

Slovenská technická univerzita  
Fakulta informatiky a informačných technológií

*Tím č. 6*

## **Sieťový protokol IPv6**

### **Tímový projekt I**

**Študijný program:** Počítačové a komunikačné systémy a siete

**Študijný odbor:** 9.2.4 Počítačové inžinierstvo

**Miesto vypracovania:** Ústav počítačových systémov a sietí, FIIT STU Bratislava

**Vedúci témy:** Ing. Peter Magula, PhD.

**Členovia tímu:** Bc. Lukáš Danielovič  
Bc. Anton Pôbiš  
Bc. Lukáš Lenčేశ  
Bc. Marek Dukát

# Obsah

<b>Zoznam tabuliek.....</b>	<b>3</b>
<b>Zoznam obrázkov.....</b>	<b>4</b>
<b>Zadanie.....</b>	<b>1</b>
<b>Úvod .....</b>	<b>1</b>
<b>1. Analýza.....</b>	<b>3</b>
1.1. Prehľad protokolu Internet Protokol verzie 6.....	3
1.1.1. Základná hlavička datagramu .....	3
1.1.2. Adresácia IPv6.....	4
1.1.3. Typy adres.....	6
1.1.4. Autokonfigurácia .....	8
1.1.5. Dopĺňujúce (rozširujúce) hlavičky.....	9
1.1.6. ICMPv6.....	12
1.1.7. Mobilita.....	13
1.1.8. Bezpečnosť Internet Protokolu verzie 6 .....	13
1.1.8.1. Bezpečnosť na linkovej vrstve .....	13
1.1.8.2. IPSec.....	14
1.1.8.3. Autentifikačná hlavička (AH) .....	16
1.1.8.4. Encapsulation Security Payload (ESP) .....	17
1.2. Možnosti nasadenia IPv6 .....	19
1.2.1. Dual Stack.....	20
1.2.2. Tunelovanie.....	22
1.2.3. Preklad .....	27
1.2.4. Jednorazový prechod na IPv6 .....	28
1.3. Existujúce portály o IPv6 .....	29

1.4. Simulátor GNS3 .....	32
<b>2. Špecifikácia požiadaviek .....</b>	<b>33</b>
2.1. Funkcionálne požiadavky.....	33
2.2. Nefunkcionálne požiadavky .....	34
<b>3. Hrubý návrh.....</b>	<b>35</b>
3.1. Štrukturálny návrh portálu .....	35
3.2. Funkcionalita z pohľadu používateľa.....	36
3.2.1. Proces prístupu používateľa k portálu .....	36
3.2.2. Proces otestovania používateľa.....	37
3.3. Návrh grafického rozhrania web stránky portálu .....	38
<b>4. Implementácia prototypu.....</b>	<b>42</b>
4.1. Dizajn hlavnej stránky prototypu .....	43
4.2. Štruktúra prototypu .....	45
4.3. Registrácia do portálu.....	47
4.4. Testovanie v prototypu .....	48
<b>5. Externé prílohy.....</b>	<b>50</b>
<b>6. Literatúra.....</b>	<b>51</b>

## Zoznam tabuliek

Tabuľka 1-1.: Oblasti skupinových adries .....	7
Tabuľka 1-2 Rozvrhnutie IPv6 adresného priestoru .....	7
Tabuľka 1-3 Čísla rozširujúcich hlavičiek IPv6 datagramu .....	9
Tabuľka 1-4 Čísla protokolov pracujúcich nad IP .....	9
Tabuľka 1-5 Poradie rozširujúcich hlavičiek.....	9

## Zoznam obrázkov

Obr. 1-1 Základná hlavička IPv6 datagramu .....	4
Obr. 1-2.: Režimy IPsec .....	15
Obr. 1-3.: IPv6 datagram zahŕňajúci rozšírenú hlavičku smerovania a voľby pre cieľ .....	16
Obr. 1-4.: IPv6 datagram obalený autentifikačnou hlavičkou .....	16
Obr. 1-5.: Formát hlavičky AH.....	17
Obr. 1-6.: ESP hlavička a datagram IPv6 .....	18
Obr. 1-7.: Hlavička ESP.....	18
Obr. 1-8.: 6in4 Smerovač - Smerovač .....	23
Obr. 1-9.: 6in4 Koncová stanica-Smerovač .....	23
Obr. 1-10.: 6to4.....	24
Obr. 1-11.: Statický tunel.....	26
Obr. 1-12.: NAT-PT.....	27
Obr. 1-13.: GNS 3 .....	32
Obr. 3-1: Moduly portálu .....	35
Obr. 3-2.: Prípád použitia: prístup k portálu .....	36
Obr. 3-3.: Prípád použitia: otestovanie používateľa .....	37
Obr. 3-4.: Rozloženie stránky .....	38

# Zadanie

*Vedúci tímu: Ing. Peter Magula, PhD.*

Analyzujte problematiku sieťového protokolu IP verzie 6 so zameraním sa na možnosti jeho nasadenia, prechodu z protokolu IP verzie 4 a jeho bezpečnosť. Na základe vykonanej podrobnej analýzy navrhnete edukačný systém určený pre sieťových odborníkov, správcov systémov a sietí, študentov ako aj širokú verejnosť. Navrhnutý systém implementujte ako webový portál. Systém musí poskytovať základné informácie pre širokú verejnosť, odborné informácie pre sieťových špecialistov, praktické informácie pre správcov systémov a sietí ako aj informácie pre študentov informatiky a príbuzných odborov spolu možnosťou testovania nadobudnutých znalostí. Pri implementácii systému použite aj multimediálne grafické prezentačné prostriedky.

## Úvod

Jedným zo základných protokolov v neustále sa zväčšujúcom digitálnom svete je sieťový protokol *Internet protokol*. Tento základný kameň a nosný múr Internetu je najčastejšie používaným protokolom v komunikácii počítačov.

Prvé verzie protokolu IP (1, 2 a 3) sa používali v dobe vývoja Internetových protokolov v rokoch 1977 – 1980. Tieto sú zdokumentované ako IEN (Internet Experiment Notes, dostupné na <http://www.rfc-editor.org/ien/ien-index.html>)

V roku 1981 bol vydaný dokument RFC 971, ktorý špecifikuje verziu 4 Internet Protokolu. Táto verzia sa v praxi ujala a stala sa veľmi obľúbenou. Po 12 rokoch používania tohto protokolu sa kvôli rýchlemu klesaniu počtu voľných IPv4 adries a vtedajšiemu nesystematickému spôsobu ich prideľovania (nakolko sa prideľovali organizáciám celé bloky adries) začalo uvažovať nad jeho nástupcom. V roku 1993 boli prednesené požiadavky na nový protokol a bola zriadená pracovná skupina *IPng*. Prvý výsledok priniesli špecifikáciou IPng (IP next generation), alebo IPv6, v dokumente *RFC 1752 (The Recommendation for the IP Next Generation Protocol)*.

Medzitým ubehli ďalšie dve desiatky rokov a protokol IPv6 ešte stále nebol plnohodnotne nasadený (v septembri 2013 bolo percento používateľov prístupujúcich ku službám spoločnosti Google prostredníctvom IPv6 protokolu rovné dvom).

IPv4 sa počas týchto rokov čakania na svojho nástupcu musela prispôbovať neustále narastajúcemu záujmu o IP adresy. Do IPv4 boli implementované nové techniky a spôsoby pridelovania adries:

- začal sa používať preklad sieťových adries (NAT) pre obmedzenie spotreby verejných adries.
- povolilo sa adresovanie s premenlivou dĺžkou adresy siete (VLSM)
- implementovalo sa smerovanie bez ohľadu na triedu adries IPv4 (CIDR)

Tieto opatrenia však ale neodstránili konečnú nutnosť nasadenia IPv6. Mechanizmus NAT sa ukazuje ako problémové riešenie pri zavádzaní bezpečnostných opatrení do siete (IPSec) a taktiež neumožňuje priamu komunikáciu *peer-to-peer*. CIDR nie je dostatočným opatrením pre narastanie smerovacích tabuliek na hraničných smerovačoch.

Nárast nárokov na IP adresy súvisí s novými inteligentnými koncovými zariadeniami (PDA, hybridné mobilné telefóny poskytujúce hlas cez IP či dokonca domáce spotrebiče ako napr. chladnička)

Nasadenie IPv6 sa neustále posúva a odkladá. Neustále sa menia dokumenty, ktoré špecifikujú tento nový protokol. Prejsť na nový protokol sa ukazuje ako problematické. Ako masívne zabezpečiť prechod všetkých teraz pracujúcich zariadení na IPv4? Je až také nákladné administratívne prečíslovať adresy? V mnohých prípadoch by bolo potrebné aj zariadenia vymeniť, prípadne softvér.

Ďalšou variantov, nie tak radikálnou zmenou, je možnosť koexistencie oboch protokolov súčasne. Staršie zariadenia komunikujúce na staršom protokole, novšie na novšom – ako bude fungovať komunikácia navzájom? Ako budú vyzeráť smerovacie tabuľky?

Cieľom tohto projektu je vytvorenie portálu, ktorý priblíži problematiku IPv6 svojim návštevníkom. Okrem širokej teoretickej analýzy problému IPv6, je jeho cieľom aj prakticky poukázať a vysvetliť túto oblasť.

# 1. Analýza

V tejto časti dokumentu je bližšie opísaná problematika, ktorú tím č. 6 rieši. Kapitola je rozdelená na dve väčšie sekcie: v prvej je analyzovaný samotný protokol IPv6, jeho vlastnosti, charakteristiky a možnosti jeho nasadenia. V druhej podkapitole sa opisuje prehľad a spôsoby, ako možno docieľiť implementáciu edukačného portálu zameraného na protokol IP verzie 6.

## 1.1. Prehľad protokolu Internet Protokol verzie 6

Pri navrhovaní nového protokolu sa návrhári zamerali hneď na niekoľko vlastností. Rozšírenie adresného priestoru nie je jediným prínosom IPv6, medzi ďalšie špecifické vlastnosti protokolu IPv6 patria:

- rozšírený adresný priestor ( $2^{128}$ , tj. až  $10^{38}$  jedinečných adries)
- automatické nastavenie parametrov
- podpora autentifikácie a šifrovania
- rozšírená podpora pre mobilitu
- podpora kvality služieb
- nové spôsoby adresovania

Aktuálny dokument, ktorý špecifikuje protokol IPv6 je:

*RFC 2460 Internet Protocol, Version 6 (IPv6) Specification.*

### 1.1.1. Základná hlavička datagramu

Každý protokol je prakticky definovaný dvojicou *pravidlá* – *datagram*. Datagram protokolu IPv6 obsahuje zase datagramy vyšších vrstiev (TCP, UDP) a vnára sa do datagramov nižších vrstiev. Datagramy na sieťovej vrstve modelu ISO/OSI (resp. internetovej vrstve modelu TCP/IP) sa všeobecne nazývajú *pakety*. Ďalej sa zameriame na hlavičku paketu IPv6.

Hlavička paketu IPv6 má pevne definovanú veľkosť 40 bajtov, čo je dvojnásobok oproti IPv4. Podstatnú časť zaberá adresa odosielateľa a príjemcu. Oproti IPv4, už základná hlavička neobsahuje informáciu o svojej dĺžke (keďže je pevne definovaná) a boli vynechané voliteľné informácie (zabezpečia ich rozšírené hlavičky). Taktiež bol vynechaný kontrolný súčet, pretože toto zabezpečuje druhá (linková) vrstva.

Počíta sa s tým, že fragmentácia sa v dobe, keď bude IPv6 hlavným protokolom Internetu, bude vyskytovať len výnimočne, a preto bola aj informácia o fragmentoch vyňatá zo základnej hlavičky a prenáša sa len ak je to potrebné v rozširujúcej hlavičke. Proces fragmentácie pre protokol IPv6 má významné odlišnosti od IPv4 a bude mu venovaná samostatná kapitola.



Obr. 1-1 Základná hlavička IPv6 datagramu

Vývojári IPv6 sa snažili zmenšiť a tým pádom aj zjednodušiť základnú hlavičku ako to len bolo možné. Zároveň ale museli vytvoriť priestor na nové vymoženosti protokolu. Dosiahli toho pomocou zreťazenia hlavičiek takzvanými doplnujúcimi hlavičkami.

### 1.1.2. Adresácia IPv6

Veľkosť IPv6 adresy je 128 bitov, čo predstavuje  $2^{128}$  adries. Adresy sa zapisujú v šestnástkovej sústave po dvojiciach bajtov (slovách), ktoré sú navzájom oddelené pomocou dvojbodky.

Príklad zápisu adresy ethernetového rozhrania:

*fe80:0000:0000:0000:0250:8dff:fea4:cdc5*

Aby bol zápis adries prehľadnejší a šetrili sa ruky správcov sietí (nikto nepredpokladá, že by používatelia museli pracovať s nejakými IPv6 adresami – vďaka autokonfigurácii), môžeme adresu zapísať v skrátenej forme, čo znamená, že viacero za sebou idúcich nulových čísel môžeme spojiť do jednej nuly, prípadne ich zápis úplne vynechať. Samozrejme, môžeme to spraviť len tak, aby sa nezmenila výsledná hodnota slova. Takže hore uvedená adresa sa dá zapísať aj takto:

*fe80:0:0:0:250:8dff:fea4:cdc5*

ale aj takto:

*fe80::250:8dff:fea4:cdc5*



Na prvý pohľad je zrejmé, že formát IPv6 adresy a MAC adresy ethernetových rozhraní má spoločný základ – hexadecimálny spôsob zápisu. To umožňuje napríklad využiť MAC adresu ako časť IPv6 adresy. Otázne je, ako to bude vplývať na pocit súkromia a anonymity v sieti Internet, pretože týmto spôsobom bude jednoznačne identifikovateľný počítač (respektíve jeho sieťové rozhranie), z ktorého bude používateľ pripojený. Našťastie je ale možné túto adresu zmeniť, takže sa to týka hlavne autokonfigurácie.

Adresy v IPv6 majú dve rôzne funkcie, ktoré v IPv4 koexistujú. Sú to funkcia umiestnenia a funkcia identifikácie.

**Informácia umiestnenia (lokátor)** – je potrebná pre smerovanie v sieti, pretože predstavuje podklad pre nájdenie cesty k cieľu. Ponúka 3 úrovne agregácie (*TLA – Top-Level aggregator, NLA – Next-Level aggregator a SLA – Site-Level Aggregator*, RFC 3587).

**Identifikácia (identifikátor)** – označuje špecifické zariadenie alebo rozhranie.

V IPv4 boli lokátor a identifikátor jedno a to isté, a preto boli problémy s mobilitou a viacnásobným pripojením k Internetu.

### 1.1.3. Typy adresies

**Unicast** predstavuje najčastejšie používané individuálne adresy, ktoré rovnako ako v IPv4 aj IPv6 adresujú sieťové rozhrania a nie uzly ako také. Môže mať niekoľko typov formátov (pozri tabuľka nižšie): globálna na základe poskytovateľa, lokálna na linke, lokálna miestne, zlučiteľná s IPv4 a adresa loopback.

Štruktúru takejto adresy najnovšie definuje dokument:

*RFC 6177 IPv6 Address Assignment to End Sites*

**Multicast** adresuje skupiny uzlov, presnejšie adresies ich sieťových rozhraní. Je to prepracovanejšia obdoba broadcastu, s ktorým sa stretávame pri IPv4. Skupinové adresy môžu byť stále alebo len dočasne pridelené.

Adresa s prefixom FF01::1 je rezervovaná pre všetky IPv6 adresy v rámci jedného rozhrania. Adresa s prefixom FF02::1 pre všetky rozhrania v rámci jedného sieťového segmentu.

