ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

BAKALÁŘSKÁ PRÁCE

2014 **Malokhatko Elena**

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra radioelektroniky

Normalizační aktivity organizace IETF

květen 2014 **Bakalantka: Malokhatko Elena**

Vedoucí práce: Ing. Zdeněk Brabec, CSc.

Čestné prohlášení

Prohlašuji, že jsem svou bakalářskou práci vypracovala samostatně a použila jsem pouze podklady (literaturu, projekty, SW atd.) uvedené v přiloženém seznamu.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

Datum: …… ……

podpis bakalantky

Poděkování

Touto cestou bych ráda poděkovala vedoucímu bakalářské práce Ing. Zdeňku Brabcovi, CSc. za cenné profesionální rady, připomínky, trpělivost a metodické vedení práce.

Datum: …… ……

podpis bakalantky

České vysoké učení technické v Praze
Fakulta elektrotechnická

katedra radioelektroniky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Student: **Elena Malokhatko**

Studijní program: Komunikace, multimédia a elektronika
Obor: Multimediální technika

Název tématu: **Normalizační aktivity organizace IETF**

Pokyny pro vypracování:

Cílem Vaší práce je přehledně, strukturovaně a vyváženě zmapovat normalizační aktivity v oblasti internetu.

Východiskem práce je identifikace oblastí pokrytých jednotlivými standardizačními organizacemi působícími v oblasti internetu a identifikace, popis a rozbor vzájemných vazeb. Seznam organizací upřesní vedoucí práce. Jádrem práce pak bude podrobná analýza činnosti organizace Internet Engineering Task Force (IETF) a jejich vazeb na další organizace. Vaše práce je komplementární k práci Normalizační aktivity organizace W3C.

Při zpracování práce věnujte pozornost oblastem souvisejícím s multimediální technikou – Vámi studovaným oborem. Práci koncipujte tak, aby její výsledky bylo možno využít i ve výuce.

Seznam odborné literatury:

[1] Kabelová, A. – Dostálek, L.: Velký průvodce protokoly TCP/IP a systémem DNS. 3. aktualizované a rozš.vyd. Praha: Computer Press, 2005. 542 s. ISBN 80-722-6675-6
[2] Pužmanová, R.: Jak se orientovat v RFC aneb Průvodce profesionála. Dostupné z: http://www.lupa.cz/clanky/jak-se-orientovat-v-rfc-aneb-pruvodce-profesionala/
[3] Webové stránky organizace The Internet Engineering Task Force (IETF). Dostupné z: http://www.ietf.org/

Vedoucí: Ing. Zdeněk Brabec, CSc.

Platnost zadání: do konce letního semestru 2014/2015

Prof. Ing. Miloš Klíma, CSc.
vedoucí katedry

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE Fakulta elektrotechnická L.S.

prof. Ing. Pavel Ripka, CSc.
děkan

V Praze dne 10. 2. 2014

Anotace

Bakalářská práce se věnuje tématu normalizačních aktivit Komise techniky Internetu (originální název: Internet Engineering Task Force - IETF), která je jednou z nejstarších organizací v oblasti regulace a vývoje internetových aktivit a správy světové sítě Internet.

Bakalářská práce má úvod, pět kapitol a závěr. V první kapitole jsou vymezeny teoretické předpoklady, zejména definice pojmů Internet, multimédia, World Wide Web. Ve druhé kapitole je diskutováno o tom, jaké organizace existují a vydávají standardy v oblasti Internetu. Ve třetí kapitole se pojednává o vzniku a dosavadní činnosti organizace IETF, zejména její historii, vzniku, organizační struktuře a delegování pravomocí v rámci organizace a mezi jejími pracovními skupinami. Významným je i pojednání o celkových výsledcích práce a aktivit organizace IETF. Ve čtvrté kapitole se pojednává o hlavních procesech probíhajících v organizaci, zejména normalizačních aktivitách, aktuálních úkolech a perspektivách vývoje aktivit této organizace a jejích jednotlivých skupin. V páté kapitole se pojednává o problémech a řešeních v oblasti multimédií, s nimiž se setkává organizace IETF v průběhu své existence a v důsledku své činnosti, a z toho vyplývají návrhy a doporučení pro zlepšení nebo zefektivnění činnosti této organizace v oblasti multimédia.

Cílem práce je přehledně, strukturovaně a vyváženě zmapovat normalizační aktivity v oblasti internetu vykonávané organizací Internet Engineering Task Force (IETF), zejména její aktivity v oblasti multimédií.

Klíčová slova:

IETF, Komise techniky Internetu, normalizační aktivity, multimédia, World Wide Web, standardy, protokoly.

Summary

Bachelor’s thesis is dedicated to the topic of normalisation activities of Internet Engineering Task Force (IETF), which is one of the main organisations in the field

of internet activities and World Wide Web maintenance.

Bachelor's thesis contains Introduction chapter, five body chapters and Conclusion chapter. The first body chapter contains theoretical background, definition of the terms Internet, multimedia, WWW. The second chapter examines organisations and standards related to the Internet infrastructure and environment. The third body chapter consists of the description of the previous performance of IETF organisation, its history, structure and delegation of competencies and power between its working groups. In the fourth chapter of the bachelor's thesis we mention the main processes taking place in the organisation, normalisation activities and perspectives of further development of IETF. The fifth chapter describes the problems and solutions proposed by this organisation for the sphere of multimedia during its performance and existence. Bachelor's thesis also contains proposals and suggestions for improvements of IETF's performance in terms of multimedia sphere.

The main objective of the thesis is to map activities of the IETF (especially in the sphere of multimedia) in a structuralised and clear way.

Keywords:

IETF, Internet Engineering Force Task, normalisation activities, World Wide Web, standards, protocols.

Obsah

Úvod

Bakalářská práce se věnuje tématu normalizačních aktivit Komise techniky Internetu (originální název: Internet Engineering Task Force - dále jen IETF), která je jednou z nejstarších organizací v oblasti regulace a vývoje internetových aktivit a správy světové sítě Internet. Tato organizace vyvíjí svou hlavní činnost – vydává standardy a normy (internetové protokoly) již od roku 1986, a prostřednictvím svých orgánů se snaží maximálně efektivně zlepšovat, zdokonalovat, zefektivňovat a monitorovat interaktivní procesy.

Organizační struktura IETF je velmi zajímavá, protože funguje prostřednictvím svých pracovních skupin, které se zaměřují na různé oblasti: bezpečnost, aplikace, správu a management, transport apod. Právní subjektivitu má prostřednictvím svých zastoupení, zejména organizací Internet Society (ISOC). Pro účely práce bude vybrána a analyzována oblast multimédií, v níž daná organizace provádí velmi aktivní politiku a v níž jsou určitá zlepšení díky integraci a aktivitám IETF.

V průběhu posledních dvaceti pěti let fungování a existence dané organizace oblast internetu prošla obrovskými změnami. Technologický vývoj a pokrok je nezastavitelný a přizpůsobivost lidí je neomezená. Proto se internet stal nejenom velmi užitečným, ale též značně nebezpečným prostředím, ve kterém je nutné kontrolovat veškeré aktivity a procesy. Internet svědčí nejenom pozitivním cílům a misím, ale také podporuje nelegální a nebezpečné aktivity zlodějů (interaktivní a reálné). Internet je otevřenou komunikační sítí, což je hlavní odlišností internetu od jiných komunikačních sítí, které byly především uzavřeného charakteru (v rámci některých sociálních skupin). V důsledku přílišné otevřenosti se začala vyvíjet politika „blokování“ některého obsahu, cíleného zastavení nepovoleného nebo nebezpečného sdílení. Co je „přípustné“, jaký obsah je nutno blokovat prostřednictvím automatických protokolů, to je vymezeno právě v průběhu činnosti jednotlivých pracovních skupin IETF.

V rámci svých aktivit IETF se přizpůsobuje aktuálním problémům moderní společnosti a reaguje na vzniklé problémy. Jednou z normalizačních aktivit IETF je

reakce na zjištěné monitorování soukromí jednotlivců prostřednictvím internetového připojení ze strany vládních organizací, které začalo být běžnou praxí ve Velké Británii a USA. IETF nabídla svou asistenci a pomoc při vypracování speciálního kryptomechanismu, který dovolí šifrovat veškerá data posílaná mezi jednotlivými servery a znemožnit tak přístup osobních informací o uživateli. To svědčí o tom, že IETF reaguje pohotově na vzniklé problémy spojené se sítí internet a snaží se přispět k jeho bezpečnému využívání. Významným přínosem je blokace obsahu v kanálech multimédií a kontrola integrace všech multimediálních zařízení.

Bakalářská práce má úvod, pět kapitol a závěr. V první kapitole se věnujeme vymezení teoretických předpokladů nutných pro následující výzkum. Ve druhé kapitole je diskutováno o tom, jaké organizace existují a vydávají standardy v oblasti Internetu. Ve třetí kapitole se pojednává o vzniku a dosavadní činnosti organizace IETF, zejména její historii, vzniku, organizační struktuře a delegování pravomocí v rámci organizace a mezi jejími pracovními skupinami. Významným je i pojednání o celkových výsledcích práce a aktivit organizace IETF. Ve čtvrté kapitole se pojednává o hlavních procesech probíhajících v organizaci, zejména normalizačních aktivitách, aktuálních úkolech a perspektivách vývoje aktivit této organizace a jejích jednotlivých skupin. V páté kapitole se pojednává o problémech a řešeních v oblasti multimédií, s nimiž se setkává organizace IETF v průběhu své existence a v důsledku své činnosti, a z toho vyplývají návrhy a doporučení pro zlepšení nebo zefektivnění činnosti této organizace v oblasti multimédia.

Cílem práce je přehledně, strukturovaně a vyváženě zmapovat normalizační aktivity v oblasti internetu vykonávané organizací Internet Engineering Task Force (IETF), zejména její aktivity v oblasti multimédií. Práce je spíše analytického a teoretického charakteru, protože zkoumá především probíhající procesy v IETF a možnosti jejich budoucího vývoje. Nicméně v rámci bakalářské práce se zaměříme na některé metody teoretického výzkumu: retrospektivní analýzu vývoje činnosti organizace, analýzu současného vývoje a důsledky jednotlivých aktivit organizace, analýzu budoucího vývoje všech pracovních skupin.

1 Vymezení teoretických pojmů a východisek

V první části se budeme věnovat pojmu a podstatě internetu a následně se zaměříme na World Wide Web a multimédia.

Internet - je považován za celosvětový systém, v jehož rámci jsou vzájemně propojeny počítačové sítě, které spolu komunikují za přispění protokolů TCP/IP, jež jsou trvale propojeny datovými spoji s velkou průchodností. Internet je tedy propojen lokální sítí (LAN), jež právě pracuje, v rámci celého světa na základě protokolu TCP/IP. Jednoduše řečeno, cílem každého uživatele je, aby se jednalo o bezproblémovou komunikaci, a tedy i o výměnu potřebných dat. Internet jako takový je využíván již řadu let, i když do České republiky se dostal až po roce 1989, respektive až v závěru 90. let, kdy se začal pomalu rozšiřovat do domácností. Dnes se řadí do běžných informačních doplňků, které jsou součástí jednak počítačů, ale také i mobilních telefonů a dalších zařízení.

Internet je možné definovat jako globální informační systém, který:[1]

- Je logicky propojen do jednoho celku prostřednictvím globálního adresného prostoru založeného na protokolu IP (Internet Protocol) nebo jeho následných rozšířeních či nástupcích;
- Je schopen podporovat komunikaci prostřednictvím rodiny protokolů TCP (Transmission Control Protocol) nebo jeho následných rozšířeních či nástupcích nebo jiných protokolů kompatibilních s protokolem IP;
- Nabízí veřejné nebo privátně dostupné služby vyšší úrovně, které jsou založeny na komunikační a další infrastruktuře.

Vývoj internetu jde neustále vpřed v souladu s časem a také s požadavky, které jsou na něj kladeny. Ať již se jedná o kvalitu a množství poskytovaných informací, ale současně i zvyšující se poptávku služeb, jež jsou přes internet poskytované. Stejně tak se klade i vysoký důraz na to, že internet musí být dnes

[1] SKLENÁK, V. *Data, informace, znalosti a Internet*. 1. vyd. Praha: C.H. Beck, 2001. s. 38.

dosažitelný z nejrůznějších technických prostředků, jakými jsou třeba notebooky, přístroje PDA, mobilní telefony atd.

Díky internetu vzniká velká spousta nejrůznějších aplikací, které dávají možnost jejich uživatelům sledovat nejrůznější pořady, využívat nepřeberné množství aplikací, posílat e-mailovou poštu, stejně jako komunikovat přes internet díky aplikaci Skype, MSN, ICQ a mnohým dalším. Lze tedy uvést, že podstatou internetu je právě přenos informací a propojení celého světa díky velkému množství počítačových sítí po celém světě. Z tohoto důvodu je také kladen velký důraz na zkvalitnění přenosu dat a tím i na vyšší rychlost internetu, což je zase dobrá investice pro poskytovatele těchto služeb, protože mohou svým klientům nabízet nejrůznější balíčky v různých cenových relacích jenom proto, aby zákazník měl co nejrychlejší internet, který potřebuje. Většina firem po celém světě si dnes neumí představit, že by fungovala bez přispění internetu; na druhou stranu si musíme přiznat, že v případě, kdy dojde ke zhroucení celé internetové sítě, bude to mít nedozírné následky pro obchodování po celém světě, stejně jako na přenos informací, protože mnoho podniků je závislých na internetových službách a některé firmy si dokonce založily i živnost přes internet.

Podstatou internetu tedy je soustředit co nejvíce informací, které jsou následně poskytovány dalším uživatelům, stejně tak i přenos těchto dat a propojení počítačů po celém světě.

Internet pro některé lidi může znamenat i některá rizika. V dnešní době se již můžeme setkat s novým nežádoucím jevem mezi lidmi, a tím je závislost na internetu, která je již prokázána i v České republice.

Internet poskytuje lidem mnoho služeb, jak již bylo uvedeno; nejdůležitějšími jsou jednak e-mailové služby, ale tím nejzásadnějším je přístup k informačním zdrojům v informačním prostoru za přispění služby World Wide Web, které se budeme věnovat v další části.

Internet funguje na možnosti přenášení souborů a způsobu jejich uveřejňování, případně poskytování jednotlivým uživatelům prostřednictvím jednotlivých služeb. Výměna informací neprobíhá pouze mezi dvěma počítači, ale současně mezi několika vytyčenými počítači, jež jsou na trase mezi koncovými počítači. Většina

těchto služeb poskytovaných internetem se vyznačuje pasivním charakterem, což v praxi znamená, že zařízení mající zajišťovat jistou službu čekají na konkrétní uživatelské požadavky a na základě těchto požadavků teprve potom zašlou vybranému uživateli požadované soubory s informacemi.

