy VLANy vyžadují L3 brány.
- Vytvořit VLANy na L3 switchi.
- Vytvořit SVI rozhraní pro každou VLAN.
- Konfigurovat na SVI IP addresy.
- Nastavit rozhraní SVI.
- Nastavit IP routing.
- Určit, zda je potřebný dynamický protokol a konfigurovat ho.
- Identifikovat a konfigurovat autostate exclude.

Společné problémy Inter-VLAN routingu

Problem	Possible Cause
Missing VLAN	VLAN might not be defined across all the switches. VLAN might not be enabled on the trunk ports. Ports might not be in the right VLANs.
Layer 3 interface misconfiguration	Virtual interface might have the wrong IP address or subnet mask. Virtual interface might not be up. Virtual interface number might not match with the VLAN number. Routing has to be enabled to route frames between VLAN. Routing might not be enabled.
Routing protocol misconfiguration	Every interface or network needs to be added in the routing protocol. The new interface might not be added to the routing protocol. Routing protocol configuration is needed only if VLAN subnets need to communicate to the other routers, as previously mentioned in this chapter.
Host misconfiguration	Host might not have the right IP address or subnet mask. Each host has to have the default gateway that is the SVI or Layer 3 interface to communicate with other networks and VLAN. Host might not be configured with the default gateway.

Layer 2 Versus Layer 3 EtherChannel

Layer 2 Versus Layer 3 EtherChannel



Konfigurace Layer 3 EtherChannel 1/2

Krok 1. Vytvoření virtuálního L2 rozhraní:

- `Switch(config)# interface port-channel 1`

Krok 2. Změnit rozhraní na L3:

- `Switch(config-if)# no switchport`

Krok 3. Přiřazení ip adresy:

- `Switch(config-if)# ip address 172.32.52.10 255.255.255.0`

Krok 4. Nastavení rozhraní pro EtherChannel:

- `Switch(config)# interface range fastethernet 5/4 - 5`

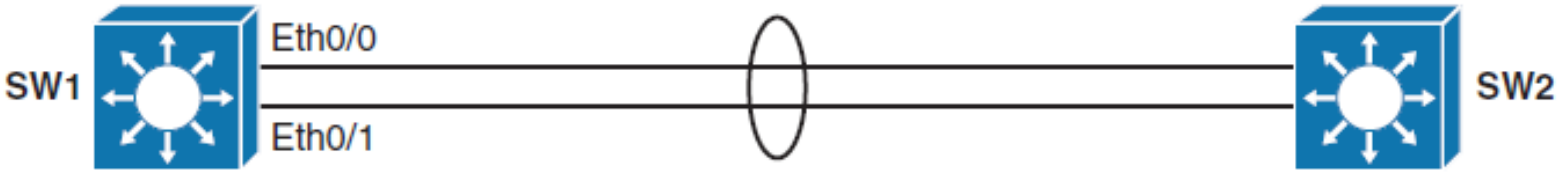
Konfigurace Layer 3 EtherChannel 2/2

Krok 5. Odstranění nezávislých funkčností L2 a L3 na portu, takže nyní bude port fungovat jako součást skupiny:

- `Switch(config-if-range)# no switchport`
- `Switch(config-if-range)# channel-protocol pagp`

Krok 6. Přiřazení skupiny:

- `Switch(config-if-range)# channel-group 1 mode desirable`




```
SW1(config)# interface range ethernet 0/0 - 1
SW1(config-if)# no switchport
SW1(config-if)# channel-group 1 mode on
SW1(config-if)# exit
SW1(config)# interface port-channel 1
SW1(config-if)# no switchport
SW1(config-if)# ip address 10.1.20.1 255.255.255.0
```

Jak konfigurovat L3 EtherChannel

- **Rychlost a duplex:** Obojí stejné na všech rozhraních.
- **Interface mode:** Vzhledem k tomu, že rozhraní kanálu portu je routed port, musí být stejný příkaz aplikován na všechny fyzické porty.
- **Verifikace konfigurace EtherChannel:**

```
show interface port-channel channel-group-number
show etherChannel channel-group-number summary
show spanning-tree vlan vlan-number detail
```

Implementace DHCP

Cíle výkladu implementace DHCP

- Vysvětlit ideu DHCP
- Konfigurovat DHCP server
- Konfigurovat manuální DHCP bindings
- Konfigurovat DHCP relay
- Konfigurovat volby DHCP

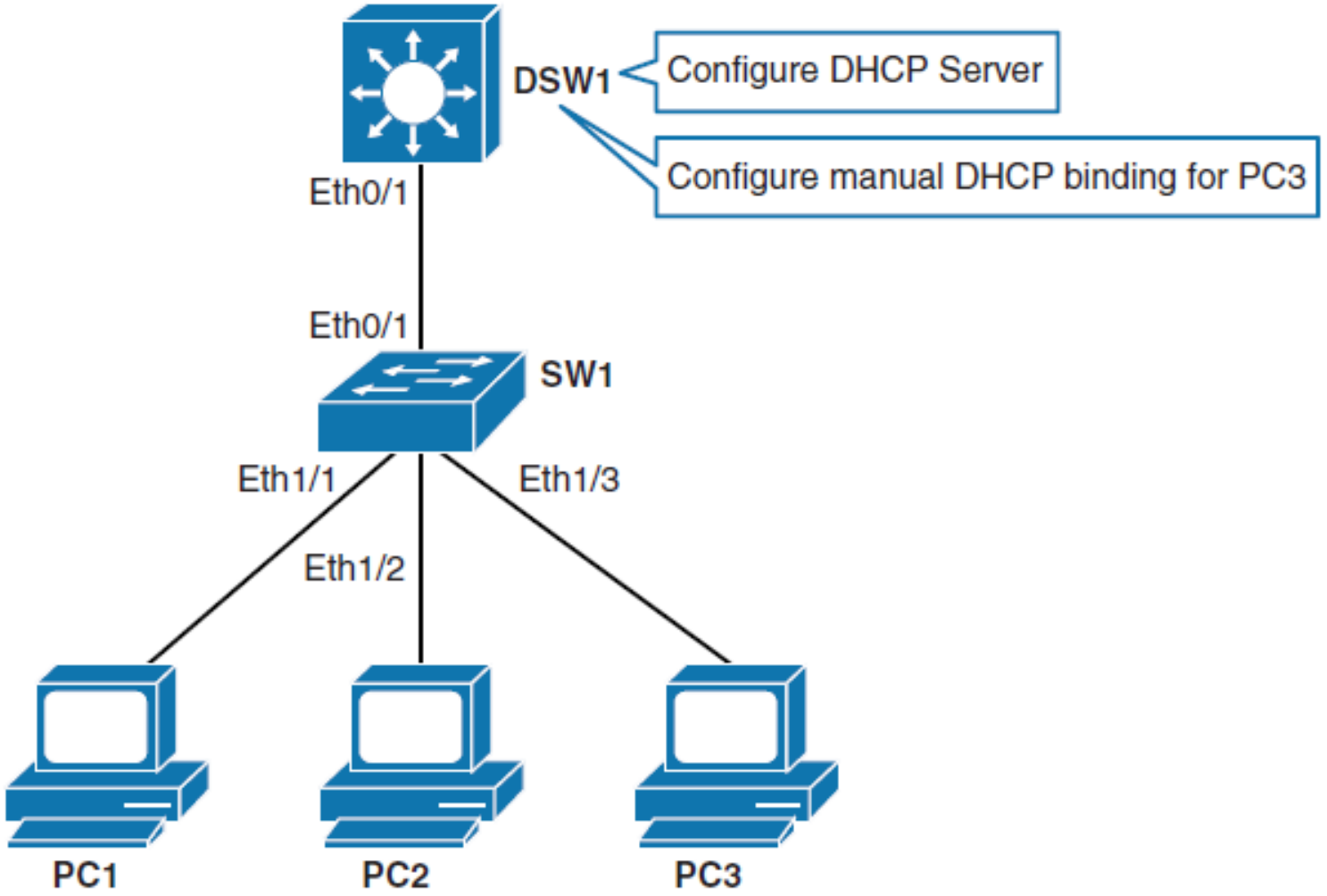
Přehled DHCP

- DHCP poskytuje konfigurační parametry hostitelům sítě.
- DHCP se skládá ze dvou komponent: protokol pro poskytování konfiguračních parametrů specifických pro hostitele z DHCP serveru hostiteli a mechanismus přidělování síťových adres hostitelům.
- DHCP je založen na modelu klient/server, ve kterém DHCP server přiděluje síťové adresy a dodává konfigurační parametry dynamicky konfigurovaným hostitelům.
- Klienti v přístupových VLAN potřebují služby DHCP a pro služby DHCP mohou být použity nejen externí servery, ale i směrovače.

DHCP na L3 přepínačích

- Mezi vícevrstvé přepínače společnosti Cisco, které používají software Cisco IOS, patří server DHCP a softwarový relay agent.
- Distribuční vícevrstvé přepínače často slouží jako brány L3 vrstvy pro klienty, kteří se připojují k přístupovým přepínačům z různých VLAN.
- Proto služba DHCP může být poskytována přímo distribučními přepínači.
- Alternativně mohou být služby DHCP soustředěny na externím vyhrazeném serveru DHCP.
- V takovém případě musí distribuční přepínače přesměrovat požadavky DHCP příchozích klientů na externí server DHCP.

Konfigurace DHCP v Multilayer Switched síti



Konfigurace DHCP v Multilayer Switched síti

DHCP Server

- DSW1(config)# **ip dhcp excluded-address 10.0.10.1**
- DSW1(config)# **ip dhcp pool VLAN10POOL**
- DSW1(config-dhcp)# **network 10.0.10.0 255.255.255.0**
- DSW1(config-dhcp)# **default-router 10.0.10.1**
- DSW1(config-dhcp)# **lease 2 (na 2 dny)**

Přiřazení ip addresy klientovi

- DSW1(dhcp-config)# **host 10.0.10.200 255.255.255.0**
- DSW1(dhcp-config)# **client-identifier 0063.6973.636f.2d61.6162.622e.6363.3030.2e30.3630.302d.4574.302f.30**

