Obchodní akademie, Vyšší odborná škola a Jazyková škola
s právem státní jazykové zkoušky Uherské Hradiště

MATURITNÍ PROJEKT

PRÁCE S IPV4 A IPV6

2023 Matěj Krajsa, 4.B

Obchodní akademie, Vyšší odborná škola
a Jazyková škola s právem státní jazykové
zkoušky Uherské Hradiště

Vnitřní předpis OA, VOŠ a JŠ, čj. 025/ORG/2021

Příloha č. 3

ZADÁNÍ MATURITNÍ PRÁCE INFORMAČNÍ TECHNOLOGIE

Jméno žáka:	Matěj Krajsa
Téma maturitní práce:	Práce s IPv4 a IPv6
Vedoucí práce:	Ing. Bc. Martin Šimůnek
Oponent práce:	Mgr. Zdenek Hrdina
Způsob zpracování:	Žák **nastuduje technologie propojování** sítí postavených na protokolech **IP v. 6 a IP v. 4**. Sepíše a do dokumentace zahrne studii dostupných technologií včetně odkazů na zdroje. Žák **vyzkouší** běžně používané technologie v Packet Traceru i prakticky. Pokud některou technologii nebude možné realizovat, zjistí co nejvíce informací z dostupných zdrojů. Žák sepíše souhrnné **srovnání jednotlivých technologií** propojování sítí. Teoretické poznatky podpoří zkušenostmi z praktického ověření. Žák sepíše **studijní materiál pro žáky 3. ročníku**, který bude zahrnovat zjištěné poznatky. Materiál ověří ve výuce po dohodě s vyučujícím předmětu Počítačové sítě. Součástí dokumentace bude zpětná vazba z ověření materiálu. (Doporučený formát materiálu buď prezentace, nebo githubový repozitář s materiály v Markdownu.) Součástí materiálu bude alespoň jedna **praktická úloha** (může využívat školní routery či lépe Packet Tracer). Žák každý týden napíše do určeného týmu v MS Teams krátký report o postupu (i pokud daný týden žádný postup nebyl). Vytvořené materiály včetně dokumentace budou po celou dobu uloženy v githubovém repozitáři, kde bude dostupná i historie vývoje projektu.

Obrázek 1 Maturitní zadání strana 1

Zdroj: Vlastní

Obchodní akademie, Vyšší odborná škola
a Jazyková škola s právem státní jazykové
zkoušky Uherské Hradiště

Pokyny k odevzdání:	**Žák odevzdá práci v tištěné a elektronické podobě** • Tištěná podoba práce obsahuje uživatelskou a technickou dokumentaci. **Tištěnou podobu** (v kroužkové vazbě) žák odevzdá v jedné verzi na studijní oddělení školy, místnost 311. **Elektronická podoba práce obsahuje** • Dokumentaci ve formátu PDF/A • Resumé ve formátu PDF/A • Výsledný projekt, zdrojové soubory a potřebné knihovny pro spuštění projektu • Prezentaci projektu **Elektronická podoba** práce se nahrává do IS školy dle pokynů vedoucího práce nebo vedení školy. V případě, že se jedná o projekt, na kterém pracovalo více žáků, je povinnou součástí dokumentace podrobné rozdělení činností při práci na projektu.
Kritéria hodnocení:	Hodnocení se skládá z celkové kvality zpracování práce, dokumentace, z kvality prezentace při obhajobě práce, diskuse a z průběžného hodnocení žáka v rámci kontrolních dnů.
Obhajoba projektu	Obhajoba projektu se skládá ze dvou části - prezentace projektu (včetně podpůrné elektronické prezentace) a diskuse nad řešením. Celková délka obhajoby je 20 minut, délka prezentace projektu by neměla překročit 10 minut.

17. 10. 2022
.....
Datum

Obchodní akademie, Vyšší odborná škola
a Jazyková škola s právem státní
jazykové zkoušky Uherské Hradiště
Masarykovo nám. 22, 686 01 Uherské Hradiště
IČO: 60371731, tel.: 572 433 011

.....
Podpis ředitele školy

Obrázek 2 Maturitní zadání strana 2

Zdroj: Vlastní

Prohlášení:

Souhlasím s tím, že s výsledky mé práce může být naloženo podle uvážení vedoucího maturitní práce a ředitele školy. V případě publikace budu uveden jako spoluautor. Prohlašuji, že jsem na celé maturitní práci pracoval samostatně a veškeré použité zdroje jsem citoval.

V Uherském Hradišti, 31.3.2023

.....

podpis absolventa

RESUMÉ

Cílem projektu je studie IPv6 technologií, zejména protokolů, a jejich vlastnosti. Dále praktická část, kde vyzkouším a ověřím některé z technologií v praxi. Pro studenty vytvořím materiál v podobě úloh s použitím Packet traceru.

OBSAH

ÚVOD

Práce s IPv4 a IPv6 protokoly, maturitní práci jsem si vybral ze dvou hlavních důvodů, jeden z problémů se týká budoucnosti, internetového inženýrství, a to obsazení všech dostupných globálních IPv4 adres, které byly obsazeny pár let zpátky, ze všech dostupných 4,294,967,296 adres není dostupná už ani jedna adresa. Z důvodu této nepříjemné globální situace se bude brzy přecházet na IPv6 adresy, kterých je prakticky neomezené množství a to 2^{128}. Druhým důvodem je moje vlastní touha a zajímavost o síťové technologie. V této práci vysvětlíme, co jsou IPv4 a IPv6 adresy a protokoly, popíšeme důkladně nastudované materiály těchto technologiích a možnosti řešení problému vyzkoušíme a prezentujeme žákům 3. ročníku.

1 IP ADRESY

1.1 Adresy IPv4

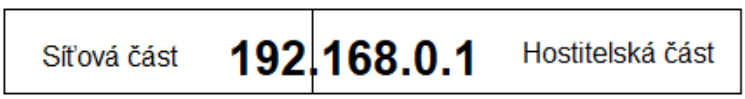
1.1.1 Charakteristika

IP adresa, je unikátní identifikační číslo síťového rozhraní v počítačových sítích komunikující pomocí Internetového Protokolu (dále jen IP). Z tohoto poznatku vyplývá, že každé zařízení komunikující pomocí internetu musí mít přidělenou svoji IP adresu, přestože se může jednat i o žárovku kterou ovládáme pomocí našeho telefonu. Z toho důvodu v dnešní době, kdy už všech 2^{32} IP adres verze 4 je přiděleno, samozřejmě na tenhle problém se myslelo už při zavádění IP adres verze 4, tak vznikly privátní IP adresy, aby se šetřilo místem skoro každé zařízení má svoji vnitřní IP adresu získanou od nějakého vstupního anebo výstupního bodu do sítě (např. routeru nebo switche) v lokální síti. Převážně zařízení, která komunikují s rámci internetu, a ne lokální sítě mají přidělenou IP adresu.

1.1.2 Struktura adresy IPv4

IPv4 adresa se skládá z 32 bitů, které jsou rozděleny do čtyř 8bitových oktetů. Oktety jsou odděleny tečkami a reprezentovány v desítkové soustavě, maximální hodnota v daném oktetu je 255, začínající od 0.

IPv4 adresa může být reprezentována jako 192.168.0.1, kde první oktet představuje síťovou část adresy a poslední tři oktety představují hostitelskou část.



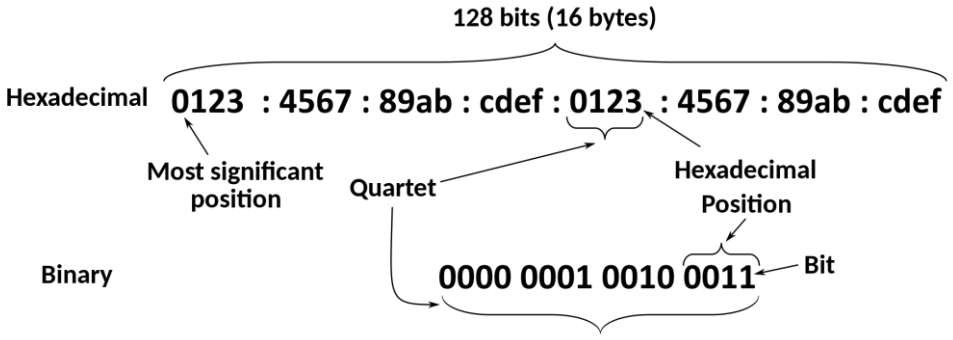
Obrázek 3 Rozdělení IPv4 adresy

Zdroj: Vlastní

1.2 Adresy IPv6

1.2.1 Charakteristika

Internet Protocol version 6 (dále jen IPv6), je nejnovější verze internetového protokolu, který definuje způsob přenosu dat přes internet. IPv6 adresy se používají k identifikaci a lokalizaci zařízení na internetu. IPv6 adresy jsou 128bitové adresy, které jsou uvedeny v hexadecimálním zápisu oddělené dvojtečkami.



