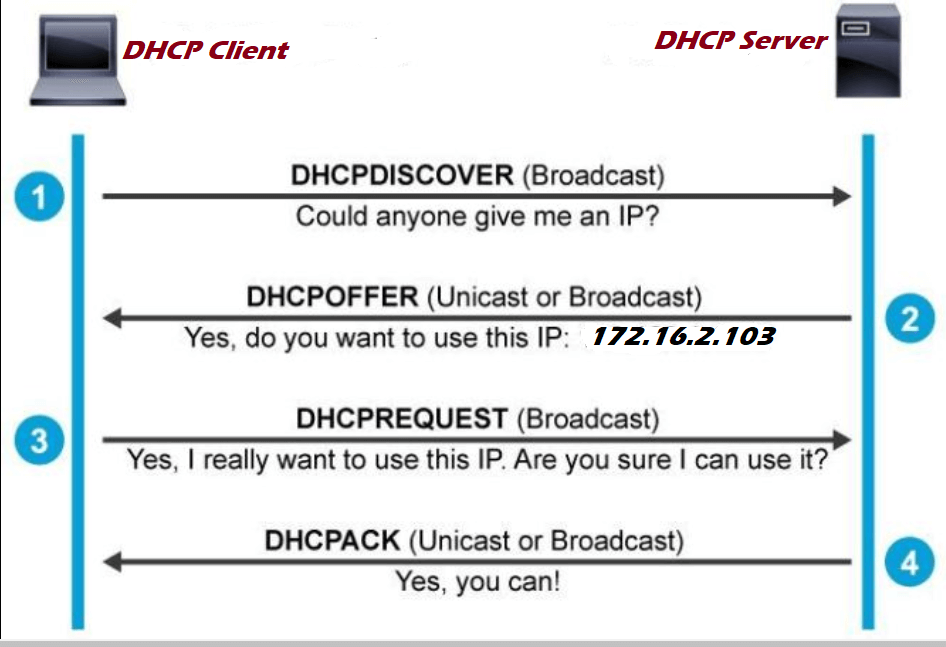
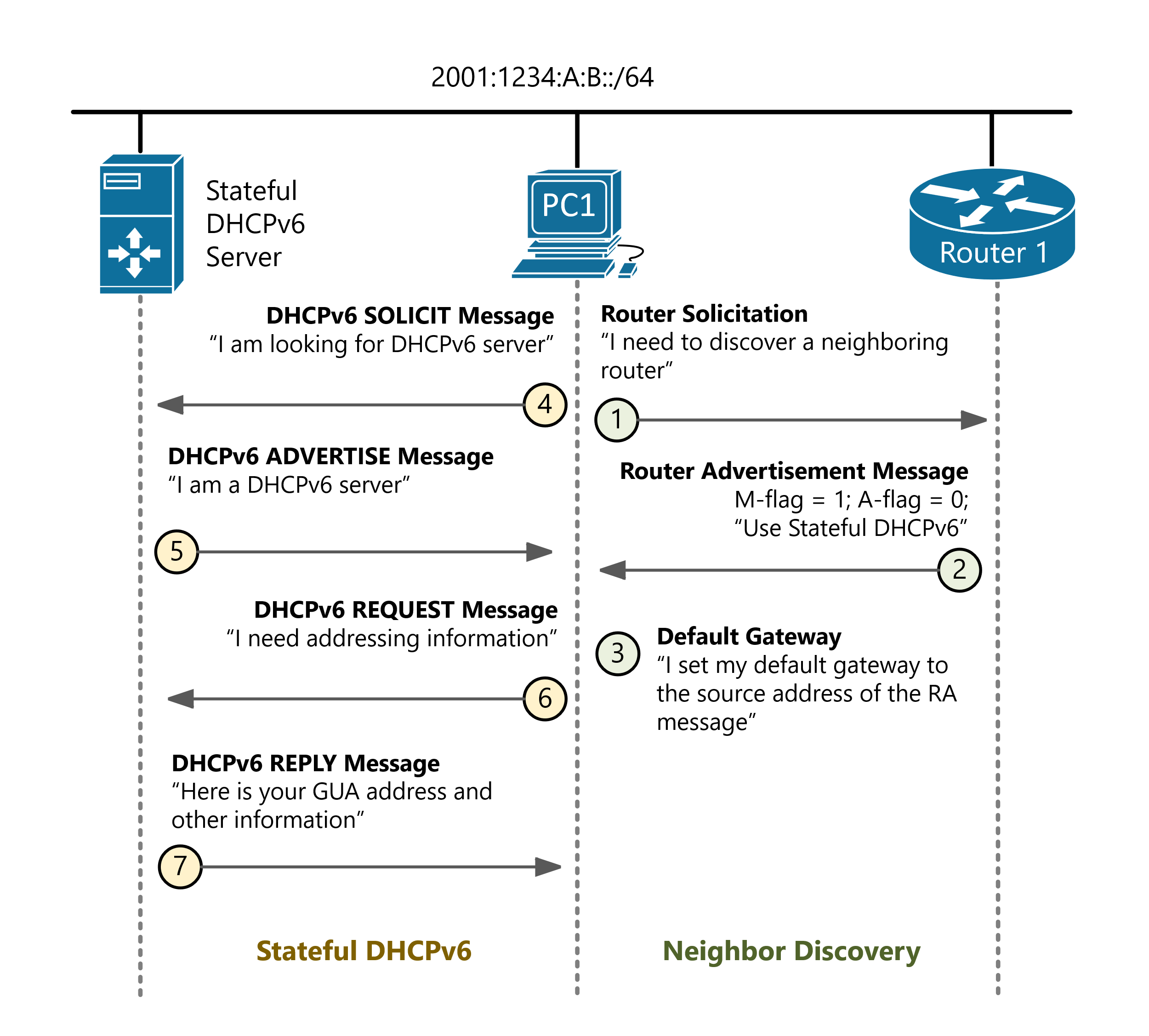
**Protokol DHCP**