World Wide Web – to je služba, která zpřístupňuje v prostředí internetu hypertextové dokumenty a je založena na architektuře klient – server.[2]

Webový prohlížeč je počítačovým programem, díky kterému lze prohlížet World Wide Web. Za přispění WWW se pohyb v uživatelském rozhraní zjednodušil; to se netýká pouze práce s hypertextovými dokumenty jako takovými, ale i mnohými dalšími službami. Tento prohlížeč dával možnost současně přistupovat i k serverům za přispění dalších protokolů, kterými jsou FTP a Gopher. Myšlenka vzniku služeb navigačního typu byla hlavně v tom, že mnohdy se na konci nacházeli uživatelé, kteří se označovali za koncové, ale sami jsou bez patřičných technických znalostí. Stejně tak jim chybějí znalosti v oblasti příkazových jazyků. Jedná se o uživatele, kteří vědí, jaká oblast je pro ně zajímavá, ovšem již nevědí, jak se k této oblasti propracovat.

Jak tento celý proces funguje? Zhruba tak, že program umožní komunikaci s http serverem, kdy dojde ke zpracování přijatého kódu (HTML, XHTML, XML apod.), který podle daných standardů zformátuje a zobrazí webovou stránku. World Wide Web se považuje za velice mladou službu z pohledu vývoje internetu. Klíčovou vlastností hypertextu je schopnost provazování obsahových komponent pomocí odkazů, a to i křížových.[3]

V dnešní době je ovšem na moderní weby kladen větší nárok, než jenom požadavek hypertextu; musejí umět formátovat - jedná se o způsoby formátování písma, vkládání tabulek atd., dále by měly mít schopnost propojovat texty s jinými druhy obsahu, což se zase týká počítačových souborů. Nakonec se nesmí zapomenout ani na schopnost přenosu a výkonu kódu počítačových programů. To se vztahuje jak na poskytovatele, tak i na uživatele.

World Wide Web je součástí služeb internetu, ovšem nesmíme si jako

[2] SKLENÁK, V. *Data, informace, znalosti a Internet*. 1. vyd. Praha: C.H. Beck, 2001. s. 39.
[3] SKLENÁK, V. *Data, informace, znalosti a Internet*. 1. vyd. Praha: C.H. Beck, 2001. s. 39.

uživatelé klamně myslet, že se jedná o samotný internet. Na samém začátku vznikla služba WWW jako prostředek určený ke sdílení informací textového charakteru, který využíval hypertextový princip. To však není všechno. Na úspěchu firmy se podílela řada faktorů. Jedním z nejvýznamnějších bylo to, že WWW dávají možnost vkládání obrázků, nepřeberného množství písma a jeho velikosti včetně grafického ztvárnění. Je zde možnost tvořit tabulky, vkládat animace, zvuky a další věci. Internet je vyhledáván nejen odbornou, ale i laickou veřejností, a proto se klade důraz na co největší jednoduchost pro koncové uživatele. Proto ho dnes využívá celá řada lidí, a to bez toho, aniž by měli větší znalosti v oblasti užívání internetu nebo počítačů vůbec.

K velké oblibě WWW přispěla interaktivita služeb, která dává možnost nacházet spousty informací, využívat velké množství služeb. Web také využívá prohlížečů, jakými jsou například Internet Explorer případně Firefox, díky kterým je zajištěn přístup k dokumentům zvaným webové stránky.

Multimédia – jedná se o poslední část, jíž se budeme věnovat v teoretické části. Co vlastně multimédia jsou? Jedná se o spojení textu, obrázků, grafiky, zvuku, animace a videa za účelem zprostředkování specifického druhu informací. Zaměříme-li se na to, co se dá označit pojmem multimédia, zjistíme, že se takto označují spojení audiovizuálních technických prostředků s počítači, případně toto spojení může proběhnout i s jinými zařízeními. Do kategorie interaktivního multimédia se řadí digitální dokumenty, případně produkty v počítačových sítích či na fyzickém nosiči. Může se tedy jednat o webové stránky, disky CD – ROM, případně i videodisky, vyznačující se dvěma vlastnostmi:

- jednak se vyznačují tím, že využívají kombinaci většího množství datových informací, jako např. text, animace, zvuk, obraz, grafika atd.;
- dále pak mají podporu interaktivní komunikace s vlastními uživateli. To znamená, že ve velké většině případů se jedná o výukové programy, podnikové materiály, herní konzole a jiné.

Multimédia nacházejí své uplatnění všude tam, kde uživatel vyžaduje mít přístup k informacím v elektronické podobě. Tvůrci se snaží se udělat výukové

programy zajímavé, aby udrželi pozornost uživatelů, a dále mohou být i tato média i zábavná.

V komerční sféře jsou multimédia využívána hlavně jako prezentace, případně reklamy, kdy je možné je doplnit o videoprojekci a vlastní hudbu. Multimédia, která se nacházejí v domácnostech, jsou například audio- a videopřehrávače, herní systémy. Nesmíme ovšem opomenout ani plě funkční multimediální počítače.

Dnes se ve velké míře multimédia využívají v učební sféře, zejména díky jejich oboustranné komunikaci, kterou umožňují. Tím dostává uživatel možnost aktivně zasahovat do průběhu celého programu. Podařilo se prokázat, že právě díky tomu, že dochází k aktivní účasti na programu, má to i pozitivní dopad na dosahované výsledky. Tím, že se prostřednictvím multimédia působí souběžně na více smyslových receptorů v jednom okamžiku, dosahuje výuka lepších výsledků, což znamená, že učivo je trvaleji a hlouběji osvojováno uživatelem.[4]

Multimédia se tedy dělí do několika kategorií, které si nyní stručně popíšeme. Jednak jsou to multimediální služby, které zahrnují přenos většího typu informací (data, text, video, audio, obrázek atd.). Sem se řadí hlavně konverzační, vyhledávací, distributivní a další služby. Ty se řadí k velmi rozšířeným zejména díky zvukovým videosouborům formátu MP3, MPGE, WMP, které jsou dnes hodně rozšířené mezi mladými lidmi, ale nejenom mezi nimi. Dále sem patří multimediální technologie, které představují souhrn postupů a prostředků vedoucích ke zpracování, archivování a přenosu informací multimediálního charakteru. Můžeme je tedy rozlišovat na multimediální informační technoologie nebo přenosové technologie. Poslední kategorií jsou multimediální soubory, jež obsahují, případně nesou zvukové, obrazové, nebo i videoinformace.

Multimediální soubory pomáhají tvořit obsah celého internetu a můžeme tedy říci, že jsou součástí většiny informačních technlogií[2]. Tyto multimediální soubory se většinou ukládají samostatně v pro nás velmi známých formátech, jako jsou MPEG,

[4] DOSTÁL, J. *Multimediální, hypertextové a hypermediální učební pomůcky - trend soudobého vzdělávání.* Časopis pro technickou a informační výchovu. Olomouc: Univerzita Palackého, 2009. Ročník 1, Číslo 2. s. 18 - 23.

JPEG, AVI, tedy v jiných souborech, než je tomu u souborů s textovou informací. Na webové stránky se ukládají jenom odkazy k těmto externím informacím.

Podíváme-li se tedy na všeobecnou podstatu multimédií, zjišťujeme, že se vše krásně prolíná jednak s internetem, ale také s World Wide Webem, ale i velkou částí zasahuje všem do života, protože mnoho zařízení, případně programů pracujících na multimediální bázi využívají lidé dnes a denně, ať již v zaměstnání nebo domácnosti. Podstatou multimédií je i určité ulehčení práce s internetem, různými soubory v počítači, ale také i s učebními materiály, které, jak již bylo uvedeno výše, jsou ve velké míře dnes převáděny do multimediální podoby právě pro svou flexibilnost, kterou posléze nabízejí.

2 Normalizační aktivity v oblasti Internetu

Standardizační a normalizační aktivity jsou prováděny mnoha organizacemi, a to jak ziskovými, neziskovými, tak státními. Pro určení působnosti různých organizací činných v oblasti Internetu je nutno především rozlišit typy standardů, které jsou přijímaná v této oblasti:

- standardy vydávané jednotlivými společnostmi (například, protokoly řady DECnet od Digital Equipment nebo grafický interface OPEN LOOK pro Unix vydaný společností SUN)
- standardy vydávané speciálními komisemi a výbory (například technologie ATM vydávané společností ATM Forum)
- standardy vydávané národními organizacemi pro standardizaci (například FDDI vydaný americkou asociací ANSI nebo standardy bezpečnosti pro operační systémy vydané Národním centrem ochrany počítačů (NCSC) Ministerstva obrany Spojených států)
- mezinárodní standardy (například, model komunikačních protokolů ISO, standardy Mezinárodního svazu elektronických komunikací – ITU, protokoly vydávané organizací W3C apod.).

Některé standardy jsou neustále aktualizovávány, dokonce mohou postupovat z jedné oblastí do druhé. Firemní standardy vypracované pro produkci, která je veřejně užívána, se postupně stávají standardy mezinárodní úrovně, protože pobízejí ostatní výrobce k využití a integrace daných standardů do svých produktů. Tímto je zajištěná kompatibilita mezi jednotlivých zařízeními. Příkladem může být standard IBM, který byl postupně přijímán mnoha výrobci v oblasti komunikačních a internet technologií.

Dále uvedeme stručné představení organizací, které jsou nejvíc aktivní a činné v oblasti normalizačních a standardizačních aktivit v oblasti Internetu.

1) Mezinárodní organizace pro standardizaci (International Organization for Standardization - ISO). Tato organizace vypracovala model vzájemného působení

některých systémů OSI, které jsou koncipovány jako základní v oblasti standardizace.

2) Mezinárodní svaz telekomunikací *(International Telecommunication Union, ITU)* je organizací, která je speciálním orgánem Organizace spojených národů (OSN). Hlavní roli v tomto procesu hraje orgán stálého působení – Konzultační výbor pro mezinárodní telefonii a telegraf (*Consultative Commitete for International Telephony and Telegraphy, CCITT*). V současné době tato organizace má aktualizovaný název – ITU-T. Zkrátka T ukazuje na technickou specializaci činnosti této organizace.

3) Institut inženýrů elektrotechniky a radioelektronických komunikací (*Institute of Electrical and Electronic Engineers, IEEE).* Je to národní organizace ve Spojených státech, která určuje standardy pro zmíněné oblasti. V roce 1981 pracovní skupiny této organizace formulovala základní požadavky, které musí splňovat lokální výpočetní sítě, včetně sítě Internet.

4) Evropská organizace výrobců počítačů (ECMA) – nekomerční organizace, která aktivně spolupracuje s ITU-T a ISO. Vypracovává standardy a technické výhledy pro počítačovou a komunikační technologie.

5) Asociace elektronického průmyslu (*Electronic Industries Association, EIA)* je národní komerční organizací ve Spojených státech, která je velmi aktivní a činná při vypracování standardů pro oblasti IT technologií a elektronickou oblast. Hlavním vypracovaných standardem je RS-232, který je široce užíván v oblasti Internetu.

6) Ministerstvo obrany Spojených států (Department of Defense - DoD) má mnoho pracovních skupin, které se zabývají vypracováním standardů pro počítačové systémy a pro fungování v síti Internet. Jedním z hlavních výsledků práce pracovních skupin Ministerstva jsou standardy řady TCP/IP.

7) Nesmíme zapomenout na „příbuznou“ organizaci – W3C neboli World Wide Web Koncorcium Internetu. Spravuje mnoho oblastí telekomunikací, multimédií, Internetového prostředí. Činnost této organizace je velmi podobná činností IETF, jsou i vzájemné průniky v práci obou společností. Struktura a principy práce obou organizací se liší, a proto je velmi složité porovnat výsledky činnosti nebo rozsah činnosti obou organizací.

3 Vymezení oblasti působení organizace IETF

IETF (The Internet Engineering Task Force) je institucí, která se zabývá vývojem protokolů a architektury internetu. IETF (v českém znění Komise techniky internetu) je otevřené mezinárodní sdružení vývojářů síťových protokolů, provozovatelů, výrobců a výzkumníků pracujících na řešení úkolů, týkajících se vývoje architektury internetu a hladkého a správného fungování jeho současné infrastruktury. Struktura IETF je tvořena pracovními skupinami, z nichž každá je zodpovědná za různé aspekty architektury internetu: tak například jde o pracovní skupinu v bezpečnostní oblasti. V rámci organizace IETF se každoročně provádějí tři fóra, tedy zasedání, na kterých se koordinuje práce různých skupin a stanoví se nové aktuální cíle.

Přestože všichni členové Komise techniky internetu pracují jako dobrovolníci, samotná organizace, jejíž přínos pro rozvoj internetu se časem stal obrovský, je sponzorována americkými společnostmi a také agenturou USA pro národní bezpečnost, fungující v rámci pravomocí americké vlády.

3.1 Historie organizace IETF

Historie organizace Internet Engineering Task Force je úzce spjatá s rozvojem samotného fenoménu internetu a její vznik se datuje polovinou osmdesátých let. Počátek organizace byl spojen se zahájením pravidelných čtvrtletních setkání, kterých se zúčastňovali především výzkumní pracovníci a která byla financována vládou USA ve snaze kontrolovat rozvoj nové technologie - internetu - s již tehdy uznávaným obrovským potenciálem. První z těchto setkání se konalo v lednu roku 1986 a přilákalo 21 členů z akademických pracovišť.[5] V říjnu téhož roku se setkání Komise techniky internetu zúčastnili i jiní experti - zástupci nevládních organizací. Dodnes používaná koncepce pracovní skupiny v rámci dané organizace byla prezentována na 5. zasedání IETF v únoru 1987. A o šest měsíců později počet účastníků zasedání IETF přesáhl už 100 lidí.

[5] IETF. *IETF Meeting Proceedings.* [olnline]. [cit. 2014-02-10]. URL: <http://www.ietf.org/meeting/proceedings.html>.

Původně americká organizace Internet Engineering Task Force se s časem začala rozšiřovat i mimo americké území, stejně jako se šířil internet samotný a s ním spojené otázky a problémy. První setkání IETF mimo území Spojených států se konalo v Amsterdamu v roce 1993. Podíl účastníků ze zemí mimo USA v tomto roce poprvé dosáhl 50%. Co se týče geografické lokace zasedání IETF v dnešní době, nyní se asi polovina ze všech setkání Komise techniky internetu koná v Evropě nebo Asii a druhá polovina v Severní Americe. Nicméně dokonce i na zasedáních, která se odehrávají ve Spojených státech, mimoameričtí účastníci často tvoří většinu přítomných účastníků. Dá se z toho usoudit, že původně americká organizace IETF dnes efektivně působí i v evropském a asijském prostředí.