Obrázek 4 Rozdělení IPv6 adresy
Zdroj: By Michel Bakni - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=90057474

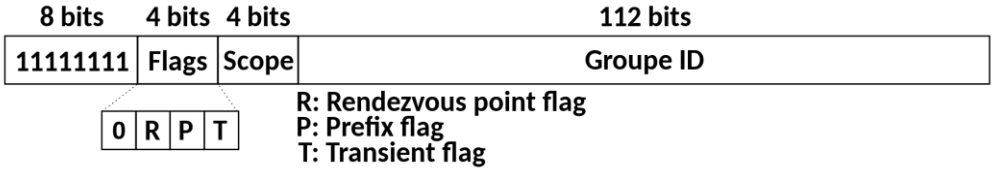
IPv6 adresa je rozdělena do osmi 16bitových bloků oddělených dvojtečkami. Každý blok je reprezentován čtyřmi hexadecimálními číslicemi a nuly na začátku v bloku můžou být vynechány. Adresu lze také zkrátit nahrazením libovolných po sobě jdoucích bloků nul dvojtečkou (::), ale lze to provést pouze jednou v jedné adrese. Adresy IPv6 se dělí na dvě části, předponu sítě a ID rozhraní. Předpona sítě se používá k identifikaci síťové adresy, zatímco ID rozhraní identifikuje konkrétní zařízení. IPv6 také zahrnuje speciální adresy, jako jsou loopbackové a mulicastové adresy.

1.2.2 Vetší adresní prostor

IPv6 adresy jsou nutné kvůli vyčerpání dostupných IPv4 adres. IPv6 poskytuje mnohem větší adresní prostor než IPv4, což umožňuje připojení k internetu prakticky neomezenému počtu unikátních zařízení, reálné číslo však je 2^{128}.

1.2.3 Mulicasting

Multicasting se týká přenosu dat od jednoho odesílatele k více příjemcům v síti pomocí jediné operace. Multicastová adresa se používá k identifikaci skupiny hostitelů, kteří projevili zájem o příjem multicastového vysílání. Když se hostitel připojí k multicastovému vysílání, vyjadřuje svůj zájem přijímat pakety odeslané na multicastovou adresu přidruženou ke skupině. Multicastové adresy jsou identifikovány předponou ff00::/8.



Obrázek 5 Struktura multicastové adresy

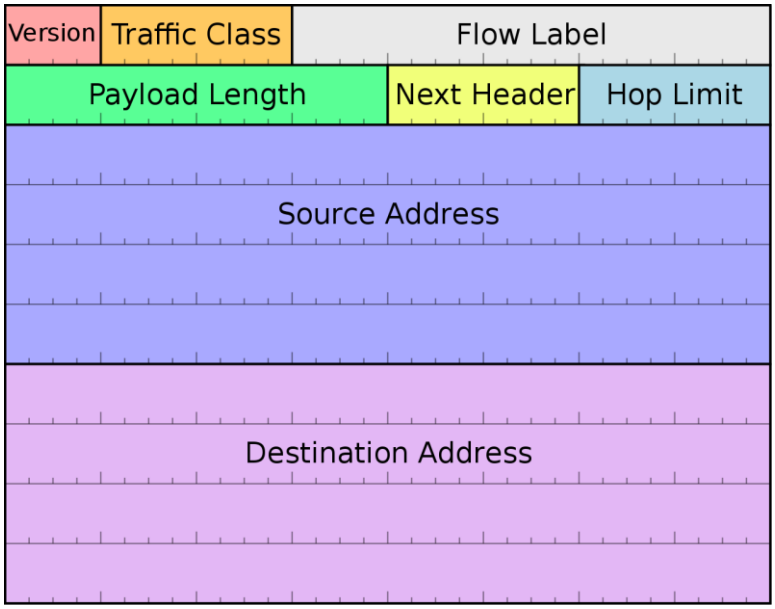
Zdroj: By Michel Bakni - R. Hinden, S. Deering (February 2006) RFC 4291, IPv6 Addressing Architecture, The Internet Society, p. 13 DOI: 10.17487/RFC4291., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=90190485

Multicastové pakety jsou doručeny všem členům skupiny a každý člen zpracovává pakety podle svých vlastních potřeb. Multicasting je užitečný, pokud daná aplikace potřebuje posílat stejná data více klientům současně, např.: videokonference, streamování multimédií ale také, správa sítě. IPv6 také umožňuje multicastovému vysílání, předávat pakety mezi různými segmenty sítě nebo dokonce přes globální internet. Pro tyto účely se používají další protokoly jako Protokol Independent Multicast (dále jen PIM) a Multicast Listener Discovery (dále jen MLD).

1.2.4 IPv6 packety

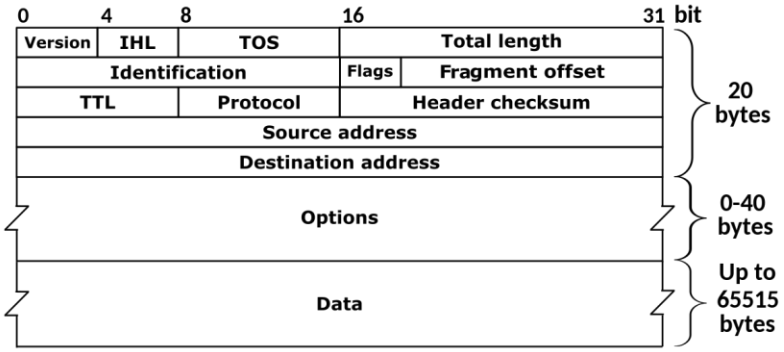
IPv6 pakety jsou základní jednotkou komunikace v síti IPv6. Používají se k přenosu dat mezi hostiteli. IPv6 paket se skládá ze dvou hlavních částí, IPv6 hlavičky a datové části. IPv6 hlavička obsahuje informace o paketu, včetně zdrojové a cílové adresy, typu protokolu, označení toku a hop limitu. IPv6 hlavička má pevnou délku 40 bajtů a je efektivnější než IPv4 hlavička, která má proměnnou délku. Velikost dat, se může lišit a může být fragmentována do více paketů, pokud překročí Maximum Transmission Unit (dále jen MTU). IPv6 pakety jsou obvykle odesílány pomocí adresování unicast, multicast nebo anycast. Unicast se používá k odesílání paketů jednomu hostiteli, multicast se používá k odesílání paketů skupině hostitelů a anycast se používá k odesílání paketů

nejbližšímu ze skupiny hostitelů. Rozhodnutí o směrování se provádí na základě cílové adresy v hlavičce paketu a informací ve směrovací tabulce.



Obrázek 6 IPv6 paket

Zdroj: By Mro - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=10394859



Obrázek 7 IPv4 paket

Zdroj: By Michel Bakni - Postel, J. (September 1981) RFC 791, Internet Protocol, DARPA Internet Program Protocol Specification, The Internet Society, p. 11 DOI: 10.17487/RFC0791., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=79949694

1.3 Porovnání IPv4 a IPv6

Obě verze internetového protokolu, jsou základními protokoly používanými k přenosu dat přes internet. Zatímco se IPv4 používá již mnoho let, IPv6 byl vyvinut, aby řešil některá omezení IPv4.

1.3.1 Adresní prostor

IPv4 používá 32bitové adresy, což omezuje počet unikátních adres na 2^{32}. IPv6 používá 128bitové adresy, což poskytuje mnohem větší adresní prostor, umožňující 2^{128} jedinečných adres.

1.3.2 Fragmentace

IPv4 routery mohou potřebovat fragmentovat pakety, pokud překročí MTU, což může mít za následek další zpracování a zpoždění. IPv6 routery pakety nefragmentují, místo toho je fragmentuje hostitel před odesláním, což routerům snižuje práci.

1.3.3 Bezpečnost

Hlavním rozdílem v bezpečnosti je že, IPv4 poskytuje zabezpečení prostřednictvím protokolů, jako je IPSec, ale není povinné. Narozdíl IPv6 zahrnuje IPSec jako povinný protokol, který poskytuje vyšší úroveň zabezpečení.

1.3.4 Automatické Konfigurace

IPv4 vyžaduje servery DHCP nebo protokol APIPA pro přidělování adres a konfiguraci, což může být složité na správu. IPv6 zahrnuje stateless automatickou konfiguraci adres, SLAAC, která umožňuje hostitelům automaticky konfigurovat své adresy, což zjednodušuje přidělování adres, a tím pádem není nutný DHCPv6 server.