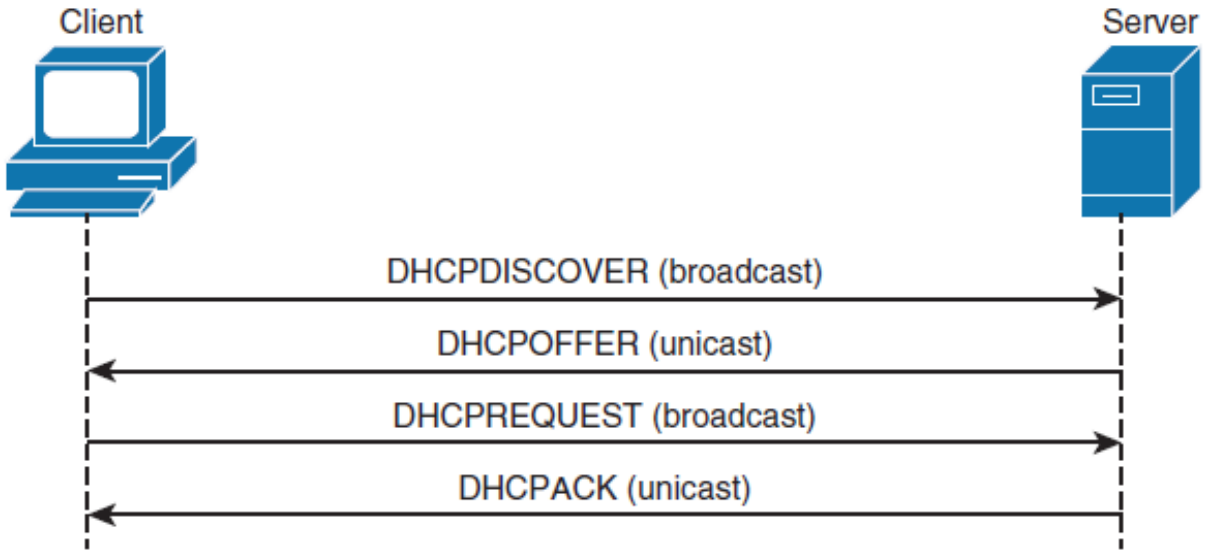
anebo

- DSW1(dhcp-config)# **hardware-address *MAC-address***

Konfigurace DHCP v Multilayer Switched síti

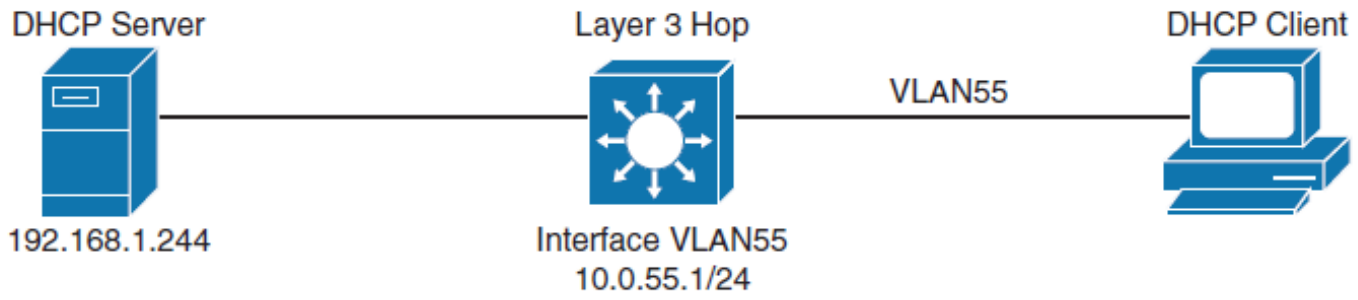
Command	Description
ip dhcp excluded-address *start-ip end-ip*	If there are addresses within the IP subnet that should not be offered to DHCP clients, this command will make sure that the specified addresses are not offered. In the example, 10.0.10.1 was excluded from the DHCP pool because this is the IP address of the Layer 3 interface on DSW1.
ip dhcp pool *pool-name*	The *pool-name* parameter defines a DHCP pool. Using this command, you enter the DHCP pool configuration mode.
network *ip-address subnet-mask*	Specifies the address range through IP subnet and subnet mask. The network command will bind the DHCP server to matching Layer 3 interface. In the example, DHCP server VLAN10POOL is bound to VLAN 10 interface. Broadcast and network IPs are not offered to clients. You can assign multiple subnets per pool.
default-router ip-address [*ip-address2*] [*ip-address3*] ...	Sets the default router address that will be offered to clients. In the example, this is the IP address of the Layer 3 interface on the switch.
lease {infinite | {days [hours [minutes]]}}	Sets IP address lease duration. By default, the IP address is leased to a client for 1 day. In the example, it is set to 2 days.

Proces DHCP Discovery



- **DHCPDECLINE:** Adresa je již použita.
- **DHCPNAK:** Server odmítá potvrzení.
- **DHCPRELEASE:** Klient informuje server o tom, že se vzdává použití přidělené adresy.
- **DHCPINFORM:** Klient žádá jiné parametry.

Konfigurace DHCP Relay



Klient ve VLAN 55 potřebuje forwardovat DHCP broadcasty k centralizovanému serveru 192.168.1.244:

- Multilayer switch má L3 IP adresu 10.0.55.1/24, na které přijme DHCP požadavek. Tato adresa může být routed port SVI.
- **ip helper-address** Požadavek přijde jako broadcast a odejde jako unicast.

Příkaz **ip helper-address** nejen přeposílá DHCP UDP pakety, ale také přeposílá defaultní pakety TFTP, DNS, time, NetBIOS, name server, a BOOTP.

Konfigurace DHCP Options

- Použití DHCP voleb k „rozšíření“ příkazů DHCP.
  - **Option 43**: Možnost zapouzdření dodavatele, která umožňuje dodavatelům, aby měli vlastní seznam možností na serveru. Můžete jej například použít k určení lehkého přístupového bodu, kde je Wireless LAN Controller (WLC).

    Příklad: **option 43 ascii “10.126.126.2,10.127.127.2”** (dva WLC)
  - **Option 69**: SMTP server, chcete-li klientovi zadat dostupné servery SMTP.
  - **Option 70**: POP3 server, chcete-li klientům zadat dostupné servery POP3.
  - **Option 150**: server TFTP, který umožňuje telefonům přístup k seznamu serverů TFTP.

```
Switch(config)# ip dhcp pool TELEPROFILES
Switch(dhcp-config)# options 150.10.10.1
```

Tři kategorie formátů adres

- **Statické adresy** zůstávají v provozu po dlouhou dobu, jako např. v modifikovaném formátu EUI-64 a staticky přiřazených adresách.
- S**emistatické adresy,** které vyžadují za určitých okolností specifikace změny - tyto se však v praxi vyskytují zřídka. Patří sem sémanticky neprůhledné identifikátory rozhraní a kryptograficky generované adresy.
- **Dynamické adresy** jsou ty, které se mění pravidelně, např. každý den. V současné době tato skupina formátů adres zahrnuje pouze privacy extension IPv6.

Semistatické a dynamické formáty adres jsou určeny pro klienty, zatímco servery mají tendenci používat výhradně statickou adresu.

Privacy extension – RFC 4941 (2007)

- Je to formát definující dočasné adresy, které se mění v pravidelných časových intervalech; po sobě jdoucí adresy se navzájem neshodují pro cizí uživatele a jsou prostředkem ochrany proti korelování adres. Jejich pravidelná změna je nezávislá na prefixu sítě; Tímto způsobem chrání proti sledování pohybu a také proti časové korelaci.
- Protivník je může získat vnitřní stav algoritmu přes postranní kanál, a předpovídat všechny budoucí adresy hostitele. Proto operační systémy implementující rozšíření IPv6 Privacy Extension používají namísto toho náhodná čísla adres, protivník nyní musí najít (náhodnou nebo pseudonáhodnou) dočasnou adresu namísto statické, což je náročnější úkol.

Semantically Opaque Interface ID – RFC 7217 (2014)

- Důvodem tohoto mechanismu je získat stabilní identifikátory rozhraní pro předponu, aby se snížila administrativní zátěž při zachování určité úrovně ochrany soukromí v jiné síti. **Tyto IID jsou generovány hashováním síťového prefixu, tajného klíče a různých dalších parametrů**. Tímto způsobem se identifikátor rozhraní změní při přechodu na jinou předponu sítě; při návratu do původní sítě se však vrátí na stejnou hodnotu.
- Sémanticky neprůhledné IID **zabraňují korelaci adres** a zejména sledování pohybu, pokud je tajný klíč neznámému protivníkovi neznámý. Nechrání však před časovou korelací, tj. protivník je schopen připsat transakce v různých časových bodech jedinému (stacionárnímu) hostiteli. Pro ochranu před takovými hrozbami jsou zapotřebí dynamická schémata adres, jako je rozšíření ochrany soukromí IPv6.
- Sémanticky neprůhledné identifikátory rozhraní jsou z hlediska síťového skenování určeny k tomu, aby se náhodně zobrazovaly z vnějšího pohledu a jejich nalezení by mělo zůstat zdlouhavým úkolem; jeho kvalita je však závislá na konkrétní implementaci. V současné době RFC 8064 doporučuje identifikátory sémanticky opaque rozhraní jako výchozí stabilní identifikátory namísto formátu Modified EUI-64.

Kryptograficky generované adresy – RFC 3972

- Kryptograficky generované adresy jsou generovány hašováním veřejného klíče hostitele s jinými parametry a jsou tedy vázány na příslušného hostitele.
- Jejich **vlastnictví je ověřeno podpisem zpráv vzniklých z této adresy příslušným privátním klíčem**. V kombinaci to zabraňuje spoofingu adres a bylo zamýšleno k ochraně před útoky pocházejícími z lokální sítě. Z hlediska ochrany soukromí jsou tyto adresy srovnatelné se sémanticky opaque IID: protože předpona sítě je zahrnuta do hash, adresa je změněna při přesunu do jiné sítě. Kromě toho může být nová adresa vytvořena bez pohybu; to by umožnilo ochranu před časovou korelací srovnatelnou s rozšířením ochrany soukromí IPv6.
- Vytváření kryptograficky generovaných adres je však nákladné a v důsledku toho brání častým změnám adresy v praxi. Pokud jde o skenování, tento typ adres se jeví z pohledu protivníka jako náhodný , který poskytuje účinnou ochranu.
- Kryptograficky generované adresy (stejně tak Secure Neighbor Discovery – SeND) nejsou podporovány žádným z hlavních operačních systémů, a to je jejich největší potíží.

Co z toho plyne pro budoucnost a praxi

- Budoucí internetová zařízení již nelze striktně klasifikovat do dvou rolí serveru a klienta: existují servery, např. brány zařízení IoT, které slouží pouze velmi omezené skupině uživatelů, např. obyvatelům domácnosti, a také potřebují nějakou formu ochrany soukromí. Například adresy serverů se mohou stát dočasnými a mohou být odvozeny ze sdíleného tajemství. Legitimní klient je schopen vypočítat aktuální adresu, protože má tajemství, zatímco protivník by musel vyčerpávajícím způsobem prohledat síť, aby našel server. Dále, protokoly typu peer-to-peer, jako je bitcoin, by mohly využít podobné mechanismy.

- Zařízení pro připojení k internetu musí přiřadit adresu. Bylo by moudré je definovat v nejbezpečnějším a nejbezpečnějším způsobem, aby byla zajištěna co největší ochrana. Tento aspekt je obzvláště zajímavý pro omezená zařízení, jako je internet věcí, protože pro výkonná ochranná opatření obvykle nemají dostatek výpočetního výkonu. Flexibilita adresování IPv6 je proto velkou příležitostí, kterou je třeba využít.

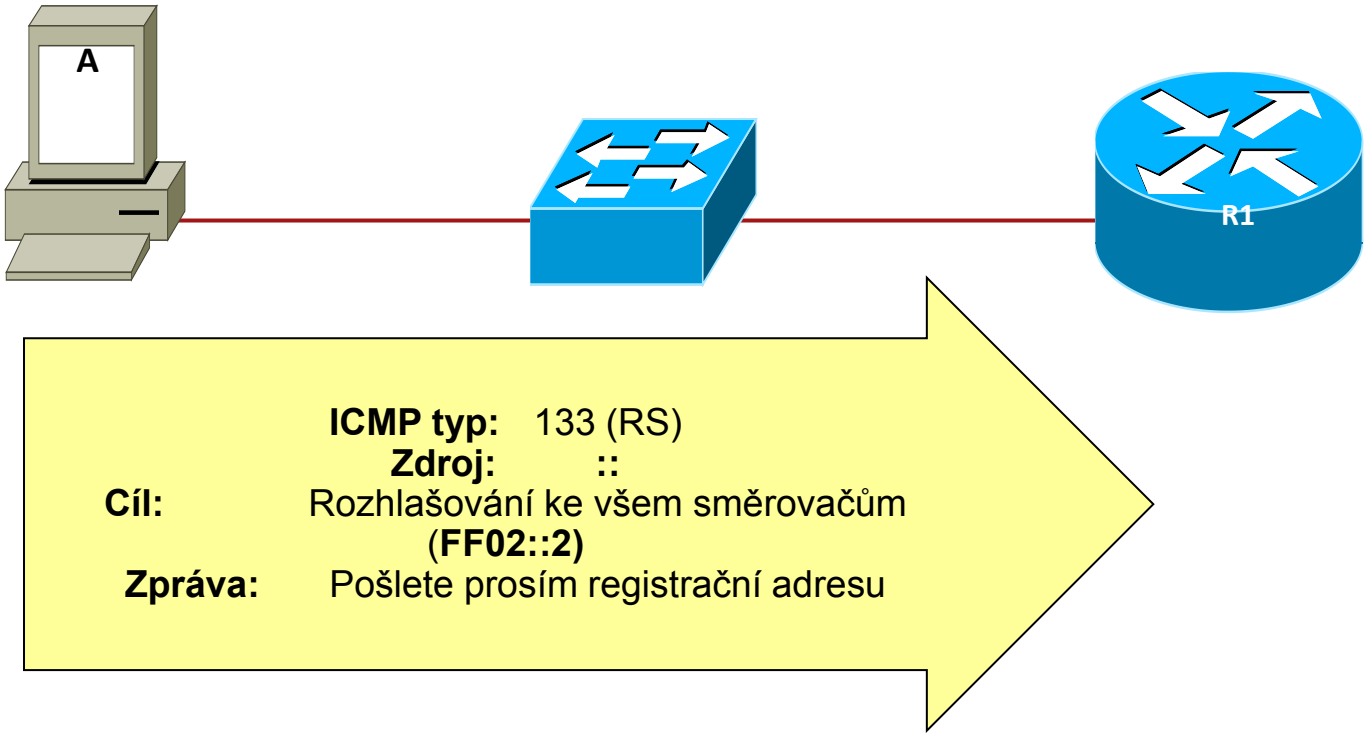
Chapter 5 Labs

- **CCNPv7.1 SWITCH Lab5.1 IVL-ROUTING**
- **CCNPv7.1 SWITCH Lab5.2 DHCP4/6**

Které zprávy používá SLAAC?