Formát a pridelenie skupinovej adresy špecifikujú dokumenty:

*RFC 2375 IPv6 Multicast Address Assignments*

*RFC 3306 Unicast-Prefix-based IPv6 Multicast Addresses*

*RFC 3307 Allocation Guidelines for IPv6 Multicast Addresses*

*RFC 3587 IPv6 Global Unicast Address Format*

*RFC 3956 Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*

*RFC 4489 A Method for Generating Link-Scoped IPv6 Multicast Addresses*

**Anycast** je novým typom adresy, ktorá umožňuje mať definovanú skupinu uzlov, pri ktorej kontaktovaní bude vytvorené spojenie len s jedným uzlom – tým, ktorý je k nám najbližšie. To umožňuje optimalizovať sieťovú prevádzku, šetriť drahé chrbticové linky a rozkladať záťaž medzi jednotlivé uzly v skupine.

Dokument *RFC 4007 IPv6 Scoped Address Architecture* definuje pre jednotlivé typy adresies tzv. „oblasti“ (zóny platnosti). Každá adresa má určenú oblasť, v ktorej je táto adresa jednoznačná. Typickým príkladom adresy s výrazne obmedzenou oblasťou sú lokálne linkové adresy – pre ne platí, že majú ako oblasť určenú len jednu linku (Ethernet, Wi-Fi, a podobne).

Pre individuálne adresy (unicast) sú špecifikované dve oblasti: lokálne linkové (na linke) a globálne (celosvetový dosah). To tiež platí aj pre výberové adresy (anycast).

Pre skupinové adresy (multicast) sú určené rôznorodejšie oblasti (zóny platnosti). Skupinová adresa začína prefixom *11111111 (FF)*, nasledujú 4 bity určujúce voľby a ďalšie 4 bity určujú oblasť. Podľa hodnoty v týchto bitoch, sa určuje rozsah platnosti konkrétnej adresy:

Hodnota	Oblasť	Platnosť adresy
<b>0, F</b>	<i>Rezervované</i>	
<b>1</b>	<i>Rozhranie (interface)</i>	Jediné rozhranie, používa sa pre skupinové vysielanie do slučky
<b>2</b>	<i>Linka</i>	Jedna linka (Ethernet, Wi-Fi...), segment siete
<b>4</b>	<i>Riadenie, správa</i>	Oblasť musí byť nakonfigurovaná správcom
<b>5</b>	<i>Miesto</i>	Časť sieťovej topológie, ktorá patrí jednej organizácii a nachádza sa v jednej lokalite, koncová zákaznícka sieť
<b>8</b>	<i>Organizácia</i>	Pokrýva niekoľko miest organizácie
<b>E</b>	<i>Globálna</i>	Celosvetová platnosť
<b>ostatné</b>	<i>Nepripravené</i>	

*Tabuľka 1-1.: Oblasť skupinových adries*

Adresa s prefixom *ff01::1* je rezervovaná pre všetky IPv6 adresy v rámci jedného rozhrania a adresa s prefixom *ff02::1* pre všetky rozhrania IPv6 v rámci jedného sieťového segmentu. Adresa všetkých uzlov v danom mieste je *ff05::1*.

Prehľad preddefinovaných adries a rozdelenie prefixov ukazuje nasledujúca tabuľka:

Prefix	Význam
<b>::/128</b>	Nedefinovaná adresa
<b>::1/128</b>	Lokálna slučka (loopback)
<b>::IPv4</b>	Adresa zlučiteľná s IPv4
<b>::FFFF:IPv4</b>	IPv4 adresa namapovaná do IPv6
<b>FF00::/8</b>	Skupinové adresy
<b>FE80::/10</b>	Individuálne lokálne linkové
<b>FEC0::/10</b>	Individuálne lokálne miestne
<b>Ostatné (prefix 001)</b>	Individuálne globálne, RFC 3587

*Tabuľka 1-2 Rozvrhnutie IPv6 adresného priestoru*

#### 1.1.4. Autokonfigurácia

Kvôli zložitosti zápisu adres je pri IPv6 autokonfigurácia priam nutnosťou. Je teda špecifikovaná ako pevná súčasť protokolu.

Automatická konfigurácia je založená na objavovaní susedov (*neighbor discovery*). Stanica, ktorá je pripojená k IPv6 sieti, si najskôr vytvorí svoju lokálnu adresu (*link-local*) z preddefinovaného prefixu *FE80*, ku ktorému pripojí svoj identifikátor *EUI*. Túto adresu si následne verifikuje v sieti, či neprichádza ku konfliktu (duplicita adres na sieti). K tejto komunikácii sa využíva skupinové vysielanie na danom segmente siete (oblasť 2 – *Linka*). Po ukončení procesu objavovania susedov môžu stanice medzi sebou komunikovať bez použitia serverov alebo smerovačov.

Stanice taktiež počúvajú na sieti aj hlásenia smerovačov. Smerovače (ak sú pripojené) pravidelne vysielajú *ohlasovania* (*Router advertisement*), ktoré staniciam oznamujú prefix adres danej siete a informáciu o implicitnom smerovači (*default gateway*). Súčasne tieto oznámenia informujú, či majú stanice použiť stavovú alebo bezstavcovú konfiguráciu. Stanice si tieto oznámenia od smerovača môžu aj vyžiadať a nemusia tak čakať na periodické vysielanie. V rámci bezstavovej konfigurácie si stanice z ohláseného prefixu vygenerujú jedinečnú IPv6 adresu tak, že si k inzerovanému prefixu pripoja *EUI* z lokálnej adresy. Pri stavovej konfigurácii sa použije protokol DHCPv6.

RFC pre autokonfiguráciu:

*RFC 4862 IPv6 Stateless Address Autoconfiguration*

*RFC 4941 Privacy Extensions for Stateless Address Autoconfiguration in IPv6*

*RFC 4861 Neighbor Discovery for IP version 6 (IPv6)*

*RFC 3122 Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification*

### 1.1.5. Doplnujúce (rozširujúce) hlavičky

V základnej hlavičke sa nachádza jedno-bajtová hodnota s označením "Ďalšia hlavička" (*Next Header*). Táto hodnota určuje, či bude nasledovať nejaká rozširujúca hlavička (a aká), respektíve aký protokol nesie telo paketu (protokol vyššej vrstvy). Tabuľka ukazuje príklad najčastejšie používaných hodnôt rozširujúcich hlavičiek:

0	Voľby pre všetkých (hop-by-hop options)
43	Smerovanie (routing)
44	Fragmentácia (fragment)
50	Šifrovanie obsahu (ESP)
51	Autentizácia (AH)
59	Posledná hlavička (no next header)
60	Voľby pre cieľ (destination options)
62	Mobilita

Tabuľka 1-3 Čísla rozširujúcich hlavičiek IPv6 datagramu

V prípade, že datagram už nenesie žiadnu rozširujúcu hlavičku, špecifikuje sa tu priamo protokol transportnej vrstvy (rovnako ako u IPv4). Nasledujúca tabuľka uvádza hodnoty nesených niektorých protokolov:

6	TCP
8	EGP
9	IGP
17	UDP
46	RSVP
47	GRE
58	ICMP

Tabuľka 1-4 Čísla protokolov pracujúcich nad IP

Aby sa ušetril výkon smerovačov, mali by byť rozširujúce hlavičky uvádzané v určenom poradí. Smerovač teda bude musieť prezerať rozširujúce hlavičky iba po prvú, ktorá sa ho už netýka - čiže bude iná ako Voľby pre všetkých. Poradie je odporúčané takto:

1	Základná hlavička IPv6
2	Voľby pre všetkých
3	Voľby pre cieľ (pre prvú cieľovú adresu, prípadne ďalšiu uvedenú v hlavičke smerovania)
4	Smerovanie
5	Fragmentácia
6	Autentizácia
7	Šifrovanie obsahu
8	Voľby pre cieľ (pre konečného príjemcu)

Tabuľka 1-5 Poradie rozširujúcich hlavičiek

Každý druh hlavičky by sa mal vyskytovať iba raz, výnimku tvoria len voľby pre cieľ, ktoré sa môžu vyskytnúť dvakrát (pred smerovaním a pred prenášanými dátami). Ak má nejaká hlavička označenie 59 (posledná hlavička), akékoľvek dáta, ktoré by nasledovali, budú ignorované.

### **Voľby (pre všetkých/pre cieľ)**

Hlavička obsahujúca v prvom rade informáciu o tom, čo má uzol spraviť v prípade, že nerozumie voľbám v nej uvedeným. Môže ich buď ignorovať, zahodiť datagramu, zahodiť datagramu a poslať ICMP odosielateľovi, alebo zahodiť a ICMP poslať odosielateľovi len v prípade, že cieľová adresa nebola skupinová. Momentálne má reálne využitie len voľba Upozornenie smerovača, ktoré označuje datagramy zaujímavé práve pre smerovače (napríklad to môžu byť RSVP pakety určené k rezervácii prenosovej kapacity, ktoré sú zaujímavé pre všetky smerovače po ceste).

### **Smerovanie**

Je obdobná hlavička ako voľby zdrojového smerovania pri IPv4. Táto hlavička uvádza, ktorými smerovačmi musí paket prejsť, kým príde ku cieľovej stanici. Tieto smerovače nemusia byť jediné, medzi nimi môžu byť ďalšie uzly, ktoré nemusia byť v hlavičke uvedené. Posledná uvedená adresa, je adresa cieľovej stanice. V hlavičke sa nachádza počítadlo zostávajúcich adries, ktoré ešte musia byť navštívené. Každý uzol, ktorý bol zaradený do zoznamu skokov, zníži počet zostávajúcich adries o jednotku. Keď je toto počítadlo nulové, znamená to, že datagram dorazil do cieľa.

Dokument *RFC 5095 Deprecation of Type 0 Routing Headers in IPv6* kritizuje používanie typu 0 v hlavičkách smerovania z bezpečnostných dôvodov – útočník by mohol využiť „vkladanie next hopov“ a striedať dve IP adresy a vyvolať útok typu *DoS*.

Bežnejšie sa používa typ 2 pre podporu mobility (*RFC 6275 Mobility Support in IPv6*).

### **Fragmentácia**

V IPv6 je datagram rozdelený na dve časti – fragmentovateľnú a nefragmentovateľnú. Nefragmentovateľná je časť od základnej hlavičky až po rozširujúcu hlavičku smerovania. Fragmentovateľná časť teda začína rozširujúcou hlavičkou fragmentácie. Fragmentovať v IPv6 môže len odosielateľ (v IPv4 to mohol vykonať ľubovoľný smerovač na ceste paketu). Každý fragment má svoje identifikačné 32-bitové číslo, ktoré je medzi dvomi komunikujúcimi uzlami jedinečné a inkrementuje sa o jednotku každým datagramom.

Fragmentácia v IPv6 a jej bezpečnostné riziká sú opísané v dokumentoch:

*RFC 5722 Handling of Overlapping IPv6 Fragments*

*RFC 6946 Processing of IPv6 "Atomic" Fragments*

*RFC 6980 Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery*

### **Jumbogramy**

V prípade, že budú v budúcnosti existovať prenosové linky s MTU väčším ako 65535 bajtov (maximálna veľkosť paketu je v IPv4 aj IPv6 65535 bajtov) plus 40 bajtov IPv6 hlavička, tento prípad bude riešiteľný v IPv6 pomocou jumbogramov. Tieto pakety budú môcť dosiahnuť veľkosť až 4 GB. Smerovače, ktoré nebudú mať MTU na portoch väčšie ako 65535 bajtov, nemusia jumbogramy vôbec podporovať. Zaujímavosťou je, že dnešné protokoly vyšších vrstiev definujú svojimi prostriedkami veľkosť datagramov (UDP), alebo segmentov (TCP) a ich hodnoty môžu nadobúdať opäť maximálne 65535 bajtov. Preto je pri UDP odporúčané pre všetky jumbogramy používať ako veľkosť datagramu nulu a pri TCP veľkosť segmentu 65535. Reálna veľkosť sa prevezme zo zisteného MTU mínus veľkosť UDP/TCP hlavičky.

Jumbogramy sú opísané v dokumente *RFC 2675 IPv6 Jumbograms*.

### **Flows/Toky**

IPv6 prichádza so zaujímavou vlastnosťou, ktorá by sa dala označiť ako identifikácia súvisiacej komunikácie. Pri komunikácii nastaví zdrojový uzol parameter toku na nenulovú hodnotu, ktorá je medzi dvomi uzlami vždy jedinečná a počas komunikácie sa nemení. Týmto spôsobom môžeme uľahčiť smerovačom identifikovať tok dát, ktorý má mať nastavené nejaké parametre, napríklad QoS, alebo smerovanie bez nutnosti ďalšej podrobnej analýzy rozširujúcich hlavičiek. Smerovač identifikuje toky podľa zdrojovej a cieľovej adresy a čísla toku.

### 1.1.6. ICMPv6

Internet Control Message Protocol určený na riadenie prevádzky na IP sieti je naďalej pevnou súčasťou sieťovej vrstvy a teda aj protokolu IPv6. Bol rozšírený o funkcie vyhľadávania susedných uzlov (Neighborhood Advertisement a Neighborhood Solicitation - náhrada ARP z IPv4), smerovačov (Router Advertisement a Router Solicitation) na lokálnej sieti a registráciu do multicastových skupín.

Činnosť protokolu ICMP je možné veľmi ľahko zneužiť a použiť ho ako útočnú zbraň k obmedzeniu činnosti siete. Pri verzii IPv4 dochádza k takýmto útokom. Celý mechanizmus spočíva v tom, že cieľový zdroj sa zahltí haldou ICMP správ a takmer nič iné nemá šancu prejsť sieťou. Dôsledkom toho je, že správcovia sietí začali blokovať ICMP datagrami na svojich firewalloch za cenu obmedzenia možností diagnostiky siete (naviac je to proti *RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*, ktorý špecifikuje ICMPv6 ako povinnú implementáciu každého uzla v sieti IPv6).

ICMPv6 implementuje bezpečnostné mechanizmy, aby správcovia nemuseli konať takto obmedzujúce opatrenia. Ako prvým variantom je možnosť umožniť správcovi nastaviť niektoré kvantitatívne parametre (minimálny časový odstup medzi ICMP správami alebo maximálny podiel na šírke pásma). Druhým variantom je založená na spolupráci ICMPv6 s bezpečnostnými mechanizmami IPv6 (správy ICMP sa obalia o autentizačnú hlavičku).

#### PMTU Discovery (Path Maximal Transfer Unit)

V prípade, že sa snažia dva uzly komunikovať medzi sebou cez smerovače, ktoré majú MTU na rozhraniach, ktorými budú pakety prechádzať menšie ako uzol, ktorý paket odoslal, smerovač pošle tomuto zdrojovému uzlu ICMP správu Packet Too Big. Ten musí následne pôvodný paket zmenšiť a odoslať po viacerých častiach (fragmentácia). Tento proces sa opakuje, až pokiaľ paket úspešne prejde, alebo dosiahne veľkosti 1280 bajtov. Nižšie MTU nie je v IPv6 povolené. V jednoduchých zariadeniach, ktoré musia napríklad kvôli obmedzenej veľkosti ROM pamäti mať čo najjednoduchší IP zásobník, je možné vždy používať MTU 1280, ktoré by malo vždy prejsť sieťou, a tým pádom odpadá implementácia PMTU.