2 PROTOKOLY

2.1 IPv6 Protokoly

2.1.1 SLAAC

Definice

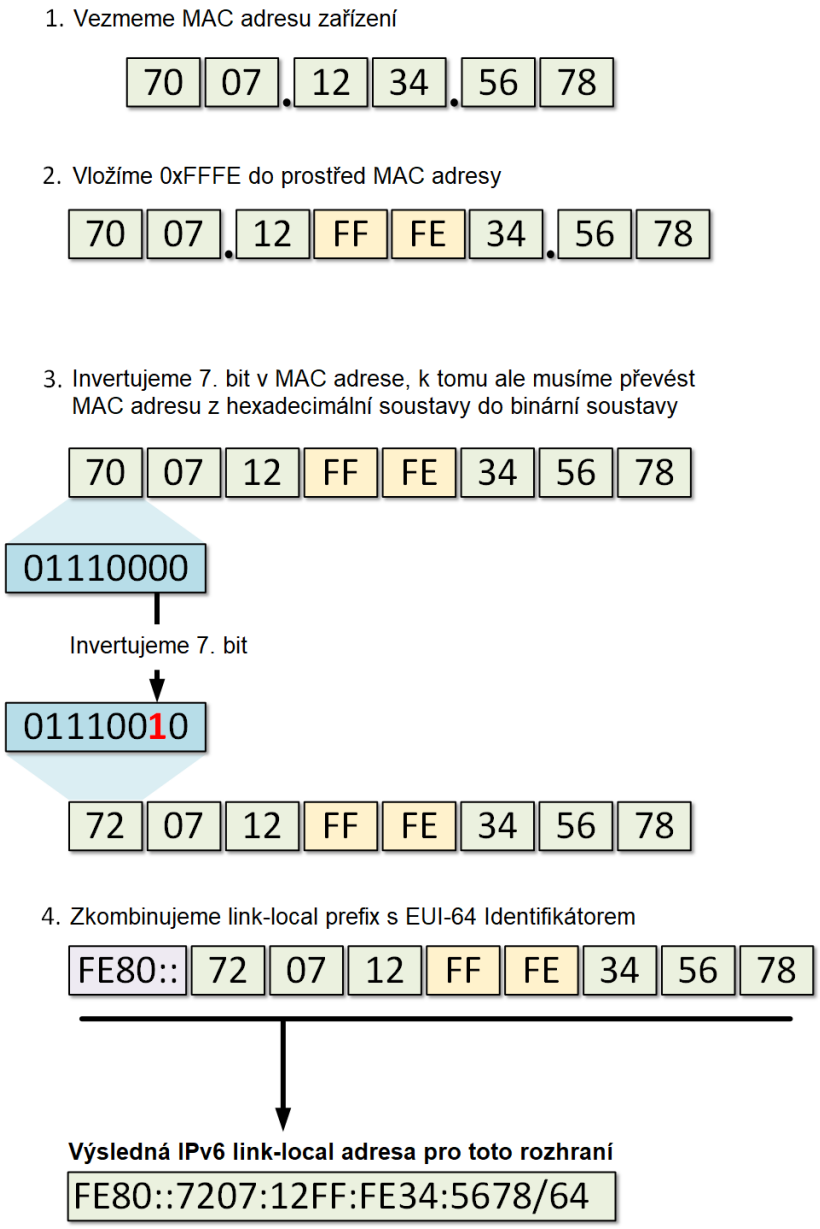
Stateless Address Autoconfiguration (dále jen SLAAC), je protokol patřící do skupiny síťových protokolů. SLAAC může automaticky nakonfigurovat rozhraní zařízení používající IPv6 adresy, bez potřeby pro použití DHCPv6 serveru.

Funkcionalita

K použití nepotřebujeme žádný server nebo jiné zařízení, které by sledovalo přiřazování adres. Uzly mají na starosti kontrolu a řešení duplicity. Tuto problematiku řeší pomocí Duplicate Address Detection (dále jen DAD), funguje na principu porovnávání, prvně vygeneruje adresu, poté adresu otestuje pomocí DAD. Pokud se zjistí že adresa je duplicitní vygeneruje novou IPv6 adresu a opakuje proces, dokud se nenajde volná IPv6 adresa.

Když se zařízení připojí k IPv6 síti, dostane link-local adresu, důvodem je komunikace s ostatními zařízeními, tuto adresu je však nutné nakonfigurovat. Mezitím zařízení dostává od routeru Router Advertisment (dále jen RA), který obsahuje informace pro vytvoření IPv6 link-local adresy pro dané zařízení. Tento úkol musí zajistit samo zařízení následujícími kroky.

1. Zjistí si MAC adresu zařízení.
2. Vloží do prostřední části MAC adresy hodnotu 0xFFFE.
3. Invertuje 7. bit MAC adresy, první ho však musí převést z hexadecimální soustavy do binární soustavy, tím nám vzniká Extended Unique Identifier-64 (dále jen EUI-64).
4. Kombinace EUI-64 s prefixem link-local adresy vznikne IPv6 link-local adresa pro toto rozhraní.



Obrázek 8 Proces vytvoření IPv6 link-local adresy v SLAAC

Zdroj: https://www.networkacademy.io/ccna/ipv6/stateless-address-autoconfiguration-slaac

2.1.2 DHCPv6

Definice

Dynamic Host Configuration Protocol version 6 (dále jen DHCPv6), je protokol patřící do skupiny internetových protokolů. DHCPv6 automaticky konfiguruje rozhraní IPv6 zařízení, jako je IP adresa, IP prefix, výchozí cestu, MTU, a další parametry pro IPv6. Je prakticky ekvivalentní s Dynamic Host Configuration Protocol version 4 (dále jen DHCP).

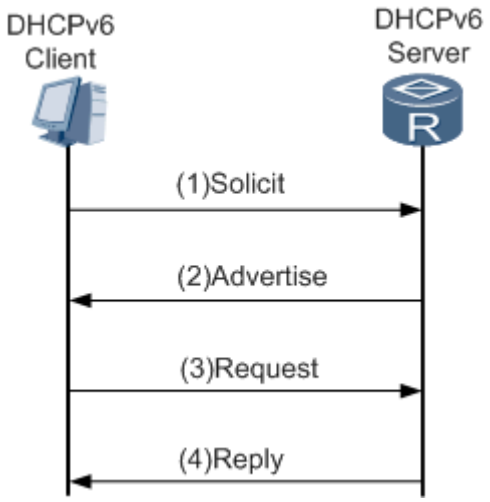
Funkcionalita

V IPv6 síti plní DHCPv6 stejnou funkci jako DHCP v IPv4 síti. Poskytuje centrální bod správy pro přidělování IP adres a dalších informací o konfigunaraci sítě zařízením v síti. DHCPv6 funguje na základě modelu klient-server. Když se klient připojí k IPv6 síti, odešle zprávu s žádostí o adresu a další konfigurační informace na DHCPv6 server. DHCPv6 server odpoví zprávou, která obsahuje IPv6 adresu a další konfigurační parametry, jako je adresa serveru DNS, výchozí brána a maska podsítě. Klient tyto informace použije ke konfiguraci svého síťového rozhraní a připojení k síti. DHCPv6 také podporuje stateless automatickou konfiguraci adres, která umožňuje zařízením automaticky generovat IPv6 adresu, např.: SLAAC. To znamená, že DHCPv6 není nezbytně nutné pro přidělování IPv6 adres, ale je stále užitečný nástroj pro přidělování dalších konfiguračních parametrů a správu sítě. Právě při předávání těchto informací, DHCPv6 definuje několik typů zpráv, které se používají při výměně informací mezi klienty a servery.

Tabulka 1 Typy zpráv
Zdroj: https://en.wikipedia.org/wiki/DHCPv6 (CC)

Kód	Typ	RFC
1	SOLICIT	RFC 8415
2	ADVERTISE	RFC 8415
3	REQUEST	RFC 8415
4	CONFIRM	RFC 8415
5	RENEW	RFC 8415
6	REBIND	RFC 8415
7	REPLY	RFC 8415

8	RELEASE	RFC 8415
9	DECLINE	RFC 8415
10	RECONFIGURE	RFC 8415
11	INFORMATION-REQUEST	RFC 8415
12	RELAY-FORW	RFC 8415
13	RELAY-REPL	RFC 8415
14	LEASEQUERY	RFC 5007
15	LEASEQUERY-REPLY	RFC 5007
16	LEASEQUERY-DONE	RFC 5460
17	LEASEQUERY-DATA	RFC 5460
18	RECONFIGURE-REQUEST	RFC 6977
19	RECONFIGURE-REPLY	RFC 6977
20	DHCP-QUERY	RFC 7341
21	DHCP-RESPONSE	RFC 7341
22	ACTIVELEASEQUERY	RFC 7653
23	STARTTLS	RFC 7653



Obrázek 9 Model komunikace s DHCPv6

Zdroj: https://support.huawei.com/enterprise/en/doc/EDOC1000097281/329fa152/dhcpv6-working-principles

Unikátní indentifikátor DHCPv6

DHCPv6 Unique Identifier (dále jen DUID) je hodnota, která identifikuje klienta. Slouží k zajištění, že klient obdrží stejnou IPv6 adresu při každém připojení k síti. DUID je generováno a odesláno klientem na server DHCPv6. DUID bylo zavedeno proti problému s duplikací v sítích používající DHCP. DUID je 128bitový identifikátor, který je jedinečný pro všechny klienty v síti. Generuje se kombinací MAC adresy, a identifikátorem specifickým pro ISP. Existují dva typy DUID.