- Od klienta:
- Od serveru:

Bezestavová autokonfigurace

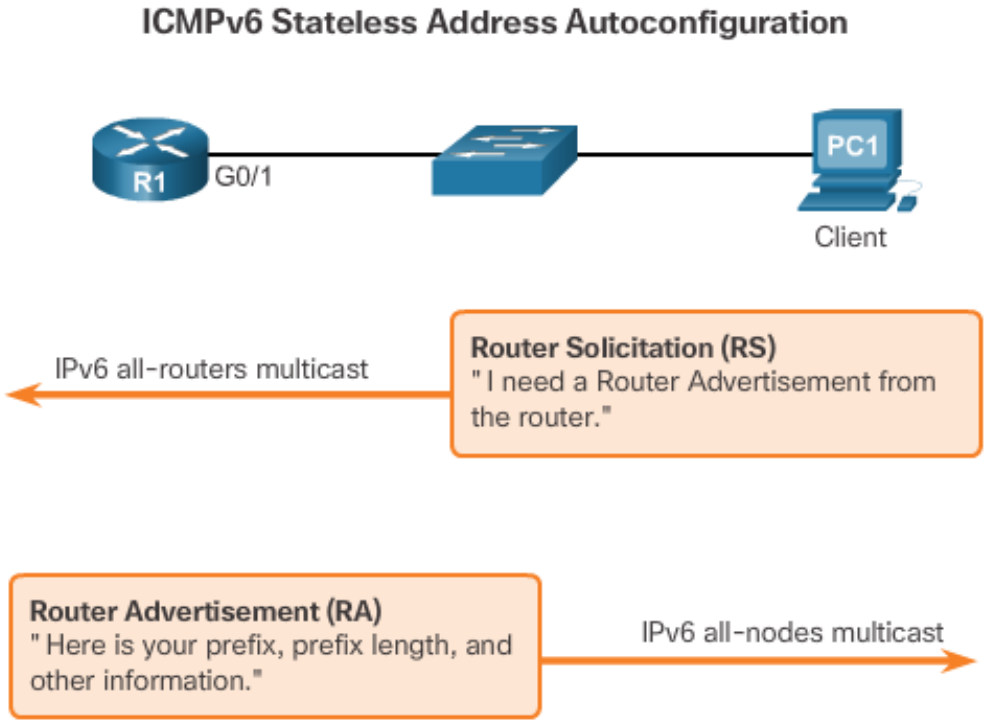


Směrovače také registrační adresy rozesílají periodicky, zde se její přidělení pouze urychluje

Stateless Address Autoconfiguration (SLAAC)

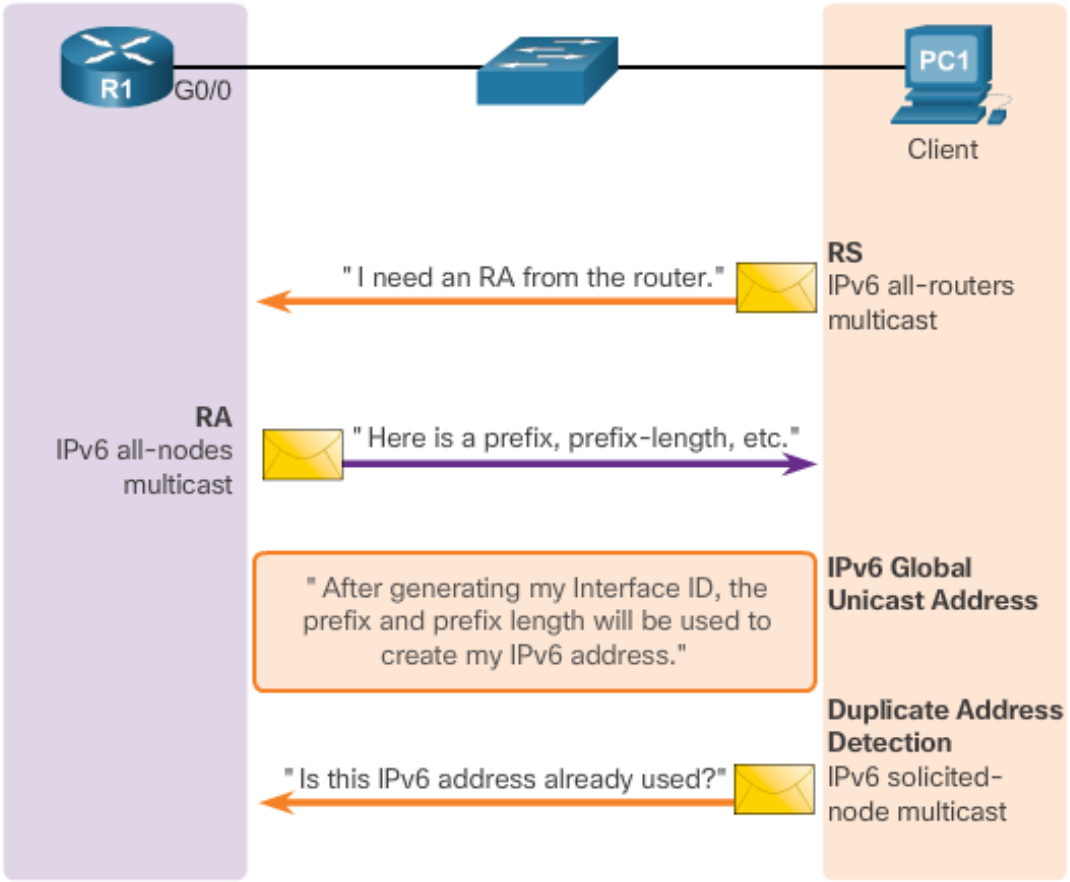
SLAAC používá dvě zprávy:

- ICMPv6 Router Solicitation (od klienta)
- Router Advertisement (od DHCP serveru: prefix, délku prefixu atd.)

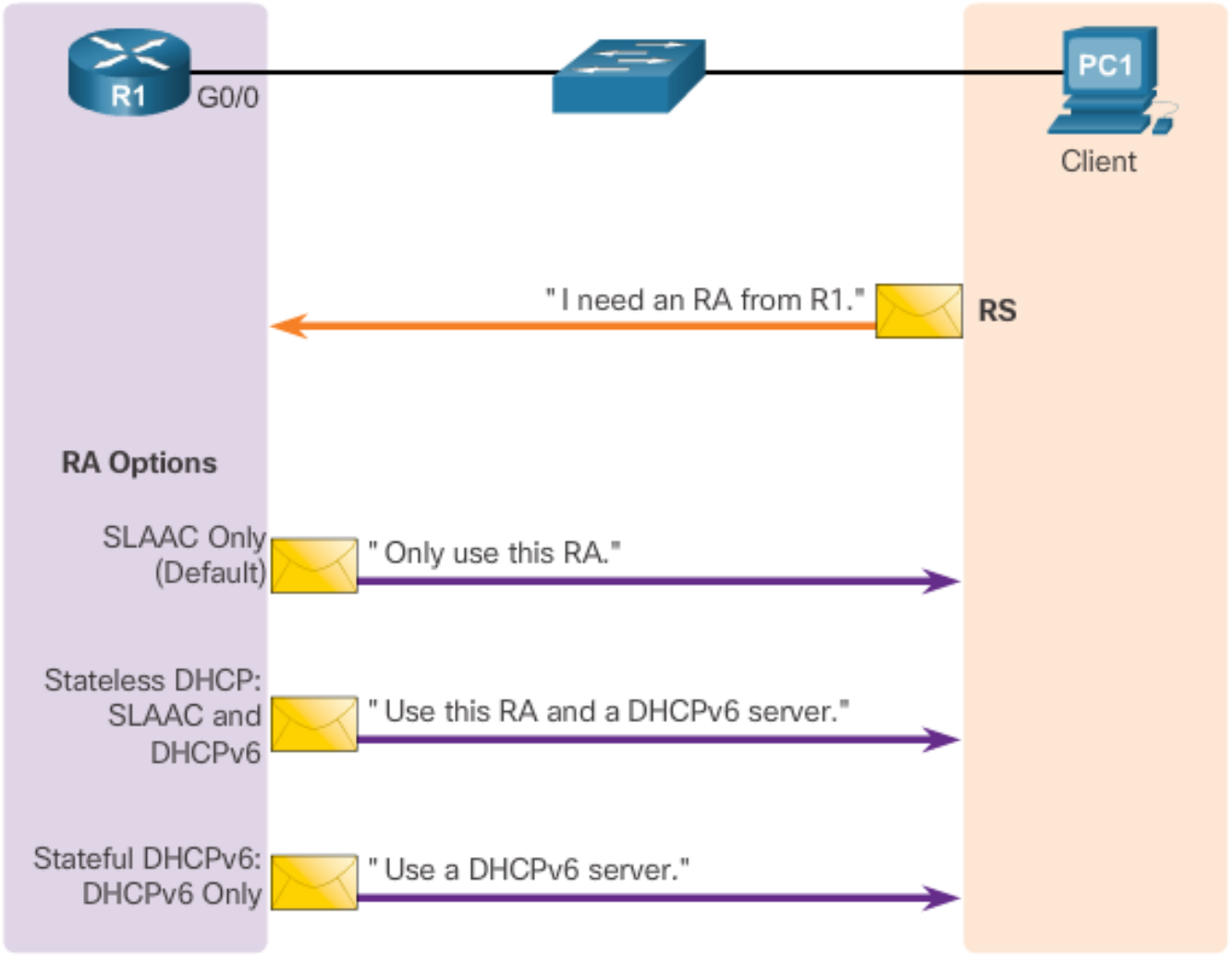


Čtyři kroky operace SLAAC

- Před poslání RA zprávy musí mít router nastaven IPv6 routing: Router(config)# **`ipv6 unicast-routing`**