3.2 Role a oblasti působení organizace IETF

Internet Engineering Task Force jen obtížně lze nazvat běžnou organizací: nemá sídlo ani významný počet stálých zaměstnanců. Naopak téměř všechna práce se v IETF provádí dobrovolně. Avšak všechny tyto skutečnosti neznamenají, že IETF nemá žádnou vymezenou organizační strukturu. Naopak tato struktura je velice promyšlená a efektivně slouží především realizaci podpory hlavní funkce IETF - vypracování a zveřejnění norem a standardů v oblasti internetu.

V obecné rovině standardy jsou zapotřebí pro zajištění kompatibility a interoperability mezi prvky jakéhokoli systému - počítačové sítě, distribuované aplikace nebo samotného počítače. Jinými slovy to znamená, že tyto prvky mohou být vytvořeny různými výrobci a být nekompatibilní navzájem. IETF v daném případě se snaží o odstranění takových bariér metodou zavedení standardů.

V kontextu sociálních a ekonomických norem standardy (včetně standardů v oblasti internetu) mají za úkol podporovat volný pohyb zboží a služeb. Pomocí snížení technických překážek pro vytváření, zavádění a používání internetových služeb standardy mají pomoci otevřít nové příležitosti pro hospodářský rozvoj, podporovat hospodářskou soutěž a rozlišování mezi různými produkty a zároveň mají přispět k zajištění interoperability, tedy kombinováni různých produktů. Dá se říci, že

normy jsou nezbytnou součástí samoregulace internetového prostředí.

Poslední poznámka může být plně platná pouze pro otevřené dobrovolné standardy a normy přijaté na základě konsensu. Pokud se hovoří konkrétněji o "Internet standardu", ve většině případů se odkazuje na technické specifikace protokolu, softwarové rozhraní, databáze schémat a podobné záležitosti. Standard je v daném pojetí druh "stavebního kamene", který je určen v kombinaci s dalšími prvky k vytvoření systému nebo řešení určitého problému. Pro naplnění daného cíle spolu se standardy existují také informační podklady, obsahující doporučení pro uplatnění dané normy nebo technologie pro specifické úkoly. Normalizační aktivity organizace IETF zahrnují rozvoj obou typů specifikací.

Veškeré aktivity IETF jsou zaměřeny především na identifikace aktuálních provozních a technických problémů v oblasti internetu a návrh řešení pro tyto problémy.[6] Co se týče konkrétních operací, komise techniky internetu se zabývá určením směru vývoje nebo využívání protokolů a krátkodobých elementů architektury internetu, což by takové technické problémy na internetu umožnilo řešit. Kromě toho IETF spolupracuje s dalšími organizacemi, například s Internet Research Task Force (IRTF) v oblasti usnadnění transferu technologií z této komise do širší internetové komunity nebo s Internet Engineering Steering Group (IESG) co se týče tvorby doporučení pro standardizaci protokolů a jejich použití na internetu. Každopádně hlavní funkcí komise techniky internetu zůstává poskytování prostoru pro výměnu informací v rámci internetové komunity mezi dodavateli, uživateli, výzkumnými pracovníky, představiteli agentur a správci sítí.

Různé funkce Internet Engineering Task Force jsou plněny různými organizačními jednotkami. Pracovní skupiny, fungující v rámci IETF, jsou spojeny v tzv. tematické oblasti, z nichž každá je zpravidla vedena dvěma vedoucími.[7] První z těchto tematických oblastí je oblast aplikací (Application Area, APP).

Hlavním zaměřením činnosti IETF v této oblasti je sféra aplikaci a protokolů aplikační úrovně. Tato oblast zahrnuje 12 pracovních skupin, jejichž předmětem

[6] IETF. *Mission Statement*. [olnline]. [cit. 2014-02-10]. URL: <http://www.ietf.org/about/mission.html>.
[7] IETF. *Concluded WGs*. [olnline]. [cit. 2014-02-10]. URL: <http://www.ietf.org/wg/concluded/>.

práce jsou takové aplikace, jako e-mail, kalendáře, web, adresáře a registry, peer sítě a aplikace, stejně jako otázky internacionalizace. Další oblastí působení organizace IETF jsou transportní protokoly (Transport Area, TSV). Pracovní skupiny v této oblasti se zabývají transportními protokoly jako TCP, UDP, SCTP, DCCP. K této oblasti také patří pracovní skupina „behave“, která se věnuje problémům interakce aplikací za přítomnosti vysílacích zařízení (NAT) s důrazem na rozvoj výkonnostních norem pro tato zařízení. V této oblasti existují také skupiny zabývající se problematikou ukládání dat (NFSv4, storm).

Bezpečnost (Security Area, SEC) je také jednou z klíčových sfér činnosti Internet Engineering Task Force. V této oblasti se organizace dotýká problematiky bezpečnosti a ochrany dat. Jde o vývoj a kontrolu bezpečnostních protokolů a aplikací pro zajištění kontroly integrity, autentičnosti, diskrétnosti dat a kontroly přístupu k nim. V rámci existujících pracovních skupin v této oblasti se diskutuje o otázkách, týkajících se protokolů IPsec, TLS, SASL, S/MIME, Kerberos.

Na routování (Routing Area, RTG) je v IETF nahlíženo z hlediska směrovacích protokolů (OSPF, IS-IS, BGP) a zabezpečení směrování (sidr). Pracovní skupina zabývající se správou provozu (Operations and Management, OPS), jak už napovídá název samotný, věnuje svoji činnost kontrole provozu a také správě sítí a systémů. Daná pracovní skupina se zaměřuje na hledání řešení pro problémy spojené s takovými systémy internetu jako DNS (dnsop), dále sítí, které podporují IPv6 (v6ops) a směrovací systém (grow). V rámci dané sféry se také odehrávají rozvojové činnosti věnované kontrolním protokolům - SNMP, netconf, capwap.

Aplikace a infrastruktura reálného času (Real-Time aplikace a infrastruktura, RAI) je dalším tématem, o jehož řešení se pokouší v rámci své činnosti organizace IETF. Zájmy pracovníků této pracovní skupiny jsou spojeny s takovými real-time aplikacemi, jako jsou hlasové služby a videokomunikace v sítích založených na protokolu IP, SIP a IP telefonie a také systémy instant messaging, umožňující odesílání a přejímání rychlých zpráv.

Spojení pracovních skupin s nejširším spektrem zájmů v rámci Komise techniky internetu se jednoduše jmenuje Internet (Internet, INT). Pracovní skupiny v

této oblasti pokrývají širokou škálu otázek týkajících se základní architektury a protokolů internetu, počínaje protokoly IPv4 a IPv6 a konče otázkami mobility, dynamické konfigurace, virtuálních sítí a DNS.

3.3 Organizační struktura a pracovní skupiny (IANA, IESG, IETF Trust...)

Jak již bylo zmíněno, hlavní práce IETF se provádí v rámci pracovních skupin. V podstatě pracovní skupina představuje mailing list, pro jehož odebírání se lze přihlásit, a tak se podílet na práci v dané oblasti. Každá pracovní skupina má listinu, která definuje předmět pracovní náplně skupiny a cíle, jichž chce skupina dosáhnout v rámci své činnosti, a také pracovní plán. Úkol koordinace všech členů a aktivit v rámci skupiny je plněn jedním nebo dvěma vedoucími.

Příkladem pracovní skupiny je Internationalized Domain Names IETF working group (IETF IDN).[8] Je to pracovní skupina IETF, jejímž cílem je vytvoření podmínek pro realizaci přístupu k doménovým jménům pomocí použití nejen latinských písmen, ale i znaků jiných národních abeced. Zmezinárodněná doménová jména (IDN) jsou doménová jména druhého nebo třetího stupně a také webové adresy prezentované pomocí znaků místních jazyků. Na konci názvu domény, zastoupené pomocí symbolů místního jazyka, je uvedena doména nejvyšší úrovně (TLD) s použitím latinských písmen, například „.com“ nebo „.net“. Pomocí IDN uživatelé mohou používat známý systém písma při prohlížení internetu a jedinečné značky obchodních společností mohou být uvedeny v různých způsobech jazykových kódování. Jedním z úkolů skupiny je zkoumání možných řešení a jejich dopadu na současný systém doménových jmen, stejně jako podání návrhů, které berou v úvahu jak technické, tak i sociální aspekty používání těchto doménových jmen.

I když převážná část prací se odehrává v diskuzích dokumentů mezi členy pracovní skupiny, kteří jsou na e-mailových seznamech, odebírají novinky a komunikují přes tyto seznamy, většina z pracovních skupin také volí i občasná fyzická

[8] Data tracker. *Internationalized Domain Name (idn) (concluded W*G). [olnline]. [cit. 2014-02-10]. URL: <http://datatracker.ietf.org/wg/idn/charter/>.

setkání a schází se v rámci zasedání IETF. Ve skutečnosti setkání Internet engineering Task Force není společným zasedáním všech členů dané organizace, ale skládá se ze schůzí dílčích pracovních skupin organizace IETF. Tato setkání hrají velmi důležitou roli: kromě toho, že umožňují účastníkům vidět spolupracovníky, s nimiž se po některou dobu pomocí internetových komunikací vedly diskuze (což je velmi užitečné v případě práce ve virtuálním světě), setkání poskytují možnost účinné společné reflexe klíčových momentů, strategii další práce konkrétní pracovní skupiny a organizace, stejně jako i umožňují shrnout dosavadní výsledky práce.

Tato fyzická setkání organizace IETF jsou velmi užitečná, pokud se jeden z členů pracovní skupiny chystá navrhnout nové téma, kterému by se skupina mohla věnovat, nebo nápad, týkající se řešení určitého problému. Úvodní prezentace ze strany člena, který s nápadem přišel, a pak krátká společná diskuze je obvyklým postupem navrhování nových myšlenek v Komisi techniky internetu, která umožňuje předběžně vyhodnotit význam daného návrhu pro pracovní skupinu, poukázat na jeho silné a slabé stránky, a to i předtím, než začne časově náročná práce podrobné specifikace návrhu a detailního uvažování o něm.

Důležitým prvkem pro úspěch pracovní skupiny je bezesporu její předseda. Stejně jako v případě řádných členů pracovní skupiny činnost předsedy má dobrovolný charakter, ale přesto jeho pracovní náplň jen těžko lze označit za jednoduchou. Předsedovým úkolem je definování pracovního plánu a účinné prosazování aktivit skupiny v souladu s ním. Manažerská činnost předsedy pracovní skupiny IETF zahrnuje také dosažení konsensu na klíčových místech a také koordinaci plodné diskuse jak v prostoru internetu v rámci běžné komunikace pracovní skupiny pomocí e-mailových seznamů, tak i na zasedáních. Tak například se stává, že se skupina začne „brzdit“ na nějaké otázce. V tomto případě úkolem předsedy je posunout diskuzi od mrtvého bodu ke konsensu a následně ukončit diskuzi dosažením uspokojujícího výsledku. Předseda dílčí pracovní skupiny je zodpovědný za interakci s ostatními účastníky a orgány IETF, například s již zmíněným IESG. Jak si lze lehce představit, práce předsedy vyžaduje nejen vysoké technické kompetence v oboru, ale také organizační schopnosti, psychickou odolnost, diplomacii a takt.

Jak již bylo uvedeno, rozhodování v rámci pracovní skupiny probíhá na základě principu konsensu, v souladu se dvěma základními zásadami fungování IETF: hrubý konsensus a běžící programový kód (rough consensus and running code).[9] Zde je vhodné hovořit o postupu pro stanovení konsensu, který se používá při formálních jednáních pracovních skupin v Komisi techniky internetu. Na rozdíl od klasického hlasování předseda obvykle žádá členy pracovní skupiny, aby projevili vlastní názor vůči konkrétní problematice (například přijetí návrhu jako budoucího dokumentu pracovní skupiny) pomocí krátkého tónu píšťalky. Kupříkladu předseda nejprve požádá, aby se ozvali účastníci, kteří jsou „pro“ daný návrh, a pak ti, kdož jsou „proti“. Následně na základě rozdílu v celkové síle a intenzitě zvuku předseda určuje názor skupiny jako celku k otázce.

Dalším zajímavým rysem organizační struktury organizace Internet engineering task force jsou názvy pracovních skupin. Mnohé z nich jsou běžnými slovy v angličtině, avšak ve skutečnosti všechny z nich jsou také zkratkami jiných slov. Například pracovní skupina behave (anglicky „chovat se“) je zkratkou Behavior Engineering for Hindrance Avoidance („behaviorální inženýrství pro vyhýbání se překážkám“) a hokey („hokej“) znamená Handover Keying („předávání klíčování“). Chytlavý a zároveň smysluplný název pracovní skupiny vyžaduje určitou vynalézavost, a tak se stává předmětem jednání na zasedáních zvláštního druhu - BOF .

Co se týče vzniku nových pracovních skupin, nezbytnými podmínkami jsou existence listiny a předsedy, ale také dostatečný počet zájemců o konkrétní téma, kteří by se následně stali členy dané pracovní skupiny. Kromě toho pro založení nové pracovní skupiny je třeba také přesvědčit vedoucího tématické domény (tedy spojení pracovních skupin s blízkým předmětem zájmů) o důležitosti dílčího tématu a jeho odlišnosti od pracovního záměru již existujících jednotek v rámci organizace IETF.

Pro účely diskutování o těchto otázkách a také vypracování pracovního plán slouží tzv. BOF zasedání. Název BOF je zkrácené Birds of Feather (ptáci se stejným peřím), které zase pochází od rčení “birds of feather flock together” (jehož český

[9] MATHIASON, J. *Internet Governance: The New Frontier of Global Institutions*. New York: Routledge, 2008. s. 35.

analog zní „vrána k vráně sedá“). Jinými slovy BOF je setkání lidí, kteří se zajímají o stejné téma.

Pokud se po krátké diskuzi ukáže, že téma opravdu stojí za další pozornost, účastníci BOF se dohodli na zakládací listině a konkrétním pracovním plánu a jsou připraveni i nadále spolupracovat na daném tématu, výsledkem zasedání BOF může být založení nové pracovní skupiny. Nicméně často se stává, že setkání BOF nemá žádný pozorovatelný výsledek, například pokud se strany nemohly dohodnout na cílech a oblastech činnosti v souvislosti s existujícím problémem.