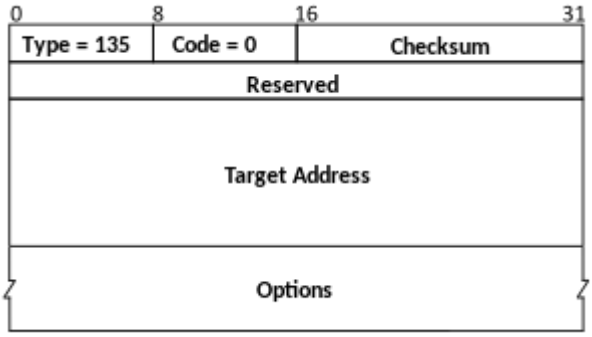
a) Link-layer address plus Time (dále jen DUID-LLT), tento DUID obsahuje časové razítko spolu s MAC adresou zařízení, časové razítko pomáhá zajistit, že DUID zůstane jedinečné, i když se MAC adresa zařízení změní.
b) Universally Unique Identifier (dále jen DUID-UUID), toto DUID používá náhodně generovaný UUID jako specifický identifikátor pro zařízení. UUID je generováno pomocí specifického algoritmu, aby bylo zajištěno, že je jedinečné.

2.1.3 NDP

Neighbor Discovery Protocol (dále jen NDP) Jedná se o protokol používaný sítěmi IPv6 k odhalování dalších zařízení ve stejném segmentu sítě a k určení adres linkové vrstvy pro tato zařízení. NDP plní funkce podobné Address Resolution Protocol (dále jen ARP), ale s možnostmi, jako je zjišťování routerů a detekce duplicitních adres. Umožňuje zařízením zjistit MAC adresu jiných zařízení ve stejné síti a udržovat tyto informace v mezipaměti.

NDP definuje pět typů paketů Internet Control Message Protocol version 6 (dále jen ICMPv6), NS, NA, RS, RA. Každý paket je strukturován jinak a obsahuje věci podle potřeby zprávy nebo odpovědi.

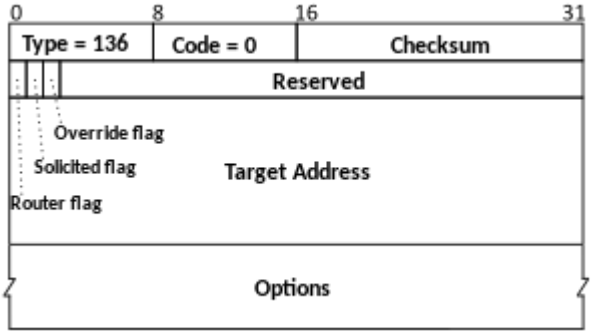
Neighbor Solicitation (NS), požadavek odeslaný zařízením k určení adresy jiného zařízení ve stejné síti.



Obrázek 10 Vizualizace NS paketu

Zdroj: By Michel Bakni - T. Narten, E. Nordmark, W. Simpson and H. Soliman (September 2006) RFC 4861, Neighbor Discovery for IP version 6 (IPv6), The Internet Society, p. 18 DOI: 10.17487/RFC4861., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=112559830

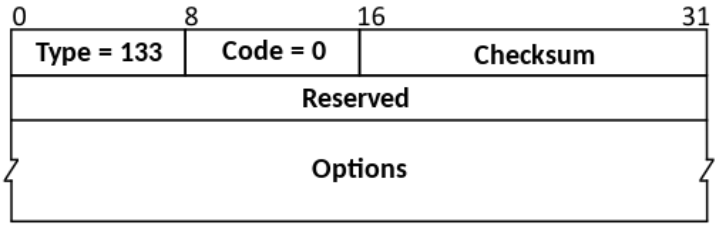
Neighbor Advertisement (NA), odpověď odeslaná zařízením za účelem poskytnutí adresy jinému zařízení, které odeslalo zprávu NS.



Obrázek 11

Zdroj: By Michel Bakni - T. Narten, E. Nordmark, W. Simpson and H. Soliman (September 2006) RFC 4861, Neighbor Discovery for IP version 6 (IPv6), The Internet Society, p. 18 DOI: 10.17487/RFC4861., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=112559830

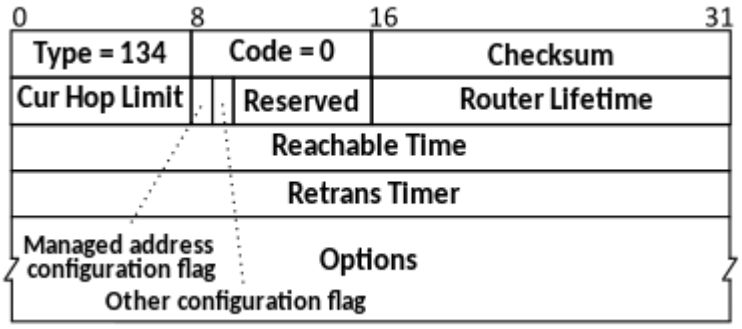
Router Solicitation (RS), zpráva odeslaná zařízením za účelem zjištění přítomnosti routerů v síti.



Obrázek 12

Zdroj: By Michel Bakni - T. Narten, E. Nordmark, W. Simpson and H. Soliman (September 2006) RFC 4861, Neighbor Discovery for IP version 6 (IPv6), The Internet Society, p. 22 DOI: 10.17487/RFC4861., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=112538022

Router Advertisement (RA), zpráva odeslaná routerem, zpět zařízením a poskytnutí, konfiguračních informací.



Obrázek 13

Zdroj: By Michel Bakni - T. Narten, E. Nordmark, W. Simpson and H. Soliman (September 2006) RFC 4861, Neighbor Discovery for IP version 6 (IPv6), The Internet Society, p. 22 DOI: 10.17487/RFC4861., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=112538022

2.1.4 DNSv6

Domain Name System version 6 (dále jen DNSv6), je nejnovější verzí systému DNS, který se používá k překladu lidsky čitelných doménových jmen na strojově čitelné IP adresy. Hlavní rozdíl mezi DNSv6 a jeho předchůdcem, DNS, je ten, že DNSv6 používá IPv6 adresy, zatímco DNS používá IPv4 adresy. To znamená, že DNSv6 je vhodnější pro zpracování většího adresního prostoru. DNSv6 obsahuje několik vylepšení oproti DNS, jako je lepší podpora bezpečnostních funkcí, jako Domain Name System Security Extensions (dále jen DNSSEC), vylepšená škálovatelnost, vylepšená podpora pro internacionalizaci a vícejazyčné názvy domén.

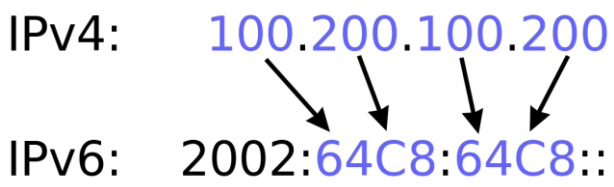
2.1.5 IPv6 Tunelovací protokoly

Definice

Jedná se o protokol používaný k přenosu IPv6 paketů přes IPv4 sítě. Ve většině případech se IPv6 pakety zapouzdří uvnitř IPv4 paketů, což jim umožní přenos přes IPv4 sítě. Existuje několik formátů IPv6 tunelovacího protokolu jako, 6to4, 6in4, 6over4, Teredo, ISATAP a GRE.

Formáty a jejich funkcionalita

a) 6to4 –je formát tunelování IPv6, který umožňuje komunikaci mezi sítěmi IPv6 prostřednictvím infrastruktury IPv4. IPv6 pakety se zapouzdří do IPv4 paketů, a jsou následně přeneseny přes IPv4 síť. V 6to4 je každému IPv6 zařízení přiřazena jedinečná globální IPv6 adresa s prefixem 2002::/16, která je vyhrazena pro tunelování. Prvních 16 bitů prefixu označuje, že se jedná o adresu formátovanou pro 6to4, zatímco dalších 32 bitů představuje převedenou IPv4 adresu z decimální soustavy do hexadecimální soustavy.



Obrázek 14 Zapouzdření
Zdroj: https://www.instaluj.cz/magazin/jak-zjistit-ip-adresu

Poté co je modifikovaný IPv4 paket přenesen do cíle, koncový uzel odstraní zapouzdření a předá originální IPv6 paket příjemci. Výhodou je, že umožňuje přenos IPv6 paketů přes stávající IPv4 infrastrukturu. Existují však omezení, jako je vliv na pakety procházením Network address translation (dále jen NAT) nebo fragmentace paketů.