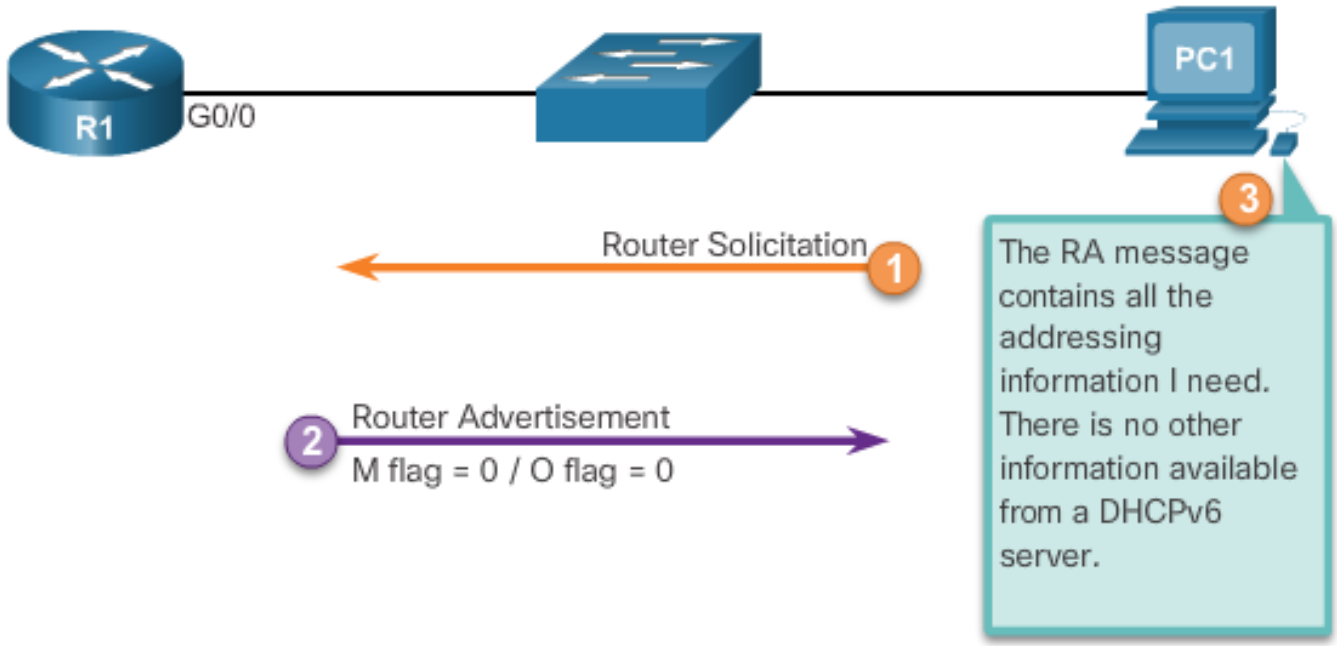


Tři varianty SLAAC



Jak funguje SLAAC defaultně: Stateless

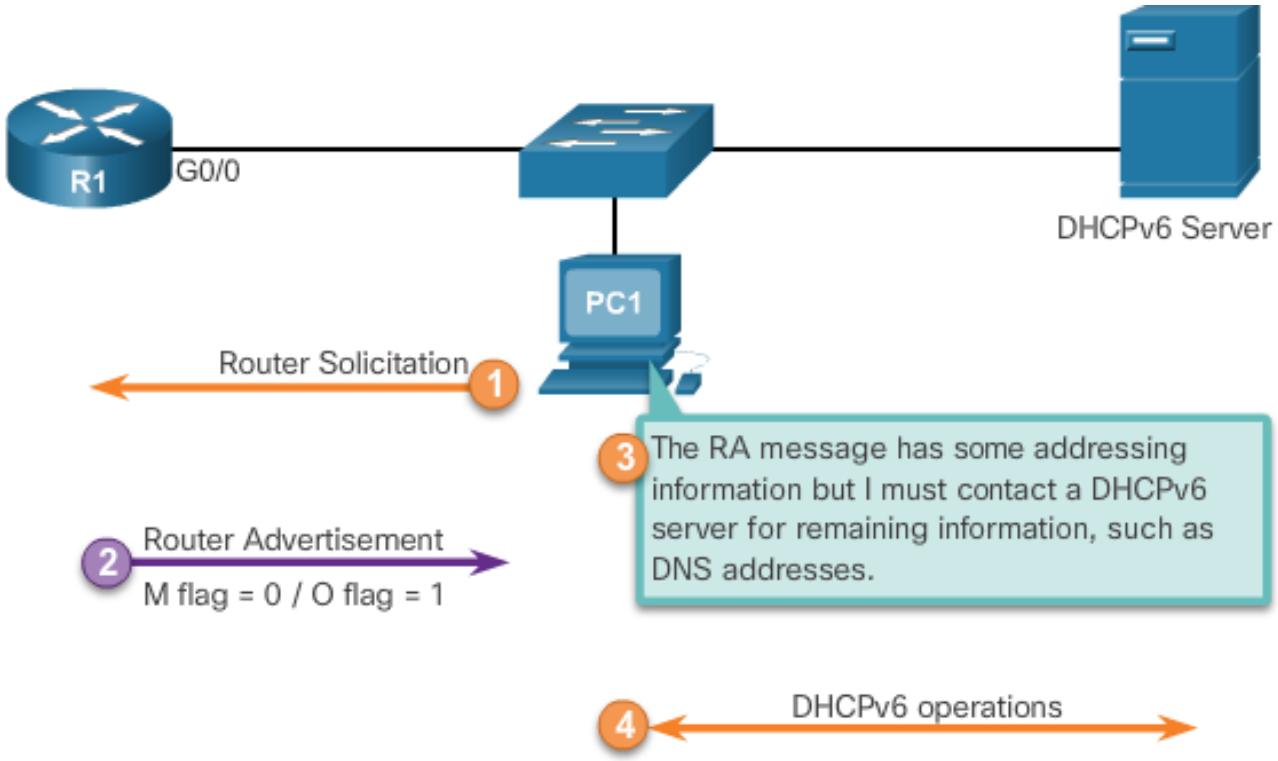
- Příznaky M (managed) a O (other) jsou nastaveny v RA na 0.



Stateless DHCPv6 volba

- Vezmi informaci ještě jinde:

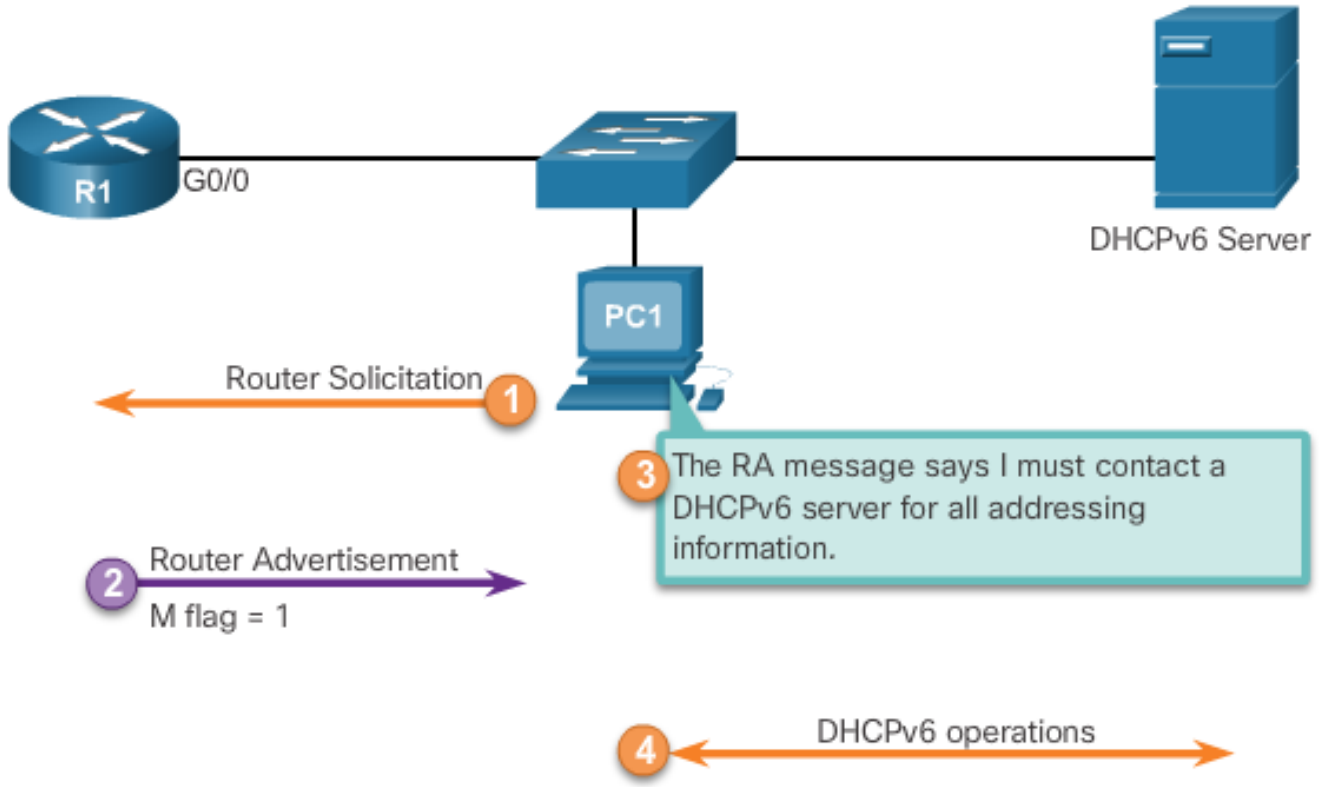
Router(config-if)# `ipv6 nd other-config-flag`



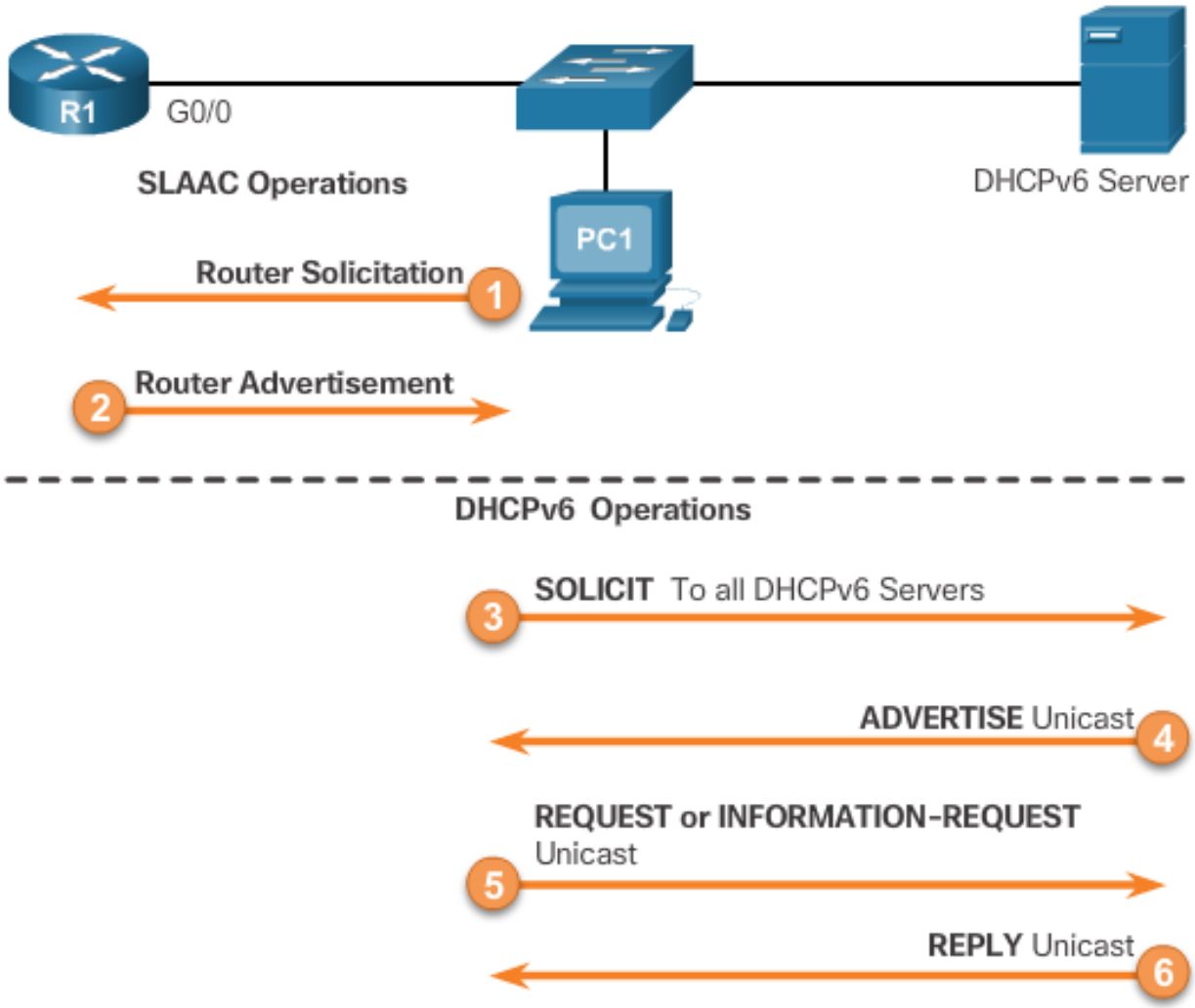
Stateful DHCPv6 volba (podobná DHCPv4)

- Zpráva RA říká: neber informaci ode mne, ale od stateful DHCPv6 serveru.