Jak již víme, rozvoj standardů se odehrává v pracovních skupinách. Pracovní skupiny jsou spojeny do tematických oblastí a práce každé z nich je koordinována předsedou dané tematické oblasti. Avšak v organizační struktuře IETF existují i jiné elementy, které působí na odlišných úrovních než pracovní skupiny. V dalším textu se budu věnovat několika nejvýznamnějším jednotkám, fungujícím v rámci Internet Engineering Task Force. Jednou z nich je Internet Engineering Steering Group (IESG). Přestože v rámci Komise Techniky Internetu existuje velké množství pracovních skupin, odpovědnost za celkovou technickou správu činnosti IETF a procesů vytváření internetových standardů leží na zvláštním výboru, kterým je právě IESG.[10] Složení IESG je vytvořeno z předsedů dílčích oblastí, kteří jsou voleni Nominačním výborem na dobu dvou let.

Činnosti IESG jsou prováděny v souladu s pravidly a postupy, které byly ratifikovány správní radou Internet Society (ISOC). Nicméně charakter stylu vedení IESG není normativní. Jak už napovídá samotný název (steering), úkolem daného výboru je správně identifikovat oblasti práce, ale nikoli dávat konkrétní pokyny. IESG ratifikuje nebo koriguje výsledky aktivit pracovní skupiny, kontroluje proces vytváření a uzavírání pracovních skupin a obecně dohlíží na proces standardizace, probíhající na všech úrovních organizace IETF.

Výbor zkoumá každý návrh standardu před tím, než může být publikován jako RFC. Pochopitelně jde o těžkou práci, vyžadující od členů výboru mnohostranné

[10] JOHNSTON, A. *Sip: Understanding the Session Initiation Protocol*. Norwood: Artech House, 2009. s. 19.

znalosti předmětu a čas. Předpokládá se, že každý člen výboru, tedy ředitel tematické oblasti, lépe než kdokoliv jiný zná celkové složení všech pracovních skupin v rámci vlastní tematické oblasti. Ve stejné době musí také pečlivě sledovat dynamiku organizace IETF jako celku a brát v potaz i celkový směr rozvoje organizace.

Protože práce IETF je založena na konsenzu, jedním z úkolů IESG je dohlížet nejen na dosažení konsensu v pracovní skupině, ale zároveň i v Internet Engineering Task Force jako celku. Například výsledky pracovní skupiny mohou být v rozporu se standardy vytvořenými jinými skupinami. Zároveň se může i stát, že výsledky práce skupiny nejsou v souladu se základními principy kvality a IETF. V takových případech IESG přistoupí k akci a blokuje další ratifikaci konkrétního standardu.

Internet Architecture Board (Internet Architecture Board, IAB) je dalším klíčovým prvkem IETF. Zatímco IESG sleduje kvalitu práce IETF, a to jak z hlediska procesu a z hlediska souladu s normami a zásadami, IAB se věnuje sledování samotných principů a strategického řízení IETF jako celku.[11]

Seznam úkolů tohoto výboru zahrnuje definování a řešení základních dlouhodobých aspektů architektury fungování a rozvoje internetu. Tyto aktivity souvisejí s pořádáním diskusí o klíčových momentech, řešení problémů shody a architektonické celistvosti v procesu vytváření nových pracovních skupin, stejně jako otázky strategických vztahů s dalšími organizacemi, které se zabývají normami a standardy v prostředí internetu. Ve věcech architektonického vývoje internetu také hraje důležitou roli IRTF (Internet Research Task Force); v daném případě jde o výbor, který se zabývá výzkumem nových slibných internetových technologií. V této souvislosti je důležité poznamenat, že právě IAB jmenuje předsedu IRTF. IAB je také poradním orgánem ISOC, o němž bylo zmíněno dříve, ve vývoji technologií internetu. Kromě toho IAB také vykonává řadu důležitých administrativních funkcí jako schvalování kandidátů na pozice v IESG, včetně předsedy IETF, rozhodnutí o odvolání některé z akcí IESG, jmenování a kontrolu editora RFC. Funkcí IAB je také odpovědnost za realizace funkce registrace protokolů jednotkou IANA.

[11] JOHNSTON, A. *Sip: Understanding the Session Initiation Protocol*. Norwood: Artech House, 2009. s. 19.

Správa adresového prostoru internetu (IANA, Internet Assigned Numbers Authority) je jednotkou organizace IETF, která je zodpovědná za celkovou koordinaci a řízení systému doménových jmen (DNS), a zejména za proces delegování částí jmenného prostoru, tzv. domény nejvyšší úrovně.[12] Většina domén nejvyšší úrovně se shoduje s dvoupísmenným kódem země podle ISO 3166. IANA pak vybírá a určuje registrační servis, v jehož rámci by se měla provádět každodenní správa systému doménových jmen (DNS). Žádosti o nové domény nejvyšší úrovně (například pro země, které se teprve chystají připojit k internetu) jsou zpracovány registračním servisem ve spojení s IANA. V současné době centrálním registračním servisem je INTERNIC.NET.[13]

Tento dokument popisuje pravidla používaná při tvorbě nové domény nejvyšší úrovně, obvykle pomocí delegování řízení této domény nově jmenovanému koordinátorovi domény nejvyšší úrovně. Zabývá se také otázkami, vyplývajícími z potřeby změnit delegování existující domény z jedné strany na druhou. Většina aspektů definovaných v rámci tohoto dokumentu je důležitá také při delegování subdomény a obecné principy v něm popsané platí rekurzivně pro všechny případy delegace domén na internetu. Základní požadavky pro výběr koordinátora domény jsou jeho schopnost plnit nezbytné úkoly a také závazek spravedlivého a kompetentního plnění těchto povinností.

Poslední jednotkou, o které je třeba se zmínit, je výbor IETF Trust. Účelem tohoto elementu organizační struktury Komise Techniky Internetu je snaha o rozvoj znalostí a veřejného zájmu o získávání, udržování a licencování existujícího a potenciálního duševního vlastnictví a dalšího majetku, který je využíván v souvislosti s procesem vytvoření internetových standardů a jejich správy. Tyto aktivity IETF Trust mají za konečný cíl podpořit pokrok vědy a techniky spojený s internetem a souvisejícími technologiemi především pomocí ochrany intelektuálního vlastnictví v tak nebezpečném prostředí, jako je internet.

---

[12] JOHNSTON, A. *Sip: Understanding the Session Initiation Protocol*. Norwood: Artech House, 2009. s. 19.

[13] ICANN. *InterNIC — Public Information Regarding Internet Domain Name Registration Services*. [olnline]. [cit. 2014-02-10]. URL: <http://www.icann.org/en/resources/compliance/complaints/registrars>.

4 Procesy a procedury probíhající v organizaci

Jak již bylo uvedeno, Internet Engineering Task Force (IETF) je jednou z předních organizací, které zavádějí nové a podporují existující internetové standardy. To znamená, že konečným účelem dané organizace je zlepšení fungování internetu za pomocí vydávání vysoce kvalitních nezbytných technických dokumentů, které definují, jak se bude navrhovat, spravovat a používat internet a různé dílčí aspekty jeho fungování.

Co se týče konkrétních událostí, probíhajících v IETF, tato organizace třikrát ročně pořádá týdenní setkání svých členů (tzv. "kmenovou radu"), jejichž hlavním účelem je umožnit klíčovým pracovním skupinám efektivně ukončit plnění svých průběžných úkolů a získat možnost komunikace s ostatními pracovními skupinami se zájmy v různých disciplínách. Setkání IETF obvykle přilákají jen relativně nízký počet členů prodejních a marketingových oddělení, ale jsou velmi zajímavou možností pro inženýry a vývojáře internetových technologií.

IETF jedná jako velké otevřené mezinárodní společenství síťových designérů, dodavatelů, výzkumných pracovníků a dalších zainteresovaných odborníků. I když většina práce v rámci pracovních skupin IETF se provádí pomocí e-mailové konference, osobní setkání umožňují lepší pochopení procesu standardizace mezi účastníky, podporují jejich aktivní účast v aktivitách IETF a také mohou sloužit jako zdroj navazování osobních kontaktů s dalšími odborníky z příbuzných oborů. Určitým problémem je, že se v současnosti na IETF setkáních podílí jen pouze omezený počet technických odborníků z rozvojových zemí a zemí s transformující se ekonomikou.

4.1 Normalizační aktivity

Dále se zaměřím na popis obecného procesu standardizace, který probíhá v rámci Internet Engineering Task Force. Prvním krokem ve vývoji jakéhokoli standardu je popis návrhu neboli idejí dané normy v dokumentu, který se nazývá Internet-draft,

zkráceně I-D.[14] Každý člen organizace IETF se může stát autorem I-D, ale je důležité poznamenat, že I-D je pouze prvním stupněm, předběžnou vizí standardu a zdaleka ne každý I-D se na konci stává platným standardem. I když požadavky na formální stránku I-D jsou docela přísné: formát a obsah I-D by měly být velmi podobné standardu. Tento typ dokumentu se nachází ve stadiu diskuze, může podléhat významným změnám a může být dokonce zamítnut kvůli nedostatku zájmu nebo nedostatečné propracovanosti jeho provedení. Jinými slovy budoucnost jednotlivého I-D je nepředvídatelná a použití takového dokumentu (stejně jako protokolu nebo systémů zastoupených v něm) vyžaduje velkou opatrnost.

Proto ne všechny dokumenty, které se prodiskutovávají v rámci IETF, dosahují své konečné fáze - publikace v sérii RFC. RFC znamená Request for Comments (požadavek komentářů). Historie RFC sahá až do dob projektu ARPANET, tedy konce 60. let minulého století, kdy RFC používala výzkumníky z ARPA ke skutečným žádostem o komentáře. Dnes tuto roli hraje I-D, zatímco RFC, naopak tvoří závěrečnou fázi procesu standardizace. Avšak i v daném případě je třeba také poznamenat, že ne všechny RFC jsou standardy. Část z nich má experimentální, informativní funkci či charakter doporučení, což se obvykle odráží ve stavu RFC dokumentu. Práce na standardu je kolektivní a obvykle se vykonává v rámci pracovní skupiny. Více než sto dvacet pracovních skupin IETF se zaměřuje na různé aspekty internetu, počínaje transportními protokoly a konče aplikacemi, otázkami řízení, konfigurace sítě a směrovacích protokolů.

Pokud navrhovaná norma odpovídá rozsahu oblasti zájmu pracovní skupiny a podle účastníků skupiny se týká poměrné důležitého problému, projekt se stává dokumentem pracovní skupiny. Zajímavé v daném kroku rozvoje standardu je, že právě v této fázi autor předává svůj návrh pracovní skupině, která se od daného okamžiku stává odpovědnou za jeho osud, a všechny změny v dokumentu jsou zavedeny v souladu s míněním celé pracovní skupiny na základě konsensu. Dokumenty se tak mohou stát předmětem významného přepracování, včetně výrazných změn specifikace, jména protokolu, atd. Autor protokolu, tedy člen IETF,

[14] MATHIASON, J. *Internet Governance: The New Frontier of Global Institutions*. New York: Routledge, 2008. s. 34.

který řešení navrhnul a rozhodl se proměnit svou myšlenku na standard IETF, by měl být na to připraven. Když všechny hlavní otázky ohledně konkrétního návrhu protokolů jsou vyřešeny, v rámci pracovní skupiny se vyhlašuje "poslední výzva" (last call, LC), neboli příležitost pro členy skupiny, aby případně dodatečně obhájili nebo poukázali na existující nedostatky návrhu. Absence námitek v daném případě znamená, že práce na standardu přejde do další fáze.

Dalším krokem v procesu vytvoření internet standardu v IETF je podání návrhu na IESG (Internet Engineering Steering Group), o němž již bylo zmíněno dříve. IESG oznamuje všeobecnou "poslední výzvu", která slouží jako signál pro ty příslušníky organizace IETF, kteří nejsou členy dané pracovní skupiny, a tak se neúčastnili diskuzí o daném projektu, že mohou nyní zvážit návrh a poslat své případné připomínky k němu. Zároveň je to příležitost pro členy pracovní skupiny, odkud návrh pochází, kteří jsou přesvědčeni, že jejich názor nebyl brán v úvahu, aby ještě jednou projevili vlastní vztah k projektu již v rámci širší komunity Internet Engineering Task Force. Takový postup při zavedení standardu poukazuje na skutečnost, že každý člen IETF (jímž se lze stát po přihlášení k odběru newsletterů IETF) může poměrně snadno přispět k rozvoji jakékoliv standardu.

Obecný last call trvá dva týdny pro I-D získané prostřednictvím pracovních skupin a čtyři týdny pro projekty jednotlivců. V případě, že IESG schvaluje dokument, je mu přiřazen status navrhovaného standardu (Proposed Standard) a následně je projekt publikován jako dokument RFC. V tomto stavu se dokument může nacházet nejméně 6 měsíců a praxe ukazuje, že mnoho dokumentů v tomto stavu zůstává navždy. Příčinou je skutečnost, že daný typ dokumentů je téměř reálným platným standardem, a proto mnozí autoři nevidí žádný důvod, proč by měli vyvíjet úsilí o zvýšení jeho pozice. Pro většinu aplikací primární status Proposed Standard se jeví jako zcela vyhovující.

Nicméně po uplynutí šesti měsíců autor standardu nebo předseda pracovní skupiny, od níž projekt původně pocházel, mohou požádat o "zvýšení" statutu dokumentu do stavu Draft Standard. Nezbytným předpokladem v daném případě je, aby se prokázala interakce dvou nezávislých implementací daného standardu. Velmi

často se v této fázi objevuje, že jednotlivé prvky navrhovaného standardu nefungují tak, jak bylo zamýšleno, a proto norma potřebuje revizi. Také se stává, že některé funkce nebyly vůbec použity, protože nikdo nevidí jejich zvláštní přínos. Takové prvky musí být ze standardu odstraněny a zvyšuje se tím kvalita standardu.

Teprve poté tato norma může postoupit do další úrovně. V této fázi konečně některé standardy dosahují nejvyššího statusu konečného standardu - Internet Standard. Proces zvažování a povyšování statutu je v organizaci IETF velmi přísný a je prováděn výhradně pro velmi široce používané protokoly, nezbytné pro provoz internetu.

Celkem v rámci IETF existuje osm tematických oblastí, ve kterých probíhá proces vytvoření standardů. Jsou to hlavní oblast, sféra internetového prostředí, managementu operací, oblast aplikací a infrastruktury, směrování (routing), bezpečnost a dopravní oblast. Ve stejných oblastech realizují svou činnost pracovní skupiny IETF, které řeší problémy internetové komunity (Active IETF Working Groups), aktuální v současné době z pohledu celé organizace. Každá z těchto oblastí vykonává zvláštní druh aktivit, jehož příklady představím v následujících podkapitolách.