**Význam služby DHCP:**

* **Automatická konfigurace IP adres**: DHCP automaticky přiděluje IP adresy zařízením v síti, čímž eliminuje nutnost manuálního nastavování IP adres.
* **Úspora času a snížení chyb**: Správci sítí nemusejí přiřazovat adresy ručně, což minimalizuje chyby a urychluje proces připojování zařízení do sítě.
* **Efektivní správa IP adres**: Protokol umožňuje dynamické přidělování adres, čímž zajišťuje optimální využití omezeného rozsahu IP adres v síti.
* **Přidělení dalších síťových parametrů**: DHCP také zajišťuje přidělení dalších nezbytných síťových parametrů, jako je maska sítě, výchozí brána (gateway), DNS servery, aj.
* **Podpora mobilních zařízení**: DHCP umožňuje zařízením snadný přechod mezi různými sítěmi bez potřeby manuálního nastavení, což je důležité pro mobilní zařízení.
* DHCPv4 používá UDP porty:
  + 67 — Server
  + 68 — Client
* DHCPv6 používá UDP porty:
  + 546 — Server
  + 547 — Client
* IP adresy pronajaté pomocí DHCP jsou jen na určitou dobu
  + Aby se zabránilo vyčerpání možných IP adres

**Průběh komunikace v DHCPv4:**

1. **DHCP Discover - broadcast:**
   * Klient, který nemá přidělenou IP adresu, vyšle **broadcast** zprávu (DHCP Discover) na adresu 255.255.255.255.
   * Cílem je nalézt dostupné DHCP servery v síti, které mohou klientovi přidělit IP adresu.
   * Zpráva obsahuje např. MAC adresu klienta, což serverům umožňuje identifikovat zařízení, které o IP adresu žádá.
   * Zarezervuje IP parametry pro klienta a zapíše si ji
2. **DHCP Offer - unicast:**
   * DHCP server odpoví klientovi zprávou **DHCP Offer**, ve které navrhne volnou IP adresu a další síťové parametry.
   * Tato zpráva obsahuje navrženou IP adresu, dobu zapůjčení (lease time), masku podsítě, výchozí bránu a DNS servery.
   * Pokud v síti existuje více DHCP serverů, může klient obdržet více nabídek.
3. **DHCP Request - broadcast:**
   * Klient si vybere jednu z nabídek a odpoví zprávou **DHCP Request**, ve které požádá konkrétní DHCP server o přidělení navržené IP adresy.
   * Tento krok zároveň signalizuje ostatním DHCP serverům, že jejich nabídky byly odmítnuty, a proto si mohou uvolněné IP adresy vrátit do svého poolu.
4. **DHCP Acknowledgement - unicast**:
   * DHCP server, jehož nabídka byla klientem vybrána, odpoví zprávou **DHCP Acknowledgement (ACK)**.
   * Tato zpráva potvrzuje přidělení IP adresy a poskytuje finální síťovou konfiguraci.
   * Od této chvíle klient může začít využívat přidělenou IP adresu a komunikovat v síti.
5. **Obnova adresy (renewal)**:
   * Když se blíží konec platnosti přidělené IP adresy (lease time), klient zašle DHCP serveru žádost o obnovu adresy (DHCP Request), aby mohl IP adresu nadále používat.
6. **Odvolání přidělení (DHCP NAK)**:
   * Pokud DHCP server nemůže IP adresu přidělit (např. protože klient žádá adresu, která již není dostupná), server zašle zprávu **DHCP NAK** (Negative Acknowledgement), což znamená, že klient musí začít celý proces znovu.