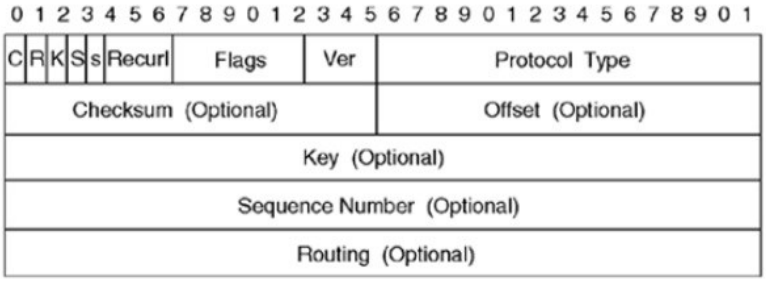
b) 6in4 – je formát tunelování IPv6, který umožňuje přenos IPv6 paketů přes IPv4 síť. Na rozdíl od 6to4, které používá automatické adresování, tento formát vyžaduje ruční konfiguraci koncových bodů tunelu. Každému konci tunelu je manuálně přiřazena adresa IPv4 a adresa IPv6. IPv6 pakety jsou zapouzdřeny uvnitř IPv4 paketů, přičemž cílová adresa je nastavena na IPv4 adresu koncového bodu tunelu. IPv4 pakety jsou poté přenášeny přes IPv4 síť na druhý konec tunelu, kde jsou IPv6 pakety extrahovány a předány do svého cílového konce. 6in4 se používá k vytváření tunelů typu point-to-point IPv6 v IPv4 síti. Jednou z výhod 6in4 je, že umožňuje detailnější konfiguraci tunelu ve srovnání s formáty tunelování, jako je 6to4.

c) 6over4 – je formát IPv6 přenosu, který je určený k přenosu IPv6 paketů mezi dual-stack uzly přes IPv4 síť s multicast vysíláním. V 6over4 je každému IPv6 uzlu přiřazena jedinečná IPv6 link-local adresa a také multicastová adresa v rozashu fe80::/64. Uzel pak naslouchá multicastovým paketům odeslaným na multicastovou adresu a následně odpovídá. Když je třeba přenést paket IPv6 z jednoho hostitele na druhého, je zapouzdřen do paketu IPv4 s cílovou adresou nastavenou na adresu vícesměrového vysílání 6over4. IPv4 paket je poté multicastově vyslán přes Local Aarea Network (dále jen LAN) všem ostatním uzlům nakonfigurovaným pro formát 6over4, cílový hostitel poté IPv6 paket odpouzdří a zpracuje. Jednou z výhod 6over4 je, že nevyžaduje žádnou speciální konfiguraci nebo vyhrazené tunely pro stávající konfiguraci sítě IPv4 v LAN. Naopak není vhodné pro přenos IPv6 paketů přes Wide Area Network (dále jen WAN).

d) Teredo - je protokol pro tunelování IPv6, který umožňuje komunikaci mezi zařízeními podporujícími IPv6 protokol prostřednictvím IPv4 sítě bez nutnosti jakýchkoli změn v síťové infrastruktuře. Byl navržen tak, aby pomohl přechodu z IPv4 na IPv6. Každému klientovi používající teredo je přiřazena jedinečná IPv6 adresa, která je odvozena z jeho IPv4 adresy a předdefinované předpony. Následně se adresa používá k zapouzdření IPv6 paketů do IPv4 paketů, které jsou odeslány přes IPv4 síť na přenosový server teredo. Server přijímá zapouzdřené IPv6 pakety a následně tyto pakety server zapouzdří i s odpovědí a odešle je zpět klientovi. Teredo může fungovat i v situaci, kdy je klient v NAT, teredo používá techniku "NAT hole punching" k navázání spojení přes NAT, která funguje následujícím způsobem. Klienti se připojí přes veřejnou IP adresu k serveru třetí strany a ten mezi nimi zprostředkuje spojení, tak že předá vnitřní a vnější adresu s číslami portů druhé straně. Strany si poté mezi sebou vytvoří spojení a díky znalosti portů mohou obejít restrikce firewallů nebo routerů.

e) Intra-Site Automatic Tunnel Addressing Protocol – Neboli ISATAP, jedná se o tunelovací protokol, který umožňuje komunikaci mezi zařízeními podporujícími IPv6 prostřednictvím IPv4 sítě bez nutnosti jakýchkoli změn v síťové infrastruktuře. ISATAP funguje ta stejném principu jako teredo, ale je určen pouze pro použití v NAT a nemůže poskytnout připojení mimo tuto síť.

f) Generic Routing Encapsulation – Neboli GRE, je to protokol používaný k zapouzdření jednoho protokolu přes jiný protokol, jako je zapouzdření IP paketů do IP paket. GRE se často používá ve Virtuální Privátní Síti (dále jen VPN) k vytvoření tunelu mezi dvěma body, což umožňuje bezpečný přenos dat přes nedůvěryhodnou síť. V tunelu GRE jsou koncové body identifikovány svými IP adresami a GRE hlavičkou. Po příjezdu do cílového koncového bodu je hlavička GRE odstraněna a původní paket je předán příjemci.



Obrázek 15 GRE paket

Zdroj: https://networkinterview.com/what-is-gre-generic-routing-encapsulation/

Tunely GRE lze použít k propojení sítí, které jsou odděleny, což jim umožňuje bezpečnou komunikaci, jako by byly připojeny přímo. Tunely lze také použít k obcházení firewallů nebo jiných síťových omezení. Jednou z výhod GRE je možnost zapouzdření ostatních síťových protokolů, jako je IPv4, IPv6 nebo Ethernet. GRE také podporuje použití více protokolů v jednom tunelu.

2.1.6 ICMPv6

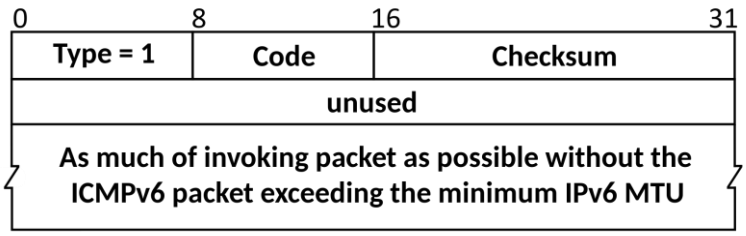
Definice

Internet Control Message Protocol version 6 (dále jen ICMPv6) je protokol používaný sítěmi IPv6 k odesílání chybových zpráv a provozních informací o síti. ICMPv6 zprávy používají síťová zařízení ke vzájemné komunikaci o problémech sítě a k provádění diagnostických funkcí.

Funkcionalita

Když ICMPv6 uzel přijme paket, musí provést akce, které závisí na typu zprávy. Protokol obsahuje několik chybových zpráv ty jsou značeny jako type.

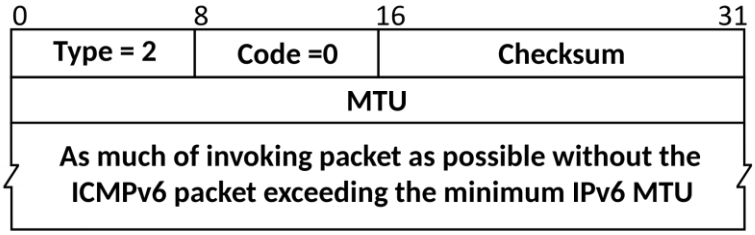
a) Destination Unreachable Message (Type 1) - je zpráva ICMPv6, která informuje odesílatele, že cílová síť nebo hostitel je nedosažitelný. Je generován routerem nebo hostitelem, když nemůže doručit IPv6 paket do destinace, taky obsahuje informace, které pomohou diagnostikovat problém.



Obrázek 16 Zpráva typu 1

Zdroj: By Michel Bakni - A. Conta, S. Deering and M. Gupta (March 2006) RFC 4443, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, The Internet Society, p. 10 DOI: 10.17487/RFC4443., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=112501440

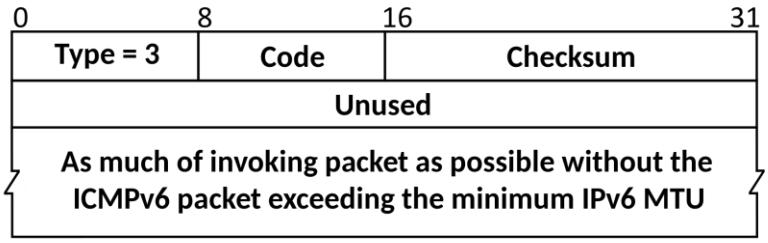
b) Packet Too Big Message (Type 2) - je zpráva ICMPv6, která informuje odesílatele, že paket je příliš velký na to, aby mohl být routerem předán bez fragmentace. Tato zpráva pomáhá předcházet zahlcení sítě a fragmentaci.



Obrázek 17 Zpráva typu 2

Zdroj: By Michel Bakni - A. Conta, S. Deering and M. Gupta (March 2006) RFC 4443, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, The Internet Society, p. 8 DOI: 10.17487/RFC4443., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=112501827

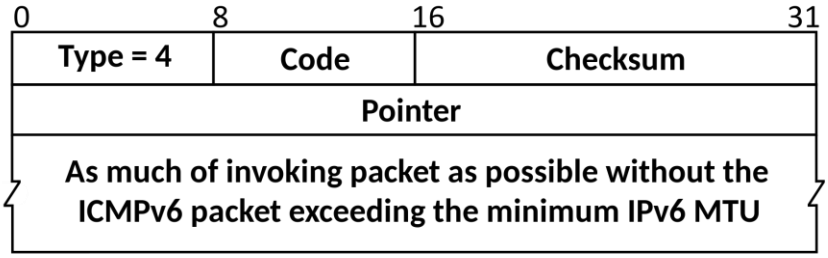
c) Time Exceeded Message (Type 3) - je chybová zpráva ICMPv6, která označuje, že paket nemohl být doručen, protože překročil maximální povolenou dobu pro průchod sítí.