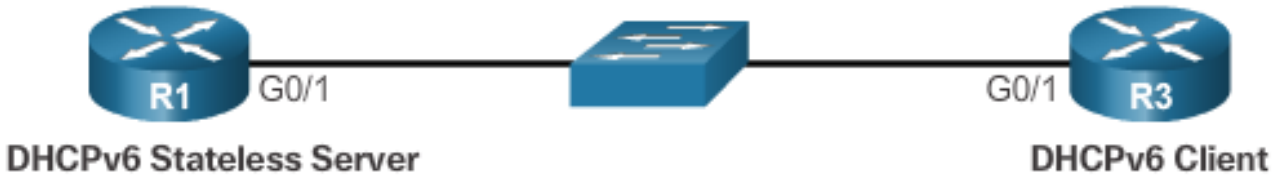
  Router(config-if)# `ipv6 nd managed-config-flag`



A pak už běží standardní čtyřfázový proces

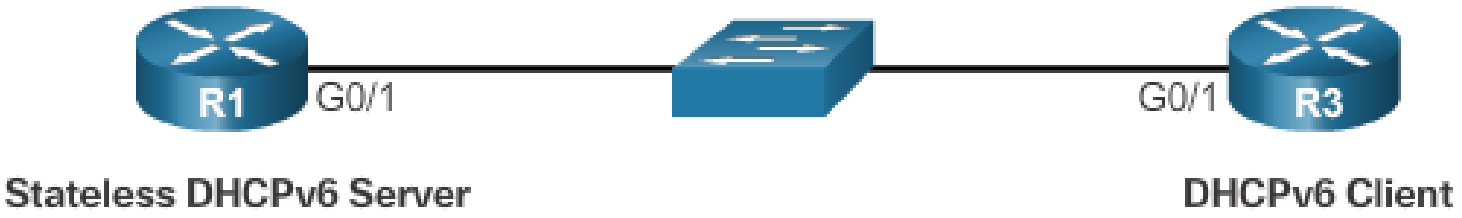


Konfigurace routeru jako Stateless DHCPv6 serveru



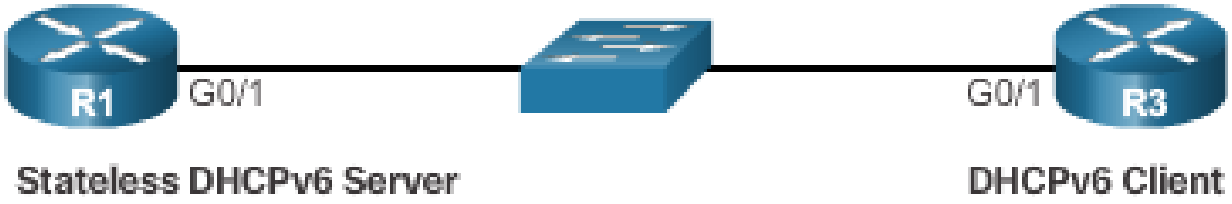

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATELESS
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server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

Konfigurace routeru jako Stateless DHCPv6 klienta




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

Verifikace Stateless DHCPv6




```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6-STATELESS
  DNS server: 2001:DB8:CAFE:AAAA::5
  Domain name: example.com
  Active clients: 0
R1#
```

Příkazy:

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

Konfigurace routeru jako Stateful DHCPv6 serveru

Step 1. Enable IPv6 Routing

```
Router(config)# ipv6 unicast-routing
```

Step 2. Configure a DHCPv6 Pool

```
Router(config)# ipv6 dhcp pool pool-name
Router(config-dhcpv6)#
```

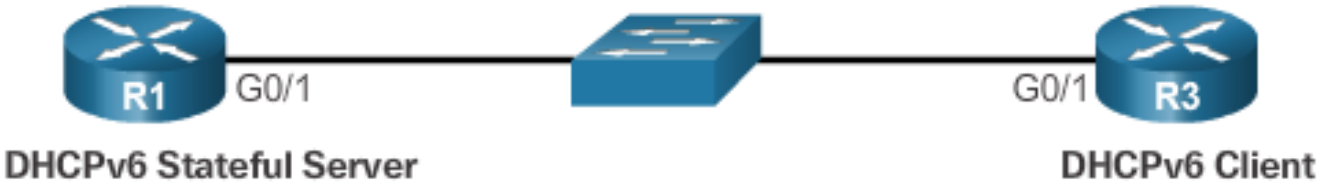
Step 3. Configure Pool Parameters

```
Router(config-dhcpv6)# address prefix/length [lifetime
                       {valid-lifetime preferred-lifetime
                       | infinite}]
Router(config-dhcpv6)# dns-server dns-server-address
Router(config-dhcpv6)# domain-name domain-name
```

Step 4. Configure the DHCPv6 Interface

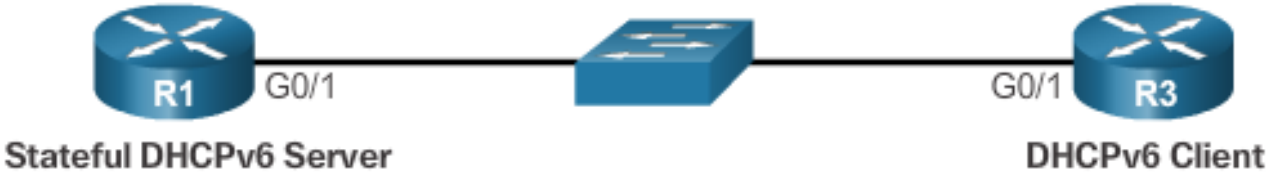
```
Router(config)# interface type number
Router(config-if)# ipv6 dhcp server pool-name
Router(config-if)# ipv6 nd managed-config-flag
```

Příklad konfigurace Stateful DHCPv6 serveru




```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATEFUL
R1(config-dhcpv6)# address prefix 2001:DB8:CAFE:1::/64
                    lifetime 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
```

Konfigurace routeru jako Stateful DHCPv6 klienta




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

Verifikace Stateful DHCPv6 1/2

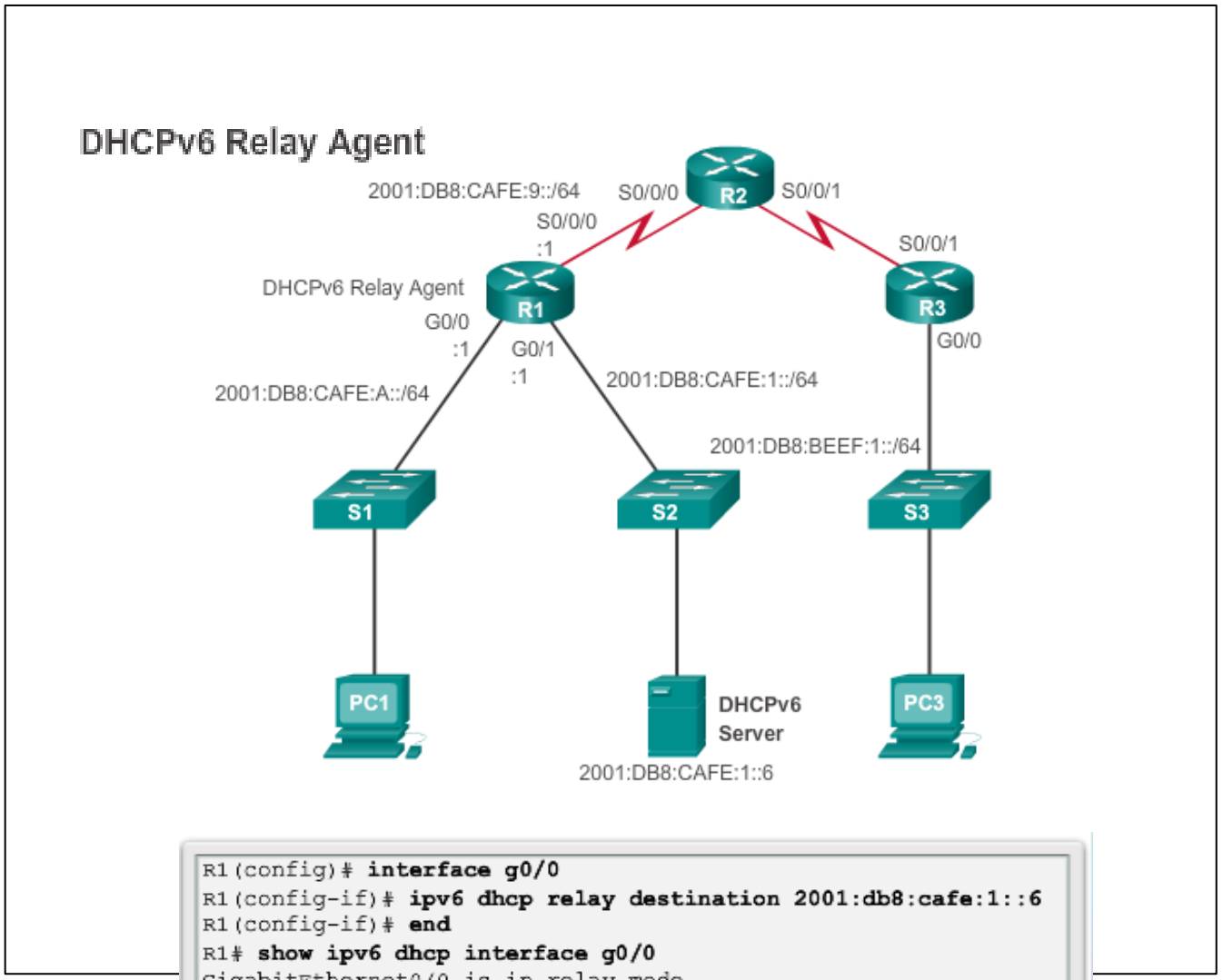

```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6-STATEFUL
  Address allocation prefix: 2001:DB8:CAFE:1::/64 valid
4294967295 preferred 4294967295 (1 in use, 0 conflicts)
  DNS server: 2001:DB8:CAFE:AAAA::5
  Domain name: example.com
  Active clients: 1
R1#
```

```
R1# show ipv6 dhcp binding
Client: FE80::32F7:DFF:FE25:2DE1
  DUID: 0003000130F70D252DE0
  Username : unassigned
  IA NA: IA ID 0x00040001, T1 43200, T2 69120
    Address: 2001:DB8:CAFE:1:5844:47B2:2603:C171
            preferred lifetime INFINITY, , valid lifetime
INFINITY,
R1#
```

Verifikace Stateful DHCPv6 2/2

```
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
  GigabitEthernet0/1
R3#
```

Konfigurace routeru jako DHCPv6 Relay agenta




```
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
R1#
```

Tak to RS si rozebereme podrobněji a v souvislostech

1. RS – Router Solicitation: klient žádá o adresní informaci

2. RA – Router Advertisement: Router odpovídá a sdělí jeden ze tří způsobů způsob volby

Jsou tři volby

- RA Option 1: Jen SLAAC – vše, co klient potřebuje, dostane rovnou ve 2. kroku od routeru (prefix, jeho délku, defaultní bránu) a tím to končí.
- RA Option 2: SLAAC a DHCPv6: Gateway klient získá od routeru, na údaj o DNS se ptá všech serverů DHCPv6.
- RA Option 3: Router klientovi sděluje, že veškeré informace získá od DHCPv6.