**Průběh komunikace v stateful DHCPv6:**

1. **DHCP Solicitation - multicast**:
   * Klient, který potřebuje získat IPv6 adresu, vysílá zprávu **DHCP Solicitation** na multicast adresu určenou pro DHCP servery.
   * Cílem této zprávy je informovat DHCP servery, že klient hledá síťovou konfiguraci, včetně IP adresy a dalších parametrů (DNS servery, doménové jméno apod.).
2. **DHCP Advertise - unicast:**
   * Servery, které obdržely žádost klienta, odpoví zprávou **DHCP Advertise**. Tato zpráva obsahuje návrh konfigurace včetně IPv6 adresy, kterou může server klientovi přidělit.
   * Klient může obdržet nabídky od více DHCP serverů.
3. **DHCP Request - multicast:**
   * Klient si z odpovědí vybere jednu nabídku a odpoví zprávou **DHCP Request**, ve které požádá konkrétní server o přidělení navržené IP adresy a dalších parametrů.
   * Stejně jako u DHCPv4 ostatní servery, jejichž nabídky nebyly vybrány, uvolní své adresy zpět do svého poolu.
4. **DHCP Reply - unicast**:
   * DHCP server odpoví na žádost klienta zprávou **DHCP Reply**, kde potvrzuje přidělení IPv6 adresy a ostatních síťových parametrů.
   * Klient může od této chvíle využívat přidělenou IPv6 adresu a konfigurované síťové služby.
5. **Obnova a uvolnění adresy**:
   * Stejně jako u DHCPv4, i zde může klient požádat o prodloužení platnosti IPv6 adresy, když se blíží konec leasingového období.

**Stateless DHCPv6:**

1. **Pouze doplňkové informace**: V tomto režimu si klient nastavuje svou IP adresu sám pomocí **SLAAC**, zatímco DHCPv6 server poskytuje pouze doplňkové informace, jako jsou DNS servery, doména.

**SLAAC (Stateless Address Autoconfiguration):**

* **Nastavení IP adresy bez DHCP serveru**: SLAAC umožňuje klientům nastavit si IPv6 adresu sami pomocí informací obdržených od routeru. Proces probíhá následovně:
  1. Klient vyšle **Router Solicitation** zprávu, aby zjistil dostupné routery.
  2. Router odpoví zprávou **Router Advertisement**, ve které poskytne informace o síťovém prefixu.
  3. Klient použije tento prefix společně se svou MAC adresou k vytvoření své jedinečné IPv6 adresy (EUI-64).
* **Výchozí brána**: V SLAAC výchozí bránu určuje router prostřednictvím **Router Advertisement** zprávy. Klient tuto bránu uloží a použije ji pro směrování dat do externí sítě.

**Vytvoření globální unicast adresy z globálního prefixu**

* Ke globálnímu prefixu si uzel přidá svůj identifikátor rozhraní — Interface ID
* Jsou dvě možnosti generace Interface ID:
  1. EUI-64 → Využije se 48 biutová MAC adresa
  2. Náhodně generované → 64 bitů se vygeneruje náhodně na OS

**Ověření duplicity adres — DAD**

* Uzel zašle ICMPv6 Neighbor Solication zprávu na svou adresu
  + Když nikdo neodpoví Neighbor Advertisment zprávou, adresa je unikátní
  + Když někdo odpoví, uzel si musí udělat novou adresu

**Router Solicitation a Router Advertisement:**

1. **Router Solicitation**:
   * Klient vysílá zprávu **Router Solicitation** na multicast adresu routerů, aby zjistil dostupné routery v síti. Tato zpráva je zasílána při prvním připojení k síti nebo při obnově síťové konfigurace.
2. **Router Advertisement**:
   * Směrovač odpovídá zprávou **Router Advertisement**, která obsahuje:
     + Informace o prefixu sítě (pro nastavení IP adresy pomocí SLAAC).
     + Výchozí bránu.
     + Další doplňkové parametry (např. možnost použití DHCPv6).
   * Zprávy Router Advertisement mohou být vysílány buď pravidelně, nebo jako odpověď na Router Solicitation.