### **1.1.7. Mobilita**

Nárast počtu používateľov mobilných elektronických zariadení s možnosťou pripojenia do siete za posledné roky výrazne stúpol a dopyt po jednoduchom a nerušenom pripojení do siete Internetu tiež. Autori IPv6 našli riešenie a navrhli jeho implementáciu. Tá spočíva v tom, že každé mobilné zariadenie bude mať takzvaného domáceho agenta. Je to smerovač, cez ktorý je doma mobilné zariadenie (agent) pripojené do siete. V prípade, že sa mobilný agent pripojí do siete inde ako doma, pošle svojmu domovskému agentovi informáciu o svojej novej polohe. Následne všetky pokusy o pripojenie na mobilného agenta presmeruje domáci agent na novú adresu. Mobilný agent pokračuje so zdrojom v komunikácii so zdrojovou adresou z aktuálnej siete, v ktorej je pripojený a dá vedieť, že komunikovať sa už má na priamo s ním. Ak túto informáciu zdrojový uzol nevie spracovať, môže celá komunikácia prebiehať cez domáceho agenta, ale to nie je žiadaný stav a mal by nastať výnimočné, ak vôbec. Mobilný agent môže o svojej novej polohe informovať aj uzly, s ktorými bol v kontakte pred zmenou lokalizácie, aby bolo obnovenie komunikácie plynulejšie.

### **1.1.8. Bezpečnosť Internet Protokolu verzie 6**

Klasické IP neobsahovalo vôbec žiadne bezpečnostné opatrenia. Postupom času sa však hľadali spôsoby, ako komunikáciu v Internete zabezpečiť. Prístupy sa vymysleli rôzne: od hardvérových až po aplikačné. Všeobecným mechanizmom pre siete TCP/IP na úrovni vrstvy IP sa stal IPsec.

#### **1.1.8.1. Bezpečnosť na linkovej vrstve**

Bezpečnosť na linkovej vrstve sa zameriava najmä na bezpečnosť uzlov, bezpečnosť infraštruktúry LAN a protokolov. Útoky, ktoré spadajú do tejto kategórie sú falšovanie zdrojových adries a odmietnutie služieb. Cieľom útokov sú zvyčajne prepínače.

Bezpečnostné mechanizmy, ktoré sa môžu implementovať v tejto súvislosti, sú:

- VLAN – rozdeľujú uzly do oddelených skupín,
- port security – definuje maximálny počet MAC adries na porte prepínača,
- IEEE 802.1x – štandard IEEE, zabezpečuje autentizačné mechanizmy pre zariadenia, ktoré sa chcú pripojiť do siete LAN.
- IEEE 802.1ae – MACSec štandard zabezpečuje integritu dát pre prístup protokolov nezávislých na prístupe médiu.

### 1.1.8.2. IPSec

IPSec je bezpečnostné rozšírenie IP protokolu založené na autentizácii a šifrovaní. Je navrhnuté k aplikovaniu ako v IPv4, tak aj v IPv6. Definovaný je v *RFC 4301 Security Architecture for the Internet Protocol*.

IPSec využíva dva protokoly pre zabezpečenie komunikácie: *Authentication Header AH* (pre zabezpečenie autentizácie) a *Encapsulation Security Header ESP* (pre zabezpečenie šifrovania). Cieľom autentizácie je overiť, že dáta odoslal skutočne ten, kto to o sebe tvrdí. Šifrovanie umožňuje utajiť obsah komunikácie. ESP je povinná súčasť IPSecu, AH je voliteľná súčasť.

Množina bezpečnostných informácií, ktoré opisujú konkrétne zabezpečené spojenie, sa nazýva *Bezpečnostná asociácia (Security Associations SA)*. Súčasťou bezpečnostnej asociácie sú všetky potrebné informácie – použitý bezpečnostný protokol (AH, ESP), jeho režim, šifrovací algoritmus a kľúče, počítadlá, doba životnosti, ochranné prvky proti opakovaniu a podobne. SA sú jednosmerné – pri komunikácii je nutné ich nadväzovať vždy vo dvojici: jednu pre vysielanie, druhú pre príjem (*Pozn.: bezpečnostný protokol môže byť v SA použitý len jeden, pokiaľ sa použijú v komunikácii oba, budú potrebné 4 SA (dvojica pre AH + dvojica pre ESP)*).

SA je definovaná na základe troch parametrov:

- *Security Parameter Index (SPI)* – index bezpečnostných parametrov, 32-bitové číslo pre jedinečnú identifikáciu príslušnej SA
- *IP Destination Address* – adresa zdroja, z ktorého je SA nadviazané
- *Security Protocol Identifier* – špecifikuje, či ide o asociáciu pre AH alebo ESP

Nadviazanie SA spočíva v dohodnutí sa oboch strán na kryptografickom algoritme a výmene kľúčov. Výmena kľúčov sa často vykonáva cez nezabezpečené spojenia. Isté protokoly boli navrhnuté tak, aby sa táto výmena udiala automaticky (ISAKMP, IKEv1, IKEv2).

Bezpečnostné hlavičky je možné dopĺňať v dvoch režimoch:

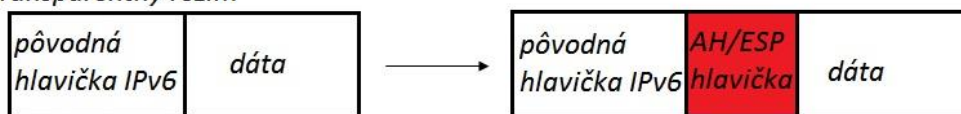
### Transparentný režim

- hlavičky sa vkladajú priamo ako súčasť datagramu medzi rozširujúce hlavičky.
- AH a ESP poskytujú ochranu primárne pre protokol nasledujúcej vrstvy
- v IPv4 sa hlavička vkladá hneď za IP hlavičku a pred akúkoľvek hlavičku vyššej vrstvy (TCP, UDP...)
- v IPv6 sa hlavička vkladá za základnú hlavičku a za vybrané hlavičky, ale mala by sa nachádzať pred alebo za *Voľbami pre cieľ* (*destination options*)
- pri ESP sa šifrujú iba údaje za hlavičkou ESP (teda nie IP hlavička a prípadné rozširujúce hlavičky pred hlavičkou ESP)

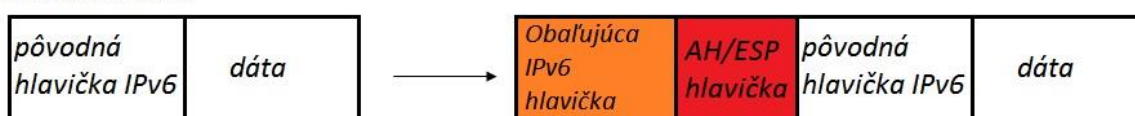
### Tunelovací režim

- celý datagram sa zabalí ako dáta do nového datagramu, ktorý sa obalí novou hlavičkou

#### *Transparentný režim*



#### *Tunelovací režim*



Obr. 1-2.: Režimy IPsec

### 1.1.8.3. Autentifikačná hlavička (AH)

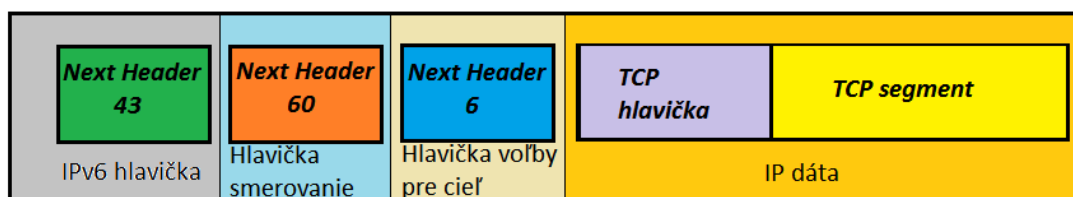
Autentifikačná hlavička (*Authentication Header, AH*) je protokol, ktorého základnou úlohou je autentizovať odosielateľa a zabezpečiť autentickosť a neporušenosť IP paketov. Zabraňuje dvom prípadom: nelegálnej modifikácii hlavičky a paket spoofingu. Podrobne je jeho činnosť špecifikovaná je v dokumente *RFC 4302 IP Authentication Header*.

Uzol, ktorý obaľuje datagram AH hlavičkou, pracuje nasledovne:

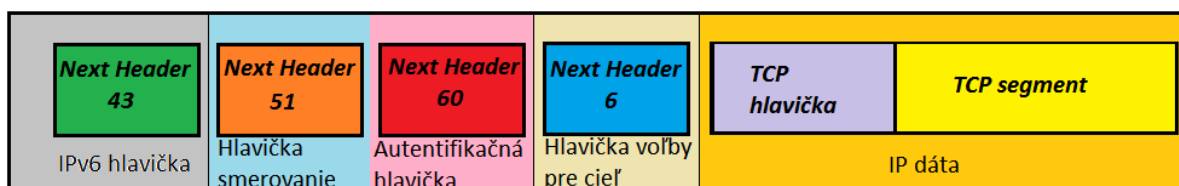
1. Vloží do datagramu hlavičku AH
2. Vyplní jej položky – identifikáciu *nasledujúcej hlavičky*, svoju vlastnú *dĺžku*, zodpovedajúci *index bezpečnostných parametrov* a *poradové číslo* (to sa zväčšuje o jednotku pre každý nasledujúci datagram)
3. Nasleduje výpočet autentizačných údajov. Pre jeho potreby je však potrebné datagram upraviť, aby ho príjemca mohol overiť. Niektoré hlavičky upraví na hodnoty, ktoré budú mať pri príchode datagramu (napr. cieľovú adresu). Tie, ktoré sa predpokladať nedajú, vynuluje. Pre takto zmenený datagram vypočíta *autentizačné údaje* a uloží ich do príslušnej položky v AH.

Pre výpočet autentizačných dát sa používajú jednosmerné hešovacie funkcie (napr. MD5). Obe strany disponujú rovnakým bezpečnostným kľúčom a vykonávajú rovnaký výpočet. Prijemca opäť vynuluje nepredvídateľné hodnoty a *autentizačné údaje* z hlavičky AH. Na základe identifikátora SPI získa kľúč a algoritmus a nad upraveným datagramom vykoná rovnaký výpočet ako odosielateľ. Výslednú hodnotu potom porovná s tou, ktorá bola uvedená v hlavičke AH. Pokiaľ sa nezhoduje, znamená to, že datagram bol zmenený a autentizácia zlyhala. Taký datagram IPSec zahodí bez informovania odosielateľa (aby prípadný útočník nemal spätnú väzbu).

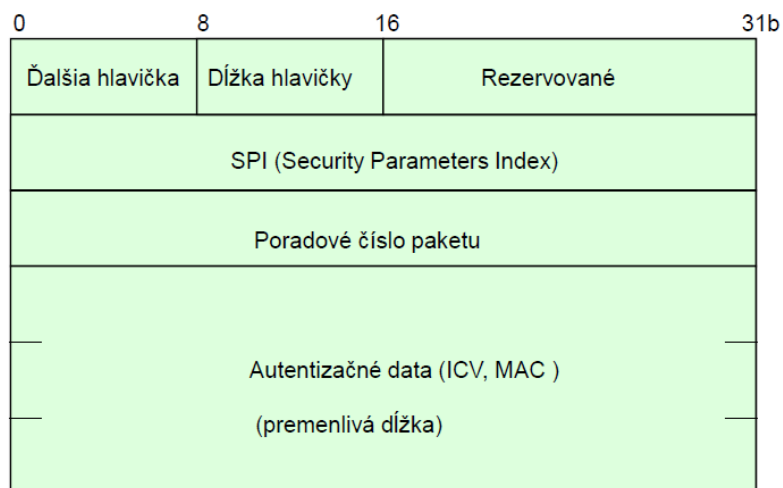
AH hlavička používa číslo protokolu 51 (v IPv4) a číslo Next Header (v IPv6). Enkapsuláciu a výsledné šifrovanie v sieťach IPv6 a formát hlavičky AH znázorňujú nasledovné obrázky:



Obr. 1-3.: IPv6 datagram zahŕňajúci rozšírenú hlavičku smerovania a voľby pre cieľ



Obr. 1-4.: IPv6 datagram obalený autentifikačnou hlavičkou



Obr. 1-5.: Formát hlavičky AH

#### 1.1.8.4. Encapsulation Security Payload (ESP)

Základnou službou hlavičky ESP je šifrovanie. Okrem nej však ponúka aj možnosť autentizácie odosielateľa, kontrolu pôvodnosti dát a ochranu proti opakovaniu (podobne ako AH). Definované je v *RFC 4303 IP Encapsulating Security Payload (ESP)*.

ESP hlavička obaľuje datagram z oboch strán. Hlavička pochopiteľne obsahuje *Index bezpečnostných parametrov*, podľa ktorého si príjemca vyhľadá parametre pre jej spracovanie. *Poradové číslo* slúži ako prevencia proti opakovaniu. *Autentizačné údaje* slúžia k overeniu totožnosti odosielateľa.

ESP hlavička je tvorená troma komponentmi:

- *ESP Header* – obsahuje dve polia (SPI a sekvenčné číslo) a nachádza sa pred šifrovanými dátami
- *ESP Trailer* – umiestňuje sa za šifrované dáta. Niektoré algoritmy vyžadujú, aby dĺžka datagramu bola násobkom istej hodnoty. Ak datagram takúto veľkosť nedosahuje, doplnia sa na koniec tzv. „padding“ bity.
- *ESP Authentication Data* – ak sú použité autentifikačné prostriedky ESP protokolu, tak tu sa nachádza *Integrity Check Value ICV*, vypočítané podobným spôsobom ako v AH.

Odosielanie datagramu cez ESP prebieha nasledovne:

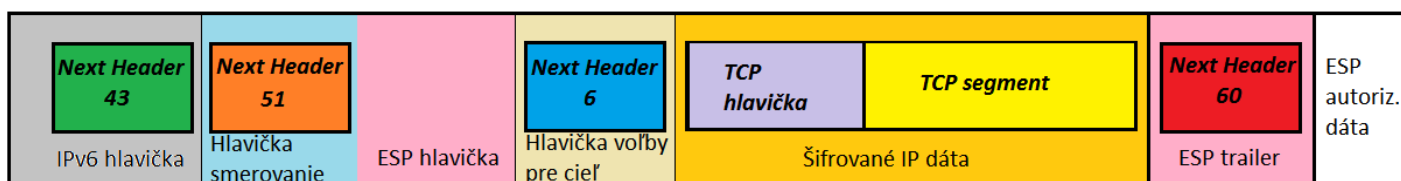
1. Odosielateľ nájde vhodnú pozíciu pre vloženie ESP hlavičky. Zvyšok datagramu prípadne doplní padding bitmi. Datagram zašifruje podľa parametrov stanovených v bezpečnostnej asociácii SA.
2. Vygeneruje poradové číslo (zväčšuje sa o jednotku)
3. Ak je požadovaná autentizácia a kontrola integrity, vypočíta kontrolnú hodnotu pre prenášané údaje a uloží ich do ESP ako položku *Autentizačné dáta*.

IPSec operácie sa vykonávajú vždy pre celý datagram. Prípadná fragmentácia sa vykonáva až po šifrovaní. Príjemca si najskôr datagram vyskladá a až potom začne dešifrovať.