Obrázek 18 Zpráva typu 3

Zdroj: By Michel Bakni - A. Conta, S. Deering and M. Gupta (March 2006) RFC 4443, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, The Internet Society, p. 11 DOI: 10.17487/RFC4443., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=112509177

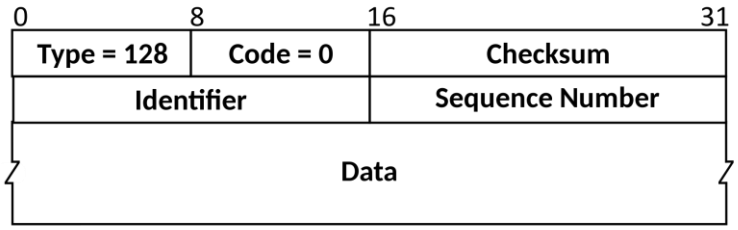
d) Parameter Problem Message (Type 4) - je zpráva ICMPv6, která informuje odesílatele, že paket obsahuje nesprávnou hlavičku IP adresy.



Obrázek 19 Zpráva typu 4

Zdroj: By Michel Bakni - A. Conta, S. Deering and M. Gupta (March 2006) RFC 4443, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, The Internet Society, p. 12 DOI: 10.17487/RFC4443., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=112509377

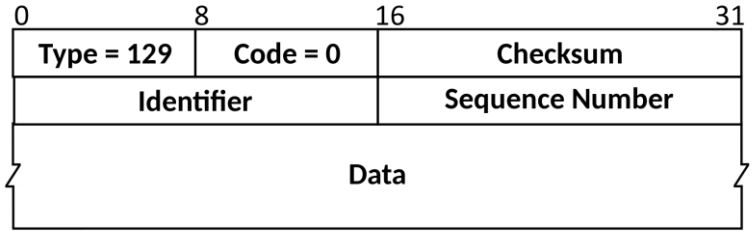
e) Echo Request Message (typ 128) - je zpráva ICMPv6, která se běžně používá k testování síťové konektivity. Odesílá se z jednoho uzlu na druhý a obsahuje identifikátor a pořadové číslo, které lze použít k identifikaci konkrétního paketu a sledování případných zpoždění nebo ztrát paketů.



Obrázek 20 Zpráva typu 128

Zdroj: By Michel Bakni - A. Conta, S. Deering and M. Gupta (March 2006) RFC 4443, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, The Internet Society, p. 13 DOI: 10.17487/RFC4443., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=112512448

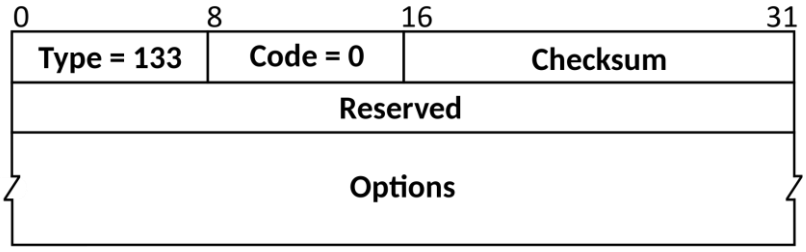
f) The Echo Reply Message (Type 129) - je zpráva ICMPv6, která je odeslána jako odpověď na zprávu typ 128. Obsahuje stejný identifikátor a pořadové číslo jako původní zpráva, což umožňuje odesílateli ověřit přijetí původního paketu a změřit případné zpoždění nebo ztrátu paketu.



Obrázek 21 Zpráva typu 129

Zdroj: By Michel Bakni - A. Conta, S. Deering and M. Gupta (March 2006) RFC 4443, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, The Internet Society, p. 14 DOI: 10.17487/RFC4443., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=112512897

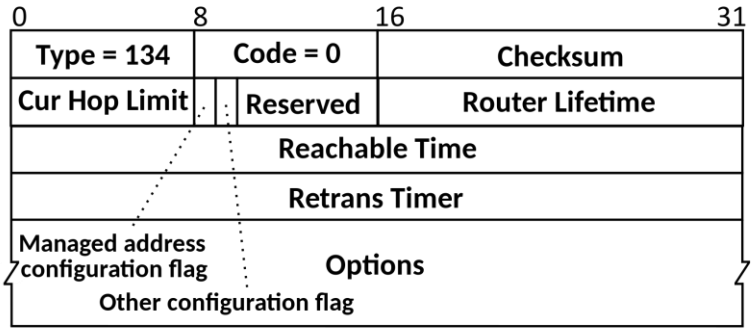
g) Router Solicitation Message (typ 133) - je zpráva ICMPv6, kterou odesílá hostitel, aby si vyžádal informace o konfiguraci routeru. Stejnou zprávu používá protokol NDP.



Obrázek 22 Zpráva typu 133

Zdroj: By Michel Bakni - T. Narten, E. Nordmark, W. Simpson and H. Soliman (September 2006) RFC 4861, Neighbor Discovery for IP version 6 (IPv6), The Internet Society, p. 22 DOI: 10.17487/RFC4861., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=112538022

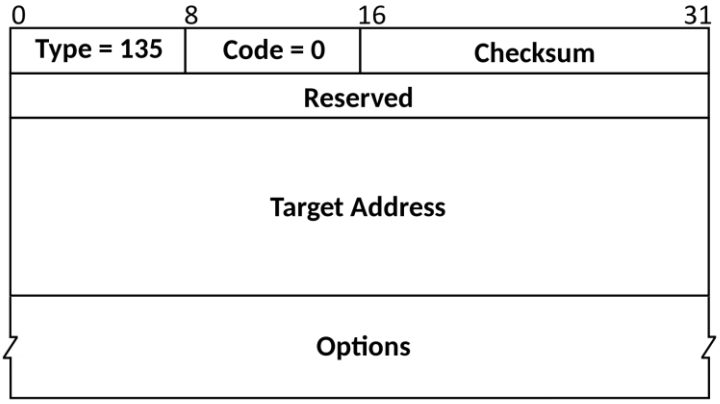
h) Router Advertisement Message (Type 134) - je zpráva ICMPv6, kterou odesílá router, aby oznámila svou přítomnost a konfigurační informace sousedním hostitelům. Obsahuje stejné informace jako a je zároveň používán u protokolu NDP.



Obrázek 23 Zpráva typu 134

Zdroj: By Michel Bakni - A. Conta, S. Deering and M. Gupta (March 2006) RFC 4443, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, The Internet Society, p. 10 DOI: 10.17487/RFC4443., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=112501440

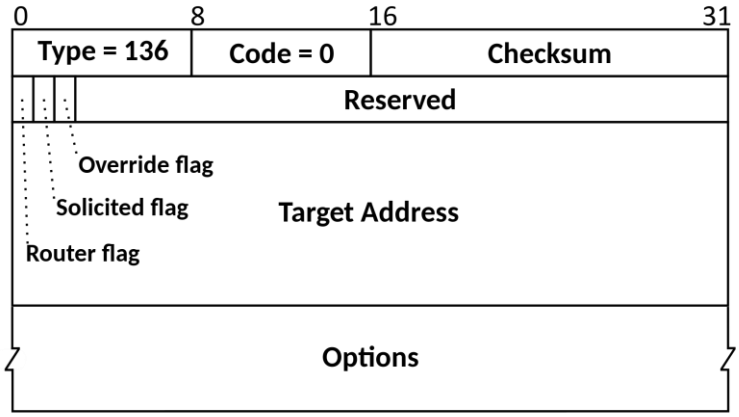
i) Neighbor Solicitation Message (Type 135) - je zpráva ICMPv6, která se používá k určení adresy sousedního uzlu. Funguje stejně jako u protokolu NDP.



Obrázek 24 Zpráva typu 135

Zdroj: By Michel Bakni - T. Narten, E. Nordmark, W. Simpson and H. Soliman (September 2006) RFC 4861, Neighbor Discovery for IP version 6 (IPv6), The Internet Society, p. 18 DOI: 10.17487/RFC4861., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=112559830

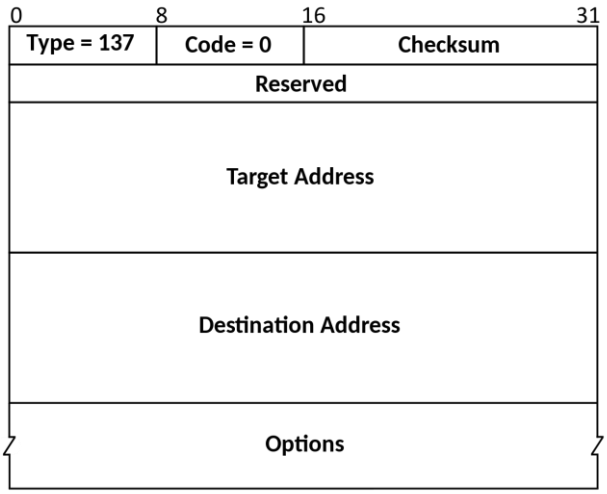
j) Neighbor Advertisement Message (Type 136) - je zpráva odeslaná uzlem v IPv6 síti, aby zjistil jeho přítomnost a aktualizoval sousedy o jeho stavu. Tato zpráva je obvykle zasílána jako odpověď na NS zprávu od souseda. Funguje stejně jako u protokolu NDP.