**Komunikace v DHCPv6 jinak**

* DHCPv6 komunikace započne, když uzel díky RA zjistí, že má použít stateless/stateful DHCPv6
* Tím, že IPv6 nemá broadcast, DHCPv6 používá pro komunikaci lokální linkovou adresu, tudíž nikdy nedává uzlu informaci o defaultní gatewayi
* DHCPv6 podporuje DHCP relay — Toto se zavedlo zpětně do IPv4

Jednotlivé fáze komunikace:

1. Po vygenerování Interface ID a uzlu (viz. pod body), uzel osloví agenty (zprostředkovatele + servery) na multicastové adrese ff02::1:2 (ano, je za tím ještě :2 → označuje všechny DHCP agenty) s žádostí o IP údaje → tzv. **výzvě** — **Solicid**
   * Lokální linková adresa
   * DUID — DHCP Unique Identifier
     + Například výrobní číslo síťového rozhraní
   * IA — Identity Association
     + Slouží k rozlišení síťových rozhraní rámci v rámci uzlu klienta
2. Výzvu obdrží…
   * Server → Uzel je ve stejném linkovém segmentu
     + Server rovnou odpoví na lokální linkovou adresu uzlu **ohlešením serveru** (**advertise**) s nabízenými konfiguračními parametry
   * Zprostředkovatel (agent) → Předá dotaz serverům (jejich seznam je v konfiguraci) nebo na multicast adresu ff05::1:3 ve formě tzv. **předání (relay forward)**
     + Server odpoví zprostředkovateli, ten pak odpoví clientovi
3. Klient vyhodnotí nabídky, vybere jeden server a pošle **žádost (request)** opět na multicast agentů (ff02::1:2)
   * V žádnosti je DUID vybraného serveru
4. Vybraný server vrátí **odpověď (reply)** s potvrzením nabídkou parametrů

<aside> 💡 Ostatní servery ignorují odpověď

</aside>

1. Klient ověří případnou duplicitu IP adresy
   * Když zjistí, že ji již někdo má, odešle zprávu **odmítnutí (decline)**
2. Parametry jsou přiděleny na omezenou dobu → Po jejím uplynutí klient žádá svůj server o **obnovení (renew)**
   * Když server neodpoví, osloví zase ostatní servery
3. Když by klient v síti končil (aka, odpojoval by se), měl by informovat svůj server zprávou **uvolnění (release)**
   * Tím se rovnou adresa uvolní někomu jinému
4. Při návrtatu klienta do sítě (resetart, probuzení počítače, atd.) je třeba ověřit, zda jsou údaje stále platné, pomocí zprávy **potvrzení (confirm)**
   * Kdy server změní konfigurační paraemtry, rozešle zprávu **rekonfigurace (reconfigure)** každému uzlu, kterému přidělil parametry
     + Klient reaguje požadavkem na obnovení parametrů
       1. Server je pošle v odpovědi

* V DHCPv6 je zavedena volitelná vlastnost autentizace → Používá ji klient při úvodní zprávě
  + Určí současně metodu ověření totožnosti
    - Základní je HMAC s MD5

<aside> 💡 HMAC = Keyed-hash Message Authentication Code

</aside>

* + Server pak ke každé zprávě přiklládá digitální podpis

**IV. Útoky na DHCP**

**DHCP Spoofing**

* Útočník se snaží vydávat za legitimní DHCP server a vysílá falešné nabídky IP adres nebo jiné konfigurační informace klientům v síti.
* To může vést k nežádoucím situacím, jako jsou konflikty IP adres nebo přiřazení neplatných konfigurací.

**DHCP Starvation**

* Útočník se snaží vyčerpat dostupnost IP adres v síti tím, že požaduje přidělení velkého počtu IP adres pomocí falešných žádostí DHCP.
* Tím může znemožnit přidělení IP adres legitimním klientům.

**DHCP Injection**

* Útočník se snaží vložit škodlivý kód do konfiguračních dat poskytovaných DHCP serverem.
* Tím může vést k infikování klientů v síti.

**DHCP Denial of Service (DoS)**

* Útočník se snaží znemožnit komunikaci mezi DHCP serverem a klienty v síti tím, že například přetíží server žádostmi nebo vysílá falešné zprávy, které přeruší komunikaci mezi klientem a serverem.