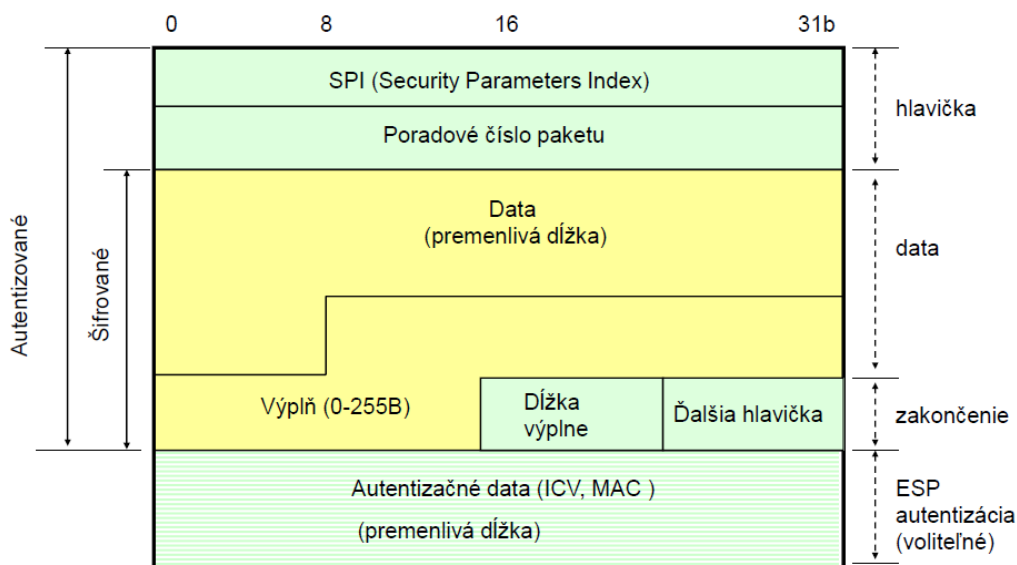
Príjem datagramu vyzerá nasledovne:

1. Najskôr si príjemca vyhladá zodpovedajúcu bezpečnostnú asociáciu. Ak neexistuje, datagram zahodí.
2. Nasleduje kontrola poradového čísla. Ak datagram obsahuje číslo už použité, bude zahodený.
3. Ďalším krokom je autentizácia – príjemca vypočíta *autentizačné dáta* a porovná ich. Ak sa nezhodujú s prijatou hodnotou, preč s datagramom.
4. Ak boli splnené predchádzajúce kroky, dešifruje sa paket.

Nasledujúci obrázok znázorňuje umiestnenie hlavičky ESP v protokole IPv6.



Obr. 1-6.: ESP hlavička a datagram IPv6



Obr. 1-7.: Hlavička ESP

Dokumenty špecifikujúce bezpečnosť IP protokolu:

*RFC 4301 Security Architecture for the Internet Protocol*

*RFC 4302 IP Authentication Header*

*RFC 4303 IP Encapsulating Security Payload (ESP)*

## 1.2. Možnosti nasadenia IPv6

Najdôležitejším problémom prechodu z IPv4 na IPv6 je ich vzájomná nekompatibilita. Toto vedie k nie príliš veľkej motivácii riešenia prechodu na novú verziu. Faktom je, že počet IPv4 adries sa minie a tento problém nevyriešil ani mechanizmus NAT, ktorý skrýval celé siete za jednu IP adresu a ani beztriedne adresovanie.

Nasadenie protokolu IPv6 je otázkou, ktorou sa viaceré organizácie zaoberajú už niekoľko rokov. V súčasnosti existujú viaceré možnosti nasadenia protokolu IPv6 do reálneho používania. Každý mechanizmus je niečím špecifický, dokonca v niektorých prípadoch infraštruktúr sa odporúča používať kombinácia viacerých nižšie uvedených mechanizmov.

Možné mechanizmy prechodu z IPv4 na IPv6

- Dual Stack
- Tunelovanie
- Preklad
- Jednorazový prechod na IPv6

### 1.2.1. Dual Stack

Dual stack je jednou z metód, ktorá umožňuje prechod IPv4 protokolu na IPv6. Ide asi o najmenej náročnú stratégiu z hľadiska samotného prechodu, nakoľko sú oba protokoly prevádzané spoločne. Zjednodušene sa dá povedať, že Dual Stack je integračná metóda, kde každá stanica (aj smerovač a prepínač) implementuje aj IPv4, aj IPv6 protokol. Protokoly sú od seba nezávislé. Stanica s Dual Stack zásobníkom vyberie na základe cieľovej IP adresy typ zásobníka, ktorý použije. Ak hostiteľ chce komunikovať s iným klientom, ktorý má dostupný len IPv4 protokol, vyberie IPv4 zásobník. V prípade, ak sú do druhej strane komunikácie dostupné oba protokoly, uprednostní sa IPv6 protokol. Metóda Dual Stack je jednou z najpoužívanejších metód vďaka jej malej náročnosti implementácie.. Aplikácie navrhnuté iba pre IPv4 protokol naďalej spoľahlivo fungujú ako pred tým. Nové a upravené aplikácie vedia využiť obe IP vrstvy.

Nové rozhrania pre programovanie aplikácií (API) majú zadefinovanú podporu oboch protokolov (IPv4 aj IPv6). Toto nové rozhranie API nahrádza volania „*gethostbyname*“ a „*gethostbyaddr*“. Prevedené aplikácie môžu tak využívať protokol IPv4 aj IPv6. Pre väčšinu aplikácií ide o minimálne zmeny v niektorých miestach v zdrojovom kóde. Táto technika umožňuje postupné aktualizovanie aplikácií jednej za druhou.

Dual stack respektíve IPv6/IPv4 uzly môžu byť prevádzkované v jednom z troch uvedených režimov:

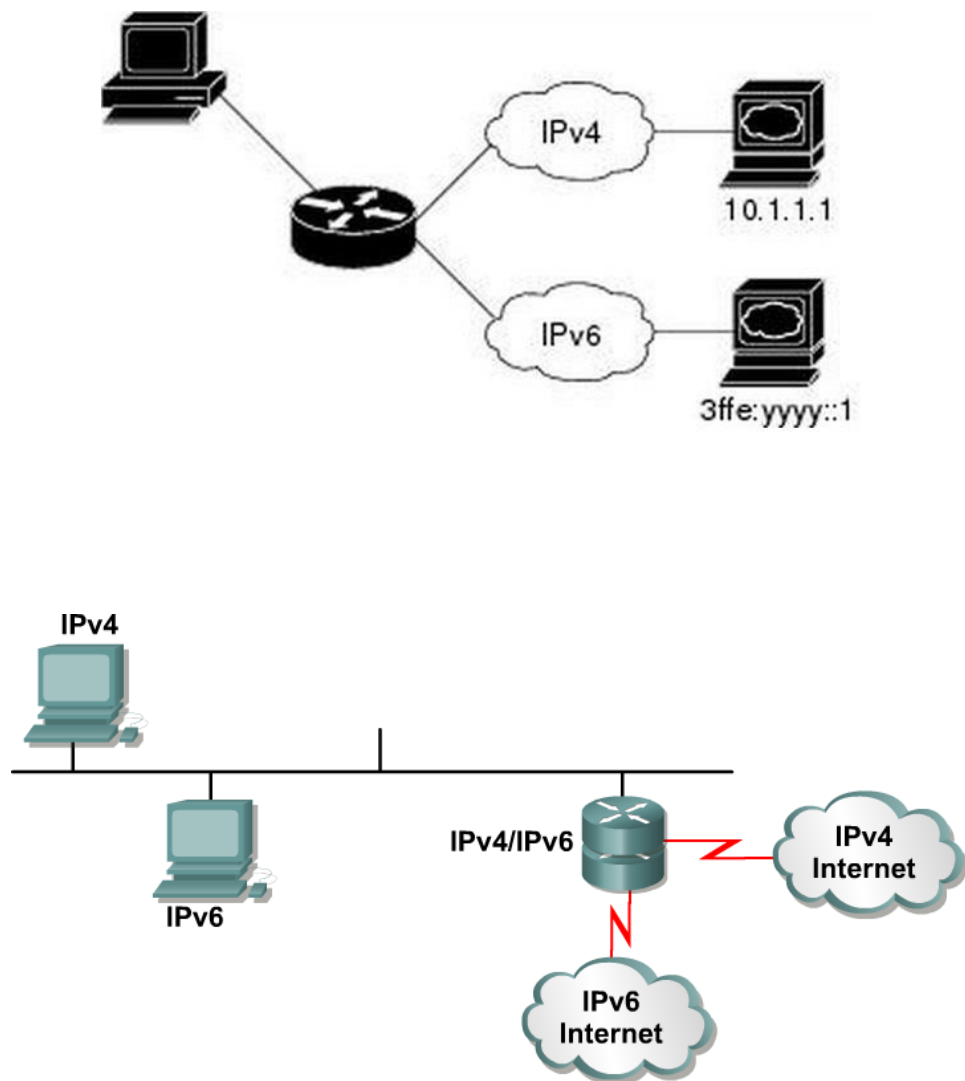
- So zásobníkom IPv4 povoleným a IPv6 zásobníkom zakázaným
- So zásobníkom IPv4 zakázaným a IPv6 zásobníkom povoleným
- S oboma zásobníkmi povolenými

Ak má IPv6/IPv4 uzol zakázaný IPv4 zásobník, funguje ako IPv6 uzol. Podobne ak má IPv6/IPv4 uzol zakázaný IPv6 zásobník, funguje ako IPv4 uzol. IPv6/IPv4 uzly môžu obsahovať konfiguračný prepínač, ktorý zakáže ich IPv4 alebo IPv6 zásobník.

K opísanej Dual Stack technike môže ale nemusí byť aj navyše použitá technika *Tunelovania*, ktorá je opísaná nižšie.

Problematika Dual Stack je popísaná taktiež v RFC dokumente **4213**.





### 1.2.2. Tunelovanie

Technika tunelovania sa využíva v prípadoch, keď chceme prepojiť dva systémy fungujúce na rovnakom protokole a medzi nimi sa nachádza protokol, ktorý nie je podporovaný v nich. Typickým príkladom je prenos paketov medzi IPv6 stanicami cez IPv4 sieť, ktorá je na ceste medzi nimi. Tunelovanie sa dá chápať ako zapuzdrenie IPv6 paketov do paketov protokolu IPv4. Pakety IPv6 môžu byť priamo zapuzdrené do IPv4 paketov použitím protokolu 41. Niektoré smerovače, respektíve NAT, blokujú prenos protokolu 41. Potom sa IPv6 pakety zapuzdrujú do UDP paketov, čím sa prekoná blokovanie protokolu 41. V rámci princípu tunelovania sa rozoznávajú nasledujúce mechanizmy:

#### 6in4 (RFC 4213)

Podstatou tohto princípu tunelovania je zapuzdrenie IPv6 hlavičky do IPv4 hlavičky. V hlavičke IPv4 sa ako protokol použije číslo 41, ktorý je akýmsi identifikátorom IPv6 v IPv4. Výhodou použitia tohto mechanizmu je menšia réžia, t.j. hlavička IPv4 bez voliteľných častí s veľkosťou 20 bajtov.

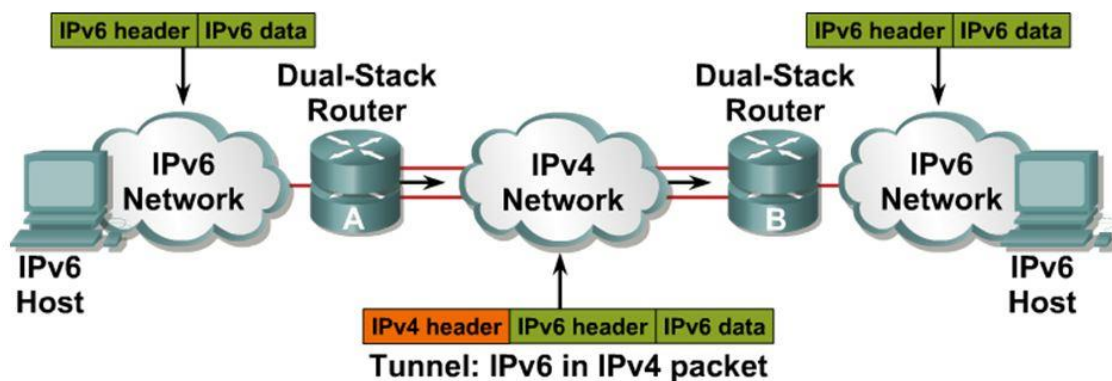
6in4 tunelovanie sa používa na prepojenie sietí cez nekompatibilnú existujúcu sieť. Tento mechanizmus pre svoje fungovanie vyžaduje používanie Dual Stack smerovačov. Pri tunelovaní IPv6 cez IPv4 sieť vstupný uzol tunela zapuzdrí paket protokolu IPv6 do vnútra paketu IPv4 a odošle ho. Na druhej strane tunela sa nachádza výstupný uzol, ktorý tento zapuzdrený paket prijme, rozbalí ak je to nutné, odstráni IPv4 hlavičku a následne paket spracuje alebo pošle ďalej.

Zapuzdrenie môže robiť nie len smerovač, ale aj pracovná stanica, ak jej operačný systém ovláda príslušný spôsob tunelovania.

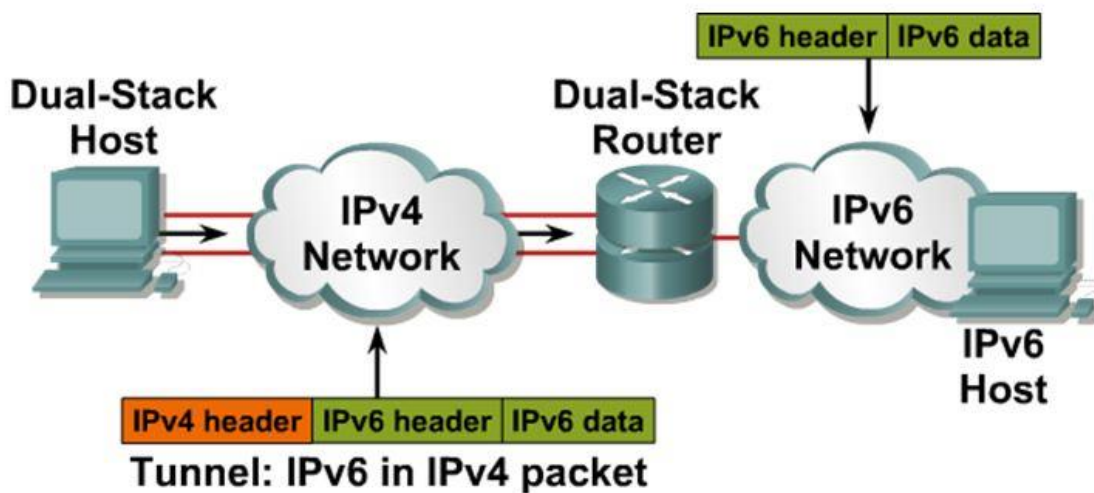
Tunelovanie môže byť použité v rôznych cestách podľa toho, aké zariadenia sú na koncoch:

- smerovač – smerovač (IPv6/IPv4 smerovače navzájom prepojené IPv4 infraštruktúrou môžu medzi sebou tunelovať IPv6 pakety)
- host – smerovač (IPv6/IPv4 host môže tunelovať IPv6 pakety k sprostredkovateľskému IPv6/IPv4 smerovaču, ktorý je dostupný cez IPv4 infraštruktúru)
- host – host (IPv6/IPv4 stanice /počítače/ prepojené cez IPv4 infraštruktúru môže tunelovať IPv6 pakety medzi sebou navzájom)
- smerovač – host (IPv6/IPv4 smerovač môže tunelovať IPv6 pakety do ich cieľového IPv6/IPv4 uzla)

Nevýhodou tohto mechanizmu je potreba verejnej IP adresy domáceho smerovača, respektíve počítača. Ďalšou nevýhodou je nefunkčnosť viacnásobného NATu a smerovače v rámci tunelu nesmú blokovať protokol 41.



Obr. 1-8.: 6in4 Smerovač - Smerovač



Obr. 1-9.: 6in4 Koncová stanica-Smerovač

S MTU 1500 bajtov môže jeden IPv6 paket poslať 1480 bajtov naraz bez fragmentácie. Koncové body tunela musia byť konfigurované staticky. Existujú nástroje, napríklad AICUU, ktorý dokáže konfigurovať parametre tunela automaticky po načítaní informácií z informačného tunela.

## 6to4 (3056)

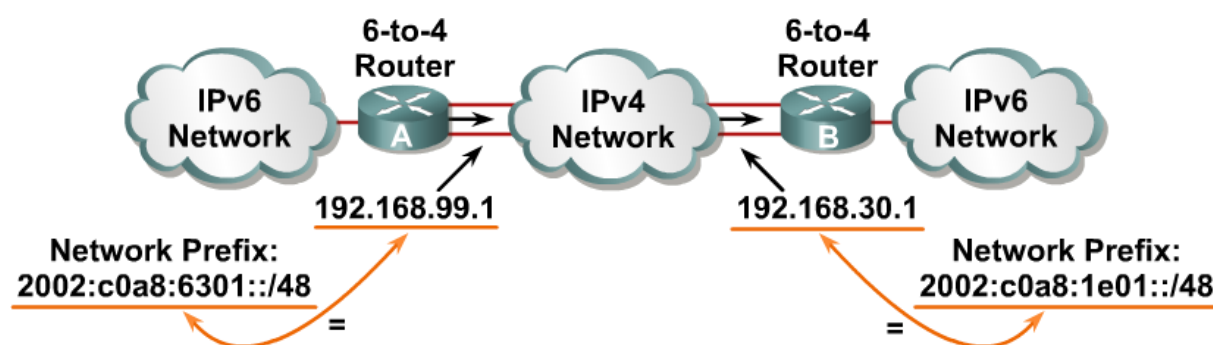
Mechanizmus tunelovanie 6to4 je veľmi podobný predchádzajúcemu mechanizmu 6in4. Tento mechanizmus je určený len ako nástroj používaný počas obdobia koexistencie IPv4 a IPv6. Nie je určený ako trvalé riešenie. 6to4 mechanizmus je takmer výhradne určený pre hraničné smerovače, bez špecifických hosťateľských úprav. Len malé množstvo smerovačov požaduje konfiguráciu pre tento mechanizmus.

6to4 tunely sú (na rozdiel od trvalých statických tunelov) tunely, ktoré môžu mať mnoho koncových bodov. IPv6 prefixy jednotlivých IPv6 ostrovov oddelených IPv4 internetom sú navrhnuté tak, aby v sebe obsahovali priamo IPv4 adresu tunelujúceho smerovača, ktorý je na okraji tohto ostrova. IPv6 adresy pri použití 6to4 tunelov využívajú prefix 2002::/16. Ďalších 32 bitov vyjadruje IPv4 adresu smerovača, ktorý je na vstupe/výstupe nášho IPv6 ostrova a ktorý realizuje tunelovanie. Výsledný 48-bitový prefix je prefix spoločný pre celý IPv6 ostrov. Zostáva tak k dispozícii 16 bitov pre ID podsiete a 64 bitov pre ID rozhrania, rovnako ako v bežných Global Unicast adresách.

Príklad:

- Smerovač na vstupe do nášho IPv6 ostrovčeka má verejnú IPv4 adresu 192.0.2.36
- Hexadecimálny prepis tejto adresy je C0.0.2.24
- Všetky IPv6 zariadenia v našom ostrovčeku majú teda IPv6 prefix 2002:C000:0224::/48
- Smerovače na susedných IPv6 lokalitách musia mať akurát vhodne nastavené smerovanie, aby pre prístup do IPv6 sietí s prefixom 2002::/16 používali 6to4 tunel

6to4 tunel nevyžaduje cieľovú adresu, pretože to nie je point-to-point spojenie. Každý IPv6 ostrov má jednoznačný globálne platný prefix.



Obr. 1-10.: 6to4

System 6to4 umožňuje spojenie s IPv6 ostrovom cez medzil'ahlú IPv4 sieť. Dá sa teda aj použiť na prístup do IPv6 sveta. Stačí vhodná brána, ktorá akceptuje 6to4 tunely. Na túto bránu budeme smerovať všetko, čo pôjde do IPv6. RFC 3068 stanovuje, že poskytovatelia podľa svojho rozhodnutia môžu takúto bránu vytvoriť. Táto brána musí mať adresu 192.88.99.1. Smerovače na prístup do IPv6 internetu použijú statický smer **ipv6 route 2000::/3 2002:c058:6301::**

## **ISATAP tunely (5214)**

ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*) tunely sú obdobou 6to4 tunelov. Majú primárne zabezpečovať vnútro firemnú (intra-site) komunikáciu. Takisto využívajú mapovanie medzi IPv4 a IPv6 adresou. Tvar ISATAP IPv6 adresy:

- Prvých 64 bitov: link-local alebo global unicast prefix
- Ďalších 32 bitov: 0000:5EFE (konštanta)
- Zvyšných 32 bitov: IPv4 adresa stanice
- Dĺžka prefixu: 64 bitov

Novinka: Využitie pomocných mechanizmov (DHCP, DNS, manuálna konfigurácia) pre lokalizáciu smerovačov schopných zabezpečiť smerovanie medzi rôznymi IPv6 sieťami.

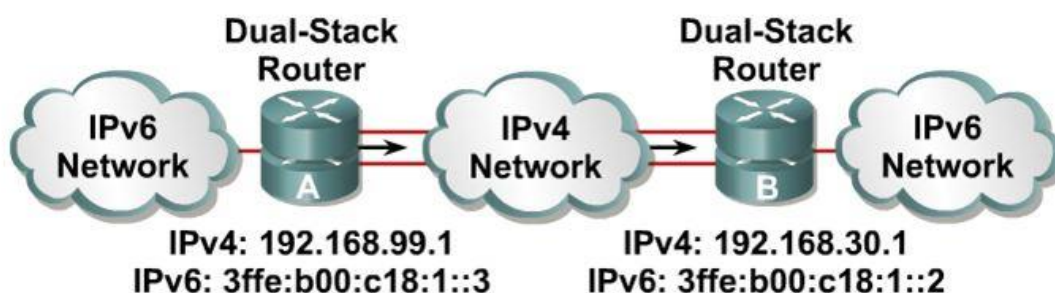
Na tunelovanie používajú či už globálnu alebo privátnu IPv4 adresu.

## **Teredo**

Teredo je v modernejších verziách Windowsu jeho súčasťou. Pre Linux či BSD je známy pod menom Miredo. Pracuje obvykle spôsobom plug&play. Vo Windowse sa spúšťa automaticky a netreba takmer nič konfigurovať. Tento mechanizmus je navrhnutý najmä pre koncové stroje umiestnené za NAT. Preto sa snaží, aby NAT dokázalo prejsť čo najrýchlejšie. To vyžaduje vždy na začiatku komunikácie s novým cieľom výmenu niekoľkých paketov otvárajúcich cestu v NAT. Výkon je všeobecne veľkou slabinou. Ďalšou slabinou je spoľahlivosť, nakoľko takmer 40% nadviazaní spojenia končí neúspešne. Operačné systémy berú Teredo ako poslednú možnosť a obvykle preferujú IPv4 pred IPv6.

## **Statické tunely**

Pre správne fungovanie metódy statických tunelov sú potrebné Dual-Stack smerovače, pričom IPv4 a IPv6 adresy sa konfigurujú na oboch stranách tunela. Pričom smerovače nemôžu dynamicky meniť smerovanie medzi sieťami.



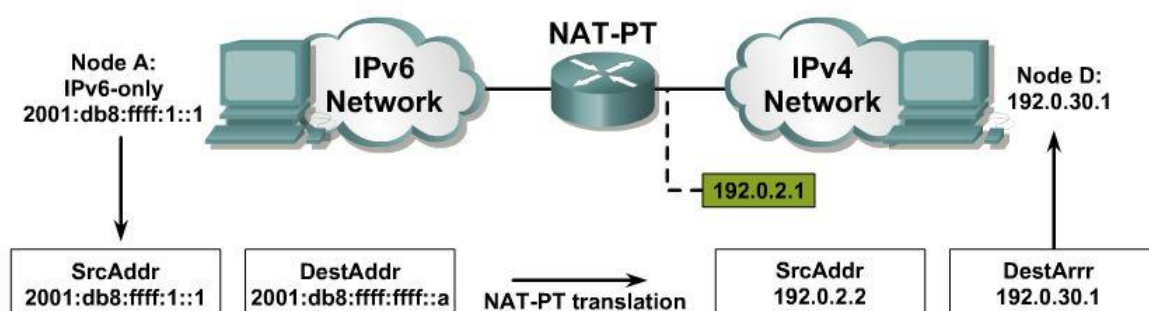
Obr. 1-11.: Statický tunel

### 1.2.3. Preklad

Jedná sa o techniku prevodu IPv4 paketu na IPv6 a obrátene. Väčšina implementácií však neprešla praktickým testovaním, nakoľko neboli považované za príliš spoľahlivé. Predstaviteľom prekladačov je *Network Address Translation – Protocol Translation* (NAT-PT) a jeho nástupca NAT64 alebo TRT.

#### NAT-PT

NAT-Protocol Translation (NAT-PT) je prekladový mechanizmus na rozhraní medzi IPv6 a IPv4 sieťou. Jeho úlohou je prekladať IPv6 pakety na IPv4 a naopak. Tento prístup je vhodný pre umožnenie spolupráce medzi uzlami, z ktorých jeden je výhradne IPv4 alebo výhradne IPv6. NAT-PT sa v súčasnosti už neodporúča.



Obr. 1-12.: NAT-PT

#### NAT64

Ide o jeden z mechanizmov na prechod IPv4 k IPv6. Jeho cieľom je vzájomný preklad datagramov, aby spolu mohli komunikovať zariadenia podporujúce odlišné verzie protokolu. Vychádza zo svojho predchodcu NAT-PT, ktorý kvôli svojim problémom (zásahy do DNS) bol odmietnutý. NAT64 je navrhnutý asymetricky, čiže umožňuje naviazať komunikáciu z koncovej IPv6 siete do internetu (IPv4). Zariadenia, ktoré majú implementovaný NAT64 sú umiestňované medzi IPv6 sieťou a IPv4 internetom. IPv4 adresy sú do adresného priestoru IPv6 mapované dynamicky a stavovo. NAT64 obsahuje dynamickú mapovaciu tabuľku, ktorá obsahuje vzájomne mapované dvojice s IPv6 adresou a portom stroja z miestnej siete a IPv4 adresou a portom. Mapovacie tabuľky sú udržiavané oddelené pre protokoly TCP, UDP a ICMP. Položky sa do nich pridávajú automaticky, keď niektoré zariadenie nadväzuje spojenie do IPv4 siete. Ak pre položku neexistuje žiadny živý aktívny dátový tok, automaticky sa položka z mapovacej tabuľky odstráni. Dátové toky sú rozlišované číslami portov. NAT64 je obvykle nasadzovaný s DNS64, pričom zaisťuje mapovanie adries pri vyhľadávaní v DNS.

#### **1.2.4. Jednorazový prechod na IPv6**

Teoretická stratégia určená pre novo budované siete. Hlavný princíp spočíva v nahradení celej infraštruktúry vrátane softvérových produktov za IPv6 kompatibilné. Predpokladá sa samozrejme aj s kompletným IPv6 adresovaním. Pre prístup do vzdialených IPv4 sietí sa počíta aj s riešením kompatibility s IPv4. V súčasnom svete je však tento princíp vo veľkej miere nerealizovateľný.



### 1.3. Existujúce portály o IPv6

V rámci projektu bolo analyzovaných niekoľko existujúcich portálov zaoberajúcich sa problematikou IPv6. Táto kapitola poskytuje prehľad niektorých z nich.

#### **6DISS.org - IPv6**

Edukačný portál o IPv6 dostupný online. Portál je riešený jednoducho, poskytuje informácie pre vzdelávanie sa v oblasti IPv6 prostredníctvom videí. Poskytuje rýchlu orientáciu v témach. Chýbajú tu však textové zdroje preberanej témy a chýba aspoň krátky opis kľúčových slov.

Dostupný na: na <http://www.6diss.org/e-learning/index.html>

#### **Deep Space 6 - The Linux IPv6 Portal**

Priemerne spracovaná webová stránka určená primárne na rozširovanie IPv6 na Linuxových OS. Poskytuje prezentácie, postupy a inštalácie na sfunkčnenie IPv6 na Linuxoch.

Dostupné na: <http://www.deepspace6.net/>

#### **IPv6:Security::nl**

IPv6 edukačný portál zameraný aj na bezpečnosť v IPv6. Jednoduchý, prehľadný, dobre spracované počítadlo vyčerpania IPv4 vo svete. Obsahuje porovnávanie IPv4 a IPv6, ako aj nastavovanie firewallu vo systéme Windows a prehľadnú tabuľku poskytovateľov IPv6 služieb. Obsahuje niekoľko videí na tému IPv6, no stránka je stále pod vývojom.

Dostupné na: <http://www.ipv6security.nl/?cat=12>

#### **IPv6 – Google**

Web stránka patriaca spoločnosti Google, na ktorej je znázornená vizualizácia adopcie IPv6 vo svete a rozšírenosť za posledné roky zobrazené v grafe. Použiteľné pre štatistickú oblasť portálu.

Dostupné na: <http://www.google.com/ipv6/statistics.html>

#### **IPv6 – Wikipédia**

Známa Wikipédia ponúka krátke vysvetlenie postavenia IPv6 protokolu a jeho stručnú funkciu. Wikipédia je všeobecne uznávaná a je najrozšírenejší edukačný portál vo svete. Systém orientácie sa v miliónoch článkov je jednou z výhod, ktoré by bolo možné využiť v navrhovanom edukačnom portáli.

Dostupné na: <http://sk.wikipedia.org/wiki/IPv6>

### **IPv6 Act Now**

Web stránka zameraná na prípravu organizácií ku prechodu na IPv6. Obsahuje edukačnú časť vyobrazením typológií. Poskytuje aj štatistické údaje o rozšírenosti IPv6.

Dostupné na: <http://www.ipv6actnow.org>

### **IPv6.cz**

Web portál so širokou teóriou o protokole IPv6 a jeho mechanizmoch. Dajú sa z neho čerpať základné informácie o protokole IPv6 (formáty adres, datagramov...). Spísané sú tu tiež návody, ako si implementovať nový protokol vo svojej sieti. Žiaľ, stránka je neaktuálna (posledný update z roku 2012), chýbajú mnohé ďalšie teoretické sekcie.

Dostupné na: <https://www.ipv6.cz>

### **Otestuje připojení k IPv6**

Portál poskytujúci len otestovanie svojej konektivity pre protokol IPv6. Neposkytuje žiadne materiály ani edukáciu.

Dostupné na: <http://test-ipv6.com/>

### **Portal IPv6 – LACNIC**

Regionálny internetový register pre latinskú Ameriku a karibské oblasti spracoval portál venovaný nasadeniu IPv6. Sú tu opísané mechanizmy prechodu na IPv6. Taktiež sa tu nachádzajú odkazy na tutoriály a videá (konkrétne na web stránku 6deploy.org a web stránku ipv6tf.org). Poskytujú tiež vlastné videá, tie však len v španielčine.

Dostupné na: <http://portalipv6.lacnic.net/en/>

### **TCP/IP v4 and v6**

Stránka spoločnosti Microsoft venovaná podpore IPv6 v jeho systémoch. Je tu mnoho dokumentov ku príslušnej oblasti ako aj návody na nastavovanie koncových zariadení (PC) pre podporu IPv6. Dokumenty sú dobre spracované a voľne stiahnuteľné vo formáte programu Word.

Dostupné na: <http://technet.microsoft.com/en-us/network/bb530961.aspx>

### **CCIE IPv6 Study Resources**

Je tu pomerne podrobnejšie spracovaná téma o IPv6. Obsahuje pekné a logické rozdelenie kapitol, ktoré však nie sú priamo spracované na stránke ale každá kapitola je odkazom na stránky Cisco, kde sa rozoberá daná téma.

Dostupné na: <http://www.internetworkexpert.com/resources/ipv6.htm>

### **IP Version 6 (IPv6) - Cisco Systems**

Portál spoločnosti CISCO zameraný vo všeobecnosti na počítačové siete. Problematika IPv6 je tu detailne spracovaná vo forme textov a obrázkov. Stránka má logické rozloženie kapitol témy a detailné spracovanie informácií o tomto protokole.

Dostupné na:

[http://www.cisco.com/en/US/tech/tk872/tsd\\_technology\\_support\\_protocol\\_home.html](http://www.cisco.com/en/US/tech/tk872/tsd_technology_support_protocol_home.html)

### **IPv6 | The Number Resource Organization**

Web stránka sa zameriava na postupy, ktoré treba dodržať a podniknúť pri nasadení IPv6. Neposkytuje detailné informácie ohľadom samotného protokolu IPv6 a jeho špecifických vlastností.

Dostupné na: <http://www.nro.net/ipv6>

### **IPv6 Tutorial**

Veľmi dobre spracované textové podklady pre štúdium problematiky IPv6. Poskytuje tiež mnoho tabuliek a obrázkov. Stránka je organizovaná ako tutoriál s viacerými kapitolami, ktoré sú logicky rozdeľované.

Dostupné na: <http://www.tutorialspoint.com/ipv6/index.htm>

### **IPv6.com - The Source for IPv6 Information, Training, Consulting & Hardware**

Web stránka poskytuje mnoho teoretických informácií. Zameriava sa na IPv6 aj z technického hľadiska a poskytuje prehľad možností riešenia na rôznych technológiách ako napríklad WiMax, či Microsoft Vista.

Dostupné na: <http://ipv6.com/>

### **IPv6.net - All the Ipv6 Resources You Need**

Portál venujúci sa výhradne problematike získavania vedomostí o IPv6. Poskytuje niekoľko zaujímavých videí a prezentácií. Problémy je možné riešiť aj pomocou fóra.

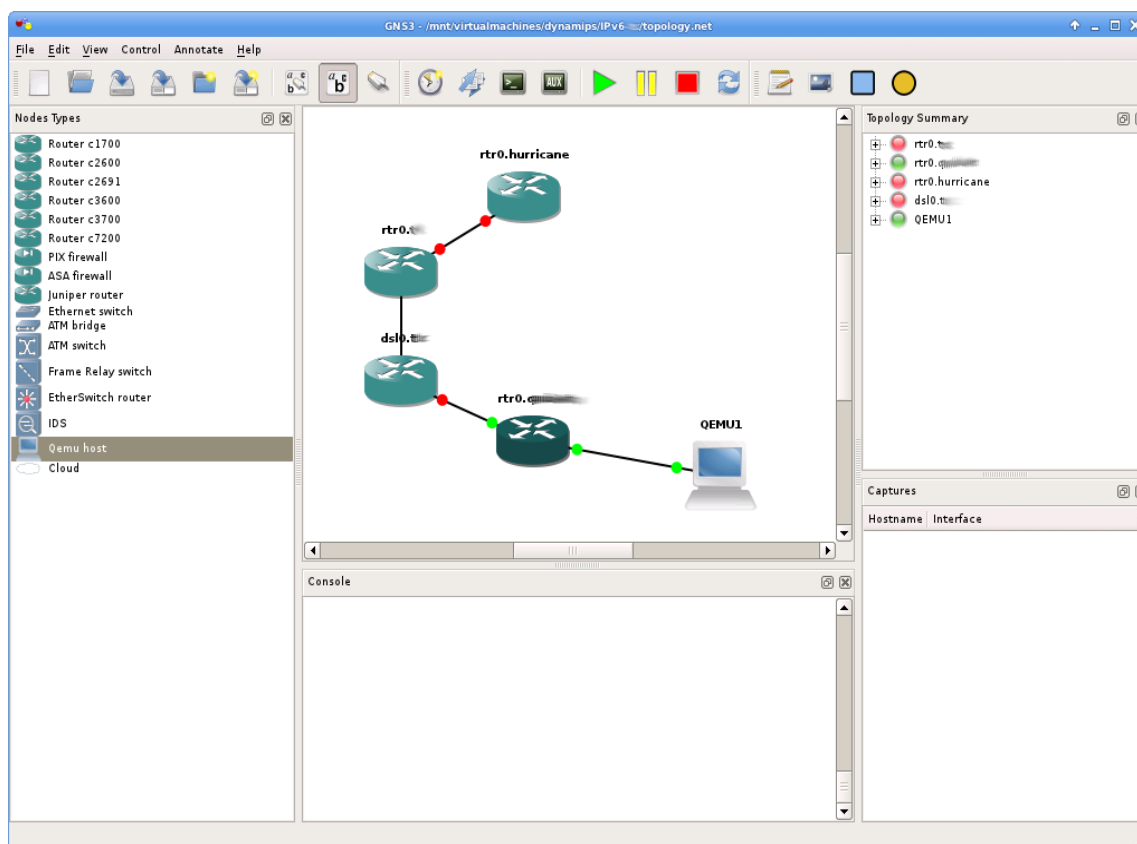
Dostupné na: <http://ipv6.net/>

## 1.4. Simulátor GNS3

K portálu, ktorý sa zaoberá IPv6 je veľmi žiaduce vyskúšať si možnosť otestovať možnosti IPv6 na simulácii typológie. Aktuálnym problémom je poskytnúť a sprevádzkovať vytvorený OpenSource simulátor na otestovanie si IPv6 tunelov alebo bezpečnostných mechanizmov. Aktuálne RFC dokumenty sa pravidelne menia a neposkytujú pravidelné aktualizácie. Táto skutočnosť odrádza všetkých vývojárov vytvárať a už vôbec nie pravidelne prerábať kód programu, ktorý poskytuje zdarma.

Jedným z možných modulov na simuláciu je napríklad IPv6Suite založený na OMNet++, ktorý poskytuje všetky potrebné možnosti simulácie na otestovanie IPv6. Bol vytvorený v roku 2004 a od tej doby bolo vtedy aktuálne „RFC 2373 IP Version 6 Addressing Architecture“ zastarané RFC 3513 a neskôr na aktuálne RFC 4219. Tento aktuálny bol dokonca dva krát aktualizovaný.

Graphic Network Simulator 3 (GNS3) je voľne dostupné aktuálne simulačné prostredie dostupné pre viacero platforiem. Pre softvér existuje veľké množstvo dokumentácie a veľká finančná podpora zaisťuje aktuálnosť aj pri zmenách RFC dokumentácii. Je určená prevažne na Cisco platformy a obsahuje komponenty Cisco zariadení.



Obr. 1-13.: GNS 3

GNS3 je postavený na zastaraných emulátoroch Dynamips a Qemu. Verzie programu sú dostupné pre OS Linux, Mac OS X a Windows. Táto možnosť je dostupná aj vďaka základu od VirtualBox programu na virtualizáciu prostredí na architektúrach x86 a AMD64/Intel64. GNS3 je postavený na jazyku Python a preto je možné ho implementovať priamo na web. Pre vlastné implementovanie softvéru je potrebné mať nainštalovaných niekoľko doplnkov a to Qt, Python, Sip, a PyQt. Softvér poskytuje ukladanie sieťových topológií do súboru a tie budú dostupné na našom portáli.

Dynamips, emulátor Cisco zariadení na ktorom je GNS3 postavený, je už zastaraný a nevydávajú sa nové aktualizácie. Packet tracer, ako oficiálny simulátor Cisco zariadení, neposkytuje dôveryhodné prostredie aké je na reálnych zariadeniach. GNS3 softvér túto možnosť poskytuje a preto poskytne bohatý doplnok k edukačnému portálu na ukážky konfigurácii a otestovanie si pripravených sieťových topológií vo vlastnom počítači alebo na stránke a preto bude použitý ako základ testovania na našom portáli.

## 2. Špecifikácia požiadaviek

Táto kapitola obsahuje požiadavky na navrhovaný portál. Požiadavky sú rozdelené do dvoch kategórií: funkcionálne a nefunkcionálne. Funkcionálne požiadavky spisujú vlastnosti portálu, ktoré má implementovať a poskytovať.

### 2.1. Funkcionálne požiadavky

#### ➤ Portál poskytuje edukačné texty v logickom usporiadaní do kapitol

Táto požiadavka špecifikuje, aby navrhnutý portál poskytoval materiály o IPv6 v textovej forme. Tieto texty majú byť usporiadané do jednotlivých logických celkov (kapitol, podkapitol...).

#### ➤ Portál zahŕňa a poskytuje aktuálnu pavučinu RFC dokumentov

Požaduje sa, aby v portály používateľ našiel aj pavučinu aktuálnych dokumentov, pričom pavučina RFC dokumentov sa vytvára na ich závislostiach a vzájomných odkazoch.

#### ➤ Portál implementuje fórum

Portál má implementovať fórum pre používateľov. Každý používateľ, ktorý sa prišiel na portál vzdelávať, má právo sa pýtať. Pýtať sa môže prostredníctvom fóra rozdeleného do rôznych tém. Vo fóre používateľovi zodpovedajú otázky autori portálu alebo iní používatelia.

#### ➤ Portál implementuje virtuálne simultačné prostredie

Požaduje sa, aby portál umožňoval používateľom otestovať svoje nadobudnuté znalosti v simulačnom prostredí. V tejto požiadavke je zahrnutá aj požiadavka na vyhodnotenie správnosti simulácie.

➤ Portál poskytuje testové úlohy

Požiadavka požaduje, aby portál poskytoval teoretické otestovanie používateľov. Nešpecifikuje sa, či ide o otázky typu „výber odpovede z možností“ alebo „zadanie odpovede“. Táto požiadavka, tak ako aj predchádzajúca, zahŕňa aj požiadavku na vyhodnotenie správnosti zadaných odpovedí.

➤ Portál poskytuje vyhľadávanie

Nakoľko problematika IPv6 je široká oblasť, portál má poskytovať vyhľadávanie na základe kľúčových slov. Vyhľadávanie je v rámci učebných textov portálu, ale aj v rámci RFC dokumentov.

## **2.2. Nefunkcionálne požiadavky**

➤ Portál je webová aplikácia

Od navrhovaného portálu je požadované, aby fungoval ako webová aplikácia, čo zabezpečí portálu „všadeprítomnosť“ a odstraňuje nutnosť inštalácie.

➤ Portál má jednoduché rozhranie

Portál má obsahovať jednoduché rozhranie pre používateľa. To znamená, že používateľ pri svojej prvej návšteve portálu by nemal mať problémy rýchlo sa zorientovať v hlavnej ponuke portálu.

➤ Portál je zameraný výhradne na IPv6

Portál má zahŕňať problematiku Internet Protokolu verzie 6. Nemal by zachádzať do iných oblastí a zbytočne tak sypať na používateľa zbytočné informácie.

### 3. Hrubý návrh

V tejto kapitole sa zameriavame na opis návrhu portálu.

#### 3.1. Štrukturálny návrh portálu

Architektúra navrhovaného portálu sa skladá z 5 modulov:

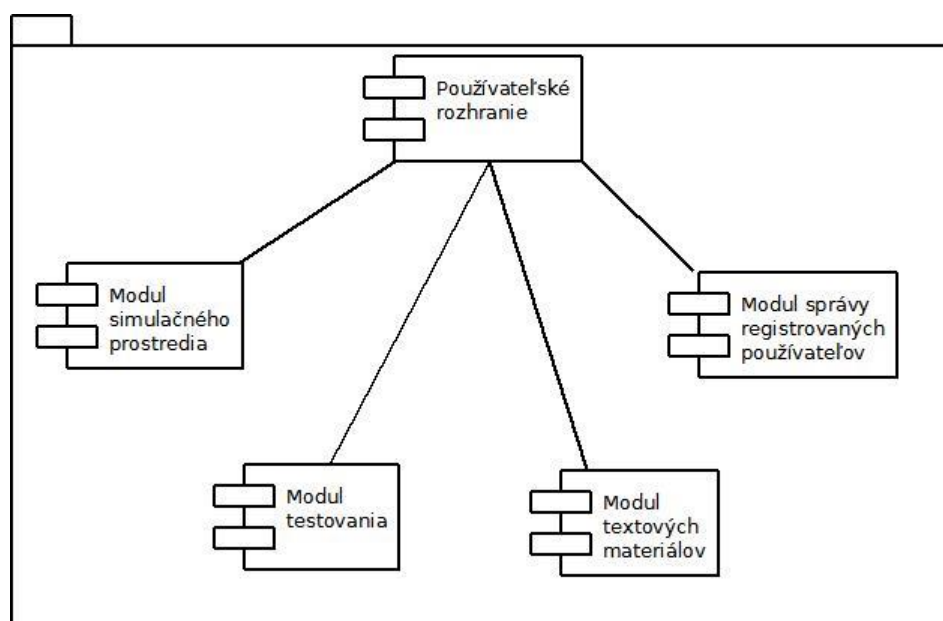
**Používateľské rozhranie** – modul poskytujúci grafické rozhranie medzi používateľom a samotným programom. Tento modul interpretuje používateľove príkazy a spracováva ich. Podľa zadaných príkazov spúšťa činnosti ďalších modulov.

**Modul simulačného prostredia** – implementuje možnosť simulácie virtuálneho prostredia. Tento modul zabezpečuje zobrazenie interaktívneho virtuálneho prostredia. Zabezpečuje tak praktické otestovanie používateľových znalostí.

**Modul testovania** – modul zabezpečuje testové odskúšanie používateľových znalostí.

**Modul textových materiálov** – modul, ktorý poskytuje textové materiály pre používateľa. Po vyžiadaní od používateľa cez Používateľské rozhranie, tento modul poskytne na výstup požadovaný text.

**Modul správy registrovaných používateľov** – modul, ktorý zabezpečuje správu registrovaných používateľov. Jeho úlohou je zabezpečiť registráciu a archivovanie používateľov.



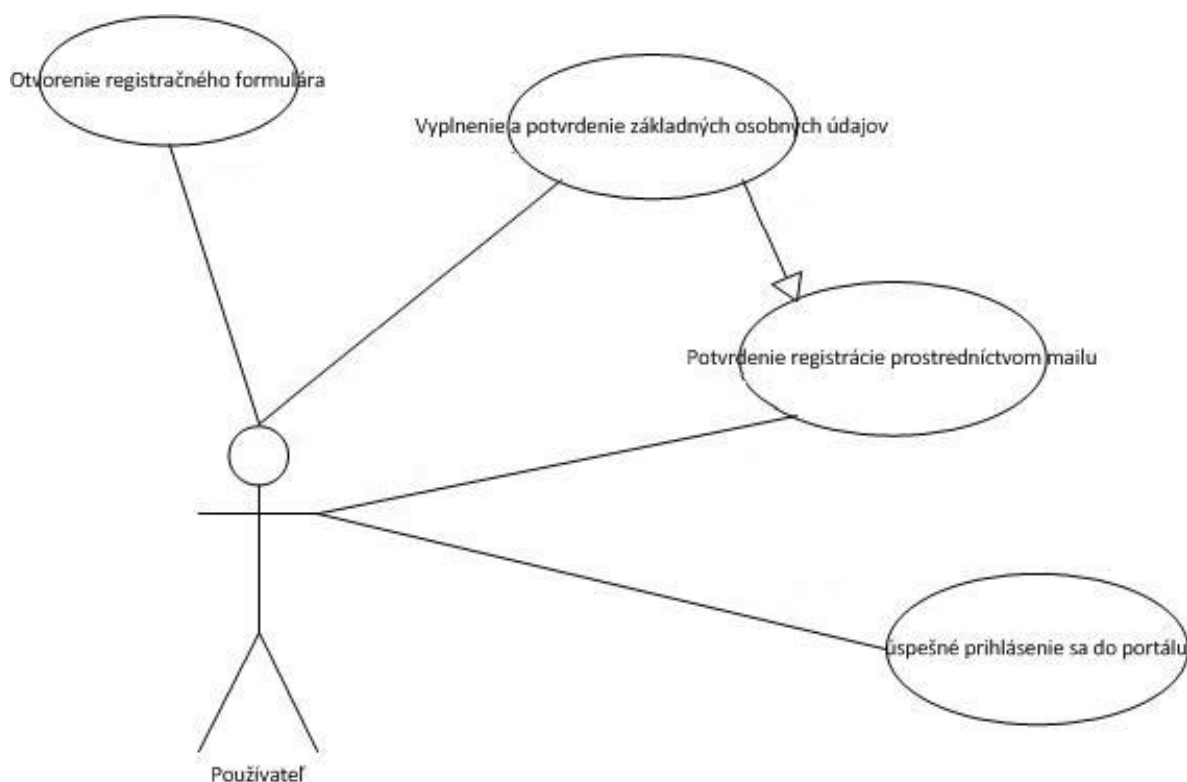
Obr. 3-1: Moduly portálu

## 3.2. Funkcionalita z pohľadu používateľa

Z pohľadu používateľa sa v portály implementujú nasledovné prípady použitia.

### 3.2.1. Proces prístupu používateľa k portálu

Na obrázku 3-2 je znázornený diagram prípadov použitia, ktorý poskytuje pohľad na registráciu používateľa. Na začiatku si používateľ otvorí webový portál. Portál mu automaticky ponúkne možnosť registrácie alebo prihlásenia sa, ak už má vytvorené používateľské konto. Systém bude ponúkať možnosť aj anonymného prezerania portálu, ktoré však bude mať svoje menšie obmedzenia. Po otvorení registračného formulára, používateľ vyplní základné údaje ako login, heslo, mailovú schránku. Taktiež bude mať možnosť vyplniť aj doplňujúce údaje ako kontakt na sociálne siete a komunikátory, pohlavie, vek a iné. Na jednu mailovú adresu možno registrovať jedného používateľa. Po správnom vyplnení údajov klikne používateľ na tlačidlo Potvrdiť. Systém overí správnosť údajov a na mail pošle potvrdzovaciu správu. Po kliknutí na aktivačný odkaz sa používateľ môže prihlásiť do systému a využívať portál i fórum naplno.

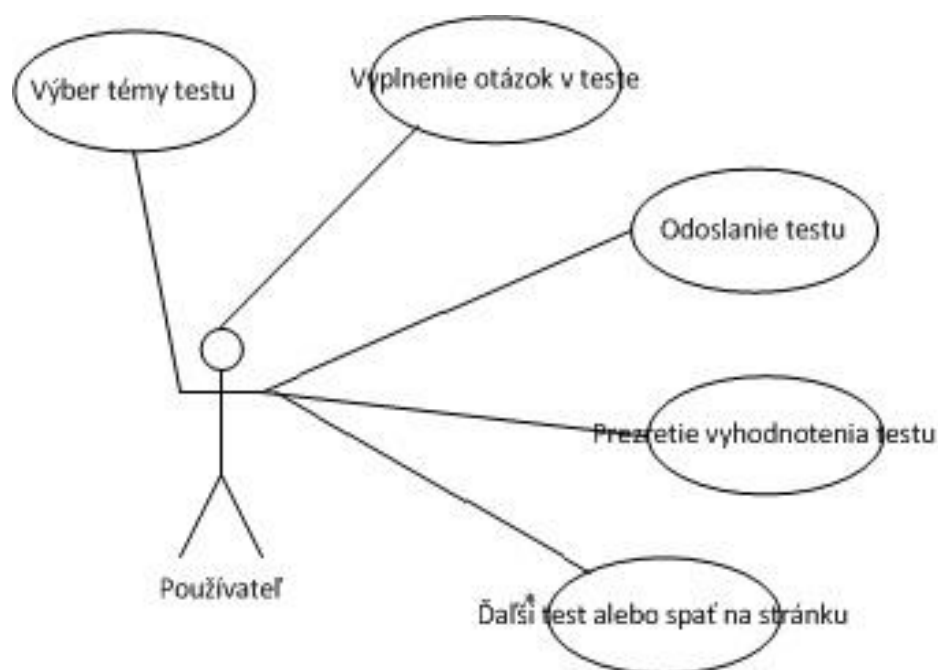


Obr. 3-2.: Prípad použitia: prístup k portálu



### 3.2.2. Proces otestovania používateľa

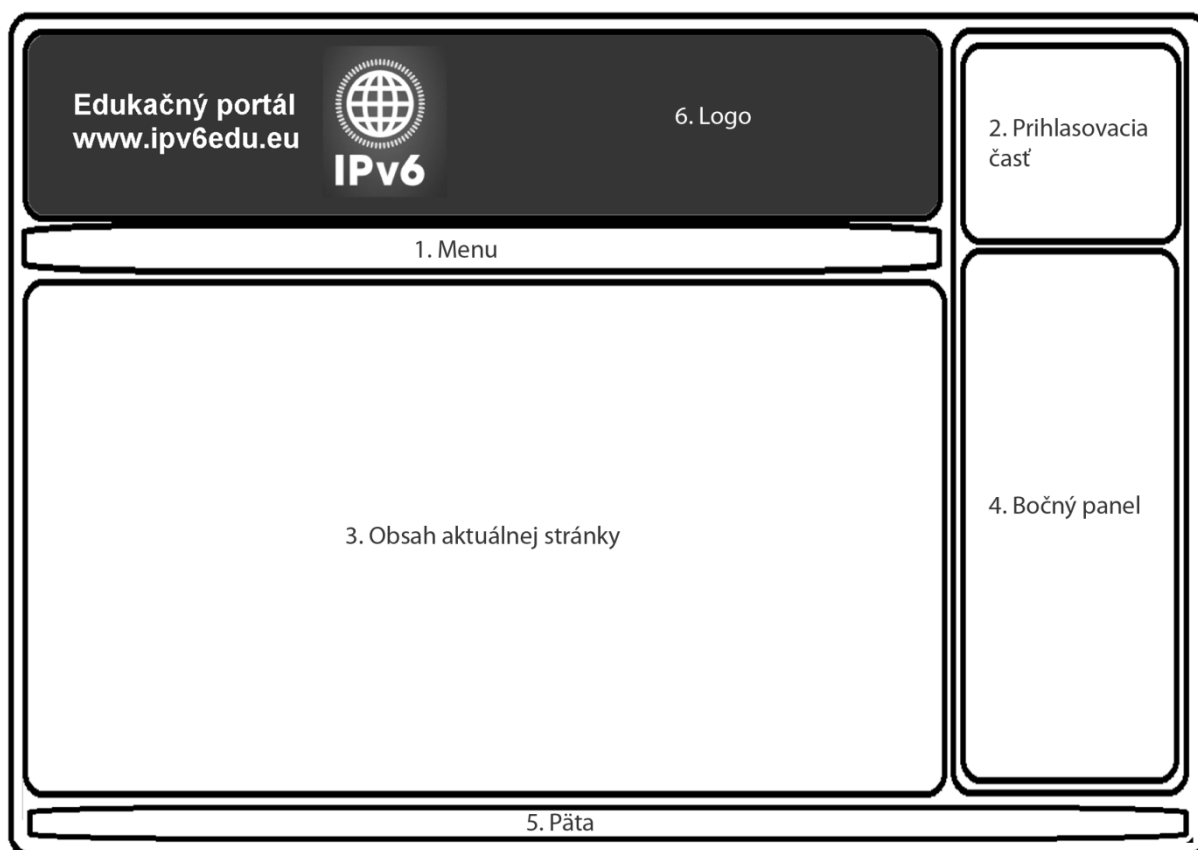
Na obrázku č. 3-2 je znázornený diagram prípadov použitia, ktorý poskytuje pohľad na testovanie vedomostí používateľa. Na začiatku si používateľ vyberie test zo skupiny testov. Systém automaticky vyberie úroveň testu podľa aktuálneho hodnotenia používateľa. Ten sa so zvyšovaním počtu správnych odpovedí zvyšuje. Portál vygeneruje používateľovi skupinu otázok, na ktoré odpovedá. Po vyplnení všetkých otázok v teste používateľ odošle odpovede, systém odpovede ihneď vyhodnotí a zobrazí používateľovi výsledok. Používateľ si môže pozrieť miesta, kde spravil chyby. Aktualizuje sa mu jeho rating a je mu ponúknutý ďalší test alebo návrat na domovskú stránku portálu.



Obr. 3-3.: Prípady použitia: otestovanie používateľa

### 3.3. Návrh grafického rozhrania web stránky portálu

V tejto kapitole je opísaný náš navrhovaný edukačný portál. Na obr. č. X je zobrazený návrh úvodnej web stránky. Táto úvodná stránka sa skladá z niektorých hlavných častí, ktoré opíšem podrobnejšie. Návrh sa bude ešte s najväčšou pravdepodobnosťou ešte rozširovať podľa potrieb, ktoré budú zistené počas implementácie.



Obr. 3-4.: Rozloženie stránky

## **1. Menu**

Menu bude obsahovať nasledujúcich 9 základných sekcií. Položky obsahujú sekcie, tie obsahujú podsekcie a tieto sa zobrazia po zastavení kurzoru myši na danej sekcii.

### **1. IPv6 aktuality**

Táto sekcia neobsahuje žiadne pod sekcie. V tejto časti nášho portálu sú pravidelne pridávané aktuálne články o aktuálnej situácii o IPv6.

### **2. Zoznámte sa s IPv6**

- I. Úvod
- II. Štruktúra IPv6
- III. Prechod z IPv4 na IPv6
- IV. Bezpečnosť IPv6
- V. RFC Štandardy

### **3. Použitie IPv6**

- I. Testovací modul IPv6
- II. Test pripojenia IPv6
- III. Verifikátor IPv6 adres

### **4. Video**

- I. Výučba videami
- II. Videá z konferencií

### **5. Odkazy**

- I. Plánované konferencie o IPv6
- II. Tréningové kurzy a certifikáty
- III. Edukačné portály o IPv6

### **6. Stiahnuť**

- I. Prezentácie a videa z konferencií
- II. Knihy

### **7. Testovanie**

- I. Kvíz
- II. Testy
- III. Ankety

### **8. Udalosti**

- I. Kalendár udalostí
- II. Prehľad

### **9. Fórum**

Po kliknutí na sekciu fórum Vás premiestni na inú stránku, kde bude využívaný modul

### **10. O nás**

Všetky údaje o našom tíme a taktiež odkaz na stránku nášho tímového projektu.

## **11. Profil**

Sekcia profil sa zobrazí len prihláseným používateľom a bude v nej možné upravovať údaje prihláseného používateľa.

## **2. Prihlasovacia časť**

Používateľ má možnosť si prezerať edukačný portál bez prihlásenia, no po prihlásení sa mu zobrazia ďalšie možnosti, napríklad komentovanie článkov. V prihlasovacej časti sa bude možné registrovať alebo prihlásiť po zadaní prihlasovacieho mena a hesla.

## **3. Obsah stránky**

Obsah stránky je dynamický podľa toho v akej sekcii sa nachádzame.

## **4. Bočný panel**

V najvrchnejšej časti sa bude nachádzať vyhľadávanie na stránke a na Googli. Bočný panel bude slúžiť na informovanie používateľov o nových zmenách na stránke, taktiež vytvoríme rad ankiet, ktoré sa budú striedať, a takto ľahko a rýchlo získame výsledky od používateľov, pretože takáto anketa bude viditeľná pri prezeraní hocijakej stránky na portáli. V tomto bočnom paneli bude taktiež priestor pre reklamu.

## **5. Päta**

V päte stránky sa budú nachádzať kontaktné údaje na výrobcov stránky a päta bude taktiež obsahovať mapu stránok, ktorá uľahčí používateľovi sa rýchlejšie orientovať na našom portáli.

## **6. Logo**

Logo stránky máme navrhnuté, no možno ho ešte zmeníme po presnejšom grafickom návrhu celej stránky, aby ladilo s farebnou škálou celého edukačného portálu.

**Fórum:**

Vytvorenie fóra pre návštevníkov nášho portálu, ktoré bude umožňovať diskutovať a riešiť rôzne problematiky o internetovom protokole IPv6. Použijeme už vytvorenú štruktúru fóra, ktorú nastavíme podľa našich potrieb. Daná štruktúra nám umožní vytvárať kategórie, v ktorých sa budú nachádzať témy vytvorené autormi i používateľmi. Používatelia budú môcť pridávať príspevky do daných tém, čím sa vlastne vytvorí diskusia, ktorá bude môcť viesť k vyriešeniu problému. Štruktúra fóra sa bude počas meniť počas chodu stránky podľa zistení potrieb používateľov, taktiež môžu byť zmenené kategórie. Na začiatku budú pravidlá a návody, ako vytvárať a prispievať do tém.

## 4. Implementácia prototypu

Pri implementovaní prototypu sa vyčlenili tieto funkcionality:

- Základný vzhľad stránky
- Implementovanie databázy
- Prihlasovanie a registrovanie užívateľov
- Generovanie testov a jednoduchý interfejs na vkladanie otázok
- Vloženie prvých kapitol
- Systém aktualít
- Funkčné základné odkazy, ako O nás alebo kontakt.

Stránka je dostupná na adrese [www.ipv6edu.web44.net](http://www.ipv6edu.web44.net) a je registrovaná cez portál <http://www.000webhost.com/> Na stránke sú dostupné nasledujúce súčasti:

- Zálohovanie
- Cron Jobs
- Web mail
- Ochrana hesiel
- PHP
- Vysoká rýchlosť prenosu
- MySQL databáza
- Miesto na disku: 1500MB

Tieto súčasti sú dostačujúce na implementovanie potrebného prostredia prototypu.

## 4.1. Dizajn hlavnej stránky prototypu

Vzhľad stránky je implementovaný ako kombinácia jazykov HTML5 a CSS3. Tieto jazyky postačia na vytvorenie dynamickej stránky s priemernou náročnosťou otvorenia. Návrh dizajnu prototypu zodpovedá Hrubému návrhu stránky.

Na úvodnej stránke v časti obsah aktuálnej stránky bude zobrazená aktualita pomocou prezentácie aktualít postupne sa meniacich v intervale tri sekundy. Táto prezentácia je implementovaná v jazyku CSS3. Užívateľ si môže vybrať z troch náročností obsahu stránok rozdelených:

- Začiatočnícka
- Pokročilá
- Expertná

Na úvodnej stránke je dostupný celý obsah kapitol. Kapitoly sú rozdelené podľa tejto náročnosti a na konci kapitoly je dostupný test. Ktorý bude v rámci prototypu len demonštrovaný na jednom exemplári.

V pätičke stránky sú dostupné odkazy na stránky s podobnou tematikou ako aj inštalačné súbory potrebné pre testovanie neskôr implementovaného modulu. Ďalej je v pätičke dostupné generovanie testov len pre prihlásených užívateľov podľa počtu otázok, podkapitoly a úrovne testu. Kliknutím na odkaz kontakt je možné zaslať správu na tímový mail [tim.tipsix@gmail.com](mailto:tim.tipsix@gmail.com).

Z ponúkaných záložiek umiestnených na pravej hornej strane stránky a ľavej dolnej strane budú aktívne:

- DOMOV – zobrazenie domácej stránky
- O NÁS – krátky popis tímu TIPSix
- KONTAKTY – Možnosť kontaktovať členov tímu.

Záložky v hornej lište nad aktualitami poskytujú teoretické podklady tém. V prvotnom prototypu riešime zatiaľ textové podklady.

Edukčný portál  
www.ipv6edu.eu

*Všetchno, čto potrebujete vedieť o IPv6*

DOMOV
O NÁS
FÓRUM
PROFIL
KONTAKTY

1. Úvod
2. Prehľad protokolu
3. Nové vlastnosti
4. Bezpečnosť
5. Možnosti nasadenia
6. Praktick♦ uk♦ky

Ste prihlásený ako [LukášLenčoš](#)  
[Odhlasť sa](#)

### IPv6 kongress riešil problémy prechodu globálnej siete na protokol IPv6

1. a 2. Októbra tohto roku sa konal v Singapúre stretnutie založené "IPv6 world congress". Riešili sa ponuky hladkého prechodu spoločností na IPv6 infraštruktúru sietí.

[Zobraziť viac](#)

### Úroveň kapitol:

#### Začiatočnicke

Táto časť sa venuje popisu protokolu IPv6 ako aj porovnanie s predošlým protokolom

[ZAČNI TERAZ](#)

#### Pokročilé

Táto časť vysvetľuje časti bezpečnosti IPv6 a mechanizmy koexistencie protokolov IPv6 a IPv4

[ZAČNI TERAZ](#)

#### Expertné

Najnáročnejšia časť tém je venovaná primárne expertom, ktorí majú znalosti z oblasti počítačových a komunikačných systémov a sietí. Časť pre expertov sa venuje konfigurácii sieťových zariadení na simulátore.

[ZAČNI TERAZ](#)

#### TESTOVANIE

- Generuj test
- Úroveň a počet bodov
- Zoznam kapitol na prečítanie

#### PROGRAMY NA STIAHNUTIE

Simulátor GNS3

#### ĎALŠIE IPV6 PORTÁLY

- IPV6.CZ
- 6DISS.ORG - IPv6
- Deep Space 6
- IPv6:Security.nl
- IPv6 Act Now
- Otestuje pripojenie k IPv6

#### KONTAKT

TIPSix - Tím IPv6  
Bratislava - Mlynska dolina, Slovakia

Mobil: 0123456789

## Dizajn prototypu

44



## 4.2. Štruktúra prototypu

Stránka vyžaduje na spustenie PHP server. Základ portálu je dostupný v súbore index.php a použité štýly v style.css. Portál je klasicky rozdelený na hlavičku, telo a päť. V hlavičke sú umiestnené odkazy, logo a motto portálu. Telo obsahuje v úvodnej stránke prezentáciu aktualít a rozdelenie podľa úrovne kapitol. Päť portálu pozostáva z odkazov na testovanie, programy na stiahnutie, ďalšie IPv6 portály, kontakt a odkazy hlavné menu.

Na prvej strane web stránky je zobrazovaná prezentácia aktualít vkladaná v tvare:

```
<div class="slider-holder">
  <a href="#" class="prev"></a>
  <span class="slider-shadow"></span>
  <div class="flexslider">
    <ul class="slides">
      <li>
        
        <div class="slide-cnt">
          <h3>Už jeden a pol roka je spustená IPv6</h3>
          <p>Od júna minulého roka sa spustil projekt permanentnej
implementácie IPv6 zariadení do IPv4 počítačovej siete.</p>
          <a href="#" class="slider-btn"><span></span>Zobrazit' viac</a>
        </div>
      </li><li>
        
        <div class="slide-cnt">
          <h3>IPv6 kongress riešil problémy prechodu globálnej siete
na protokol IPv6</h3>
          <p>1. a 2. Októbra tohto roku sa konal v Singapúre
stretnutie založené "IPv6 world congress". Riešili sa ponuky hladkého prechodu
spoločností na IPv6 infraštruktúru sietí.</p>
          <a href="#" class="slider-btn"><span></span>Zobrazit' viac</a>
        </div>
      </li>
    </ul>
  </div>
```

Triedy „slide-holder“ a „flexslider“ sú definované v adresári css/styles.css a css/flexslider.css linkovaný:

```
<link rel="stylesheet" href="css/flexslider.css" type="text/css"
media="all" />
```

Výber jednotlivých úrovní kapitol definuje časť kódu:

```
<section class="cols">
<div><h2 align="center"><strong>Úroveň kapitol:<strong></strong></h2>
  <p align="center">&nbsp;</p>
</div>
  <div class="col">
    <h3 class="starter-ico">Začiatocnícke</h3>
    <p>Táto časť sa venuje popisu protokolu IPv6 ako aj
porovnanie s predošlým protokolom</p>
    <a href="#" class="more">ZAČNI TERAZ</a>
  </div>
  <div class="col">
    <h3 class="awesome-ico">Pokročilé</h3>
    <p>Táto časť vysvetľuje časti bezpečnosti IPv6 a mechanizmy
koexistencie protokolov IPv6 a IPv4</p>
    <a href="#" class="more">ZAČNI TERAZ</a>
  </div>
  <div class="col">
    <h3 class="save-ico"><a href="#">Expertné</a></h3>
    <p>Najnáročnejšia časť tém je venovaná primárne expertom,
ktorý majú znalosti z oblasti počítačových a komunikačných systémov a
sietí. Časť pre expertov sa venuje konfigurácii sieťových zariadení na
simulátore.</p>
    <a href="#" class="more">ZAČNI TERAZ</a>
  </div>
```

Tie sú zoradené podľa CSS umiestnenia deklaráciou „float“ aby boli umiestnené vedľa seba, pozadie je uložené v /css/images a šírka a výška sú presne dané pre zamedzenie deformácie ponuky v prípade otvorenia v zariadeniach s menším displejom. Súbor style.css definuje triedy „col“ a „cols“ nasledovne:

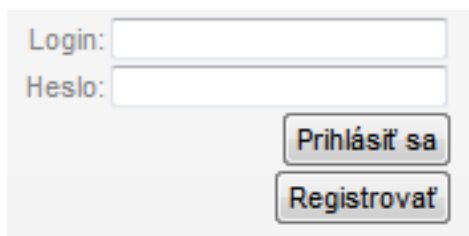
```
.main .cols { padding-bottom: 54px; }

.main .cols .col { width: 280px; float: left; }
.main .cols .col:last-of-type { width: 274px; }
.main .cols .col + .col { padding-left: 55px; }

.main .cols .col h3 { padding-bottom: 14px; padding-left: 50px; }
.main .cols .col h3 a { color: #000; }
.main .cols .col h3 a:hover { text-decoration: none; color: #333; }
.main .cols .col h3.starter-ico { background: url(images/save-ico.png) no-repeat 0 0; }
.main .cols .col h3.awesome-ico { background: url(images/awesome-ico.png) no-repeat 0 0; }
.main .cols .col h3.save-ico { background: url(images/starter-ico.png) no-repeat 0 0; }
.main .cols .col p { padding-bottom: 10px; }
.main .cols .col a.more { text-transform: uppercase; }
```

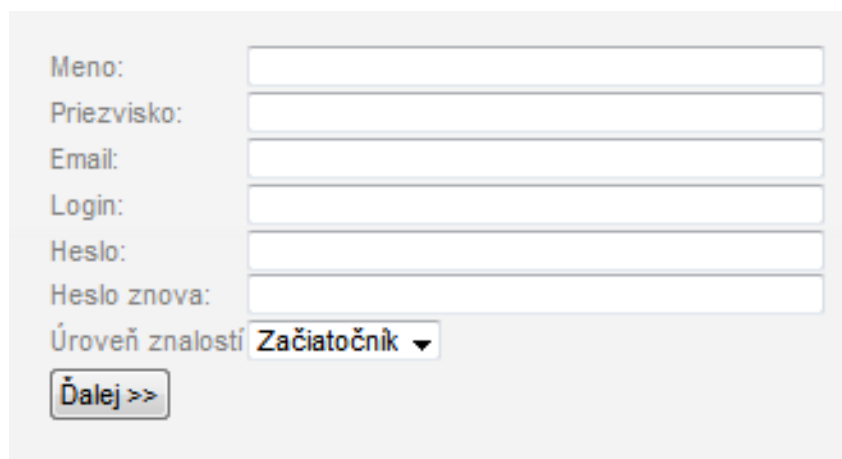
### 4.3. Registrácia do portálu

Aby mohol používateľ plnohodnotne využívať všetky možnosti portálu, je potrebné aby sa registroval (napríklad testovanie rozoberané v nasledovnej kapitole je možné len registrovaným používateľom). Registráciu vykoná jednoduchým rozhraním, ktoré spustí kliknutím na *Registrovať* na domovskej adrese portálu.

A screenshot of a web form for login and registration. It features two input fields: 'Login:' and 'Heslo:'. Below these fields are two buttons: 'Prihlásiť sa' (Login) and 'Registrovať' (Register).

#### *Registrácia a prihlásenie*

Údaje, ktoré sú potrebné vyplniť, sú meno, priezvisko, email pre verifikáciu, prihlasovací login, prihlasovacie heslo a svoju predpokladanú úroveň znalostí. Táto úroveň nijako neobmedzuje používateľov, ale v konečnej verzii portálu budú otázky testovania hodnotené a používatelia budú mať svoj rating.

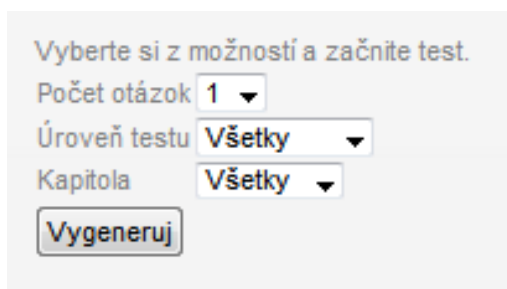
A screenshot of a registration form. It contains several input fields: 'Meno:', 'Priezvisko:', 'Email:', 'Login:', 'Heslo:', and 'Heslo znova:'. There is also a dropdown menu for 'Úroveň znalostí' with 'Začiatočník' selected. At the bottom is a button labeled 'Ďalej >>'.

Meno:	<input type="text"/>
Priezvisko:	<input type="text"/>
Email:	<input type="text"/>
Login:	<input type="text"/>
Heslo:	<input type="password"/>
Heslo znova:	<input type="password"/>
Úroveň znalostí	Začiatočník ▼
<input type="button" value="Ďalej &gt;&gt;"/>	

#### *Registrácia nového používateľa*

#### 4.4. Testovanie v prototype

Testovanie v prototype je založené na databáze otázok a odpovedí. Po registrácii a prihlásení používateľa je možné zvoliť generovanie testu v spodnej časti hlavnej stránky. Používateľovi sa zobrazí nasledovný dialóg:



Vyberte si z možností a začnite test.

Počet otázok 1 ▼

Úroveň testu Všetky ▼

Kapitola Všetky ▼

Vygeneruj

##### *Generovanie testu*

Tu si používateľ zvolí atribúty testu ako počet otázok, úroveň testu a kapitolu, z ktorej chce testy generovať. V prvotnom prototype kapitoly neimplementujeme a testy sa generujú zo všetkých kapitol.

Úroveň testu je rozdelená podľa náročnosti do troch kategórií:

- Začiatočnicke otázky
- Pokročilé otázky
- Expertné otázky

Vygenerovaný test je v prvotnom prototype implementovaný ako výber jednej správnej odpovede z viacerých možných.

Posledným krokom testovania je odoslanie testu (tlačidlo *Vyhodnotiť test*).

1. Koľko bitov má adresa odosielateľa v hlavičke IPv6 datagramu?

☒ 128

☐ 32

☐ 48

☐ 140

☐ 16

☐ 64

2. Koľko bajtov má hlavička IPv6 paketu?

☐ 60

☐ 45

☒ 40

☐ 30

☐ 20

☐ 32

3. Ako je definovaná príslušnosť adresy IPv6 ku sieti (podsieti)?

☐ prvým bajtom adresy

☐ posledným bajtom adresy

☐ prvými 4 bajtami adresy

☐ postfixom

☐ prefixom

4. Individuálna adresa sieťového rozhrania je:

☐ multicast

☐ broadcast

☐ anycast

☐ unicast

☐ žiadna z uvedených

5. Ktorý typ adresy špecifikuje skupinu príjemcov?

☐ žiadna z uvedených

☐ unicast

☐ anycast

☐ broadcast

☐ multicast

**Vyhodnotiť test**

*Vygenerovaný test*

## **5. Externé prílohy**

1. Preberací protokol – preberací\_protokol.jpg
2. Riadiaca dokumentácia – Riadiaca dokumentacia.pdf

## 6. Literatúra

- [1] 2011.GNS3 and Gentoo – fixing QEMU networking.  
<http://www.braindeadprojects.com/blog/what/gns3-and-gentoo-fixing-qemu-networking/>.  
[Cit: 12-nov-2013].
- [2] 2011. Graphical Network Simulator - GNS3. <http://www.gns3.net/>. [Cit: 12-nov-2013].
- [3] 2013. 10 Things You Should Know About IPv6 Addressing - TechRepublic.  
<http://www.techrepublic.com/blog/10-things/10-things-you-should-know-about-ipv6-addressing/>. [Cit: 12-nov-2013].
- [4] 2013. 6DISS.org - IPv6. <http://www.6diss.org/e-learning/>. [Cit: 12-nov-2013].
- [5] Dan, York, 2012. All IPv6 Resources | Deploy360 Programme.  
<http://www.internetsociety.org/deploy360/ipv6/all-ipv6-resources/>. [Cit: 12-nov-2013].
- [6] Richard, Jimmerson, 2013. Case Study: NLnet Labs | Deploy360 Programme.  
<http://www.internetsociety.org/deploy360/resources/case-study-nlnet-labs/>. [Cit: 12-nov-2013].
- [7] INE, 2013. CCIE IPv6 Study Resources. [Cit: 12-nov-2013]. <http://www.internetworkexpert.com/resources/ipv6.htm>.
- [8] Cisco, 2012. Enterprise IPv6 Solution - Cisco Systems.  
[http://www.cisco.com/en/US/products/ps6553/products\\_ios\\_technology\\_home.html](http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html). [Cit: 12-nov-2013].
- [9] Cisco. 2013. IPv6 - Cisco Systems.  
<http://www.cisco.com/web/solutions/trends/ipv6/index.html>. [Cit: 12-nov-2013].
- [10] BT Diamond IP, 2012. IPv6 Resource Center.  
[http://btdiamondip.com/IPv6\\_Resource\\_Center/](http://btdiamondip.com/IPv6_Resource_Center/). [Cit: 12-nov-2013].
- [11] Ultimo, 2013. IPv6 Resources, Information, Primers, FAQs.  
<http://www.ipv6now.com.au/resources.php>. [Cit: 12-nov-2013].
- [12] Sean, Wilkins, 2012. IPv6 Support in Windows 8 and Windows Server 2012.  
<http://www.petri.co.il/ipv6-support-windows-8-windows-server-2012.htm>. [Cit: 12-nov-2013].
- [13] RIPE NCC, 2013. IPv6 Transition Mechanisms — RIPE Network Coordination Centre.  
<http://www.ripe.net/lir-services/training/e-learning/ipv6/transition-mechanisms>. [Cit: 12-nov-2013].