Obrázek 25 Zpráva typu 136

Zdroj: By Michel Bakni - T. Narten, E. Nordmark, W. Simpson and H. Soliman (September 2006) RFC 4861, Neighbor Discovery for IP version 6 (IPv6), The Internet Society, p. 18 DOI: 10.17487/RFC4861., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=112559830

k) A Redirect Message (Type 137) - je zpráva ICMPv6, používaná routerem k informování klienta, že pro konkrétní cíl existuje lepší uzel dalšího hopu. Zpráva obsahuje adresu nového uzlu dalšího skoku a cílovou adresu, pro kterou platí přesměrování.



Obrázek 26 Zpráva typu 137

Zdroj: By Michel Bakni - T. Narten, E. Nordmark, W. Simpson and H. Soliman (September 2006) RFC 4861, Neighbor Discovery for IP version 6 (IPv6), The Internet Society, p. 26 DOI: 10.17487/RFC4861., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=112550312

2.1.7 Dual-stack

Definice

Dual-stack je síťová architektura, která umožňuje protokolům IPv4 a IPv6 existovat a komunikovat spolu na stejné síťové infrastruktuře.

Funkcionalita

Komunikacec probíhá tak, že na síťových zařízeních, běží souběžně protokoly IPv4 i IPv6.
V síti s dual-stackem mohou zařízení mezi sebou komunikovat pomocí protokolu IPv4 nebo IPv6 v závislosti na preferencích každého zařízení. Dual-stack má přednost před jinými přenosovými protokoly, jako je tunelování. Důvodem je fakt že poskytuje jednodušší a efektivnější způsob, jak umožnit komunikaci mezi zařízeními. Všechna zařízení v síti mohou mezi sebou komunikovat přímo, bez potřeby zprostředkujících zařízení, to zvyšuje bezpečnost a snižuje odezvu.

Happy Eyeballs

Happy Eyeballs je technika používaná ke zlepšení uživatelského pohodlí pro služby, které jsou dostupné přes protokoly IPv4 i IPv6. Funguje tak, že testuje oba protokoly současně a vybírá ten, který poskytuje nejmenší dobu odezvy. Když uživatel požádá o službu, jeho zařízení zahájí pokus o připojení pomocí protokolů IPv4 a IPv6 současně. K připojení bude použit rychlejší protokol, druhý protokol bude zrušen

2.1.8 OSPFv3

Definice

Open Shortest Path First version 3 (dále jen OSPFv3) je internetový směrovací protokol určený k distribuci směrovacích informací v rámci jednoho systému. OSPFv3 je nástupcem OSPFv2 a je rozšířením původního protokolu OSPF, který byl vyvinut pro podporu sítí IPv6.

Funkcionalita

OSPFv3 používá algoritmus link-state routing (dále jen LSR), což znamená, že každý router v síti má pohled na celou topologii sítě a na základě těchto informací vypočítá nejkratší cestu ke každému cíli. Výsledkem je efektivní využití síťových zdrojů. OSPFv3 používá multicast adresy (FF02::5 a FF02::6), rezervované pro zjišťování sousedů a komunikaci mezi routeri. Podporuje také více oblastí, což umožňuje rozdělit síť na menší oblasti pro lepší škálovatelnost a snadnější správu.

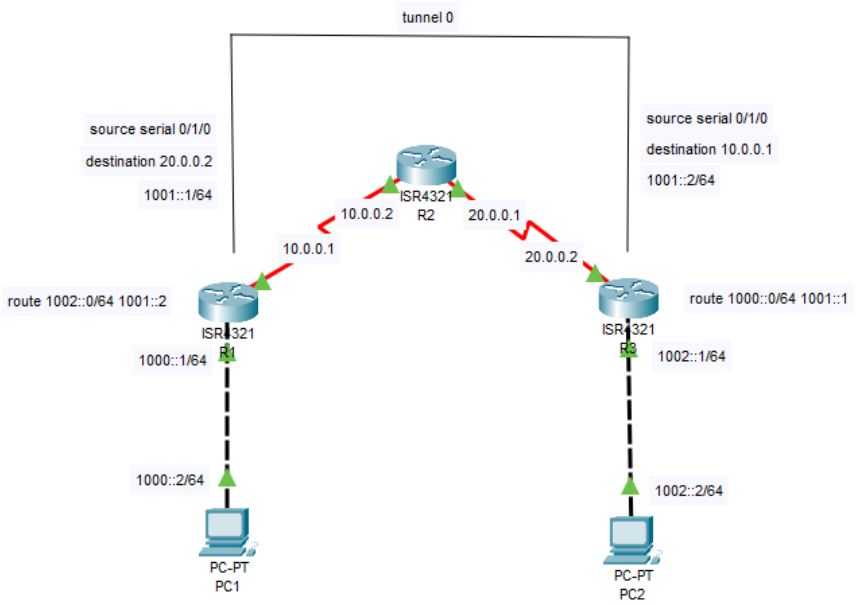
3 PRAKTICKÁ ČÁST

Zamyšlení

Před tím, než se vrhneme do samotného zprovoznění IPv6, měli bychom se zamyslet, jestli vůbec potřebujeme IPv6. Přestože se jedná o novější verzi internet protokolu a poskytuje větší rozsah adres pro rostoucí zařízení, je bezpečnější než IPv4, a to díky zabudovanému šifrování a lepší ověření pravosti. Mimo jiné poskytuje mnoho výhod v oblasti kvality služby, rychlejší, efektivnější a spolehlivější internetový provoz. Pohled do budoucna, čím víc zařízení zavede tento protokol bude velmi důležité mít IPv6 kompatibilitu, pokud bychom potřebovali tuhle metodu zavést ihned, musíme si dávat pozor, ne každé zařízení je IPv6 kompatibilní a nepodporuje tento protokol. Jestliže vám dochází IPv4 adresy může být praktické přejít na IPv6, ale nemusí to být nutně dobrý důvod k přechodu. Komplexita, jen přece je IPv6 víc komplexní protokol od IPv4, to může být velmi náročně na správu, čas a zdroje obzvlášť pokud jste malá firma nebo organizace.

3.1 Návrh

Návrh praktického úkolu jsem provedl v Packet traceru, a snažil jsem se napodobit školní vybavení. Jako praktické cvičení jsem si vybral zavedení IPv6 propojení přes IPv4 router za pomocí tunelování. Návrh infrastruktury sítě jsem si připravil v Packet traceru podle skutečné struktury ve škole.

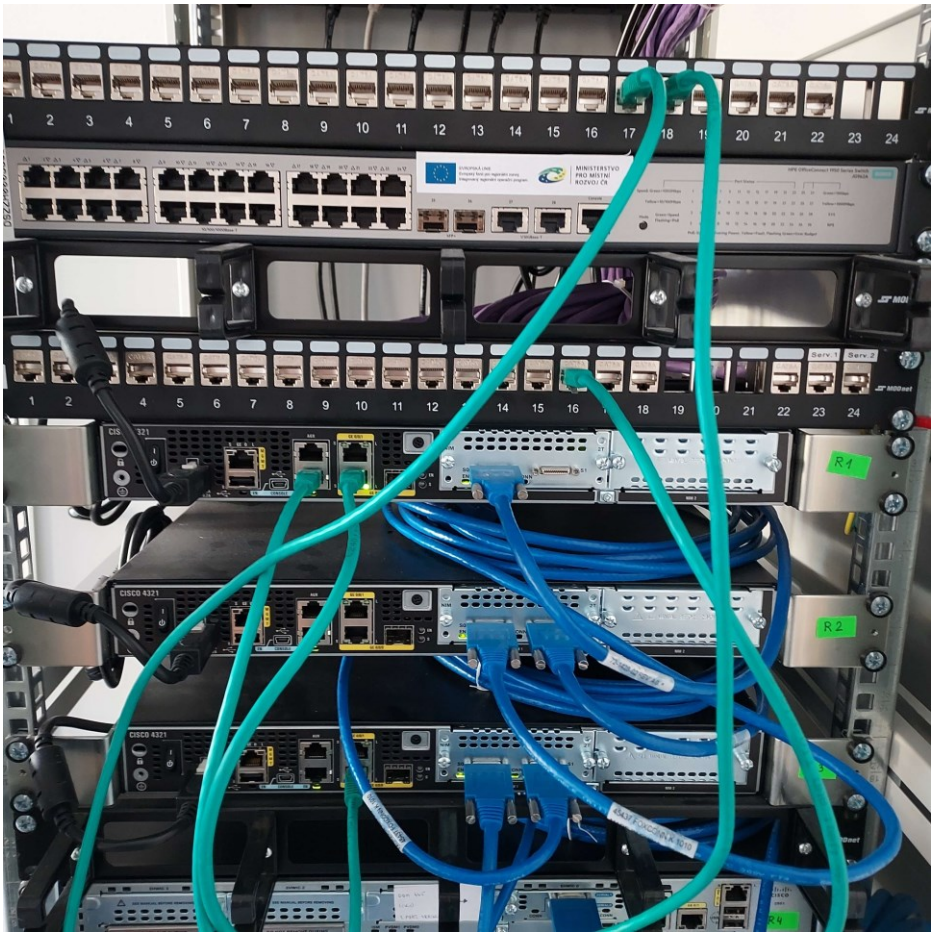


Obrázek 27 Struktura sítě

Zdroj: Vlastní

3.2 Postup

Samotný postup jsem započal zapnutím 2 počítačů s virtuálními stroji s operačním systémem Windows a nastavením síťového mostu. Síťový most zaručí že sítové připojení bude registrováno virtuálním strojem. Dále jsem zapojil několik kabelů do přiřazených rozhraní podle návrhu v Packet traceru.