Bity M a O

- ‘M’ bit - Příznak (flag) "Managed address configuration" DHCPv6. Je použito jen DHCP.
- ‘O’ bit - "Other configuration" flag. M se pak obvykle rovná 0.

Možné varianty bitů M a O

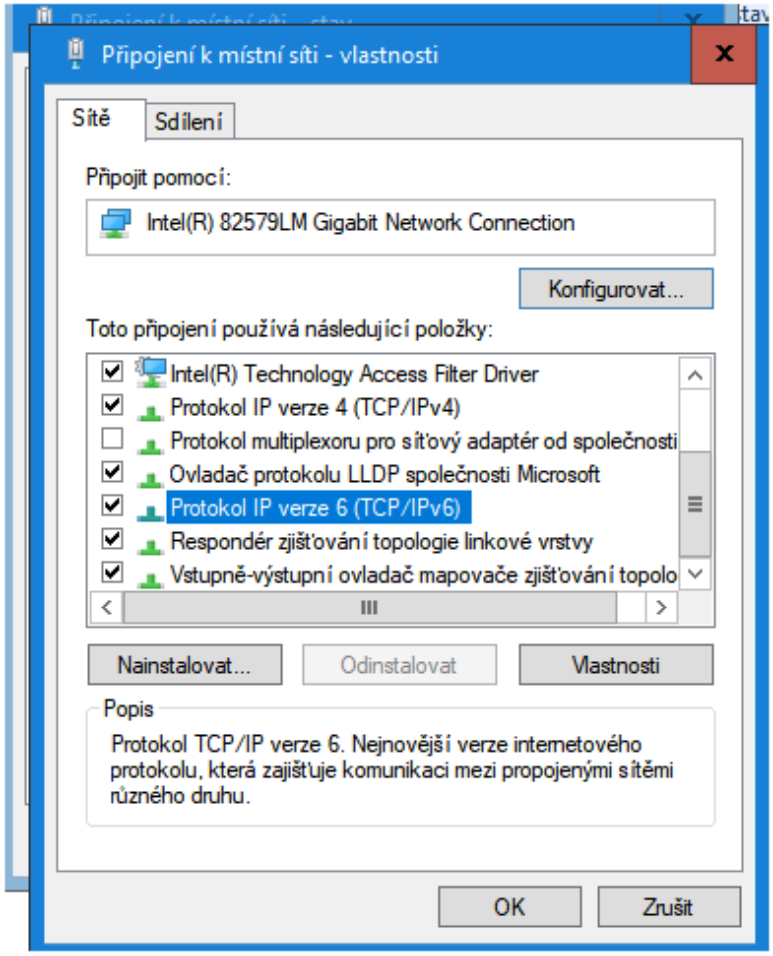
M = 0, O = 0 : Klient používá RA pro získání non-link-local adresy i dalších informací. V případě, že DHCPv6 server existuje, client ho ignoruje.

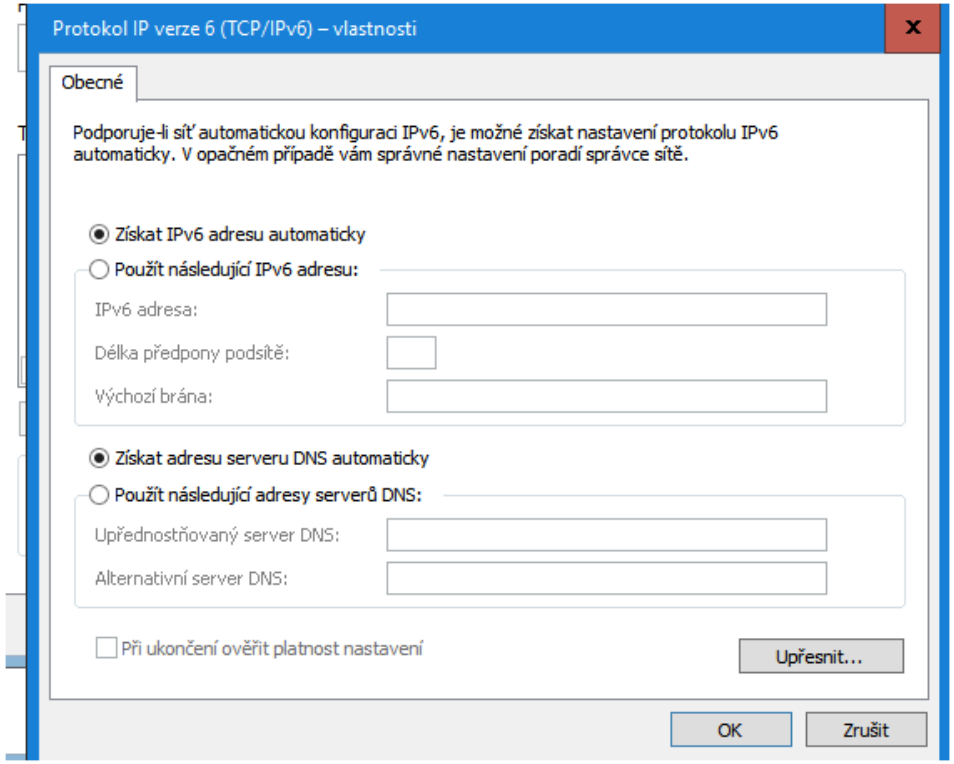
M = 0, O = 1 : Klient používá gateway adresu od RA, DHCPv6 poskytne to ostatní. Tato kombinace je označována jako DHCPv6 stateless.

M = 1, O = 0 : Klient používá DHCPv6 jak pro adresu routeru, tak pro ostatní konfigurační údaje. Tato kombinace je známa jako DHCPv6 stateful.

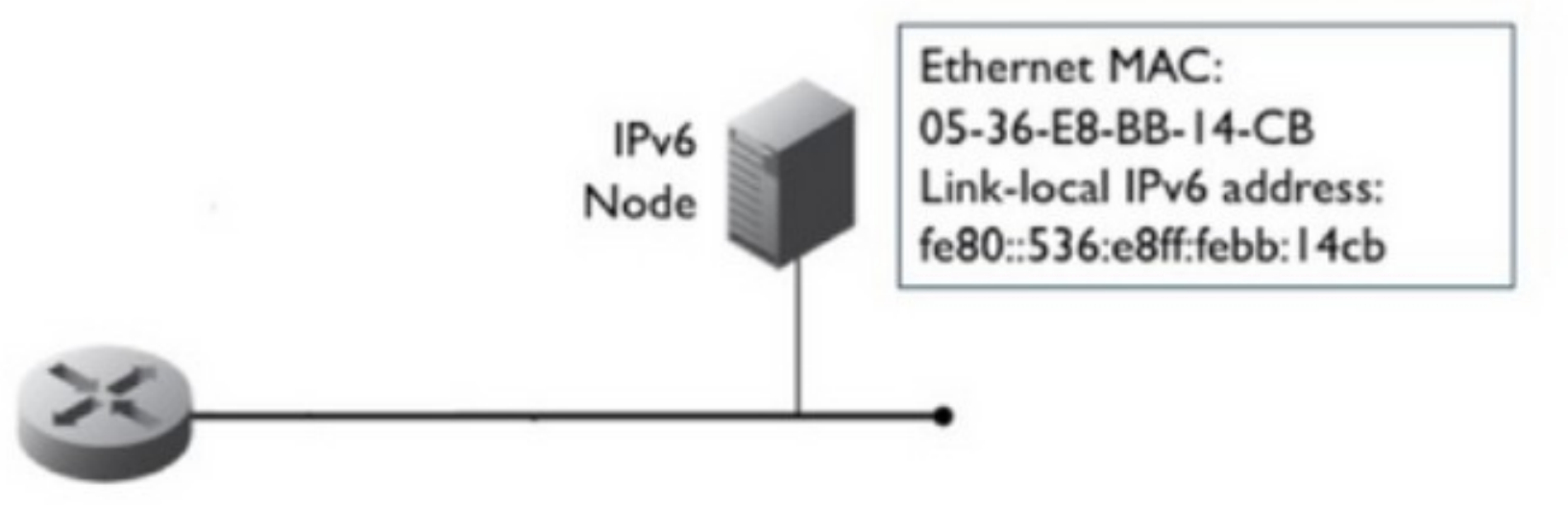
M = 1, O = 1 DHCPv6 klientu poskytuje plnou informaci zvanou stateful address. Pokud RA obsahuje prefix sítě, client navíc dostane stateless informaci od routeru (zbytečně).

Na klientovi přitom nemusíme nic dělat – jen říci, že má nastavit OPv6 adresu automaticky





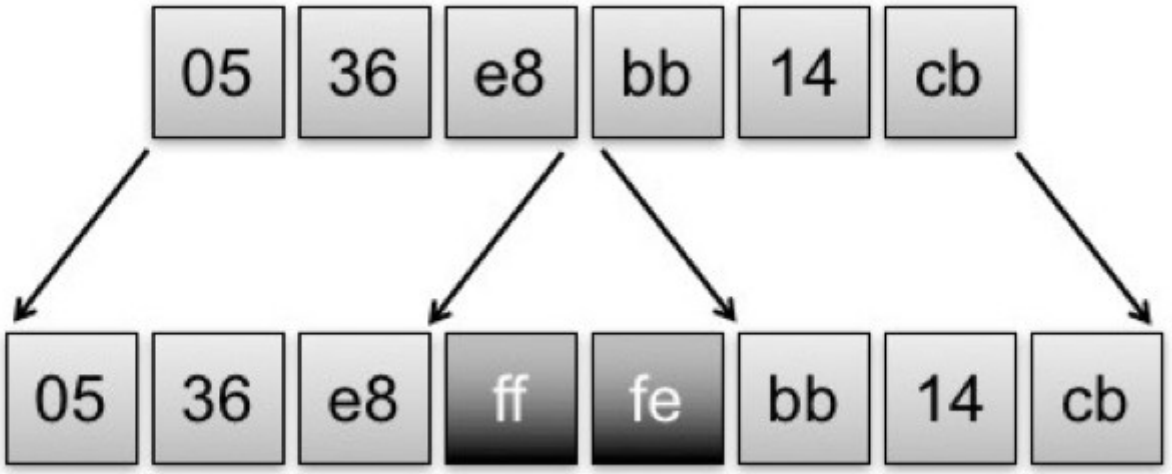
1. Uzel si sám generuje svoji IPv6 adresu (odvodil si ji ze své MAC adresy použitím metody EUI DII)



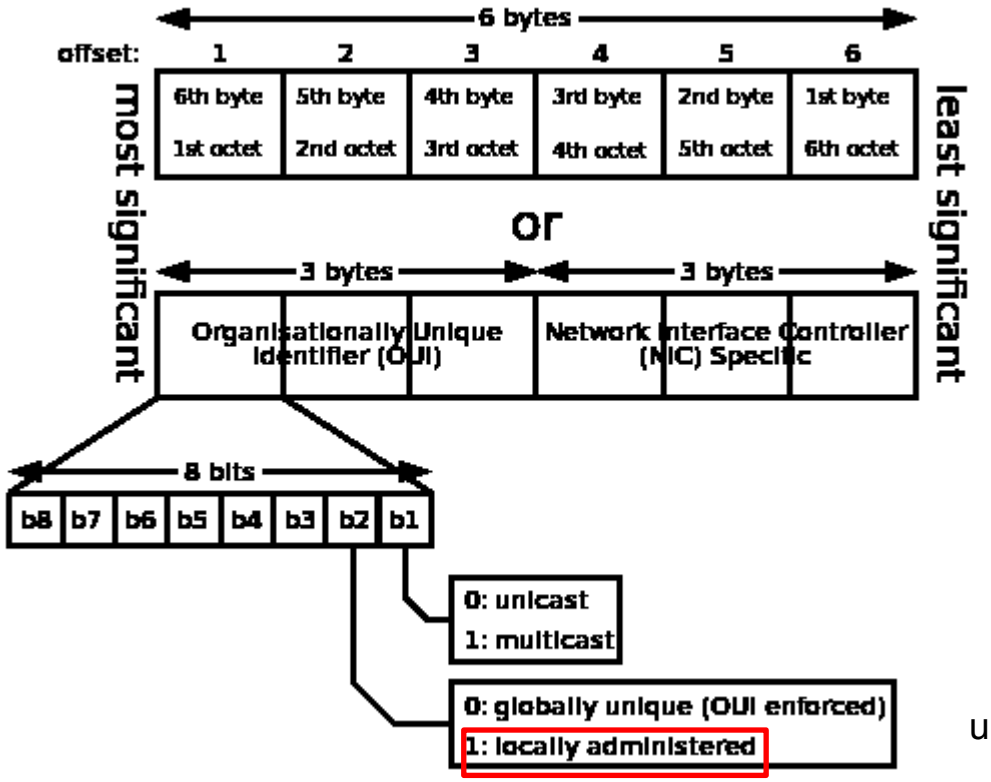
Blíže RFC 4291

1a. krok SLAAC:
použití MAC adresy klienta o 48 bitech

1b. krok SLAAC:
vložení FFFE doprostřed MAC adresy

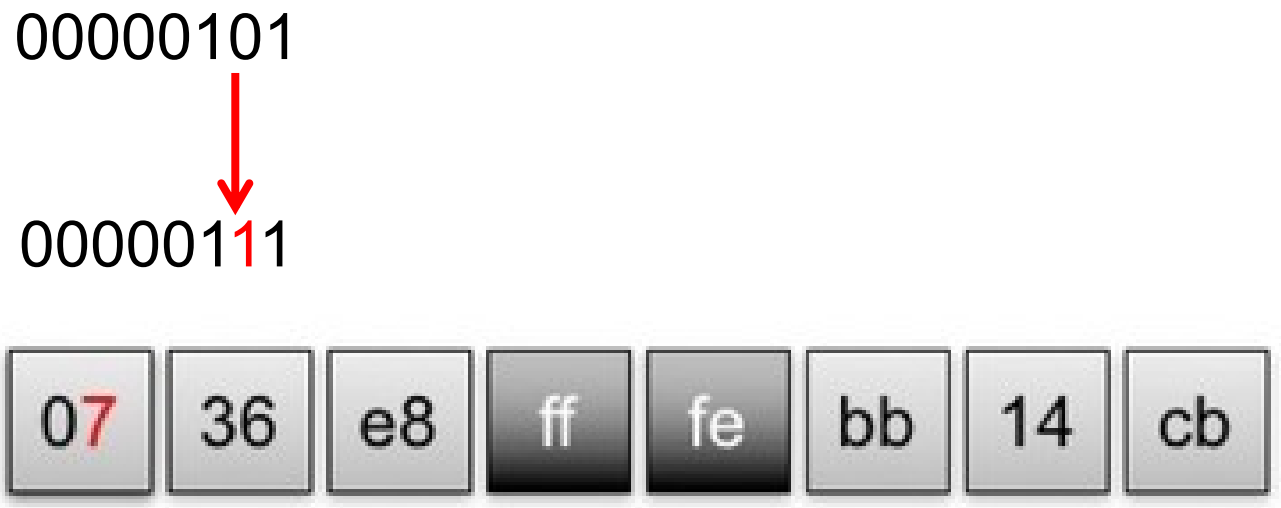


Jaká je struktura MAC adresy?
7. bit = 1… lokální administrace



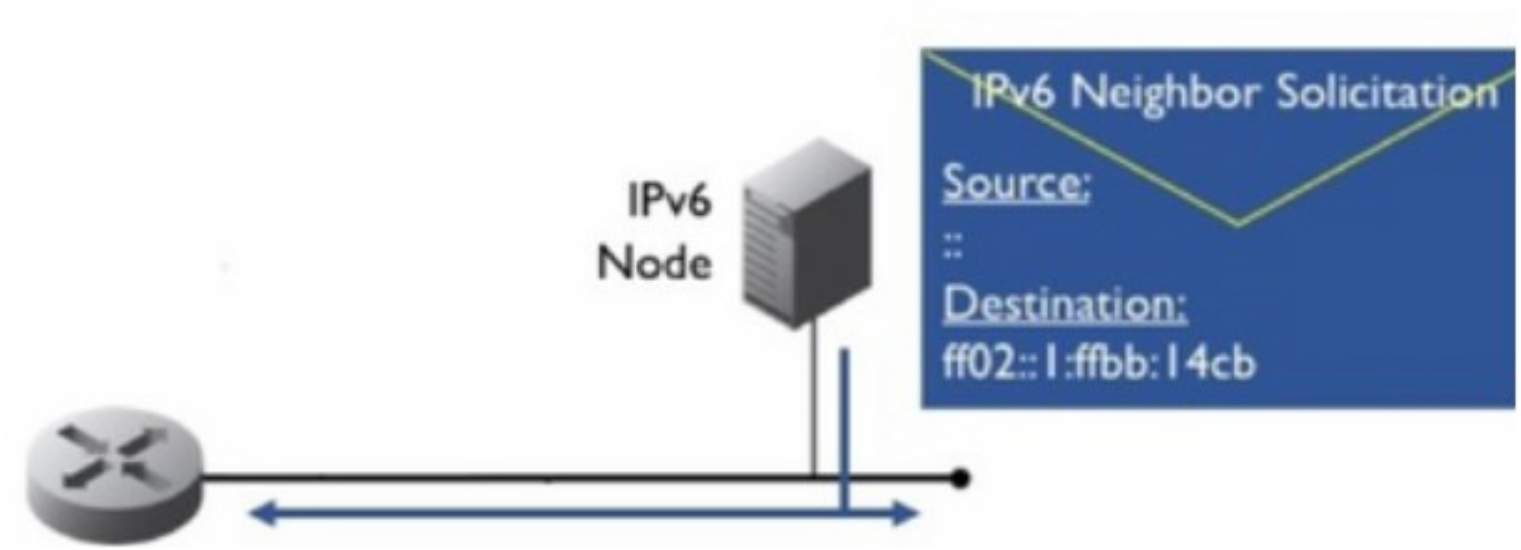
universal/local

1c. krok SLAAC:
Vsunuté 1 do 7. bitu záhlaví

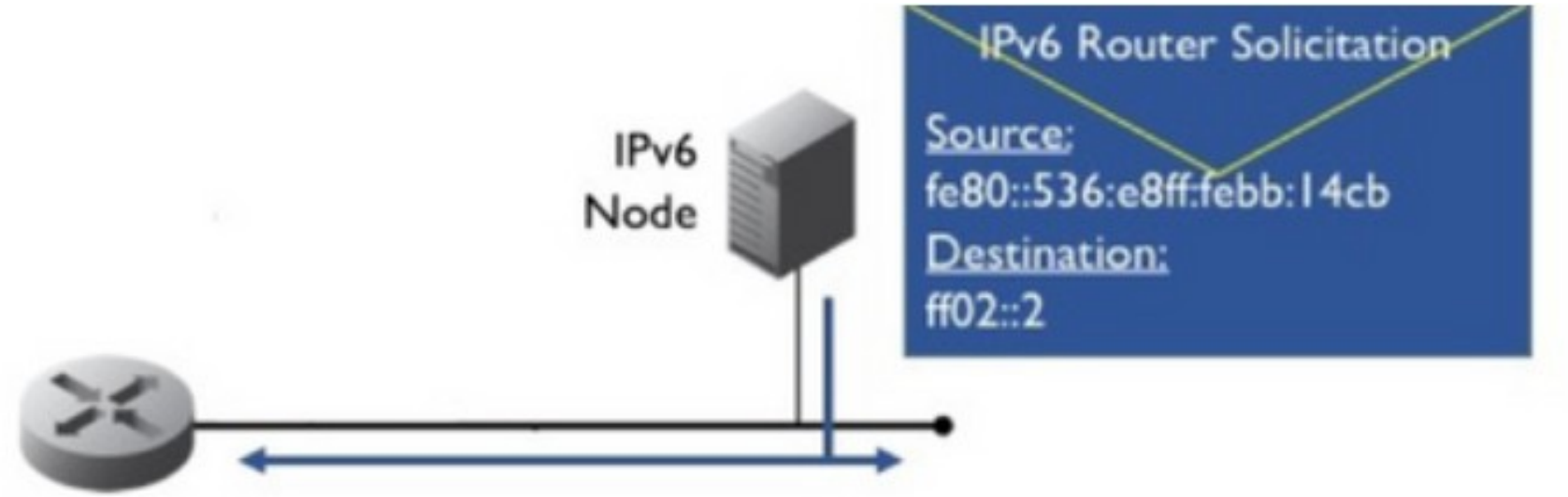


1d. krok SLAAC:
Spojení prefixu lokální IP adresy a upravené MAC adresy

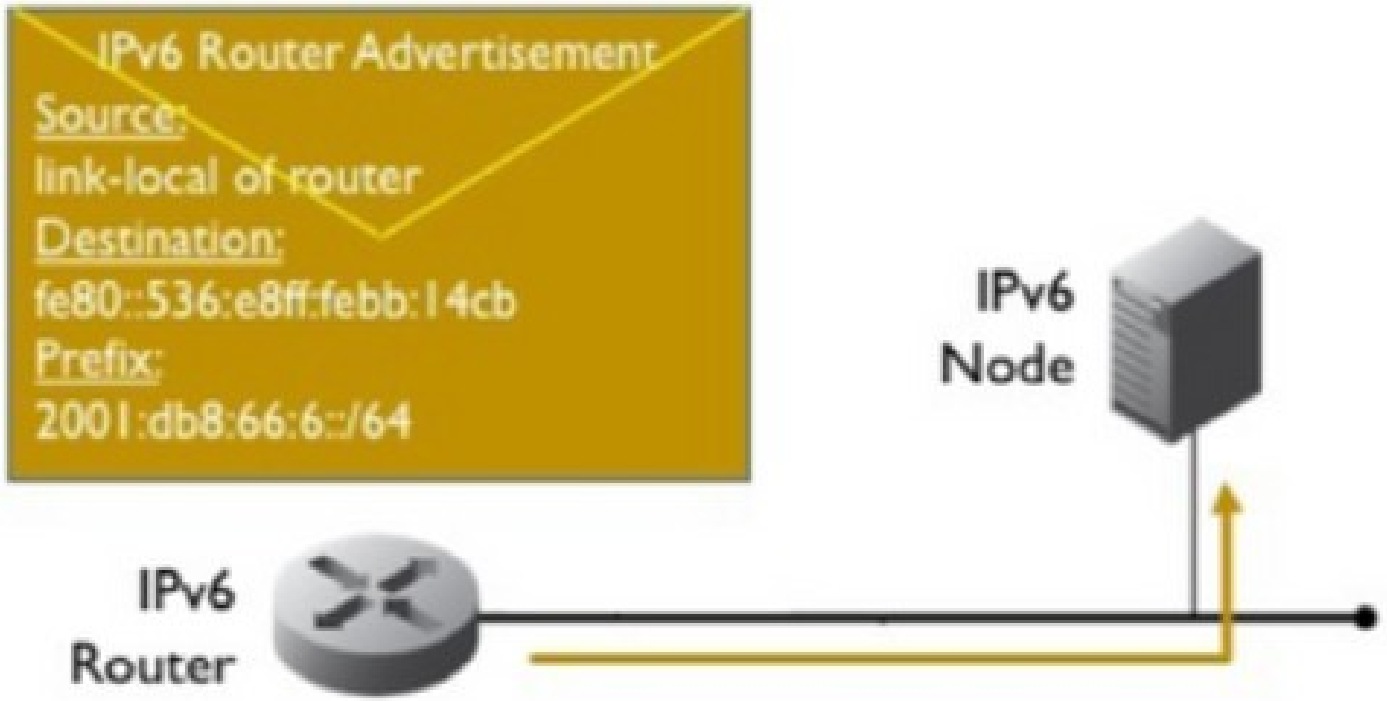
2. Uzel nyní detekuje, zda si nevygeneroval duplicitní adresu pomocí výzvy Neighbour Solicitation na adresu Solicited Mode Multicast



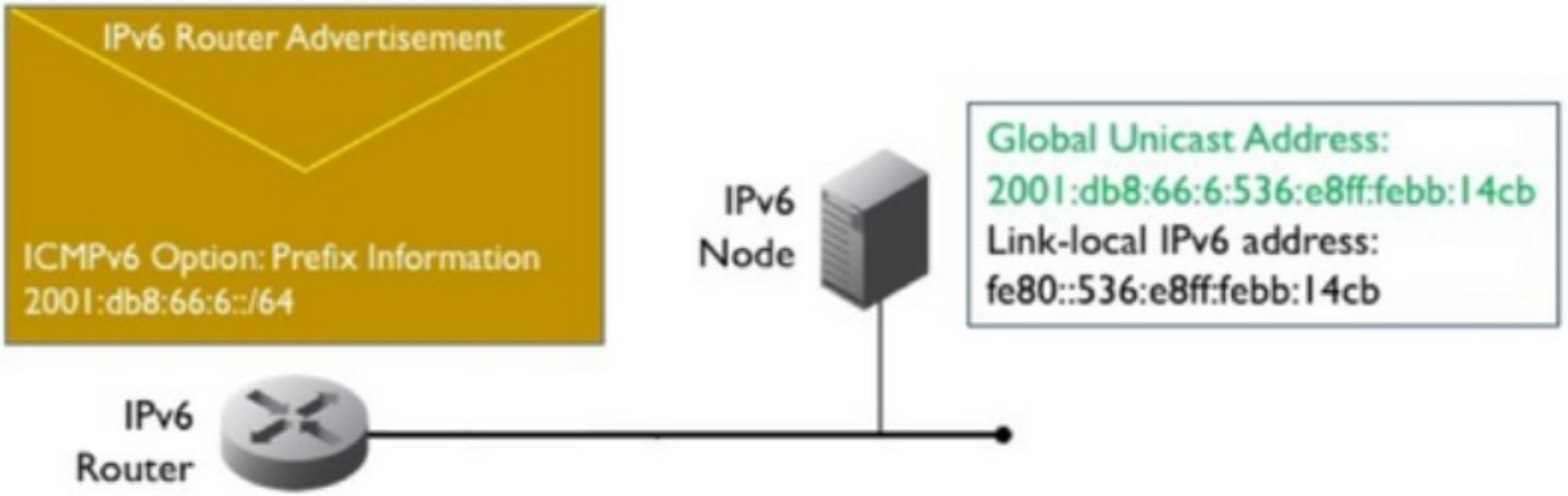
3. Uzel nedostal odpověď a tak oslovuje router se svojí nově vygenerovanou adresou – posílá zprávu Router Solicitation



4. Router posílá unicast Router Advertisement a předává uzlu prefix



5. Uzel připojí prefix ke své lokální adrese



Krok 1/3: Případ M=0, O=1 (ipv6 nd other-config-flag). Nabídka routeru (router advertisement)

```
⊞ Ethernet II, Src: ArubaNet_00:06:d0 (00:1a:1e:00:06:d0), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
⊞ Internet Protocol Version 6, Src: fe80::1a:1e00:6400:6d0 (fe80::1a:1e00:6400:6d0), Dst: ff02::1 (ff02::1)
⊟ Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0x361b [correct]
    Cur hop limit: 64
  ⊟ Flags: 0x40
      0... .... = Managed address configuration: Not set
      .1.. .... = Other configuration: Set
      ..0. .... = Home Agent: Not set
      ...0 0... = Prf (Default Router Preference): Medium (0)
      .... .0.. = Proxy: Not set
      .... ..0. = Reserved: 0
    Router lifetime (s): 1800
    Reachable time (ms): 0
    Retrans timer (ms): 0
  ⊟ ICMPv6 Option (Prefix information : 2001:1234::/64)
      Type: Prefix information (3)
      Length: 4 (32 bytes)
      Prefix Length: 64
    ⊞ Flag: 0xc0
      Valid Lifetime: 86400
      Preferred Lifetime: 14400
      Reserved
      Prefix: 2001:1234:: (2001:1234::)
  ⊟ ICMPv6 Option (Recursive DNS Server 2001:1234::14)
      Type: Recursive DNS Server (25)
      Length: 3 (24 bytes)
      Reserved
      Lifetime: 1200
      Recursive DNS Servers: 2001:1234::14 (2001:1234::14)
  ⊞ ICMPv6 Option (Source link-layer address : 00:1a:1e:00:06:d0)
```

Krok 2/3: Protože M = 0 , klient použije Stateless Address Autoconfiguration (SLAAC) pro získání své IPv6 adresy, a protože O = 1, požaduje od DHCPv6 serveru informaci o DSM a případně další specifické informace, které výrobce poskytuje.

```
⊞ Ethernet II, Src: Foxconn_7e:3f:32 (00:15:58:7e:3f:32), Dst: IPv6mcast_00:01:00:02 (33:33:00:01:00:02)
⊞ Internet Protocol Version 6, Src: fe80::f978:839f:4da7:5487 (fe80::f978:839f:4da7:5487), Dst: ff02::1:2 (ff02::1:2)
⊞ User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)
⊟ DHCPv6
    Message type: Information-request (11)
    Transaction ID: 0xe1dd6e
  ⊞ Elapsed time
  ⊞ Client Identifier
  ⊞ Vendor Class
  ⊟ Option Request
      Option: Option Request (6)
      Length: 8
      Value: 0018001700110020
      Requested Option code: Domain Search List (24)
      Requested Option code: DNS recursive name server (23)
      Requested Option code: Vendor-specific Information (17)
      Requested Option code: Lifetime (32)
```

Krok 3/3: DHCP server jako odpověď posílá klientovi informaci o DNS

```
⊞ Ethernet II, Src: ArubaNet_61:66:38 (00:0b:86:61:66:38), Dst: Foxconn_7e:3f:32 (00:15:58:7e:3f:32)
⊞ Internet Protocol Version 6, Src: fe80::b:8600:6461:6638 (fe80::b:8600:6461:6638), Dst: fe80::f978:839f:4da7:5487 (fe80::f978:839f:4da7:5487)
⊞ User Datagram Protocol, Src Port: dhcpv6-server (547), Dst Port: dhcpv6-client (546)
⊟ DHCPv6
    Message type: Reply (7)
    Transaction ID: 0xe1dd6e
  ⊞ Client Identifier
  ⊞ Server Identifier
  ⊞ Preference
  ⊟ Domain Search List
      Option: Domain Search List (24)
      Length: 19
      Value: 0d61727562616e6574776f726b7303636f6d00
      DNS Domain Search List
      Domain: arubanetworks.com
  ⊟ DNS recursive name server
      Option: DNS recursive name server (23)
      Length: 16
      Value: 20011234000000000000000000000004
      DNS server address: 2001:1234::4 (2001:1234::4)
  ⊞ Vendor-specific Information
```

Ukázka konfigurace bitu M na L3 switchi

```
ipv6 address FE80::D2 link-local
ipv6 address 2001:DB8:3115:120::D2/64
ipv6 nd prefix 2001:DB8:3115:120::/64 2592000 604800 no-autoconfig
ipv6 nd managed-config-flag
ipv6 dhcp relay destination 2001:DB8:3115:99::D1 Port-channel2
```

PC získá adresu pomocí

```
ipconfig /renew6
```

Doporučené zdroje k dalšímu studiu problematiky

Pěkný porovnávací příklad na
https://networklessons.com/ipv6/cisco-dhcpv6-server-configuration/
a 84 slajdů na
https://slideplayer.com/slide/6640065/
a 93 slajdů na
https://slideplayer.com/slide/4239341/
IPv6 First-Hop Security Concerns
https://www.cisco.com/c/en/us/about/security-center/ipv6-first-hop.html

Domácí úkol:
Popište některý SLAAC attack

INFORMATIONAL

Internet Engineering Task Force (IETF)
Request for Comments: 6104
Category: Informational
ISSN: 2070-1721

T. Chown
University of Southampton
S. Venaas
Cisco Systems

February 2011

Rogue IPv6 Router Advertisement Problem Statement

Abstract

When deploying IPv6, whether IPv6-only or dual-stack, routers are configured to send IPv6 Router Advertisements (RAs) to convey information to nodes that enable them to autoconfigure on the network. This information includes the implied default router address taken from the observed source address of the RA message, as well as on-link prefix information. However, unintended misconfigurations by users or administrators, or possibly malicious attacks on the network, may lead to bogus RAs being present, which in turn can cause operational problems for hosts on the network. In this document, we summarise the scenarios in which rogue RAs may be observed and present a list of possible solutions to the problem. We focus on the unintended causes of rogue RAs in the text. The goal of this text is to be Informational, and as such to present a framework around which solutions can be proposed and discussed.

https://resources.infosecinstitute.com/slaac-attack/

Windows machines compromised by default configuration flaw in IPv6

As anyone who has watched the reimagined Battlestar Galactica will tell you, Sixes are trouble. They are undoubtedly alluring, but all the while they are working covertly, following The Plan, right under the noses of their targets. Nobody realizes the true nature of the threat until it's too late.

The Internet also has its own Six, IPv6 (formerly IPng – IP Next Generation). Modern operating systems ship with it by default, but adoption has been slow for many reasons. Despite the passing of the IPocalypse, it lies largely dormant within today's networks, waiting for the chance to rise up and usurp its IPv4 predecessor.

This article describes a proof of concept of an interesting application of IPv6. I'm going to show you how to impose a parasitic IPv6 overlay network on top of an IPv4-only network so that an attacker can carry out man-in-the-middle (MITM) attacks on IPv4 traffic.

This new **SLAAC Attack**, if you will, is named for the process it is exploiting.

IPv6 Background

Aside from the increased address space, IPv6 is fundamentally different to IPv4 in several key areas. This article isn't intended to be an IPv6 primer, but I'll highlight the main features that are relevant to the attack.

Test slabiny SLAAC attack: Sudden Six

Overview

Sudden Six is an automation script for conducting the SLAAC attack outlined in Alec Water's blog post.
This attack can be used to build an IPv6 overlay network on an IPv4 infrastructure to perform man-in-the-middle attacks.

The script installs and configures the following packages:

sipcalc

tayga

radvd

wide-dhcpv6-server

bind9

Requirements This script has been tested on Ubuntu 12.04 LTS and Kali Linux 1.0.x.
We suggest using Wireshark to view the intercepted traffic.

Usage

Execute the suddensix.sh script as the root user. The script will prompt you for the interface to conduct the attack from as well as ask you to specify a free IP address on the local IPv4 network you are attacking.
After the script is running, run Wireshark to view the intercepted traffic.

Note: The script is not persistent, the attack host will not intercept traffic after a reboot. The script will not work on fully configured IPv6 networks.

Monitirovací řešení firmy Tenable: Nessus plugins support IPv6 interface enumeration:

25202 – Enumerate IPv6 Interfaces via SSH

24272 – Network Interfaces Enumeration (WMI)

45405 – Reachable IPv6 address