4.1.1 Aplikační oblast

Ještě před krátkou dobou webové aplikace vyžadovaly kompletní restartování stránky při výběru nabídky menu nebo vstupu uživatele. Web 2.0 tuto situaci úplně změnil. Z technologického hlediska jde o koncept Webu jako platformy pro vytváření aplikací, na rozdíl od desktopových aplikací nebo aplikací pro operační systém. V souvislosti s těmito dramatickými změnami je zřejmé, že plody standardizace, která se provádí v rámci organizace IETF, by měly být jasné a přístupné pro vývojáře jak Webu, tak i dílčích aplikací. Jinými slovy IETF by měla podporovat inovace místo toho, aby je potlačovala. Dá se konstatovat, že se to Komisi techniky internetu dosud daří.

Hlavní otázkou, kterou si IETF klade v oblasti aplikací, je to, jaká je role jejích standardů v rozvíjejícím se světě webových aplikací. Tradiční přístup rozvoje

systému, na kterém je například založen SIP („Session Initiation Protocol“ anebo protokol pro inicializaci relací), má své kořeny v minulosti, kdy základní cenu nového systému tvořilo specializované zařízení a poskytovatelé služeb, kdežto dodavatelé zařízení a uživatelé byli nezávislými skupinami.[15] V dnešní době jsou trendy zcela odlišné.

Jedním z trendů je, že poskytovatel služby je nyní také výrobcem klientského zařízení a zařízení serveru, jehož role je však nyní vykonávána pomocí software. Nová služba je novou aplikací, kterou lze snadno stáhnout z internetu. Poskytovatel služeb sám vyvíjí klientské aplikace, což vyvolává potřebu standardizace těchto aplikací. Například více než polovina mobilních aplikací používá vlastní protokol, ve většině případů založený na protokolu HTTP. Nicméně potřeba vývoje nových protokolů a jejich standardizace nemizí, ale dokonce se zvyšuje.

Standardizace aplikací je potřeba zvláště tehdy, pokud existuje mnoho poskytovatelů, kteří nabízejí podobné služby. K normalizačním aktivitám, které mají proběhnout v rámci IETF, tak v první řadě patří standardizace mezidoménních komunikačních protokolů. Zatímco interakce mezi klientem a serverem v mnoha případech nevyžaduje standardizaci, protože tato funkce může být snadno "instalována" ve formě staženého kódu JavaScript, je patrná změna povahy standardizace. V současné době nejde již o vývoj systému, ale jeho jednotlivých prvků, které jsou stavebními materiály budoucích různorodých systémů.

4.1.2 Oblast routingu

Routing neboli směřování je proces určování trasy pohybu informace v komunikačních sítích. Trasy je možné nastavit administrativně nebo vypočítat pomocí směrovacích algoritmů, které jsou založeny na informacích o topologii a stavu sítě získaných ze směrovacích protokolů (dynamické trasy). Cílené internetové zdroje, tedy IP adresy a čísla autonomních systémů, jsou základní komponentou fungování internetu. Tento systém adresování používá obecný protokol komunikace mezi

[15] JOHNSTON, A. *Sip: Understanding the Session Initiation Protocol*. Norwood: Artech House, 2009. s. 118.

zařízeními připojenými k Internetu – jde o protokol IP. Globální směrovací systém je také založen na tomto protokolu.

Jedním ze slibných směrů normalizačních aktivit organizace IETF po zlepšení dostupnosti a spolehlivosti registračních údajů je použití technologií na bázi infrastruktury veřejných klíčů - PKI (Public Key Infrastructure).[16] PKI je hierarchický systém přístupu k veřejným (public) digitálním klíčům subjektů, fungující na základě vydání digitálních certifikátů, spojujících veřejný klíč subjektu s určitými atributy subjektu, například s názvem jeho domény. Tento digitální dokument je podepsán digitálním podpisem organizace vydávající certifikát. Podrobněji je struktura certifikátu X. 509 popsána ve standardu publikovaném IETF pod názvem RFC 3280.[17]

Na druhé straně držitel certifikátu může vydat podřízený certifikát se svým podpisem a tak dále. V čele této hierarchie každopádně stojí certifikát, kterému se říká "kotva důvěry" (trust anchor). Tento certifikát nemá "mateřský" certifikát a je podepsán svým vlastním klíčem. Nicméně pokud uživatel důvěřuje danému certifikátu, pravost všech dalších certifikátů hierarchie lze snadno zkontrolovat. Příkladem této technologie je použití certifikátů SSL pro zabezpečený přístup do webových stránek pomocí protokolu HTTPS .

Technologie digitálního certifikátu X. 509, který se podřizuje standardu IETF, je založena na asymetrických klíčích a konkrétně na tom, že každý klíč má tajné a otevřené části. Pravost zprávy podepsané pomocí tajného (soukromého) klíče lze zkontrolovat pomocí veřejného klíče. Běžná praxe předpokládá, že vlastník klíče přijímá vhodná opatření pro ochranu tajného klíče a zároveň poskytuje co nejširší veřejnosti údaje o druhém, veřejném klíči, aby se usnadnil přístup k němu třetích stran, například s cílem ověření zprávy odeslané vlastníkem.

[16] KARAMANIAN, A., DESSART, F., TENNETI, S. *PKI Uncovered: Certificate-Based Security Solutions for Next-Generation Networks*. Indianopolis: Pearson Education, 2011. s. 24.
[17] IETF. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. [olnline]. [cit. 2014-02-10]. URL: <http://www.ietf.org/rfc/rfc3280.txt>.

4.1.3 Bezpečnost

Příkladem normalizační aktivity organizace IETF v oblasti bezpečnosti je zavedení standardu DANE (DNS-based Authentication of Named Entities). Podstatou tohoto standardu vytvořeného Komisí techniky internetu je umožnění operátorům serverů, například webových stránek, publikovat certifikát TLS nebo potvrzení certifikačního centra, který vydal certifikát TLS, v globálním systému DNS. Tento certifikát může být použit pro zajištění bezpečné komunikace mezi klienty - internetovými prohlížeči a serverem.

Jinými slovy standard DANE umožňuje vlastníkovi doménového jména publikovat certifikát TLS nebo ukazatel důvěryhodného systému PKI, ve kterém se takový certifikát nachází, spolu s dalšími záznamy týkajícími se názvu: například adresou nebo názvem serverů, které obsluhují doménovou zónu, atd. Tímto způsobem je zajištěna stejná kryptografická ochrana, jako v tradičních PKI, ale řetěz důvěry se v plné míře nachází v souladu s hierarchií domény. DANE tak poskytuje možnost získat důvěryhodný certifikát od majitele jména bez zprostředkovatelů.

Zavedení standardu DANE již bylo dokončeno: je to standard RFC6698[18] z roku 2013, který definuje protokol a nový záznam DNS - TLSA, sdružující certifikát nebo veřejný klíč s názvem domény. Nicméně v procesu vývoje se nacházejí nové zajímavé náměty týkající se daného standardu, protože tento přístup může být použit k zajištění bezpečnosti a autentičnosti e-mailových serverů, publikování certifikátů S/MIME, které se používají pro šifrování a elektronického podepisování e-mailových zpráv. Bezpečnost protokolů systémů rychlých zpráv XMPP nebo hlasové komunikace SIP hypoteticky může být také výrazně zlepšena pomocí standardu DANE .

Kromě toho, protože standardy DANE, vypracované v rámci IETF, zahrnují zavedení bezpečnostního rozšíření DNSSEC, můžeme uvést, že zavedení DANE zahájilo použití nové důležité aplikace DNSSEC, což může sloužit jako další pobídka pro rozšíření tohoto standardu. Přínos daného standardu IETF je těžké podcenit:

[18] Data tracker. *The DNS - Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA*. [olnline]. [cit. 2014-02-10]. URL: <http://datatracker.ietf.org/doc/rfc6698/>.

použití DANE umožní výrazně zlepšit úroveň ochrany kritických internetových aplikací, jako jsou například web a e-mail.

4.1.4 Dopravní oblast

Pracovní skupiny Komise techniky internetu v této oblasti se zabývají vývojem transportních protokolů, jako jsou TCP, UDP, SCTP a DCCP. Dopravní oblast IETF také zahrnuje pracovní skupinu "behave", jejíž činnost je věnována problému interakci aplikací za přítomnosti vysílacích zařízení (NAT) s cílem rozvoje výkonnostních standardů pro tato zařízení. K této oblasti také patří skupiny zabývající se problematikou ukládání dat (nfsv4, storm).

Jedním z nejvýznamnějších příkladů normalizačních aktivit Komise techniky internetu je činnost pracovní skupiny MPLS, která vyvíjí standard se stejným názvem. Dnes je protokol MPLS široce používán pro budování Core a WAN sítí po celém světě, ale stále má nějaké problémy se škálováním a mezidoménními (inter-domain) interakcemi. Přímé (end-to-end) řízení výkonnosti a kvality služeb (QoS) i nadále zůstává problematickou otázkou, a to zejména v prostředí různých výrobců. Zatímco MPLS se výrazně změnil v průběhu posledního desetiletí, stále potřebuje další vývoj v rámci Komise techniky internetu pro řešení těchto problémů.

Původně standard MPLS byl vyvinut organizací IETF, především pro řešení problémů s výkonem IP směrování, ale po deseti letech se široce rozšířil mezi provozovateli za účelem vybudování síťových jader IP/MPLS a jako hlavní platforma pro zajišťování poskytování takových datových služeb, jako jsou IP-VPN a vzdálené ethernetové služby. A tak široce známý protokol MPLS se nyní aktivně přizpůsobuje požadavkům ITU - T pro tradiční dopravní sítě. V důsledku této spolupráce vzniká nový protokol dopravního profilu MPLS - TP (Transport Profile MPLS), který splňuje požadavky provozovatelů na snížení nákladů na paketové sítě a je schopen nastavit směr budoucího vývoje sítí. Nový standard MPLS-TP je výsledkem spolupráce organizací ITU - T a IETF. Již dnes někteří operátoři považují tuto technologii nejen za komutaci Ethernet, ale také za oblast nejúčinnější interakce mezi komunikačními routery, kde integrace MPLS-TP do P-OTN architektury vypadá jako logické řešení.

5 Aktivity IETF ve sféře multimédií

Protože IETF je organizací podporující rozvoj v oblasti internetových technologií obecně a regulující oblast nových technologických a technických směrů, je vhodné se zaměřit na konkrétní aktivity této organizace ve vybrané oblasti. Touto oblastí je oblast multimédií.

Multimédia jsou pravděpodobně jedním z nejužívanějších pojmů devadesátých let. V důsledku globalizačních a technologických procesů probíhajících ve světě, obzvlášť ve vysoce vyvinuté společnosti, se vyvíjely nové technologie, přístupy k pochopení multimediálního světa. Tato oblast byla dotčena změnami velmi zásadně. Vnikala nová zařízení; telekomunikační oblast se rozšířila nejenom na vnitropodnikové nebo korporátní způsoby komunikace a sdílení informací, ale na nové způsoby: telefonní komunikaci, ISDN spojení, nová média jako internet apod.

Jednou z prvních institucí, která se zabývala výzkumem v oblasti multimédií, je Vysoká škola technologií v Massachussetts. Toto vzdělávací zařízení hrálo významnou roli výzkumného prostředníka, který nabízel inovace, aplikace včetně personálních novin a časopisů, telefonů apod.[19] Časem se oblastí multimédií začaly zabývat světové organizace a regulační orgány dohledu. Zkoumaná organizace IETF se též připojila k výzkumu a normalizace činnosti v oblasti multimédií. Hlavní výsledky činnosti IETF jsou uvedeny v následující tabulce:

[19] STEINMETZ, R., NAHRSTEDT, K. *Multimedia systems*. Berlin: Springer, 2004. s. 4.

Tabulka 5.1: Standardy schválené IETF v oblasti multimédia

Název standardu	Kód standardu	Stav
Multimedia Congestion Control: Circuit Breakers for Unicast RTP Sessions	draft-ietf-avtcore-rtp-circuit-breakers-05	Schválený standard
End-to-End Session Identification in IP-Based Multimedia Communication Networks	draft-ietf-insipid-session-id-06	Schválený standard
Requirements for an End-to-End Session Identification in IP-Based Multimedia Communication Networks	draft-ietf-insipid-session-id-reqts-11	Schválený standard
Multimedia Conference Recording Use Cases and Requirements	draft-kyzivat-siprec-conference-use-cases-01	Schválený standard
Using Partial Offers and Partial Answers in a Multimedia Session	draft-roach-mmusic-pof-pan-02	Schválený standard

Zdroj: *Data tracker. Search Internet-Drafts and RFCs. [olnline]. [cit. 2014-02-10]. URL: <http://datatracker.ietf.org/doc/search/?name=multimedia&rfcs=on&activedrafts=on&sort=>.*

Tabulka 5.2: Standardy informační a navržené IETF v oblasti multimédia

Název standardu	Kód standardu	Stav
Using ODA for translating multimedia information	RFC 1197	Informační manuál
A User Agent Configuration Mechanism for Multimedia Mail Format Information	RFC 1343	Informační manuál
Network Access to Multimedia Information	RFC 1614	Informační manuál
Multimedia E-mail (MIME) User Agent Checklist	RFC 1844	Informační manuál
MIKEY: Multimedia Internet KEYing	RFC 3830	Standard

		aktualizovaný RFC4738, RFC6309
MIME Type Registrations for 3rd Generation Partnership Project (3GPP) Multimedia files	RFC 3839	Navržený standard, aktualizace ve standard RFC6381
Mapping Between the Multimedia Messaging Service (MMS) and Internet Mail	RFC 4356	Navržený standard
MIME Type Registrations for 3GPP2 Multimedia Files	RFC 4393	Navržený standard, aktualizace RFC6381
The Key ID Information Type for the General Extension Payload in Multimedia Internet KEYing (MIKEY)	RFC 4563	Navržený standard, aktualizace RFC6309
HMAC-Authenticated Diffie-Hellman for Multimedia Internet KEYing (MIKEY)	RFC 4650	Navržený standard,
Multimedia Terminal Adapter (MTA) Management Information Base for PacketCable- and IPCablecom-Compliant Devices	RFC 4682	Navržený standard
MIKEY-RSA-R: An Additional Mode of Key Distribution in Multimedia Internet KEYing (MIKEY)	RFC 4738	Navržený standard
Signaling MIB for PacketCable and IPCablecom Multimedia Terminal Adapters (MTAs)	RFC 5098	Navržený standard
On the Applicability of Various Multimedia Internet KEYing (MIKEY) Modes and Extensions	RFC 5197	Informační manuál
Multimedia Internet KEYing (MIKEY) General Extension Payload for Open Mobile Alliance BCAST 1.0	RFC 5410	Informační manuál , aktualizace RFC6309
Session Peering for Multimedia Interconnect (SPEERMINT) Terminology	RFC 5486	Informační manuál

The SIP P-Served-User Private-Header (P-Header) for the 3GPP IP Multimedia (IM) Core Network (CN) Subsystem	RFC 5502	Informační manuál
MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY)	RFC 6043	Informační manuál aktualizace RFC6309
SDP and RTSP Extensions Defined for 3GPP Packet-Switched Streaming Service and Multimedia Broadcast/Multicast Service	RFC 6064	Informační manuál
MIKEY-IBAKE: Identity-Based Authenticated Key Exchange (IBAKE) Mode of Key Distribution in Multimedia Internet KEYing (MIKEY)	RFC 6267	Informační manuál
IANA Rules for MIKEY (Multimedia Internet KEYing)	RFC 6309	Navržený standard
Session PEERing for Multimedia INTerconnect (SPEERMINT) Security Threats and Suggested Countermeasures	RFC 6404	Informační manuál
Session PEERing for Multimedia INTerconnect (SPEERMINT) Architecture	RFC 6406	Informační manuál
Framework for Emergency Calling Using Internet Multimedia	RFC 6443	Informační manuál
MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)	RFC 6509	Standard čekající na schválení

Zdroj: *Data tracker. Search Internet-Drafts and RFCs. [olnline]. [cit. 2014-02-10]. URL: <http://datatracker.ietf.org/doc/search/?name=multimedia&rfcs=on&activedrafts=on&sort=>.*

Z tabulky je vidět, že standardů v oblasti multimédia je velké množství. Z nich byly vybrány standardy a protokoly pokrývající největší rozsah činností a jsou analyzovány v následující části práce.

5.1 Profil iNOW

Komise techniky internetu se v poslední době zaměřila také na problém obecnější povahy spojený s vývojem multimediálních možností internetu. Za prvé komisí IETF byl doporučen protokol rezervace zdrojů (Resource Reservation Protocol, RSVP). Za použití RSVP multimediální programy mohou vyžadovat zvláštní kvalitu servisu (Specific Quality of Service, SQoS) prostřednictvím některého z existujících síťových protokolů - především IP, i když je možné použít i protokol transportní úrovně UDP (User Datagram Protocol). Ačkoli protokol RSVP byl navržen pro řešení problému zajištění požadované kvality služeb při poskytování dat citlivých na zpoždění, v jeho rámci není odstraněn zásadní nedostatek internetových protokolů podporujících multimediální služby, a to zaostalé prostředky pro synchronizaci dat. Jak je známo, IP protokol neposkytuje prevenci ztráty dat. Proto komise techniky internetu vyvinula přenosový protokol v reálném čase (Real-time Transport Protocol, RTP). RTP je definován v dokumentu RFC 1889 a je součástí doporučení H. 323.

Nejčastěji se RTP používá jako nadstavba nějakého síťového protokolu, který nezaručuje doručení dat, citlivých na zpoždění, například UDP. Ke každému datovému paketu zaslanému z protokolu RTP je připojena informace o času odesílání a jeho sériové číslo. Protokol RTP může být použit spolu s RSVP pro přenos synchronizovaných multimediálních informací s určitou úrovní kvality servisu. Možnosti RTP byly vylepšeny jeho spojením s jiným protokolem IETF, a to s protokolem kontroly přepravy v reálném čase (Real-time Transport Control Protocol, RTCP). Pomocí protokolu RTCP programy se mohou přizpůsobit měnícímu se zatížení v síti a oznamovat odesílatelům a příjemcům náhlé změny v dodávkách předávaných přes síť informací.

Speciální pracovní skupina pro spravování vícebodových multimediálních komunikačních relací (MMUSIC) patřící do IETF vyvinula vlastní protokol aplikační úrovně pro inicializaci relací komunikace (Session Initiation Protocol, SIP), který byl přijat jako standard RFC 2543 v březnu roku 1999. Protokol SIP se používá pro

inicializaci relací internetové telefonie a multimediální komunikace a používá nikoliv ISDN čísla jako protokol H. 323, ale IP-adresy. SIP protokol používá protokoly pro přenos dat v reálném čase RTP a RTCP a také protokol popisující technické parametry relace (Session Description Protocol, SDP). SIP a SDP jsou určeny k signalizaci v sítích založených na IP, tedy navázání, udržování a odpojování virtuálních připojení, které jsou určeny pro přenos multimediálního kontentu.

Dvě pracovní skupiny Komise techniky internetu pracují na standardu kvality servisu (QoS) pro internet. Jedna z těchto skupin se zabývá vytvořením mechanismu pro multiprotokolovou komutaci labelů (Multiprotocol Label Switching, MPLS), další se věnuje problémům specifikace diferencovaných služeb (Differentiated Services, Diff-Serv). MPLS technologie předpokládá doplňování IP-paketů o speciální značku, označující, že informace bude směrována přes internet po předem stanovených trasách. Implementace specifikace MPLS v přepínačích a směrovačích může výrazně snížit dobu hledání cest, kterými pakety mají být předány. Specifikace Diff - Serv je navržena pro přiřazení hodnot a parametrů různým aplikacím – tedy takových hodnot a parametrů, charakterizujících různé třídy kvality doručení (Class of Service, CoS). Podle Diff-Serv, bity typu služby (Type of Service, TOS) v IP-záhlavích ukazují na třídy kvality doručení pro různé druhy provozu a jsou přiřazovány na základě dohody o úrovni servisu SLA (Service Level Agreement, SLA), uzavřené mezi uživateli a poskytovateli služeb.

V současné době v komisi IETF se také realizuje projekt v oblasti správy sítě na základě pravidel. Jde o výzkum vztahující se k definici standardní infrastruktury pro uplatnění této metodiky, stejně jako získání nezbytných protokolů a schématu práce. S cílem zajistit optimální proces ukládání a extrahování z úložišť tvořících strategie pravidel by jejich vnitřní reprezentace měla být formalizována v datové struktuře. Jedna z pracovních skupin Komise techniky internetu Policy Framework Working Group (PFWG) vyvinula model politiku Policy Framework Core Information Model, který definuje sadu objektově orientovaných skupin na vysoké úrovni, dostatečnou pro reprezentování základních strategií řízení. Objektově orientované třídy se mohou rozšiřovat o odvozené třídy určitých typů strategií, například pro zajišťování požadované kvality servisu a bezpečnosti.

Provozovatelé telekomunikačních sítí se potýkají s problémem, který je společný pro veškeré nové technologie. Tímto problémem je nekompatibilita mezi zařízeními od různých výrobců. Aby tento problém byl vyřešen, přední výrobci představili iniciativu možnosti interoperability hardwaru a softwaru od různých dodavatelů (Interoperability Now, iNow). Technologie "Voice over IP" se jeví zajímavou dokonce i pro tradiční provozovatele telekomunikačních sítí, například v souvislosti s poskytováním cenově efektivních řešení pro malé kanceláře. Ve skutečnosti jde o realizaci “poslední míle” pomocí VoIP a je samozřejmé, že realizace těchto řešení může být levnější, než tradiční přístup k problému, který zahrnuje použití určitého počtu přípojek a ústředny. Specifikace iNow definují způsoby kódování zpracování signální, tedy oficiální informace při vytváření virtuálních připojení, míry zabezpečení a další funkce správy přenosového média potřebné v procesu navázání spojení mezi IP-branami. Specifikace INow jsou založeny na standardu H. 323 a příloze G k doporučení H. 225.0, které popisuje organizaci komunikaci mezi doménami, tj. autonomními součástmi větší sítě se společným regulátorem a centralizovaným řízením. V prostředí internetu doména označuje skupinu uzlů, které se vztahují ke společnému regionu nebo určité předmětové oblasti. [20]

5.2 Protokol SIP

Protokol iniciovaných relací (Session Initiation Protocol, SIP) je protokol aplikační úrovně a je určen pro organizaci, modifikaci a ukončování komunikačních relaci, tj. multimediálních konferencí, telefonních připojení, a distribuci multimediálních informací. Uživatelé se tak mohou účastnit aktuálních komunikačních relací, zvát ostatní či sami být pozváni k nové relaci. Pozvánky mohou být adresovány konkrétnímu uživateli, skupině uživatelů nebo všem uživatelům. SIP protokol byl vyvinut pracovní skupinou MMUSIC (Multiparty Multimedia Session Control) Komise

[20] Narod.ru. *IETF standardy a profil iNOW*. [olnline]. [cit. 2014-02-10]. URL: <http://rz6hpi.narod.ru/net/ip_phone/system/sub-2.4.htm>.

techniky internetu, a specifikace protokolů jsou uvedeny v dokumentu RFC 2543.

Do základu protokolu SIP pracovní skupina MMUSIC dala několik zásad. Za prvé je to osobní mobilita uživatelů, což znamená, že uživatel se může bez omezení pohybovat v rámci sítě, takže by komunikační služby mu měly být poskytovány na každém místě této sítě. Uživateli je přiřazen jedinečný identifikátor a síť mu podle tohoto identifikátoru poskytuje komunikační služby bez ohledu na to, kde se nachází; proto uživatel pomocí speciální zprávy (REGISTER) informuje o vlastním pohybu server pro určení umístění. Za druhé jde o princip škálovatelnosti sítě, která je charakterizována v první řadě možností zvýšení počtu prvků sítě při jejím rozšiřování. Struktura serverů sítě, postavené na základě protokolu SIP, plně splňuje tento požadavek.

Třetím základním principem je rozšiřitelnost protokolu. Tato zásada je charakterizována možností doplnění protokolů novými funkcemi se zavedením nových služeb a jeho přizpůsobení pro práci s různými aplikacemi. Jako příklad lze uvést situaci, kdy se protokol SIP používá k navázání spojení mezi branami, propojenými s PSTN pomocí SS7 nebo DSS1 signalizací. V současné době SIP nepodporuje transparentní přenos signalizačních informací telefonními systémy signalizace. Vzhledem k tomu doplňkové služby ISDN nejsou dostupné pro uživatele IP-sítí. Rozšíření funkce protokolu SIP může být realizováno zavedením nových záhlaví zpráv, které musí být registrovány ve dříve zmíněné organizaci IANA. Přitom obdrží-li SIP server zprávu s oblastmi pro něj neznámými, jednoduše je ignoruje a zpracovává pouze ty oblasti, které zná. Pro rozšíření možností protokolu SIP mohou být také přidány nové typy zpráv.

Další zásadou je integrace do zásobníku existujících internetových protokolů, vyvinutých organizací IETF. Protokol SIP je součástí globálního multimediální architektury vyvinuté Komisí techniky internetu. Tato architektura zahrnuje také protokol rezervace zdrojů (Resource Reservation Protocol - RSVP, RFC 2205), přenosový protokol v reálném čase (Real-Time Transport Protocol - RTP, RFC 1889), protokol přenosu datových proudů informací v reálném čase (Real-Time Streaming Protocol - RTSP, RFC 2326) a protokol popisu komunikačních parametrů (Session

Description Protocol - SDP, RFC 2327). Nicméně funkce SIP protokolu jsou nezávislé na každém z těchto protokolů. Kromě toho protokol SIP předpokládá interakci s jinými signalizačními protokoly a může být použit ve spojení s protokolem H. 323. Je také možná interakce protokolu SIP se signalizačními systémy PSTN - DSS1 a SS7. Pro usnadnění této interakce signalizační zprávy protokolu SIP mohou přenášet nejen specifickou SIP - adresu, ale dokonce telefonní číslo ve formátu E. 164 nebo v jakémkoliv jiném formátu. Kromě toho protokol SIP, stejně jako protokoly H. 323 a ISUP/IP, může být použit k synchronizaci provozu zařízení ovládajících brány, a v tomto případě musí komunikovat s protokolem MGCP. Dalším důležitým rysem SIP je to, že tento protokol je přizpůsoben k organizaci přístupu uživatelů IP-telefonie ke službám inteligentních sítí, a existuje domněnka, že právě tento protokol bude hrát hlavní roli při organizaci spojení mezi uvedenými sítěmi. [21]

I když SIP - peering má takové výhody, jako jsou například příznivé náklady a flexibilita použití, tato technologie má stejné nevýhody jako IP - telefonie obecně. Přestože samotný peering je dostatečně spolehlivý, jím poskytované služby, realizované v rámci sítě s komutací paketů, a to zejména přes internet, jsou ve větší míře vystaveny výpadkům ve srovnání s tradičními sítěmi s komutací kanálů. Navíc zajištění bezpečného přenosu informace mezi uzly SIP-peeringu vyžaduje použití kompatibilních technologií bezpečnosti, jinak hovory jsou buď nemožné, nebo nejsou bezpečné. Pracovní skupina IETF, která vyvinula standard SIP - peeringu Speermint (Session peering for Multimedia Interconnect), se snaží odstranit tyto nedostatky. Tak například tato skupina usiluje o širší používání daného standardu, a pokud jde o organizace nebo poskytovatele, kteří nejsou schopni technicky přistoupit k danému standardu, skupina Speermint poskytuje sadu návodů (Best Known Methods — BKMs), popisující metodologii řízení komunikace v reálném čase v peeringových sítích.

Hlavním úkolem pracovní skupiny Speermint je rozšíření sféry používání protokolu SIP prostřednictvím rozvoje různých architektur na zakázku. Všechny speciálně vyvinuté architektury mají zajistit identifikaci, signalizaci a směrování pro

[21] Kunegin.com. *Zásady SIP*. [olnline]. [cit. 2014-02-10]. URL: <http://kunegin.com/ref8/sip/itegr.htm>.

komunikaci v reálném čase a přenos dat, která jsou citlivá na zpoždění, a zároveň přispět k vytváření a udržování určité úrovně důvěryhodných vztahů, bezpečnosti a odolnosti vůči nekorektním způsobům využívání a útokům.

Aby SIP - peering ve skutečnosti nebyl závislý na typu sítě, skupina Speermint používá aplikační vrstvy (pátou a vyšší) modelu OSI. Tento přístup umožňuje vytvořit dostatečně obecné modely peeringu, odpovídající vlastním cílům bez ohledu na typ dopravní sítě, zda jde o komunikaci DSL nebo kanál OC - 48. Je pravděpodobné, že dnes tento předpoklad zní příliš optimisticky, protože mezi těmito dvěma technologiemi existují značné rozdíly (např. co se týče algoritmů QoS). Pracovní skupina IETF uznává tuto skutečnost a v budoucnu se chystá zdokonalit svůj koncept implementace SIP-peeringu a zahrnout do SIP-protokolu podporu mechanismů QoS a řízení šířky pásma a provozu (Traffic - Engineering - TE).

K současnému dni skupina Speermint vydala pět pracovních dokumentů (Internet Drafts), popisujících základní principy SIP peeringu. Ve skutečnosti, s cílem řešit problémy, kterým čelí skupina Speermint, se uvedené dokumenty stávají součástí nynějších standardů SIP. Je pozoruhodné, že dva z těchto dokumentů popisují vzájemné logické seskupení peeringových funkcí a následných fází přenosu toku zpráv. Pracovní dokument věnovaný přenosu toku zpráv definuje fáze detekce, harmonizace politiky a parametrů zabezpečení relace SIP, které předpokládají vzájemné poskytování zpráv a přijetí dohod o vzájemné akceptaci mezi uzly peeringu ještě před výměnou SIP signálů a navázáním spojení. Tyto dodatečné etapy jsou prvními kroky na cestě k vytvoření dynamických politik konfigurovatelných správci systému pro množství SIP peering uzlů. Ačkoli protokol Speermint, který byl vyvinut v rámci práce organizace IETF, může zajistit stejnou úroveň ochrany a spolehlivosti SIP-peeringu, jako je to u SIP - federací, lze očekávat, že v příštích letech dojde k velkému nárůstu otevřených peering komunit, které budou podporovat protokol Speermint a ke kterým se připojí zbytek společností.

5.3 Kodek Opus

Jednotlivé objevy se přetvářejí v tak praktické vynálezy, že zůstávají v každodenním životě člověka po dlouhou dobu. To samé platí i v oblasti multimédií. Například standardu pro digitální kompresi audia do formátu MP3 je téměř 20 let, což v porovnání s jinými standardy počítačové techniky je velmi dlouhá doba. Během těchto dvaceti roků v počítačové sféře došlo k mnoha objevům a technologickým průlomům, ale pro digitální audio kupodivu se toho moc nezměnilo. MP3 se dostal do všech zařízení, která existují: tento standard se používá v počítačích, chytrých telefonech, přenosných přehrávačích, DVD přehrávačích, hodinkách a dalších elektronických zařízeních. Avšak v současné době je jasné, že tento formát již neodpovídá všem požadavkům moderních technologií, a proto vzniká potřeba nového otevřeného kodeku, který by byl zbaven nejzávažnějších nedostatků MP3, avšak zároveň by byl schopen udržet si všechny výhody tohoto populárního kodeku, a dokonce získat nové.

V reakci na tuto potřebu Internet Engineering Task Force zveřejnil standard otevřeného zvukového kodeku Opus, který je distribuován pod licencí BSD a slouží pro použití v aplikacích reálného času na internetu. Opus se stal otevřeným formátem specifikovaným v RFC 6716, jehož referenční implementace je šířena pod trojnásobně podmíněnou licencí.[22] Všechny známé patenty, pod které spadá nový kodek Opus, jsou dostupné pod licencí royalty-free.

Současně se zveřejněním RFC byla představena první verze kodeku Opus. Je třeba poznamenat, že proces přechodu od fáze "navrhovaného standardu" do přijetí standardu v organizaci IETF trval tři roky a požadoval vydání šestnácti předběžných možností specifikace. Dalším krokem vypracování specifikace se stalo přidání RFC statutu návrhu standardu (Draft Standard), což znamená téměř úplnou stabilizaci protokolu a zvážení všech připomínek, týkajících se daného tématu.

V podstatě v kodeku Opus, vypracovaného IETF, leží kombinace nejlepších technologií: kodeku CELT, vyvinutého organizací Xiph.org, a otevřeného kodeku

[22] Tools.ietf.org. *Definition of the Opus Audio Codec*. [olnline]. [cit. 2014-02-10]. URL: <http://tools.ietf.org/html/rfc6716>.

SILK od Skype. Kodek Opus se liší od svých předchůdců vysoce kvalitním kódováním a minimálním zpožděním během komprese streamování audia s vysokým datovým tokem, ale také při kompresi hlasu v omezené šířce pásma u aplikací VoIP telefonie. Dříve Opus byl zvolen nejlepším kodekem při použití přenosové rychlosti 64kbit a překonal konkurenty, jako jsou Apple HE-AAC, Nero HE-AAC, Vorbis a AAC LC. Po svém vydání kodek byl součástí testovací verze Firefoxu, na jejímž základě vznikla nová verze Firefox 15.

Tento kodek je určen především pro interaktivní internetové aplikace, včetně VoIP, telekonferencí, videoher a herních chatovacích místností. Opus podporuje vzorkovací frekvence 8-48 kHz. Audiokódování se může odehrávat s přenosovou rychlostí 6-510 kbit/s, délka rámů se liší od 2,5 až 20 ms. Kromě toho Opus kóduje audio v režimech stereo a mono pomocí technologie konstantní a variabilní komprese bitratu a podporuje až 255 kanálů. Navíc tento standard kodeku umožňuje kódování jak hlasu, tak hudby.[23]

Standard audio kodeku Opus, vyvinutý pracovní skupinou Komise techniky Internetu, má několik výhod před svými konkurenty: tento kodek tak ukázal lepší kvalitu kódování než ostatní otevřené a proprietární kodeky se ztrátami. Současně jde o velmi univerzální kodek, který podporuje širokou škálu přenosových rychlostí. Struktura Opus umožňuje této technologii efektivně přistupovat ke zvukovým artefaktům. K tomu byla navržena vícestupňová architektura zpracování audiosignálu. Hlavním argumentem, který hovoří ve prospěch nového kodeku pro IP telefonii, je nízká úroveň dočasného zdržení, která je velmi důležitá v dané sféře použití kodeku.

Ze všech těchto výhod můžeme usoudit, že audio kodek Opus má velkou budoucnost. Nízká úroveň zkreslení a minimální zpoždění, alespoň v porovnání s konkurenčními algoritmy, to vše dělá Opus ideální variantou pro integraci této technologie v oblasti IP telefonie a vysílání řeči. Nasvědčuje tomu i velmi široké spektrum možností využití Opusu, protože kodek lze použít pro jakýkoli účel kromě ukládání Lossless, pro které je vhodné použít FLAC, a kromě kódování ultranízké bitové rychlosti, pro které se obvykle používá codec2. Popularita kodeku Opus

[23] Tools.ietf.org. *Definition of the Opus Audio Codec*. [olnline]. [cit. 2014-02-10]. URL: <http://tools.ietf.org/html/rfc6716>.

zajišťuje i jeho hardwarovou podporu. Protože relativní výkon nového kodeku je vynikající, brzy můžeme očekávat, že dojde k používání této nové technologie v bezdrátových sluchátkách a přenosných hudebních přehrávačích.

5.4 Multimedia Internet KEYing

Jedním ze základních problémů kryptografie je zabezpečení komunikace přes odposlouchávaný kanál: zprávy musejí být šifrovány a dešifrovány, avšak obě strany musí mít společný klíč. Pokud tento klíč bude přenášen prostřednictvím stejného kanálu, pak odposlouchávající strana ho dostane také a význam šifrování zmizí. Pro přenos citlivých informací prostřednictvím otevřených komunikačních kanálů účastníci komunikace musí mít klíče, a to konkrétně buď jeden klíč v případě symetrického šifrování, nebo dvojici klíčů pro každého účastníka v asymetrickém šifrování. Použití stejného klíče pro opakovanou komunikaci mezi účastníky umožňuje získání mnoha materiálů pro dešifrování tohoto klíče. Z tohoto důvodu s cílem zlepšit bezpečnost při výměně utajovaných informací jsou široce používány relační klíče. Klíč relace je klíč používaný účastníky v rámci jedné relace komunikace. Navíc některé kryptografické systémy předpokládají častější změnu klíče i během jedné relace, použití časových razítek a některých dalších informací, zvyšujících bezpečnost šifrovacího systému. Relační klíče umožňují také řešit druhý problém, spojený s omezením objemu škody při selhání klíče.

V této oblasti organizace IETF vypracovala technologii s názvem MIKEY, což je anglická zkratka pro Multimediální Internet KEYing, tedy protokol výměny klíčů navržený speciálně pro multimediální aplikace běžící v reálném čase, jako je například streamování audio dat. Tato technologie se používá k výměně klíčů pro šifrování hlasových relací protokolu SRTP a samotná technologie MIKEY spolu s jejím používáním je definována v standardu IETF RFC 3830.[24]

MIKEY podporuje tři různé metody. První z nich jsou dříve dohodnutá hesla

[24] Tools.ietf.org. *MIKEY: Multimedia Internet KEYing*. [olnline]. [cit. 2014-02-10]. URL: <http://tools.ietf.org/html/rfc3830>.

(angl. pre-shared key), což je nejúčinnější způsob, předpokládající, že strany si vyměnily heslo, které se následně stává klíčovým pro šifrování i pro dešifrování přenášených dat; v tomto případě jde o tzv. symetrické šifrování. Nicméně udržovat velkou strukturu hesel pro každého jednotlivého příjemce by bylo obtížné, a to zejména při změně velikosti struktury. Druhou metodou jsou soukromé a veřejné klíče (angl. private and public key), při které jde o asymetrickou kryptografii, ve které veřejný klíč je zasílán otevřeným způsobem (tj. prostřednictvím nechráněného kanálu, přístupného pro pozorování) a slouží k zašifrování zprávy. Pro dešifrování zprávy se pak používá soukromý (tajný) klíč. Problémem v daném případě je, že plný rozsah škálování vyžaduje centralizovanou podporu výměny klíčů s autorizačním centrem. Třetí možností je nakonec algoritmus Diffieho - Hellmana, který umožňuje oběma stranám získat sdílený tajný klíč přes nezabezpečený kanál. Tento klíč může být použit k šifrování další výměny informací pomocí symetrického šifrovacího algoritmu. Tato metoda vyžaduje značné výpočetní zdroje a delší čas potřebný pro počítání, než předchozí metody, a potřebuje centralizovaný systém podpory autorizace klíčů, stejně jako v případě veřejného klíče. Nicméně tato skutečnost je obrovskou výhodou pro zachování utajovaných informací.

MIKEY popisuje postup pro řízení a výměnu klíčů (Transport Encryption Key - TEK a Transport Generation Key - TGK) pro multimediální relace v reálném čase a také proces předávání dalších nastavení zabezpečení mezi účastníky komunikace. Jinými slovy, MIKEY slouží k výměně mezi účastníky hlavního klíče (K_M) a nastavení zabezpečení. Vzhledem k tomu, že TEK může být upraven (v tomto případě půjde o tzv. rekeying), K_M se také může podrobit úpravám. V závislosti na používaném základním protokolu, tj. SIP/H.323, technologie MIKEY, vyvinutá Komisí techniky internetu, podporuje připojení „uživatel – uživatel“ (peer-to-peer) a „uživatel - mnoho uživatelů“ (one-to-many), což znamená, že koncový uživatel protokolu SIP může vytvořit bezpečné komunikační spojení s koncovým uživatelem, používajícím protokol H. 323. Kromě toho technologie MIKEY je schopna podporovat více komunikačních protokolů výměny klíčů a nastavení zabezpečení pro několik relací najednou: v tomto případě RTP - RTCP - vazby, přes použití všemi účastníky TEK, mohou být chráněny současně a nezávisle na sobě.

5.5 Standard Multipurpose Internet Mail Extension (MIME) a jeho aplikace na oblast multimédia

Další významnou iniciativou organizace IETF v oblasti multimédií je technologie MIME (Multipurpose Internet Mail Extension – Víceúčelové rozšíření internetové pošty), která byla vyvinuta jako způsob přenosu připojených dat přes internet prostřednictvím e-mailu. Tento standard popisuje, jak pomocí e–mailu odesílat spustitelné soubory, grafická, multimediální a smíšená data. Typické aplikace technologie MIME zahrnují odesílání grafických obrázků, audia, dokumentů, například připravených ve WinWordu, programů, zpráv napsaných v HTML a prostých textových souborů. MIME také umožňuje v rámci jedné elektronické zprávy oddělovat části různých typů tak, aby příjemce (e-mailový program nebo PC) mohl rozlišit, co je třeba udělat s každou částí této zprávy.

Základní formát elektronických zpráv je definován v standardu IETF s názvem RFC 5322, který je aktualizovanou verzí standardu RFC 2822 (který pak je aktualizovanou verzí RFC 822). Tyto normy definují podobné formáty pro textová e-mailová záhlaví, obsah a pravidla týkajících se běžně používaných polí, například „To:“, „Subject:“, „From:“ a „Date:“. Standard MIME definuje sadu těchto záhlaví pro určení dalších atributů zprávy, včetně typu obsahu, a určuje množství kódů, které mohou být použity k reprezentaci 8-bitových binárních dat pomocí znaků ze 7-bitového ASCII.[25] MIME také stanovuje pravidla pro kódování znaků z rozšířené ASCII (s kódy 128 až 255) v názvech e -mailové zprávy, jako je například „Předmět:“.

Výhodou MIME je, že tato technologie je ve své podstatě rozšiřitelná o nové typy, protože její definice zahrnuje metodu pro registraci nových typů obsahu a dalších atributů elektronické pošty.

Tato skutečnost je spojená s tím, že technologie MIME předpokládá, že zpráva se skládá z několika částí, což se odráží na struktuře samotného standardu, který

[25] Tools.ietf.org. *Internet Message Format*. [olnline]. [cit. 2014-02-10]. URL: <https://tools.ietf.org/html/rfc5322>.

obsahuje pole Mime-Version (Verze MIME), ukazující na to, ve formátu jaké verze MIME je připravena zpráva, a Content-type (Typ obsahu), což je pole, jež se používá k označení typu dat v rámci zprávy. Norma popisuje několik typů, mezi které patří "text" (textový formát), "multipart" (zpráva se skládá z několika částí), "application" (výměna dat mezi aplikacemi, jako jsou například, tabulky), "image" (obrázek), "audio" (zvukový formát), "video" (videoklip) a další. Dalším polem je Content-Transfer-Encoding (Kódování při předávání), které může být použito k určení formátu prezentace přenesených dat. Mnoho z dat poslaných přes elektronickou poštu vyžaduje pro svou prezentaci 8 - bitovou datovou sadu, ale norma popisující elektronickou poštu umožňuje použití pouze 7 – bitových dat a také délku čáry limitovanou na 1000 znaků. Proto všechny údaje, které nesplňují tento požadavek, musí být uvedeny v 7 - bitovém formátu. Pro tuto transformaci existuje několik algoritmů: x - uuencode, base64, quoted- printable, 7bit, 8bit, binary (když hodnoty "8bit „, „7bit" a „binary" znamenají, že nedochází k žádné transformaci obsahu). Content - Description (popis obsahu) je jednou z dalších oblastí, která jednoduše popisuje data obsažená ve zprávě.

Pro předávání více zpráv do záhlaví Content-Type je přidán parametr boundary (hranice), která odkazuje na sekvenci znaků oddělujících části zprávy. Hranice se může skládat z čísel, písmen a symbolů „’( ) _ + - / : . ? =“. Při použití speciálních znaků (tzn. nikoli čísel a písmen) hodnota parametru boundary musí být uvedena ve dvojitých uvozovkách. Maximální délka hranice činí 70 znaků. Začátek každé části zprávy je označen jako „—boundary“, konec zprávy a její poslední řádek – jako „—boundary--„. První znaky přenosu řádku CRLF (kódy 13 a 10), kterými začínají a končí čáry ohraničení, nejsou zahrnuty do obsahu samotné části zprávy, ale pokud jimi následuje další přenos řádku, začínají patřit k zahrnuté části.

Prostor před- a po první části může obsahovat dodatečný text, který se nazývá preambule a epilog. V protokolu HTTP tyto prvky jsou ignorovány. V e-mailu preambule může obsahovat text, který je zobrazován e-mailovými klienty, již nerozumějí formátu MIME. Na začátku zahrnuté části jsou umístěna záhlaví, která popisují obsah (Content-Type, Content-Length, atd.). Přímo před tělem zprávy se musí nacházet prázdný řádek, i když tam žádné hlavičky nejsou. Pokud pole Content-

Type není definováno, pak ve výchozím nastavení se zobrazuje text / plain.

Zavedení standardu MIME Komisí techniky internetu umožnilo umístit do normální textové zprávy jakýkoli typ dat a abstrahovat se od počítačové platformy, tj. PC a poštovní klienti na různých operačních systémech a hardwarových platformách, které podporují tento standard, mohou snadno číst stejnou zprávu. Následně je zaručeno, že například stejný obraz připojený k dopisu bude stejně "dekódován" a zobrazí se na Macintosh v prostředí MacOS i na PC s operačním systémem Windows. MIME definuje mechanismy pro přenos informací v rámci různých druhů textových dat (zejména e-mailem), a to textu v jazycích, pro které se používá kódování jiné než ASCII, a obsahu bez textu, jako jsou obrázky, hudba, filmy a programy. Standard MIME je také základní složkou komunikačních protokolů, jako je HTTP, které potřebují, aby data byla přenesena v rámci zpráv podobných e-mailům, a to i v případě, že data skutečně nejsou e-mailem. Dodatečnou výhodou je, že MIME formát podporuje přenos více subjektů v jedné zprávě, přičemž sada subjektů se může přenášet nejen jako single-level sekvence, ale také jako hierarchie navzájem vnořených prvků. Pro označení množného – vícečetného - obsahu se používá médiatyp „multipart“. Práce s těmito typy se provádí podle obecných pravidel popsaných v RFC 2046 (není-li pro konkrétní typ média uvedeno jinak). Pokud příjemce neví, jak pracovat s určitým typem, je zpráva zpracována jako multipart či mixed.

Závěr

Bakalářská práce je zaměřena na analýzu oblasti normalizačních aktivit organizace IETF (Internet Engineering Force Task), zejména na oblast multimédií. Cílem práce je přehledně, strukturovaně a vyváženě zmapovat normalizační aktivity v oblasti internetu vykonávané organizací Internet Engineering Task Force (IETF), zejména její aktivity v oblasti multimédií. Cíl práce byl postupně naplňován ve druhé, třetí a čtvrté kapitole práce. První kapitola se věnuje popisu teoretických poznatek a vymezuje pojmy Internet, WWW a multimédia. Ve druhé kapitole se věnujeme organizacím působícím v oblasti Internetu a vydávajícím doporučení, standardy a protokoly.

Ve třetí kapitole se nejdříve přistoupilo k popisu samotné organizace a retrospektivní analýze jejího vzniku, aktivit a organizační struktury. Hlavní zjištění je následující: hlavní rolí zkoumané organizace je určení směru vývoje nebo využívání protokolů a krátkodobých elementů v architektuře internetu, což by takové technické problémy na internetu umožnilo řešit. V rámci své činnosti organizace IETF spolupracuje s dalšími organizacemi, například s Internet Research Task Force (IRTF) v oblasti usnadnění transferu technologií z této komise do širší internetové komunity anebo s Internet Engineering Steering Group (IESG). Hlavní funkcí Komise techniky internetu zůstává poskytování prostoru pro výměnu informací v rámci internetové komunity mezi dodavateli, uživateli, výzkumnými pracovníky, představiteli agentur a správci sítí.

Ve čtvrté kapitole jsme se zaměřili na popis, analýzu a výzkum normalizačních aktivit v hlavních vybraných oblastech: aplikační, routingové, bezpečnostní a v dopravní oblasti. V aplikační oblasti hlavní zjištění je následující: standardizace aplikací je potřeba, zvláště pokud existuje mnoho poskytovatelů, které nabízejí podobné služby. K normalizačním aktivitám, které mají proběhnout v rámci IETF, tak v první řadě patří standardizace mezidoménních komunikačních protokolů.

Jednou z normalizačních aktivit organizace IETF v oblasti routingu je zlepšení dostupnosti a spolehlivosti registračních údajů a použití technologií na bázi infrastruktury veřejných klíčů - PKI (Public Key Infrastructure).

Normalizační aktivitou v oblasti bezpečnosti je standard DANE (DNS-based Authentication of Named Entities). Podstatou tohoto standardu vytvořeného Komisí techniky internetu je umožnění operátorům serverů, například webových stránek, publikovat certifikát TLS nebo potvrzení certifikačního centra, který vydal certifikát TLS, v globálním systému DNS.

V oblasti multimediálních aktivit se používají standardy a doporučení organizace IETF, zejména kodek Opus, profil iNow, který byl několikrát aktualizován a změněn v kontextu integrace a společného propojení s jinými standardy. Dalším významným krokem pro normalizaci v oblasti multimédií je protokol SIP. To je protokol iniciovaných relací, který je určen pro organizaci, modifikaci a ukončování komunikačních relací. Uživatelé se tak mohou účastnit aktuálních komunikačních relací, zvát ostatní a sami být pozváni k nové relaci. Pozvánky mohou být adresovány konkrétnímu uživateli, skupině uživatelů nebo všem uživatelům. Tato služba může být velmi dobře využita pro video a audio konference.

Nesmíme zapomenout na standard MIKEY, což je protokol pro výměny klíčů navržený speciálně pro multimediální aplikace běžící v reálném čase, jako je například streamování audio dat.

Hlavním závěrem k činnosti IETF je, že tato organizace se snaží být činná a efektivní ve všech oblastech internetových komunikací. Nechybějí ani aktivity v oblasti multimédií. Hodnotím to jako velmi perspektivní směr vývoje pro organizaci IETF. Nicméně stále se vyskytují problémy, které je nutné řešit a optimalizovat. Cílem pro perspektivní vývoj je především to, že organizace musí usilovat, aby uživatelé jednotlivých možností internetu užívali vydávané standardy a zaváděli je do každodenní praxe.

Nelze nezmínit, že velmi významným výstupem práce je vytvoření metodické prezentace vhodné pro použití při výuce studentů (na CD nosiči). Prezentace vymezuje všechny hlavní oblasti působení a aktivity organizace IETF, cíle a výsledky práce. Prezentace může být využitá zejména pro výuku v příslušných předmětech bakalářského studijního oboru.

Seznam použité literatury a zdrojů

[1] BEDNÁŘ, V. *Internetová publicistika*. 1. vyd. Praha: Grada Publishing, 2011. 210 s. ISBN 978-802-4734-521.

[2] DOSTÁL, J. *Multimediální, hypertextové a hypermediální učební pomůcky - trend soudobého vzdělávání.* Časopis pro technickou a informační výchovu. Olomouc: Univerzita Palackého, 2009. Ročník 1, Číslo 2.

[3] HALSALL, F. *Multimedia communications: applications, networks, protocols, and standards.* New York: Addison-Wesley, 2000. 1034 s. ISBN 02-013-9818-4.

[4] JOHNSTON, A. *Sip: Understanding the Session Initiation Protocol*. Norwood: Artech House, 2009. 395 s. ISBN 978-16-078-3996-5.

[5] KARAMANIAN, A., DESSART, F., TENNETI, S. *PKI Uncovered: Certificate-Based Security Solutions for Next-Generation Networks*. Indianopolis: Pearson Education, 2011. 500 s. ISBN 978-15-870-5930-8.

[6] KUKUČKA, J. *Internet: učebnice.* 2. vyd. Brno: CCB, 2000. 165 s. ISBN 80-858-2543-0.

[7] MATHIASON, J. *Internet Governance: The New Frontier of Global Institutions*. New York: Routledge, 2008. 180 s. ISBN 978-02-039-4608-4.

[8] POSPÍŠIL, J. *Multimediální slovník: aneb manuál milovníka multimédií*. 1. vyd. Olomouc: Rubico, 2004. 183 s. ISBN 80-734-6019-X.

[9] SKLENÁK, V. *Data, informace, znalosti a Internet*. 1. vyd. Praha: C.H. Beck, 2001. 507 s. ISBN 80-717-9409-0.

[10] STEINMETZ, R., NAHRSTEDT, K. *Multimedia systems*. Berlin: Springer, 2004. 466 s. ISBN 35-404-0867-3.

Internetové zdroje

[11] Data tracker. *Internationalized Domain Name (idn) (concluded WG)*. [olnline]. [cit. 2014-02-10]. URL: <http://datatracker.ietf.org/wg/idn/charter/>.

[12] Data tracker. *Search Internet-Drafts and RFCs.* [olnline]. [cit. 2014-02-10]. URL: <http://datatracker.ietf.org/doc/search/?name=multimedia&rfcs=on&activedrafts=on&sort=>.

[13] Data tracker. *The DNS - Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA*. [olnline]. [cit. 2014-02-10]. URL: <http://datatracker.ietf.org/doc/rfc6698/>.

[14] ICANN. *InterNIC — Public Information Regarding Internet Domain Name Registration Services*. [olnline]. [cit. 2014-02-10]. URL: <http://www.icann.org/en/resources/compliance/complaints/registrars>.

[15] IETF. *Concluded WGs*. [olnline]. [cit. 2014-02-10]. URL: <http://www.ietf.org/wg/concluded/>.

[16] IETF. *IETF Meeting Proceedings.* [olnline]. [cit. 2014-02-10]. URL: <http://www.ietf.org/meeting/proceedings.html>.

[17] IETF. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. [olnline]. [cit. 2014-02-10]. URL: <http://www.ietf.org/rfc/rfc3280.txt>.

[18] IETF. *Mission Statement*. [olnline]. [cit. 2014-02-10]. URL: <http://www.ietf.org/about/mission.html>.

[19] Kunegin.com. *Zásady SIP*. [olnline]. [cit. 2014-02-10]. URL: <http://kunegin.com/ref8/sip/itegr.htm>.

[20] Narod.ru. *IETF standardy a profil iNOW*. [olnline]. [cit. 2014-02-10]. URL: <http://rz6hpi.narod.ru/net/ip_phone/system/sub-2.4.htm>.

[21] Tools.ietf.org. *Definition of the Opus Audio Codec*. [olnline]. [cit. 2014-

02-10]. URL: <http://tools.ietf.org/html/rfc6716>.

[22] Tools.ietf.org. *Internet Message Format*. [olnline]. [cit. 2014-02-10]. URL: <https://tools.ietf.org/html/rfc5322>.

[23] Tools.ietf.org. *MIKEY: Multimedia Internet KEYing*. [olnline]. [cit. 2014-02-10]. URL: <http://tools.ietf.org/html/rfc3830>.

Příloha: Power Point prezentace – metodická pomůcka pro výuku v rámci bakalářských programů (CD)

Seznam tabulek

Seznam zkratek

ANSI – American National Standards Institute

ARPA - Advanced Research Project Agency

API - Application programming

APP – Application Area

AVI – Audio Video Interleave

BGP – Border Gateway Protocol

BOF – Birds of Feather

BSD – Berkeley Software Distribution

CCITT – International Telegraph and Telephone Consultative Committee

CoS – Class of Service

DANE – DNS based Authentication of Named Entities

DCCP – Datagram Congestion Control Protocol

Diff-Serv – Differentiated Services

DNSSEC – Domain Name System Security Extensions

DoD – Department of Defense

DSS1 – Digital Subscriber system

ECMA – Evropská organizace výrobců počítačů

FDDI – Fiber Distributed Data

FLAC – Free Lossless Audio Codec

FTP – File Transfer Protokol

HTML - Hyper Text Markup Language

HTTPS - Hyper Text Transfer Protocol Secure

IAB – Internet Architecture Board

IANA – Internet Assigned Numbers Authority

IBAKE – Identity-Based Authenticated Key Exchange

IDN – Internationalized Domain Names

IEEE – Institute of Electrical and Electronies Engineers

IESG – Internet Engineering Steering Group

IETF - Internet Engineering Task Force

iNow – Interoperability Now

IP - Internet Protocol

IPsec – Internet Protocol Security

IRTF – Internet Research Task Foce

ISO – International Organisation for Standartization

ISOG – International Satellite Operations Group

ISQ – I seek you

IS-IS – Intermediate System to Intemediate System

ISDN – Integrated Services Digital Network

IT – Information Technology

ITU - International Telecomunication Union

JPEG – Joint Photographic Experts Group

LAN – Local Area Network

MIKEY – Multimedia Internet Key-ing

MMUSIC – Multiparty Multimedia Session Control

MPEG – Moving Picture Experts Group

MPLS – Multiprotocol label switching

MSN – Microsoft Network

MTA – Multimedia Terminal Adapter

NAT – Network Address Tranlation

NCSC – Národní centrum ochrany počítačů

NFSv4 – Network File Systém

ODA – Official development assistance

OPS – Operations and Management

OSI – Open Catalog Interface

OSN – Organizace spojených národů

OSPF – Open Shortest Path First

PDA – Personal Digital Assistant

PKI– Public Key Infrastructure

PFWG – Policy Framework Working Group

PSTN – Public Switched Telephone Network

RSVP – Resouce Reservation Protocol

RTG – Routing Area

RTP – Real-Time Transport Protocol

SASL – Simple Authentication and security Layer

SCTP – Stream Control Transmission

SDP – Session Description Protocol

SIP – Session Initiation Protocol

SLA – Service Level Agreement

SNMP – Simple Network Management Protocol

SQoS – Specific Quality of Service

SS7 – Signaling system

SSL – Secure Sockets Layer

TCP – Transmission Control Protocol

TE – Traffic Engineering

TEK – Transport Encryption Key

TGK – Transport Generation Key

TLD – Top-level domain

TLS – Transport Layer Security

TOS – Type of Service

UDP – User datagram protocol

URL – Uniform Resource Locator

USA – Spojené státy americké

W3C – World Wide Web Consortium

WMP – Windows Media Player

WWW – World Wide Web

XML – eXtensible Markup Language

XHTML- Extensible Hyper Text Markup language

XMPP – Extensible Messaging and Presence Protocol

Obsah CD

Priložené CD obsahuje 2 složky:

1. Power Point prezentace – metodická pomůcka pro výuku v rámci bakalářských studijních programů ve formátu ppt. a pdf.;

2. Bakalářska práce ve formátu pdf.