Obrázek 28 Fyzické propojení routerů a počítačů

Zdroj: vlastní

Propojil jsem tři routery sériovým kabelem, které jsem pojmenoval R1, R2 a R3, dva z těchto routerů budou složit jako koncové body tunelu, ten třetí poslouží jako zařízení výhradně jen s technologií IPv4. Jako další krok jsem nastavil IPv6 adresy dvou počítačům PC1 a PC2. A začal jsem nastavovat routery postupně od R1 až k R3. Každý router má vlastní konfiguraci, pomocí které dokáže komunikovat s ostatními zařízení. K zprovoznění tunelu jsem využil protokolu EIGRP. Po dokončení konfigurace routerů jsem si ověřil příkazem ping, jestli dostanu odpověď mezi počítači. Všechnu funkčnost si můžete vyzkoušet v přiloženém souboru s názvem PK_prakticky_ukol.pkt.

```
en
config t

hostname R1
ipv6 unicast-routing

int g0/0/0
ipv6 address 1000::1/64
no shut

int s0/1/0
ip address 10.0.0.1 255.0.0.0
no shut

int tunnel 0
tunnel source serial 0/1/0
tunnel destination 20.0.0.2
tunnel mode ipv6ip
ipv6 address  1001::1/64
exit

router eigrp 1
net 10.0.0.0
exit

ipv6 route 1002::0/64 1001::2
exit
write
exit
```

Obrázek 29 Konfigurace R1

Zdroj: Vlastní

```
en
config t

hostname R2

int s0/1/0
ip address 10.0.0.2 255.0.0.0
no shut

int s0/2/0
ip address 20.0.0.1 255.0.0.0
no shut

router eigrp 1
net 10.0.0.0
net 20.0.0.0

exit
write
exit
```

Obrázek 30 Konfigurace R2

Zdroj: Vlastní

```
en
config t

hostname R3
ipv6 unicast-routing

int g0/0/0
ipv6 address 1002::1/64
no shut

int s0/1/0
ip address 20.0.0.2 255.0.0.0
no shut

int tunnel 0
tunnel source serial 0/1/0
tunnel destination 10.0.0.1
tunnel mode ipv6ip
ipv6 address 1001::2/64
exit

router eigrp 1
net 20.0.0.0
exit

ipv6 route 1000::0/64 1001::1
exit
write
exit
```

Obrázek 31 Konfigurace R3

Zdroj: Vlastní

Úkoly pro žáky

V příloze najdete 2 cvičení s technologiemi IPv6 v Packet traceru pro žáky 3. ročníku Obchodní akademie. Zadání je napsáno přímo v úlohách. Heslo pro učitele do Packet tracer activiti wizard je krajsa2023.

ZÁVĚR

Zatímco protokoly IPv4 a IPv6 jsou používány k identifikaci síťových zařízení a usnadnění komunikace přes internet, mají významné rozdíly ve svém designu a schopnostech. IPv4 používá 32bitové adresy, což omezuje počet dostupných adres, zatímco IPv6 používá 128bitové adresy, což umožňuje prakticky neomezený počet adres. IPv6 navíc nabízí vylepšené funkce zabezpečení, zjednodušenou konfiguraci sítě a podporu pokročilých funkcí, jako je multicast a anycast. Navzdory mnoha výhodám IPv6 je přechod z IPv4 pomalý kvůli rozšířenému používání IPv4 a nákladům a složitosti vylepšení infrastruktury na podporu IPv6. Vyčerpáním IPv4 adres se však přijetí IPv6 stává stále více nezbytným pro pokračující růst a rozvoj internetu. A proto je dle mého názoru důležité, aby organizace začaly plánovat a implementovat přechod na IPv6, aby zůstaly konkurenceschopné a zajistily si dlouhou životnost své síťové infrastruktury.

SEZNAM POUŽITÉ LITERATURY

(1) *IPv6* [online]. [cit. 2022-11-02]. Dostupné z: https://en.wikipedia.org/wiki/IPv6

(2) *IBM Dual-stack* [online]. [cit. 2022-11-03]. Dostupné z: https://www.ibm.com/docs/en/zos/2.4.0?topic=ipv6-dual-mode-stack

(3) *IPv4-mapped IPv6 addresses* [online]. [cit. 2022-11-03]. Dostupné z: https://www.ibm.com/docs/en/zos/2.2.0?topic=addresses-ipv4-mapped-ipv6

(4) *Tunneling protocol* [online]. [cit. 2022-11-03]. Dostupné z: https://en.wikipedia.org/wiki/Tunneling_protocol

(5) *What is tunneling?* [online]. [cit. 2022-11-03]. Dostupné z: https://www.cloudflare.com/learning/network-layer/what-is-tunneling/

(6) *Encapsulation* [online]. [cit. 2022-11-03]. Dostupné z: https://en.wikipedia.org/wiki/Encapsulation_(networking)

(7) *Cisco Dual-stack* [online]. [cit. 2022-11-04]. Dostupné z: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/IPV6at_a_glance_c45-625859.pdf

(8) *What is IPv6?* [online]. [cit. 2022-11-29]. Dostupné z: https://www.cisco.com/c/en/us/solutions/ipv6/overview.html

(9) *IPv4* [online]. [cit. 2023-01-22]. Dostupné z: https://cs.wikipedia.org/wiki/IPv4

(10) *Microsoft DHCP* [online]. [cit. 2023-02-15]. Dostupné z: https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-dhcpe/70714561-144a-4b02-9bc2-815cd26a1dcc

(11) *RFC 2460* [online]. [cit. 2023-03-06]. Dostupné z: https://www.rfc-editor.org/rfc/rfc2460

(12) *RFC 4443* [online]. [cit. 2023-03-06]. Dostupné z: https://www.rfc-editor.org/rfc/rfc4443

(13) *RFC 4861* [online]. [cit. 2023-03-07]. Dostupné z: https://www.rfc-editor.org/rfc/rfc4861

(14) RFC 4862 [online]. [cit. 2023-03-07]. Dostupné z: https://www.rfc-editor.org/rfc/rfc4862

(15) RFC 8200 [online]. [cit. 2023-03-08]. Dostupné z: https://www.rfc-editor.org/rfc/rfc8200

(16) RFC 4291 [online]. [cit. 2023-03-08]. Dostupné z: https://www.rfc-editor.org/rfc/rfc4291.html

(17) Cisco Configuring Dual-stack [online]. [cit. 2023-03-12]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_5_1/sysConfig/CUCM_BK_SE5DAF88_00_cucm-system-configuration-guide-1151/CUCM_BK_SE5DAF88_00_cucm-system-configuration-guide-1151_chapter_01101.pdf

(18) Packet Tracer: Activity Wizard - Instructions [online]. [cit. 2023-03-15]. Dostupné z: https://www.youtube.com/watch?v=qQ7oe4thAdA&ab_channel=CPTinDepth

(19) Packet Tracer: Activity Wizard [online]. [cit. 2023-03-15]. Dostupné z: https://www.youtube.com/watch?v=4ySBbcK0hr0&ab_channel=CPTinDepth

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

1. IPv4 – Internet Protocol version 4
2. IPv6 – Internet Protocol version 6
3. IP – Internet Protocol
4. MTU – Maximum Transition Unit
5. PIM – Protocol-Independent Multicast
6. MLD – Multicast Listener Discovery
7. IPsec – Internet Protocol Security
8. DHCP – Dynamic Host Configuration Protocol
9. APIPA – Automatic Private Internet Protocol Addressing
10. SLAAC – Stateless Address Autoconfiguration
11. DHCPv6 – Dynamic Host Configuration Protocol version 6
12. DAD – Duplicate Address Detection
13. MAC – Media Access Control
14. EUI-64 – Extended Unique Identifier-64
15. DUID – DHCPv6 Unique Identifier
16. DUID-LTT – Link-layer address plus Time
17. DUID-UUID – Universally Unique Identifier
18. NDP – Neighbor Discovery Protocol
19. ARP – Address Resolution Protocol
20. NS – Neighbor Solicitation
21. NA – Neighbor Advertisement
22. RS – Router Solicitation
23. RA – Router Advertisement
24. ICMPv6 – Internet Control Message Protocol version 6
25. DNSv6 – Domain Name System version 6
26. DNSSEC – Domain Name Systém Security Security Extensions
27. DNS – Domain Name System
28. NAT – Network Address Translation
29. LAN – Local Area Network
30. WAN – Wide Area Network
31. ISATAP – Intra-Site Automatic Tunnel Addressing Protocol
32. GRE – Generic Routing Encapsulation

33. OSPFv3 – Open Shortest Path First version 3
34. OSPFv2 – Open Shortest Path First version 2
35. LSR – Link State Routing
36. EIGRP – Enhanced Interior Gateway Routing Protocol

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH