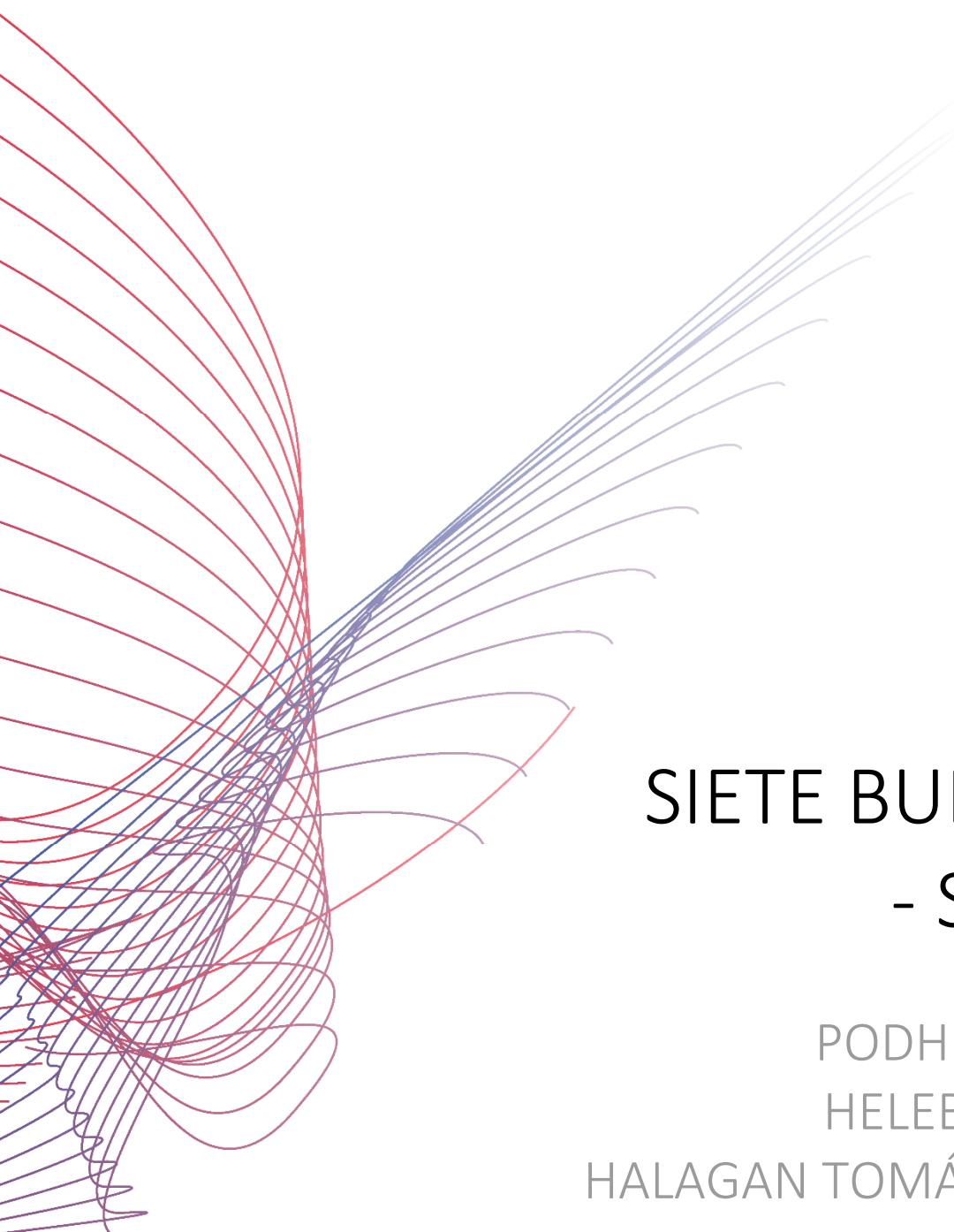




TECH pedia



SIETE BUDÚCNOSTI - SDN A NFV

PODHRADSKÝ PAVOL,
HELEBRANDT PAVOL,
HALAGAN TOMÁŠ, DROZD IVAN

Názov: Siete budúcnosti - SDN a NFV
Autor: Podhradský Pavol, Helebrandt Pavol,
Halagan Tomáš, Drozd Ivan
Vydalo: České vysoké učení technické v Praze
Fakulta elektrotechnická
Kontaktná adresa: Technická 2, Praha 6, Česká republika
Tel.: +420 224352084
Tlač: (iba elektronická)
Počet strán: 39
Edícia (vydanie): 1. vydanie, 2017
ISBN 978-80-01-06250-0

TechPedia

European Virtual Learning Platform for
Electrical and Information Engineering

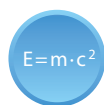
<http://www.techpedia.eu>



Tento projekt bol financovaný s podporou Európskej Komisie.

Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).

VYSVETLIVKY



Definícia



Zaujímavosť



Poznámka



Príklad



Zhrnutie



Výhody



Nevýhody

ANOTÁCIA

Súčasný Internet je stále založený na internetovom protokole, ktorý bol definovaný pred viac ako 40 rokmi pre určitý druh služieb. Počas desaťročí nadobudol Internet obrovské rozmery a nepočítalo sa tiež s novými aplikáciami ako je webové plynulé sťahovanie videa, zdieľanie súborov, ktoré zásadným spôsobom zmenili charakter internetovej prevádzky. Infraštruktúra Internetu sa vyvíjala pri nových technológiách od pevných optických k bezdrôtovým sieťam. Nové aplikácie a služby, technológie, stupeň a variabilita zariadení koncového používateľa si vyžadujú pružné riešenia. Ako najmodernejšie riešenia sa zdajú byť prepojenia programovo a softvérovo definovaných sietí a virtualizácia sieťových služieb. Tento modul sa koncentruje hlavne na tieto nádejné technológie pre Internet budúcnosti ale aj na prehľad sietí budúcej generácie.

CIELE

Hlavným cieľom tohto kurzu je poskytnúť základné poznatky o nových trendoch v informačných a komunikačných technológiách, hlavne o evolúcii súčasných sietí k sieťam budúcnosti a tiež Internetu budúcnosti. Účastníci budú oboznámení so základnými charakteristikami sietí budúcej generácie. Najdôležitejšie však bude disponovať poznatkami o stave druhov technológií ako je vytváranie softvérovo definovaných sietí a virtualizácia sieťových funkcií z hľadiska základnej architektúry, princípov a protokolov. Ďalej je pozornosť venovaná tiež platným aktuálnym obmedzeniam a požiadavkám Internetu budúcnosti.

LITERATÚRA

- [1] Mikoczy, E., Kotuliak, I., van Deventer, M. O.: Evolution of the converged NGN service platforms towards Future Networks. in Future Internet Journal, special issue Special Issue "Network vs. Application Based Solutions for NGN", 2011, ISSN 1999-5903.
- [2] Mikoczy, E.: Next Generation of Multimedia Services in Context of Future Networks. In Proceedings of ETSI Future Network Technologies Workshop, Sophia Antipolis, France, 10–11 March 2010.
- [3] Podhradský, P., Mikóczy, E., Lábaj, O., Londák, J., Trúchly, P., at al: NGN Architectures and NGN Protocols. LdV IntEleCT, Educational publication, 210 pages, Published by ČVUT Praha, ISBN: ISBN:978-80-01-04949-5, September 2011, CD version.
- [4] Podhradský, P., Mikóczy, E., Dúha, J., Trúchly, P., at al: NGN – Selected topics, LdV IMProVET. Educational publication, 137 pages, Published by ČVUT Praha, ISBN: 978-80-01-05295-2, August 2013, CD versions (SK, EN, CZ).

- [5] Nadeau, T. D., Gray, K.: SDN: Software Defined Networks. O'Reilly Media. 2013. ISBN: 978-1-449-34230-2.
- [6] Helebrandt, P., Kotuliak, I.: Novel SDN multi-domain architecture. In IEEE 12th International Conference on Emerging eLearning Technologies and Applications (ICETA), pp.139-143, 2014.
- [7] Open Networking Foundation: Software-Defined Networking: The New Norm for Networks. White Paper, 2012
<https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf>.
- [8] McKeown, N.: OpenFlow and Software Defined Networks. online, Presentation. 2011
http://www.openflow.org/documents/OpenFlow_2011.pps.
- [9] Open Networking Foundation. <https://www.opennetworking.org>.
- [10] McKeown, N. et al.: OpenFlow: Enabling innovation in campus networks. In: ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp.69-74, 2008.
- [11] Open Networking Foundation: OpenFlow Switch Specification version 1.3.5. 2015
<https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-switch-v1.3.5.pdf>.
- [12] Dong; L., Gopal, R., Halpern, J.: Forwarding and Control Element Separation (ForCES) Protocol Specification. IETF RFC 5810, 2010.
- [13] Chiosi, M., Clarke, D., Willis, P., Reid, A., Feger, J., Bugenhagen, M., Khan, W., at al.: Network Functions Virtualisation: An Introduction, Benefits, Enablers, Challenges & Call for Action. SDN and OpenFlow World Congress, 2012.
https://portal.etsi.org/nfv/nfv_white_paper.pdf.
- [14] Chiosi, M., Wright, S., Clarke, D., Willis, P., at al.: Network Functions Virtualisation: Network Operator Perspectives on Industry Progress. SDN and OpenFlow World Congress, 2013. https://portal.etsi.org/nfv/nfv_white_paper2.pdf.
- [15] ETSI GS NFV-INF 001 V1.1.1, Network Functions Virtualisation: Infrastructure Overview. Specification, 2015. http://www.etsi.org/deliver/etsi_gs/NFV-INF/001_099/001/01.01.01_60/gs_NFV-INF001v010101p.pdf.
- [16] ETSI GS NFV-MAN 001 V1.1.1, Network Functions Virtualisation: Management and Orchestration. Specification, 2014. http://www.etsi.org/deliver/etsi_gs/NFV-MAN/001_099/001/01.01.01_60/gs_NFV-MAN001v010101p.pdf.
- [17] ETSI GS NFV-SWA 001 V1.1.1, Network Functions Virtualisation: Virtual Network Functions Architecture. Specification, 2014. http://www.etsi.org/deliver/etsi_gs/NFV-SWA/001_099/001/01.01.01_60/gs_NFV-SWA001v010101p.pdf.

- [18] SdxCentral:Network Functions Virtualization Report. 2015.
<https://www.sdxcentral.com/reports/network-functions-virtualization-report-2015/>.
- [19] Gruber C. G.: CAPEX and OPEX in Aggregation and Core Networks. In: Optical Fiber Communication, IEEE, 2009, pp. 1-3.
- [20] Strategy Analytics: Global Internet Device Installed Base Forecast. August 2014.
<https://www4.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5609>.
- [21] Wu, Y. et al.: CloudMoV: Cloud-Based Mobile Social TV. In: IEEE Transactions on Multimedia, vol.15, 2013, pp. 821-832.
- [22] Roberts, J.: The clean-slate approach to future Internet design: a survey of research initiatives. *annals of telecommunications - annales des télécommunications*, Volume 64, Issue 5, 2009. pp 271-276.
- [23] Banniza, T.R., Boettle, D., Klotsche, R., Schefczik, P., Soellner, M., Wuenstel, K.: A European Approach to a Clean Slate Design for the Future Internet. *Bell Labs Technical Journal - Core and Wireless Networks*, Volume 14 Issue 2, August 2009. pp. 5-22.
- [24] McKeown, N. et al.: Openflow: Enabling innovation in campus networks. In: *SIGCOMM Computer Communication Review*, vol.38, no.2, 2008, pp. 69-74.
- [25] Bashker, D., Cascio, W., Boudreau, J.: *How to Apply HR Financial Strategies* (Collection), Addison Wesley. Chapter 1, August 2013, ISBN 9780133743173. pp. 6-10.
- [26] Barroso, L. A., Clidaras, J., Hölzle, U.: *The Datacenter as a Computer: An Introduction to the Design of Warehouse-Scale Machines - Second Edition*. Morgan & Claypool. Chapter 6., pp. 69-71, 2013, ISBN 9781627050104.
- [27] Tits, Y.: Lack of standardization concerning interfaces between network equipments. In: *Electricity Distribution (CIRED 2013)*, 22nd International Conference and Exhibition on, IET, 2013, pp. 1-4.
- [28] McKeown, N., Girod, B.: *Clean-Slate Design for the Internet A Research Program at Stanford University*. White paper Version 2.0, 18 April 2006.

Obsah

1	Úvod	8
2	Evolúcia architektúry NGN ku architektúram sietí budúcnosti	9
2.1	Koncepcie a architektúry NGN	10
2.2	Vrstvy koncepčného modelu	12
3	Softvérovo definované vytváranie sietí (SDN)	13
3.1	Úvod do SDN	13
3.2	Oddelenie rovín riadenia siete a presmerovania dát.....	15
3.3	Centralizované riadenie a programovateľnosť siete.....	17
3.4	Porovnanie sietí s distribuovanou rovinou riadenia s tradičnými sieťami	18
3.5	Protokoly SDN	20
4	Virtualizácia sieťových funkcií (NFV)	24
4.1	Čo umožňuje NFV?.....	26
4.2	Požiadavky na NFV.....	27
4.3	Architektúra NFV	28
4.4	Infraštruktúra NFV - NFVI	29
4.5	Riadenie a vzájomná koordinácia NFV (MANO).....	30
4.6	Softvérová architektúra – funkcie virtualizovanej siete (VNF)	31
4.7	Prípady použitia NFV	32
5	Internet budúcnosti	34
5.1	Limity Internetu.....	35
5.2	Charakteristiky nového Internetu	37
5.3	Redizajn internetových technológií.....	38

1 Úvod

Novou témou v oblasti informačných a komunikačných technológií je ďalšia evolúcia technológií sietí budúcej generácie **NGN** (*Next Generation Networks*) smerom k sieťam budúcnosti. Je tam niekoľko aspektov, ktoré ovplyvňujú aktuálnu architektúru NGN založenú na IMS pri zlepšovaní ďalších funkcionalít pre nasledujúcu generáciu multimediálnych služieb. Prudký vývoj internetových služieb a služieb doručovania obsahu po heterogénnych sieťach zmenil požiadavky z rôznych aspektov, takých ako ďalšie funkcionality, mobilita, vizualizácia a zdieľanie zdrojov, bezpečnosť, zjednodušenie architektúry a pružnosti v modeloch riadenia s uvedením si kontextu.

Pokračujúce diskusie o zmenách architektúr Internetu (Internetu budúcnosti) a tiež v oblasti telekomunikácií pre siete budúcnosti (**FN**, *Future Networks*) sú zaradené do výskumných projektov ako aj štandardizácie (ITU-T, ETSI).

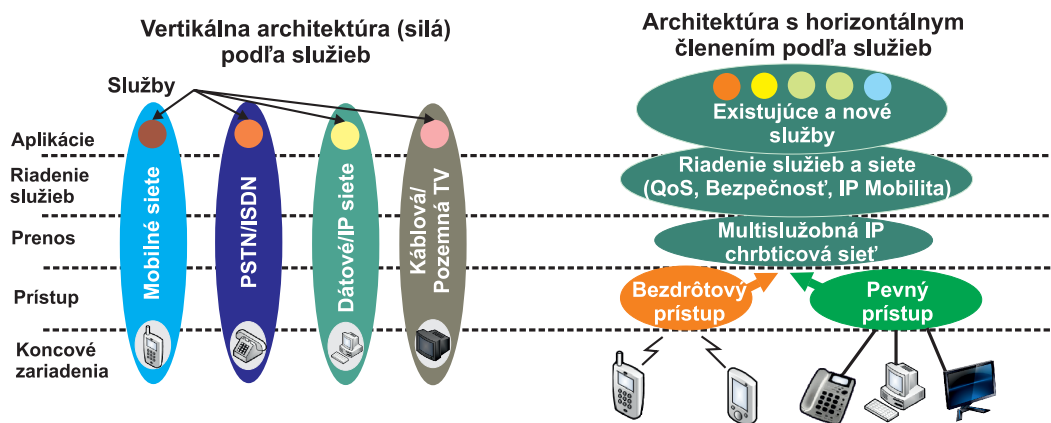
2 Evolúcia architektúry NGN ku architektúram sietí budúcnosti

Boli identifikované dva hlavné smery potenciálneho vývoja:

1. Úplná zmena postoja alebo revolučný princíp – Internet budúcnosti, ktorého nová architektúra a protokoly musia byť nanovo definované a navrhnuté (nové scenáre sietí, modely nových protokolov a testovania typov revolučnej architektúry), [1]. Revolučný skok je predpokladaný, ak by bol Internet navrhnutý úplnou zmenou postoja, s novými technológiami, bez obmedzovania súčasnými koncepciami.
2. Evolučný koncept, ktorý rozšíri súčasné architektúry NGN pomocou nových požiadaviek a funkcií, ktoré vedú ku koncepcii nazývanej sieť budúcnosti [1], [2]. Evolúcia NGN môže dosiahnuť predpokladané schopnosti sietí budúcnosti použitím existujúcich protokolov a schopností NGN (aktivovaných práve potrebným zlepšením architektúry a mechanizmov).

Druhý koncept je realistickejší postup smerom k sieťam budúcnosti z hľadiska migrácie, nakoľko siete NGN a technológie sú už dostupné.

Je vhodné posúdiť evolúciu a naznačiť budúce trendy NGN a tiež základné problémy, ktoré je nutné riešiť. Migračné scenáre pre rôzne typy sieťových platforiem sú založené na myšlienke integrovania platforiem TDM a IP do jednej konvergovanej platformy NGN (z hľadiska sieťovej infraštruktúry ako aj služieb). Nové koncepty a architektúry novej generácie ICT založené na konvergovaných ICT a NGN ponúkajú prevádzkovateľom nové možnosti na zavedenie a poskytovanie širokého spektra multimediálnych služieb a aplikácií.



Obr. 1 – Od vertikálnych štruktúr k horizontálnej architektúre NGN [1]



Preto prevádzkovatelia môžu prejsť od vertikálnej štruktúry architektúry, ktorá má pre každý typ služby určený prístup, prenos, riadenie a aplikačnú infraštruktúru na horizontálne orientovanú architektúru nezávislejšiu od poskytovaných služieb (Obr. 1).

2.1 Konceptie a architektúry NGN

Základné princípy sietí NGN boli formulované, keď vznikla samotná predstava NGN. Nasledujúce dve definície od ETSI a ITU-T popisujú podstatu NGN.




$E=m \cdot c^2$

ETSI popisuje NGN ako koncept na definovanie a vytvorenie sietí umožňujúcich formálnu distribúciu funkcionalít do samostatných vrstiev a rovín použitím otvorených rozhraní. Koncept NGN poskytuje nové podmienky na vytvorenie, implementáciu a efektívne manažovanie inovatívnych služieb.

ITU-T popisuje NGN ako sieť založenú na prenose paketov, umožňujúcu poskytovanie služieb a schopnú používať niekoľko širokopásmových prenosových technológií, umožňujúcich garantovanie QoS. Funkcie súvisiace so službami však nezávisia od základných prenosových technológií. NGN poskytuje používateľovi neobmedzený prístup k rôznym poskytovateľom služieb. Podporuje celkovú mobilitu používateľov v prípade konzistentnosti a dostupnosti služieb.

Toto hovoria definície, ale pravdepodobné výhody NGN sú dôležitejšie. Za zmienku stoja niektoré požiadavky na NGN, ktorým musia tieto siete vyhovovať:

- vysokokapacitný paketový prenos v prenosovej infraštruktúre,
- separovanie manažovacích funkcií od prenosových zariadení,
- separovanie poskytovania služby od siete,
- podpora veľkého rozsahu služieb a aplikácií,
- širokopásmovosť, kým je v súlade s požiadavkami na kvalitu služby **QoS** (*Quality of Service*),
- rôzne typy mobility (používatelia, koncové zariadenia, služby),
- rôzne schémy identifikácie a adresovania,
- konvergované služby medzi pevnými a mobilnými sieťami (ako aj konvergencia pre hlas, dáta a video),
- zhoda s regulačnými požiadavkami, ako aj s tiesňovými a bezpečnostnými požiadavkami,
- lacnejšie a efektívnejšie technológie.

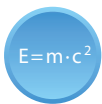


V rámci koncepcie NGN štandardizačné inštitúcie riešili nasledujúce otázky a problémy:

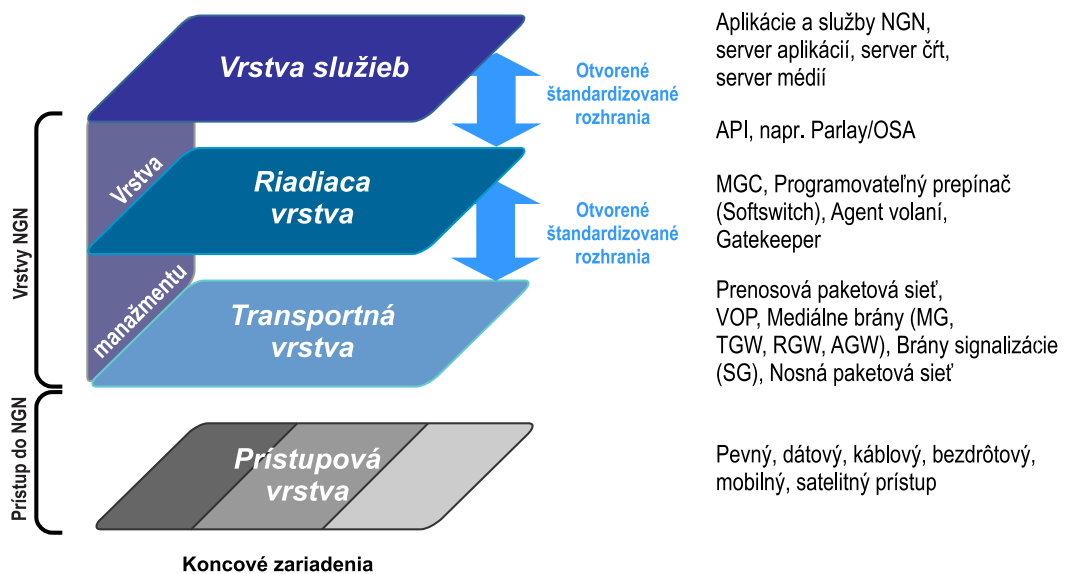
- migrácia existujúcich sietí do NGN,
- vývoj v oblasti prístupových technológií,
- pripojenie iných sietí k IP sieťam,

- poskytovanie služieb a vývoj nových,
- prepojenie systémov v oblasti adresovania,
- prepojenie signalizačných systémov,
- roaming a mobilita.

Existuje veľa koncepčných modelov a referenčných architektúr pre obidve konvergované siete a architektúry VoIP. Preto sme sa pokúsili nájsť spoločné rysy a definovať použiteľný koncepčný model NGN. Cieľom koncepčného modelu je určiť funkčné vrstvy (pokrývajúce jednoduché funkčnosti), ich entity, referenčné body (rozhrania) a informačné toky medzi nimi. Taký model potom môže ľahšie mapovať fyzickú referenčnú architektúru a jej nezávislosť od fyzických entít, teda zložiek architektúry.



Vo veľkom počte analyzovaných prípadov sú vrstvy koncepčného modelu NGN z hľadiska funkčností rozdelené na nezávislé časti nasledovne (Obr. 2): prístup (niektoré referenčné architektúry ho nezahŕňajú priamo do modelu NGN alebo ho premiestňujú pri adaptácii), odosielanie (prenos, prepínanie), riadenie (volanie/riadenie relácie) a aplikácia (služby).



Obr. 2 – Koncepčný model NGN a jeho funkčné vrstvy

2.2 Vrstvy koncepčného modelu



Prístupová vrstva predstavuje infraštruktúru, napríklad prístupovú sieť medzi koncovým účastníkom a transportnou sieťou.

Transportná vrstva zabezpečuje prenos medzi jednotlivými uzlami (bodmi) siete.

Riadiaca vrstva zahŕňa riadenie služieb a sieťových prvkov. Táto vrstva je zodpovedná za nastavenie/vytvorenie, riadenie a zrušenie multimediálnej relácie.

Vrstva služieb ponúka základné funkcie služieb, ktoré môžu byť použité na vytvorenie komplexnejších a dômyselnejších služieb a aplikácií.

U NGN sa vyžaduje, aby riadenie siete nebolo determinované len pre aplikácie koncového zariadenia, ale inteligencia siete musí uskutočňovať riadenie celej siete na všetkých úrovniach referenčného modelu. Referenčný model sieťového manažmentu naznačuje nasledujúce **úlohy pre inteligenciu siete**, ktorá má zabezpečiť:

- Manažment zdrojov (kapacita, porty a fyzické prvky), QoS od prístupu po sieť a v transportnej sieti, ak je to potrebné.
- Spracovanie rôznych médií, kódovanie, prenos dát (informačné toky).
- Manažment volaní a pripojení.
- Manažment a vzájomnú spoluprácu všetkých prvkov referenčnej architektúry.
- Riadenie služieb.

Koncepcia NGN a architektúry sú detailnejšie popísané v [3], [4].

Toto sú niektoré koncepcie a evolučné trendy smerujúce k novým architektúram sietí, ktoré budú schopné poskytnúť široké spektrum/portfólio nových multimediálnych služieb/multimediálneho obsahu.

Nové architektúry sietí založené na „softvérovo definovanom vytváraní sietí“ a „virtualizácii sieťových funkcií“ sú uvedené a popísané v kapitole 3 a 4, respektíve na koncepcii „Internet budúcnosti“ v kapitole 5 tohto výučbového modulu.

3 Softvérovo definované vytváranie sietí (SDN)

3.1 Úvod do SDN

$E=m \cdot c^2$

SDN (*Software Defined Networking*) je nový prístup k architektúre siete ICT so zameraním na programové riadenie celej siete.

To umožňuje riešiť mnohé problémy tradičných prístupov pri vytváraní sietí, ale ponúka aj nové prístupy. Vo všeobecnosti myšlienka SDN môže zvýšiť pružnosť, manažovateľnosť a rozširiteľnosť ICT sietí. Ďalším zámerom je zníženie nákladov na zariadenia. Môže to byť dosiahnuté využitím výhod rýchleho vývoja a cyklu rozmiestnenia relatívne lacných softvérových aplikácií na rozdiel od drahého špecializovaného sieťového hardvéru.

Hlavná motivácia pre SDN vznikla na začiatku z potreby nájsť lepšie riešenie pre inováciu pri výskume a vývoji sietí. Vtedy boli k dispozícii len dve použiteľné metódy testovania nových funkcií – softvérová simulácia alebo hardvérová skúšobňa (testovacia platforma).

+

Simulácia ponúka vysokú pružnosť a opakovateľnosť.

-

Naviac, simulácie nemusia bežať v reálnom čase - paralelne s tvorbou kódu a nie je ťažké pripojiť simulovanú sieť k reálnej sieti a testovať koexistenciu nových vlastností v realistickejšom prostredí. V porovnaní s tým je implementovanie hardvérovej testovacej platformy do používateľského hardvéru náročné na programovanie, môže byť obtiažne modifikovať nejaké nastavenie a je to veľmi nákladné.

To môže viesť ku kompromisom – buď sa použije zdieľaná hardvérová skúšobňa pre viac výskumných projektov, čo však limituje čas dostupný na experimenty a opakovateľnosť. Alebo sa alternatívne vytvorí vlastná testovacia platforma použitím sieťových prvkov dostupných zo zariadení prevádzkovateľov. Tieto sú väčšinou dodávané ako čierna skrinka s minimálnou úpravou podľa zákazníka, obmedzujú možnosti testovacej platformy pre nové a exotickéjšie experimenty požadované skôr pri revolučných ako evolučných inováciách.

Koncom 90-tych a začiatkom roku 2000 sa výpočtový výkon univerzálnych počítačov výrazne zvýšil v porovnaní so špecializovaným hardvérom na vytváranie sietí. Toto spolu s pokrokmí vo virtualizácii a niektorých ďalších technológiách bolo možné využiť na softvérovo realizované riadenie jednoduchých uzlov siete pri rýchlom prepínaní paketov. Riadiaci softvér môže byť modifikovaný pohodlne pomocou simulácie, kým lacný hardvér s limitovanými vyššími úrovňami vlastností, používaný na prepínanie paketov poskytuje pri spracovaní paketov rýchlosti porovnateľné so špecializovanými hardvérovými testovacími

platformami. Toto bolo jedným zo základných pilierov SDN, ktorý viedol k oddeleniu rovín riadenia a presmerovania, ktoré je popísané v nasledujúcej časti detailnejšie [5].

3.2 Oddelenie rovín riadenia siete a presmerovania dát

Predtým ako popíšeme koncept SDN bude vhodné definovať, čo je rovina riadenia a rovina presmerovania dát.

$E=m \cdot c^2$

V mnohých smerovačoch (alebo v sieťových zariadeniach pre tento účel) je špecializovaný hardvér na rýchle prepínanie dát medzi rozhraniami – rovina presmerovania dát. Presmerovanie je riadené podľa pravidiel vytváraných procesorom bežného operačného systému, smerovacími algoritmami, prekladačom adres a ďalšími vyššími funkciami – toto je rovina riadenia.

i

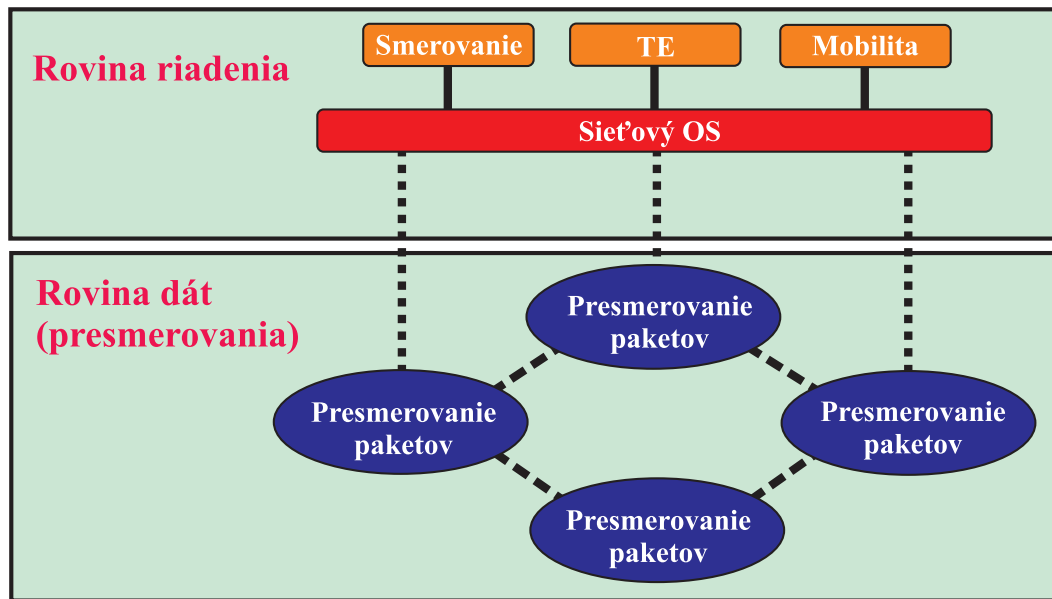
Pri tradičnom vytváraní sietí je rovina riadenia aj rovina presmerovania implementovaná do každého sieťového uzla. To umožňuje, aby boli všetky zariadenia úplne autonómne a vykonávali všetky rozhodnutia vysokej úrovne, také ako je smerovanie paketov, nezávisle.

Toto má svoj pôvod z Internetu ARPANET, pôvodne navrhnutého pre armádu, pričom primárnym cieľom bola vysoká pružnosť a schopnosť prežitia. Pružnosť, otvorenosť pre modifikácie alebo prevzatie nových vlastností bol nanajvyšš druhoradý cieľ.

Základným princípom SDN je oddelenie roviny riadenia a roviny presmerovania dát v sieti, ako je znázornené na obr. 3. Pri implementovaní samostatnej roviny riadenia a softvéru pre univerzálny počítač z roviny presmerovania sieťového zariadenia je možné centralizovať rozhodovanie pri smerovaní a prepínaní, ako aj konfiguráciu všetkých zariadení siete.

+

Centralizovaná rovina riadenia implementovaná do softvéru, vytvorená na univerzálnych procesoroch, môže priniesť pri budovaní siete veľa výhod – špeciálne zrýchlenie inovácií, vývoj nových vlastností siete a rozmiestnenia.



Obr. 3 – Základná architektúra SDN

3.3 Centralizované riadenie a programovateľnosť siete

V moderných sieťových zariadeniach rovina riadenia zbiera informácie o stave susedných pripojení a siete ako celku a poskytuje ich smerovacím algoritmom. Distribuované algoritmy zabezpečujú automaticky riešenie na smerovanie sieťovej prevádzky, ale ich nedostatkom je možný problém s konvergenciou. Keďže každé zariadenie zbiera informácie o sieti a rozhodujú o smerovaní samostatne, oneskorenie prenosu informácií o zmenách siete môže spôsobiť problémy pri prevádzke siete.



Vypustenie roviny riadenia z každého uzla siete a použitie centralizovanej roviny riadenia umožní nielen kompletný pohľad na sieť bez problémov s konvergenciou, ktoré sú pre distribuované algoritmy prirodzené, ale zníži aj náklady. Navyše, bez potreby rozloženého smerovania prevádzky je možné nové algoritmy použiť, modifikovať a zdokonaľovať. Okrem toho konfigurovanie centrálnej roviny riadenia robí riadenie siete jednoduchším. Zredukuje možnosť nesprávnej konfigurácie a urýchľuje tiež hľadanie problémov. Prídavnou výhodou implementovania softvéru v centralizovanej rovine riadenia je ľahká modifikácia a vývoj nových vlastností. Jej odstránenie vyžaduje samostatné konfigurovanie každého uzla.



Oponenti SDN a centralizovanej roviny riadenia zvlášť však poukazujú na obmedzenia pri jej použití v rozľahlých sieťach, takých ako Internet. Ich kritizmus sa sústreďuje na riadiacu jednotku, ktorá je jediným bodom spôsobujúcim výpadok celej siete a nedostatočnú škálovateľnosť.

Riešenie týchto problémov je použitie logicky centralizovanej ale fyzicky distribuovanej roviny riadenia kedy niekoľko riadiacich jednotiek riadi časť siete a komunikuje navzájom, aby sa znížilo oneskorenie roviny riadenia, poskytuje vysokú dostupnosť a jeden bod logického riadenia na správu siete. Nová architektúra pre spojenie medzi doménami s priradeným protokolom pre riadiace jednotky SDN je navrhnutá v [6].

3.4 Porovnanie sietí s distribuovanou rovinou riadenia s tradičnými sieťami

Do zariadenia tradičnej siete je začlenená rovina riadenia, sieťové aplikácie a ďalšie vybavenie vyššej úrovne v zariadeniach firmvéru. Tieto prostriedky všetkých sieťových uzlov robia rozhodnutia o smerovaní lokálne – efektívne využívajú celú distribuovanú rovinu riadenia, ako je to znázornené na obr. 4. Toto môže byť protikladom voči centralizovanej rovine riadenia v architektúre SDN uvedenej na obr. 3.



Integrovanie viacerých funkcií poskytuje vyššiu funkčnosť každého uzla a robí ho nezávislejším a takmer vylučuje zlyhanie jedného bodu.

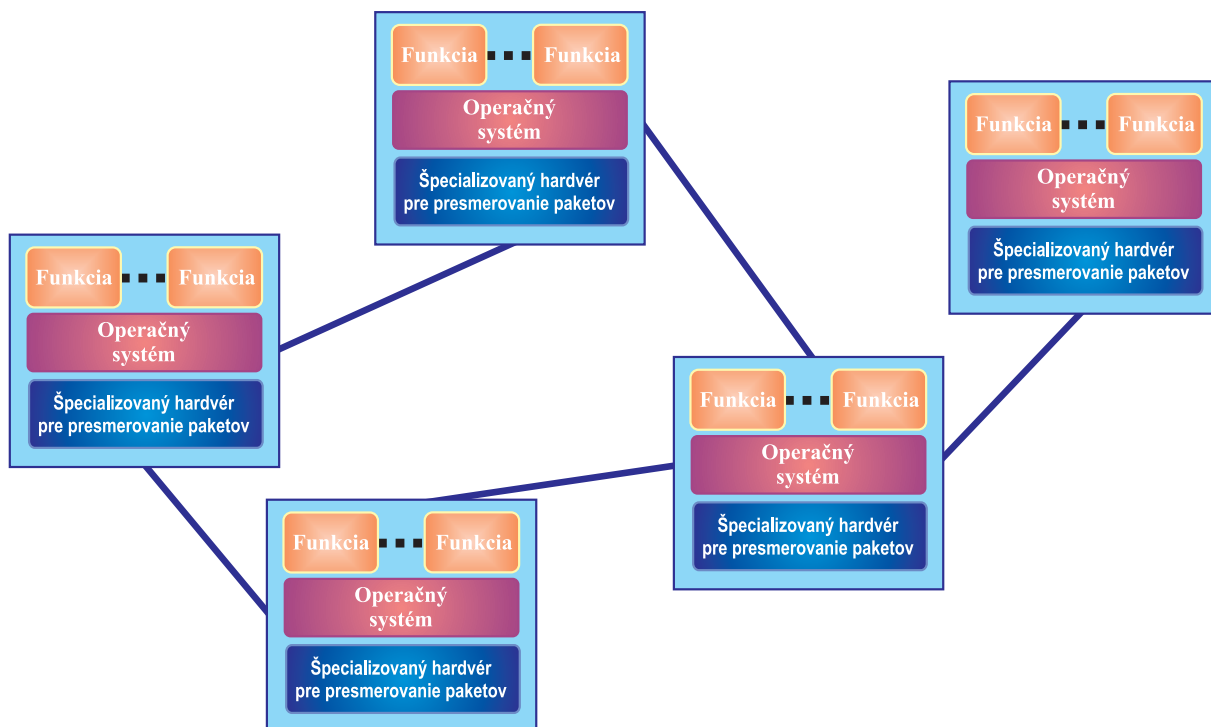


To sa ale dosahuje za cenu zvýšenej zložitosti. Súvisí to s drahším zariadením, vyšším príkonom a môže to viesť k oneskoreniam pri ovládaní prevádzky, nakoľko to vyžaduje jej spracovanie rôznymi aplikáciami. Okrem toho konfigurácia alebo modifikácia siete vyžaduje manuálnu konfiguráciu mnohých zariadení a často použitie zložitých príručiek na riadenie. Riadenie siete je navyše komplikované pri implementácii a konfigurácii rozdielností medzi jednotlivými dodávateľmi. Spôsobuje problémy z hľadiska stykovej prevádzkyschopnosti.

Ako je uvedené v [7], celá táto zložitosť vedie k statickým sieťam, čo je v protiklade s požiadavkou na dynamické prostredie s väčšou mobilitou používateľa a virtualizáciou servera. Nezrovnalosti medzi stratégiami rozľahlých sietí a obmedzenou škálovateľnosťou sietí sú ďalšími javmi tradičných sieťových komplikácií vo veľkých sieťach.



Centralizovaná rovina riadenia u SDN umožňuje správcovi siete spracovávať prevádzku bez nutnosti manuálne konfigurovať veľa zariadení a tým uľahčuje riadenie siete a zvyšuje pružnosť.



Obr. 4 – Tradičná architektúra paketovej siete [8]



Hoci sa MPLS na prvý pohľad podobá SDN s rýchlym prepínaním prevádzkových tokov zavedeným v rovine riadenia, pracuje odlišným spôsobom. Nie je to centralizovaná rovina riadenia, ktorá je v každom smerovači MPLS s každým LER schopným vytvoriť cestu a distribuovať tok použitím protokolu distribúcie návěstí **LDP** (*Label Distribution Protocol*).

3.5 Protokoly SDN

Oddelenie roviny riadenia a presmerovania dát, čo je jedným z hlavných pilierov SDN spolu s centralizáciou prostriedkov roviny riadenia, vyžaduje komunikačný protokol. V tejto sekcii uvádzame niektoré z nich a začíname s najpopulárnejším – OpenFlow.

OpenFlow

OpenFlow je otvorený štandard pôvodne vyvinutý na univerzitách a aktuálne udržiavaný Nadáciou pre otvorenú sieť ONF (*Open Network Foundation*) [9] – neziskovým konzorciom s úlohou komercializovať a podporovať SDN založené na OpenFlow. ONF bol okázalo úspešný s OpenFlow, ktorý sa stal najpopulárnejším protokolom používaným na komunikáciu medzi rovinou riadenia a rovinou presmerovania dát a v súčasnosti predstavuje fakticky štandard. Táto kampaň ONF viedla však k nedorozumeniu, že OpenFlow je vlastne SDN.



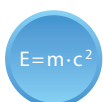
Napriek existujúcim softvérovo založeným riešeniam prepínania dovoľuje skúmať nové metódy a protokoly vytvárania sietí, nemôže však poskytnúť dostatočný výpočtový výkon a/alebo hustotu portov na rozsiahle škálovacie experimenty.

Najjednoduchším príkladom sú mnohé otvorené softvéry, založené na implementovaní protokolov smerovania alebo prepínania, bežiacie na univerzálnych počítačoch s niekoľkými sieťovými rozhraniami. Na druhom konci spektra sú hardvérovo založené riešenia výskumu vytvárania sietí ako je NetFPGA, využívajúce špecializovanú kartu FPGA schopnú spracovávať prevádzku linkovou rýchlosťou.



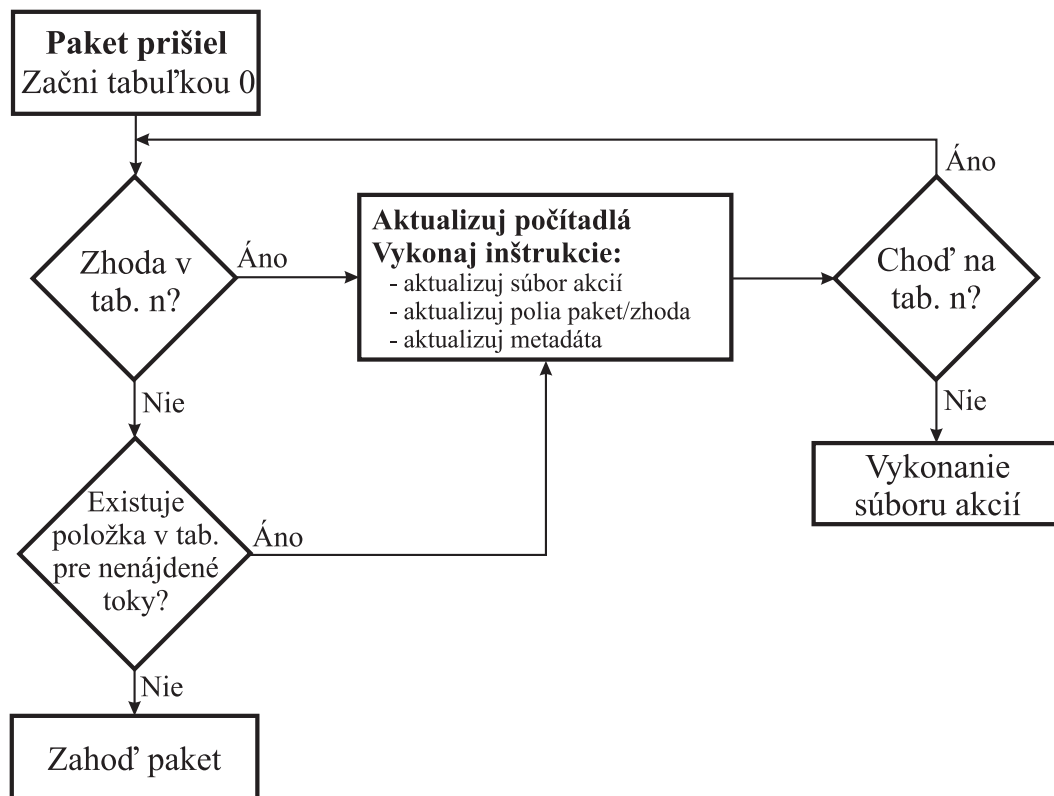
NetFPGA sa používa hlavne v akademickej obci na rýchle posúdenie prototypov, nakoľko je limitovaná len 4 portami na jednu kartu.

Ako bolo uvedené v [10] toto je limitujúci faktor pre vysokoškolských výskumníkov vytvárania sietí, pri kompromise OpenFlow medzi všeobecne nízkou výkonnosťou, nezávislosťou výskumných riešení, uzavretým a nie veľmi modifikovateľným zariadením od komerčných dodávateľov.



Protokol OpenFlow definuje komunikačné rozhranie medzi zariadeniami roviny riadenia a roviny presmerovania a preto musí byť implementovaný na oboch stranách. Pretože OpenFlow poskytuje mimoriadne granulované riadenie na úrovni tokov, umožňuje sieti reagovať na zmeny spojené s topológiou, aplikáciami alebo používateľmi v reálnom čase.

Biela kniha ONF [9] uvádza, že riešenia smerovania v klasickej sieti v súčasnosti nemôžu podporovať riadenie na takejto úrovni granularity.



Obr. 5 – Vývojový diagram spracovania paketov v logickom prepínači OpenFlow [11]

Keď je paket prijatý prepínačom podporujúcim OpenFlow, je spracovaný reťazcom OpenFlow zloženým z jednej alebo niekoľkých tabuliek tokov. Tabuľky obsahujú vstupy s pravidlami a akciami, ktoré má vykonať s paketom patriacim do toku. Ak sa nenájde zhoda pre paket v žiadnej tabuľke toku a pravidlo na odoslanie takéhoto paketu do riadiacej jednotky existuje, je odoslaný do riadiacej jednotky. Riadiaca jednotka spracuje paket a buď pripojí paket alebo zriadi nový tok vytvorením nového vstupu v tabuľke tokov. Mechanizmus spracovania prijatého paketu v prepínači OpenFlow je zobrazený na obr. 5.

ForCES

$E=m \cdot c^2$

Protokol oddeľovania presmerovacích a riadiacich prvkov **ForCES** (*Forwarding and Control Element Separation*) [12] definuje architektúru štruktúry a priradené protokoly na štandardizovanú výmenu informácií medzi rovinou riadenia a rovinou presmerovania v sieťovom prvku ForCES.

ForCES oslovuje hlavne otvorený API/protokol, ktorý poskytuje jasné oddelenie riadiacej a presmerovacej roviny.

+

Hlavnou prednosťou ForCES je jeho model prepínacieho prvku, ktorý umožňuje popísanie novej funkčnosti roviny presmerovania bez zmeny protokolu medzi rovinami riadenia a presmerovania.

Vývoj ForCES je zameraný na rozloženie sieťového prvku jednoznačne do rovín riadenia a presmerovania. Motiváciou pre to bola snaha vytvoriť rovinu presmerovania sieťovými prvkami z flexibilných hardvérových komponentov nezávisle od roviny riadenia. Výsledkom ForCES bolo vytvorenie novej architektúry pre sieťové prvky, hoci výhľadovým cieľom bolo vytvoriť novú architektúru siete.

NETCONF

$E=m \cdot c^2$

NETCONF je protokol riadenia siete, ktorý poskytuje mechanizmy na diaľkové inštalovanie, spravovanie a vymazanie konfigurácie sieťových prvkov.

Samotný protokol NETCONF je rozdelený na štyri vrstvy so súborom operácií základného protokolu s použitím metód procedúry diaľkového volania **RPC** (*Remote Procedure Call*) s parametrami správ zakódovanými podľa XML.

Jednou z predností NETCONF je to, že poskytuje programovateľné rozhranie do zariadenia, ktoré presne sleduje funkčnosti pôvodného rozhrania.

+

Hoci bol pôvodne vyvinutý ako nástupca protokolu SNMP a niektorých protokolov CLI na konfigurovanie sieťových prvkov, schopnosti NETCONF môžu byť použité na vytvorenie formy hybridnej SDN. Navyše je podpora NETCONF požiadavkou pre sieťové prvky, aby boli kompatibilné s OF-CONFIG, časťou špecifikácie OpenFlow.

PCE-P

$E=m \cdot c^2$

Výpočtový prvok trasy PCE (*Path Computational Element*) je entita, ktorá vypočítava trasy pre uzly v sieti, môže nájsť optimálne trasy pre prevádzku MPLS, GMPLS P2P a P2MP, riadenú **návestím prepínanými trasami LSPs** (*label switched paths*).

PCE potom oznámi túto trasu sieťovým uzlom použitím komunikačného protokolu PCE. Takto je možné PCE chápať ako rozšírenie schopností MPLS a GMPLS TE a znižovanie rozdielov medzi SDN a štandardnými MPLS/GMPLS.

Hoci samotný PCE nebol primárne vyvinutý ako technológia umožňujúca SDN, môže poskytnúť model logicky centralizovaného riadenia pre súčasné technológie s niekoľkými doplnkovými zlepšeniami.

Rozhranie k systému smerovania

Rozhranie k systému smerovania I2RS (*Interface to the Routing System*) je jeden z viacerých ambiciózných prístupov k SDN, ktorý je v počiatočných štádiách. Bol vyvinutý pri IETF. I2RS je obojsmerné programovateľné rozhranie na komunikáciu medzi smerovacím systémom a aplikáciami. Umožňuje monitorovanie siete, rezervovanie zdrojov a modifikovanie konfigurácie smerovania. I2RS sa týka

komunikácie do a zo smerovacieho systému a nie je určené na to, aby priamo poskytovalo rozhranie pre rovinu presmerovania. Využíva existujúce mechanizmy na distribuovanie vybratých ciest do roviny presmerovania.

Cisco ONE

Aj keď je Cisco členom nadácie ONF a aktívne sa podieľa na vývoji OpenFlow, SDN nie je jediný projekt, na ktorom pracuje. Jednou z jeho vlastných alternatív je **Prostredie otvorenej siete ONE - *Open Network Environment*** (Cisco **ONE**), ktoré poskytuje programovateľné rozhranie na priame riadenie zariadení Cisco. Kľúčovým komponentom Cisco ONE je Súprava platformy ONE - *ONE Platform Kit (onePK)*. Súčasťou súpravy je niekoľko platform API umožňujúcich jednoduchý vývoj sieťových aplikácií využitím priameho prístupu k zariadeniam vytvárajúcim sieť prostredníctvom vrstvy abstrahovania siete.

Nuage



V apríli 2013 Alcatel-Lucent otvoril dcérsku spoločnosť Nuage Networks, zameranú na vytváranie riešení SDN založených na jej skoršom Application Fluent Network (Sieť plynulých aplikácií), ale s možnosťou využiť alternatívne nové technológie. Produktom tejto snahy je Nuage Virtualized Service Platform (Vizualizovaná platforma služby Nuage), softvérové riešenie zamerané na problém vizualizácie siete v dátových centrách a u prevádzkovateľov kladovej služby - *Cloud Service Providers (CSPs)*. Nakoľko je Nuage VSP implementované do softvéru a používa VXLAN na zapuzdrovanie cez hypervízory, nie je funkčne závislé od špecifického typu alebo druhu prepínačov TOR.

4 Virtualizácia sieťových funkcií (NFV)

Neoddeliteľnou súčasťou telekomunikačných operátorov je vlastníctvo hardvérových zariadení. Telekomunikační operátori sa nemôžu vyhnúť nákupu nového hardvéru s rovnakou funkčnosťou a službami, keď sú tieto zariadenia potrebné na poskytovanie nových služieb. Predstavuje to veľa komplikácií spôsobených jednak zvýšením nákladov a tiež časom potrebným na ich rozmiestnenie. Je to **čas do uvedenia na trh TTM** (*time to market*) a **čas potrebný na nasadenie TTD** (*time to deploy*). Tieto komplikácie sú v súčasnosti pre telekomunikačných operátorov obmedzujúcimi činiteľmi pri poskytovaní kvality služieb.

Obr. 6 ilustruje nový prístup k architektúre siete založenej na **virtualizácii sieťových funkcií NFV** (*Network Functions Virtualization*).

$E=m \cdot c^2$

Tento prístup poskytuje sieťovým a telekomunikačným operátorom možnosť zjednotiť veľa typov sieťových zariadení do štandardných vysoko výkonných serverov, prepínačov a úložísk, ktoré môžu byť umiestnené v dátových centrách, sieťových uzloch a prevádzkových priestoroch používateľov.



Obr. 6 – Vízia virtualizácie sieťových funkcií [13]



Výhody pre sieťových a telekomunikačných operátorov:

- zníženie **investičných výdavkov CAPEX** (*capital expenditure*) a **prevádzkových nákladov** (takých ako opravy a údržba) **OPEX** (*operational expenses*) znížením ceny zariadenia a znížením spotreby energie,
 - kratší čas od nákupu potrebný na nasadenie nových sieťových služieb,
 - lepšia návratnosť investícií do nových služieb,
 - väčšia pružnosť, rozširiteľnosť alebo vyvinutie služieb,
 - možnosti skúšania a rozvinutia nových inovatívnych služieb s nižším rizikom.
-

V októbri 2012 bola zverejnená biela kniha, ktorá prezentuje prvé vydanie NFV [13]. ETSI vydal sériu rôznych požiadaviek, ktoré sú zamerané na technológiu a popisujú výhody, ktoré prináša technológia NFV a má táto technológia priniesť. Bola vytvorená **Skupina priemyselnej špecifikácie virtualizácie sieťových funkcií NFV ISG** (*Network Functions Virtualization Industry Specification Group*), ktorá má riešiť otázky súvisiace s touto novou technológiou. Táto skupina bola vytvorená pri **ETSI** (*European Telecommunications Standards Institute*). Od októbra 2012 sa skupina NFV ISG postupne zväčšuje a okolo 235 vedúcich spoločností sa zúčastnilo niekoľkých zhromaždení v Ázii, Európe a Severnej Amerike. Výstupy z prvého zhromaždenia skupiny NFV ISG mali formu dokumentov a prepojenie medzi nimi je popísané nižšie. V období od 2013 do 2015 prebiehala druhá fáza a novšie dokumenty sú dostupné priamo na webovej stránke NFV ISG.

4.1 Čo umožňuje NFV?



Ak je možné budovať siete spôsobom, ktorý predstavuje technológia NFV, vynára sa logicky otázka, prečo sieť od samotného začiatku jej zariadenia využíva proprietárny hardvér. Odpoveď je taká, že servery priemyselného štandardu s operačným systémom a softvérom len nedávno získali vysokú výkonnosť, aby boli schopné efektívne súťažiť s proprietárnymi zariadeniami, hlavne v zmysle cien, spotreby elektriny a spoľahlivosti.

Musíme špecifikovať čas „nedávno“ ako posledných štyri až päť rokov. Počas tohto obdobia sme svedkami dramatického zvýšenia priepustnosti siete a priepustnosti spracovania paketov x86 procesormi, ako aj rapídny zvyším počtu procesorových jadier na jednom fyzickom obvode priemyselného servera.

4.2 Požiadavky na NFV

Zoznam základných požiadaviek týkajúcich sa NFV [13]:

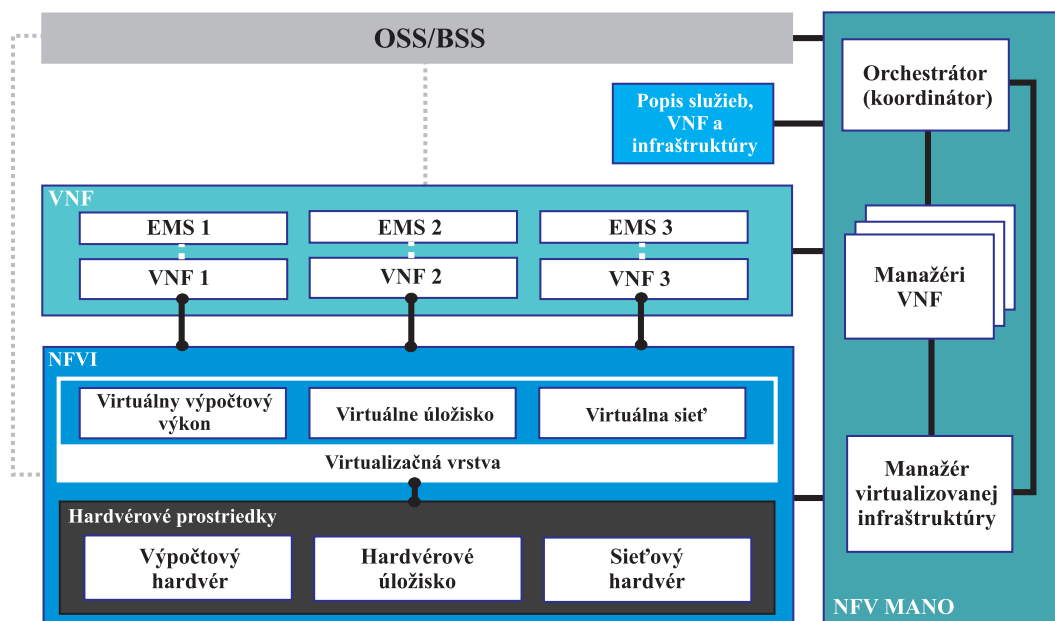
- Prenositeľnosť – vlastnosti riešenia nahrat' a spustiť meniace sa softvérové funkcie pomocou dátových centier s rôznymi štandardami.
- Výkonnosť – výkonnosť sa zameriava na funkcie softvéru.
- Riadenie a vzájomná koordinácia (orchestrácia) – mechanizmy, ktoré musia existovať na koordinovanie a riadenie životného cyklu softvérových funkcií, zdrojov, infraštruktúry a rôznych operácií, ktoré ich vytvárajú.
- Flexibilita – schopnosť poskytnúť riešenia cestou rozšíriteľnosti hardvérových zdrojov.
- Bezpečnosť – pevné proporcie, ktoré musia byť analyzované, nakoľko virtualizované prostredie môže byť objektom vonkajších útokov.
- Kontinuita služieb - funkcie, ktoré sú potrebné na kontinuálne poskytovanie služieb v súlade so špecifikáciou **dohody o úrovni služby SLA** (*Service Level Agreement*).
- Prevádzka – automatizácia prevádzkových funkcií (napr. adaptácia kapacity siete, sťahovanie aktualizácie softvéru, oprava detekovaných porúch, atď.).
- Energetická efektívnosť – pomáha minimalizovať spotrebu energie rozľahlých virtualizovaných sietí.
- Migrácia a koexistencia s existujúcimi platformami – podporuje prechod od súčasných sietí, ktoré ako nevirtualizované koexistujú s virtualizovanými bez prerušenia činnosti služieb alebo výskytu iných nežiaducich javov u používateľa.

Schopnosť diaľkového rozmiestnenia a prevádzky funkcií virtualizovanej siete na infraštruktúre NFV poskytované rôznymi poskytovateľmi služieb umožňuje príslušnú službu sprístupniť zákazníkovi celosvetovo.

4.3 Architektúra NFV

Architektúra technológie NFV bola navrhnutá v druhom vydaní bielej knihy [14] (Obr. 7) a skladá sa z nasledujúcich zložiek:

- **Infraštruktúry funkcií virtualizovanej siete NFVI** (*network functions virtualization infrastructure*) - poskytujú virtuálne zdroje potrebné na podporu implementácie funkcií virtualizovaného vytvárania sietí – komerčné hardvérové komponenty COTS, vrstvu softvéru, ktorá virtualizuje a abstrahuje základný hardvér.
- **Funkcie virtualizovanej siete VNF** (*virtualized network feature*) - softvérová implementácia sieťových funkcií schopná bežať na NFVI a môže byť doplnená o systém riadenia prvkov **EMS** (*Element Management System*), ktorý riadi VNF. VNF je entita odpovedajúca súčasnému sieťovému uzlu u ktorej sa očakáva, že bude dodaná ako čistý softvér nezávislý od hardvéru.
- **NFV MANO** (*management and orchestration* - riadenie a orchestrácia) – pokrýva vzájomné koordinovanie a riadenie životného cyklu fyzických a/alebo softvérových prostriedkov podporujúcich virtualizáciu a infraštruktúrne riadenie životného cyklu všetkých VNF. NFV MANO sa sústreďuje na úlohy riadenia virtualizácie, ktoré sú potrebné pre rámec NFV. Spolupracuje tiež s externými NFV OSS / BSS a umožňuje integráciu NFV do existujúcich sietí.



Obr. 7 - Architektúra NFV [14]

Celý systém je podporovaný súborom metadát popisujúcich funkcie (VNF) služieb NFV a infraštruktúrne požiadavky na NFV MANO pre správne riadenie. Tento popis spolu so službami, VNF a infraštruktúrou môže byť poskytnutý aj iným priemyselným výrobcom.

4.4 Infraštruktúra NFV - NFVI

Infraštruktúra NFV je rozdelená na tri domény [15]:

- Doména počítača – hlavnou úlohou je poskytnúť výpočtové a úložné zdroje. Poskytuje rozhranie do domény sieťovej infraštruktúry, ale nemôže sa pripojiť ku sieti samostatne.
- Doména hypervízora – hlavnou úlohou je sprostredkovať doméne výpočtových zdrojov spúšťanie softvéru na virtuálnych strojoch. Hypervízory majú byť vyvinuté pre potreby kladových riešení a klásť dôraz na stanovenie dostupného hardvéru, ľahko môžu dosiahnuť vysokú úroveň prenosnosti virtuálnych strojov. Hypervízor môže emulovať každý typ hardvérovej platformy a dokonca v niektorých prípadoch kompletne emulovať sadu inštrukcií tak, že virtuálny stroj si myslí, že beží na úplne rozdielnych procesorových architektúrach ako je tá reálna.
- Doména sieťovej infraštruktúry – jej úloha:
 - vytvoriť kanál komunikácie medzi viacerými **zložkami funkcií virtualizovanej siete VNFC** (*virtualized network functions components*) distribuovanej VNF (*virtualized network function*),
 - vytvoriť kanál komunikácie medzi viacerými VNF,
 - vytvoriť komunikačný kanál medzi VNF a MANO,
 - vytvoriť kanál komunikácie medzi zložkami NFVI a ich vzájomnú koordináciu a riadenie,
 - poskytnúť prostriedky diaľkového riadenia VNFC,
 - poskytnúť prostriedky spájania existujúcich operátorov sietí.

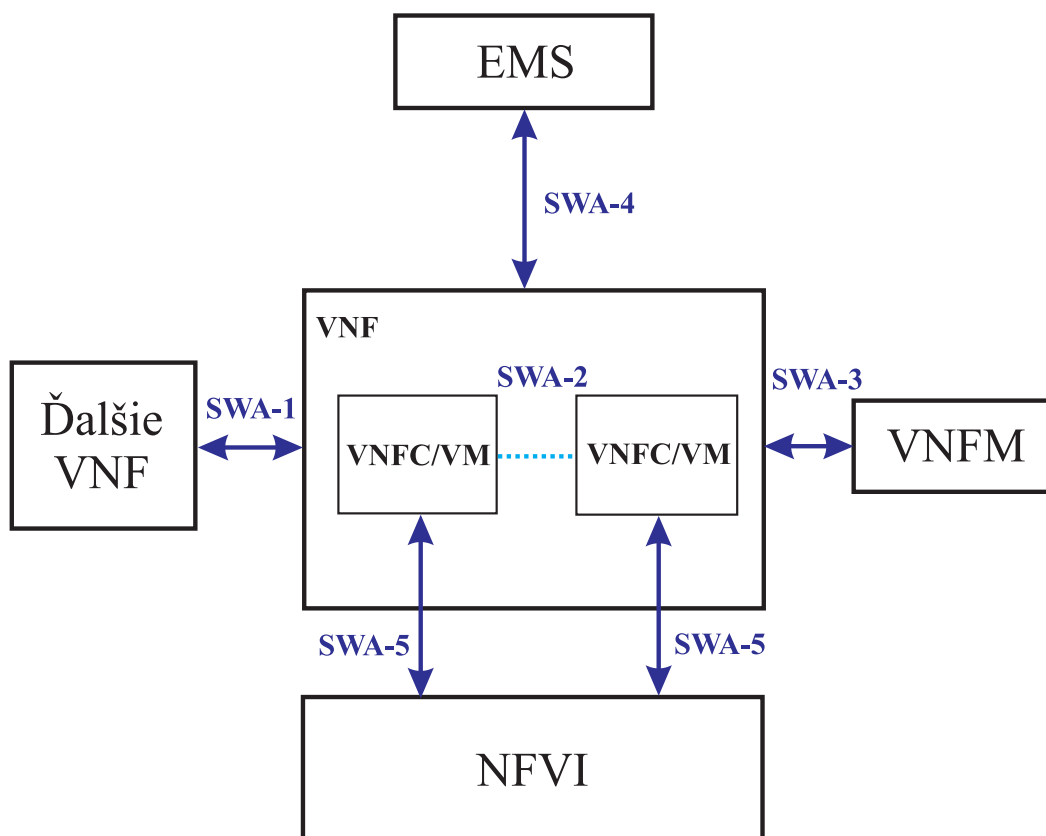
4.5 Riadenie a vzájomná koordinácia NFV (MANO)

Riadenie a vzájomná koordinácia (orchestrácia) zahŕňa tri zložky [16]:

- Koordinátor (orchestrátor) NFV – zodpovedá za koordinovanie (manažovanie) zdrojov NFVI pre viacerých manažérov virtualizovanej infraštruktúry **VIM** (*Virtualized Infrastructure Manager*), uskutočňuje funkcie koordinácie zdrojov, riadenie životného cyklu sieťových služieb (napr. prípady stratégie riadenia, rozširovanie, meranie charakteristiky, korelácia udalostí), umožňuje funkciu koordinácie pre sieťové služby, celkové riadenie prostriedkov, potvrdenie a schválenie zdrojov NFVI aplikácií.
- Manažér VNF – zodpovedá za riadenie životného cyklu prípadov VNF (môže byť pridelený na riadenie jedného prípadu a môže tiež riadiť viac prípadov rovnakého alebo rôzneho typu), celkovú koordináciu a adaptáciu konfigurácií a ohlasovanie udalostí medzi NFVI a E/NMS.
- Manažér virtualizovanej infraštruktúry VIM - zodpovedá za riadenie a manažment výpočtu NFVI, pamäťové a sieťové zariadenia v infraštruktúre poddomén jedného operátora, zbieranie a prenos meraní charakteristík a udalostí.

4.6 Softvérová architektúra – funkcie virtualizovanej siete (VNF)

Funkcia virtualizovanej siete je sieťová funkcia, ktorú je možné poskytovať v infraštruktúre NFV (NFVI) a je riadená *orchestrátorom NFV (NFVO)* a manažérom VNF. Interná architektúra VNF je znázornená na obr. 8.



Obr. 8 - Architektúra NFV [17]

Táto architektúra zabezpečuje kvalitu pripojení použitím rozhraní:

- Rozhranie SWA-1 – cez toto rozhranie niekoľko VNF komunikuje navzájom, používajú ho na to, aby riešili úlohy pre celú sieť.
- Rozhranie SWA-2 – tieto zložky rozhrania využíva, keď sú pripojené VNF, každá zložka má nejakú úlohu pri spracovaní virtualizovaných sieťových funkcií.
- Rozhranie SWA-3 – toto rozhranie je pripojené k manažérovi VNF.
- Rozhranie SWA-4 – toto rozhranie sa využíva, keď je pripojené k VNF (EMS).
- Rozhranie SWA-5 – pripája NFVI ku každému VNFC.

4.7 Prípady použitia NFV



NFV na jednej strane ponúka veľa výhod: zjednodušenie, inovatívne prístupy pri vytváraní sietí. Na druhej strane poskytuje neohraničené množstvo prípadov použitia, ktoré sú viac alebo menej užitočné v reálnej prevádzke siete.

Napriek tomu aktuálne môžeme povedať, že NFV nie je úplne samostatné funkčné riešenie, hoci organizácia ETSI vyvíja sústavne snahy na vytvorenie silne unifikovaného štandardu NFV. NFV je myšlienka ako profitovať z virtualizácie. Takýto prístup bude vyžadovať zabezpečenie funkčnosti siete a tiež toho, ako to všetko riadiť a koordinovať.



Webový portál SDxCentral každoročne uverejňuje súhrnnú správu nazývanú Správa o virtualizácii sieťových funkcií (Network Functions Virtualization Report) [18], ktorá obsahuje hlavné myšlienky NFV, jej vývoj a prehľad predajcov dodávajúcich riešenia NFV ako aj najprospešnejšie prípady použitia uvedené nižšie.

Virtualizované sieťové funkcie

V súčasnosti dobre fungujúci klaud už ponúka veľa možností ako ľahko, pružne a rýchlo distribuovať alebo vyvíjať aplikácie, infraštruktúru alebo platformy. Virtualizované sieťové funkcie sú prispôbené na plné rešpektovanie už existujúcich metód v oblasti klaudov. Pre prevádzkovateľov klaudovej služby je najpríťažlivejšie poskytovanie virtuálneho smerovania, virtuálnej privátnej siete (VPN), služby na zrýchlenie vrstvy 4 – 7 a bezpečnostné služby, umožnenie ich pripojenia, škálovania a ochrany ich aplikácií založených na klaude.

Virtualizovaná/klaudivá rádiová prístupová sieť

Tento prípad použitia je dôležitý hlavne pre poskytovateľov mobilnej služby, ktorí hľadajú cesty na zjednodušenie a zrýchlenie vytvárania nových rádiových prístupových sietí **RAN** (*radio access networks*), nakoľko ovplyvňujú náklady. Množstvo funkčností, ktoré bežia na proprietárnom hardvéri umiestnenom v základňovej stanici je možné presunúť do virtuálneho stroja alebo sady virtuálnych strojov, ktoré môžu operovať lokálne v serveroch COTS ako zoskupenie alebo ako klaud.

Virtualizované mobilné jadro

Mobilní operátori sú často konfrontovaní úlohami aktualizácie ich sietí, služieb a tiež rozšírenia ich služieb do vidieckych oblastí, ktoré sú ťažko dosiahnuteľné. Použitie spočíva v prevzatí funkcií od zákaznickeho hardvéru do mobilného jadra a ich nasadenie do serverov COTS v klaudovom prostredí. Mobilní operátori chcú virtualizovať hlavne nasledujúce služby: IMS, EPC, MME, S-GW, P-GW, HSS a PCRF.

Virtualizovaný prístup

Poskytovatelia služieb tiež skúšajú nájsť spôsob ako zjednodušiť prístup, do ktorého je zaradené **zariadenie v zákazníckych priestoroch CPE** (*Customer Premises Equipment*) a **prístupové zariadenie zákazníka CE** (*Customer Edge*), aby mohli predať viac služieb zákazníkom aj podnikateľom. NFV môže byť vhodným riešením na zvýšenie výnosov. Aby bol možný vstup NFV do prostredia poskytovateľov služieb, je nutné aby boli virtualizované zložky prístupu – v CPE a CE.

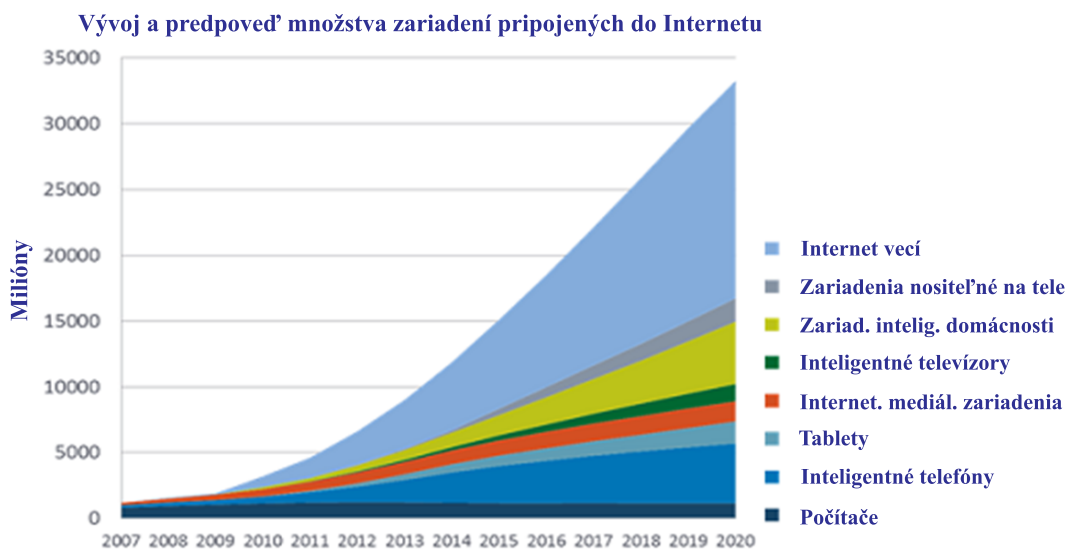
5 Internet budúcnosti

Dnešné časy môžu byť charakterizované ako časy **informačno-komunikačných technológií (ICT)**. Internet ako ho poznáme dnes, môžeme považovať za úspech. Avšak, niektoré aspekty súčasného Internetu zaostávajú ako v očakávaniach pre spoľahlivú komunikačnú infraštruktúru tak aj v budúcich požiadavkách, ktoré by sme radi vložili do týchto sietí.



Podľa autora článku [19] Clausa G. Grubera do roku 2015 bude celosvetová verejná internetová sieť pripájať približne 6 miliárd ľudí, viac ako 4 miliardy ľudí bude používať sieťové služby prostredníctvom mobilných zariadení a viac ako 2 miliardy ľudí bude používať káblové širokopásmové pripojenie k Internetu.

Taktiež predpokladal, že prevádzka v sieti bude mať tempo rastu od 40 % do 200 % v porovnaní s dnešnou sieťovou prevádzkou v nadchádzajúcich rokoch. Je preto dôležité posúdiť, v akom stave sú dnešné počítačové siete a ďalšie prvky, ktoré sú jej neoddeliteľnou súčasťou. Vysoká penetrácia Internetu povzbudzuje a rozširuje tiež používanie mobilných zariadení, ako sú notebooky, mobilné telefóny, tablety, atď. Na obr. 9 môžeme vidieť predpoveď zariadení pripojených k verejnemu internetu [20].



Zdroj: Strategy Analytics, Október 2014

Obr. 9 – Predpoveď množstva inštalovaných internetových zariadení na svete

Požiadavky mobilných sietí sú často náročnejšie než požiadavky používateľov v pevných sieťach, najmä pokiaľ ide o dostupnosť kdekoľvek a v akomkoľvek čase [21]. Preto musia dnešné siete adaptívne a pružne poskytovať nielen vysokú dostupnosť služieb, ale aj ich kvalitu.

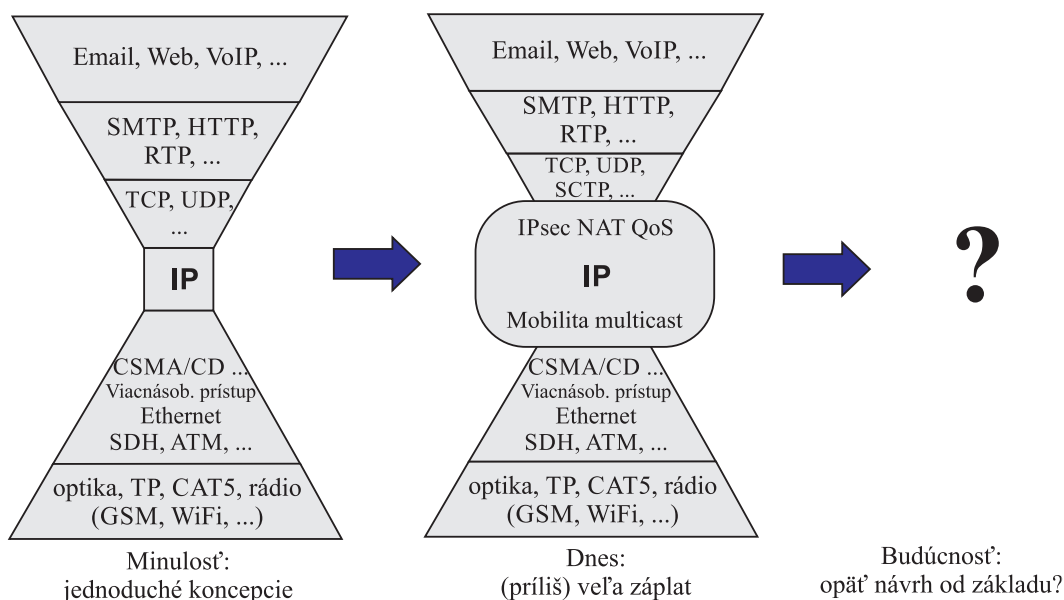
5.1 Limity Internetu

Súčasný Internet je založený predovšetkým na protokole IP. Vznikol pred viac ako 40 rokmi vďaka skupine vedcov za účelom prepojenia svojich lokálnych sietí, hlavne pre prenos súborov, e-mailovú komunikáciu atď.



Dnešný Internet výrazne prekročil pôvodné predpoklady. Z menej ako niekoľko stoviek prepojených počítačov na niekoľko stoviek miliónov v súčasnosti. Internet tiež nepočítal s novými aplikáciami ako sú web, postupné sťahovanie (streaming) videa, zdieľanie súborov, ktoré významne zmenili charakter internetovej prevádzky. Infraštruktúra Internetu sa vyvinula vďaka technologickému procesu na optickú, bezdrôtovú, atď. [22].

Na obr. 10 si môžete prezrieť vývoj Internetu od minulosti po súčasnosť. IP je v strede vrstveného modelu s aplikáciami na vrchole a technológiami nižšie.



Obr. 10 – Evolúcia Internetu [23]

V súčasnej dobe neexistuje takmer žiadna možnosť resp. praktický spôsob, ako experimentovať s novými sieťovými protokolmi, nastaveniami zariadení atď. do takého rozsahu, aby tento experiment mohol získať dôveryhodnosť pre široké nasadenie v sieťach **poskytovateľov internetových služieb (ISP)** a **poskytovateľov sieťových služieb (NSP)**.



Autori v článku [24] potvrdzujú, že obrovské množstvo už nainštalovaných sieťových zariadení na báze rovnakej sieťovej infraštruktúry s rovnakým sieťovým protokolom, ktoré sú tu už po desaťročia, tvorí obrovskú prekážku pre vstup inovatívnych riešení, výskum a vývoj v počítačových sieťach. Výsledkom tohto prístupu je aj skutočnosť, že mnohé nové nápady v oblasti výskumu sú netestované a nepodložené. Atribúty dnešných počítačových sietí sú takzvané "skostnatené".

Je dôležité poznamenať, že práve projekt Internet bol konštruovaný na účely výskumu. Architekti/vedci, ktorí vybudovali infraštruktúru Internetu si neuvedomovali možnosť príchodu veľkých sietí, ktoré v súčasnej dobe máme. Bezpečnosť, mobilita, flexibilita, odolnosť sietí neboli nikdy vyriešené, pretože v čase formalizácie Internetu počítače neboli mobilné a výskumníci chceli šíriť nové myšlienky cez otvorené prostredie. Vízie dokonalého prostredia Internetu začali blednúť s rastúcim počtom používateľov v sieti. Množstvo základných konceptov sa od času ich vzniku zmenilo. S rýchlym rozvojom technológií v oblasti informatiky a informačných technológií, nemôže Internet spĺňať a naďalej uspokojovať neustále vzrastajúce požiadavky. Je zrejmé, že dnešné siete potrebujú nový návrh, ktorý by sa lepšie prispôbil novým trendom.

Prevádzka počítačových sietí si vyžaduje rad zdrojov vzhľadom k nákladom. Náklady možno rozdeliť do investičných nákladov a operačných nákladov, ktoré sa nazývajú kapitálové výdavky (CAPEX) a prevádzkové náklady (OPEX) [25]. CAPEX sa odkazuje na investície, ktoré musia byť urobené vopred a vyradované po určitom časovom období. Príkladom môže byť výstavba dátového centra (DC) alebo kúpna cena servera, sieťových zariadení a ďalších dôležitých sieťových prvkov. Prevádzkové náklady OPEX sú spojené s opakujúcimi sa mesačnými nákladmi na vlastnú prevádzku zariadení ako sú náklady na energie, opravy, údržbu, platy administratívnych pracovníkov, atď.

5.2 Charakteristiky nového Internetu

Charakteristiky nového Internetu sú:

- Robustnosť a dostupnosť – Siete budúcnosti by mali byť robustné, odolné voči chybám a dostupné.
- Bezpečnosť – Jedným z najväčších problémov dnešného Internetu je zabezpečenie najmä bezpečnosti koncového používateľa. To je dôvod, prečo musia byť siete budúcnosti od začiatku navrhnuté s ohľadom na bezpečnosť. Tieto siete by mali poskytovať nástroje na lepšiu ochranu pred rýchlym šírením sa malvéru, zmierniť dopady útokov DDoS a poskytovať lepšie overovanie zdrojov [22].
- Podpora mobilných koncových používateľov – Ako sme sa zmienili v texte vyššie, počet koncových používateľov Internetu sa rýchlo zvyšuje a počet mobilných používateľov bude tvoriť hlavnú časť z nich. Internet budúcnosti slúži na uľahčenie mobility používateľov, terminálov a sietí a dokonca aj aplikácií, kedy je komunikácia presunutá z jedného zariadenia na druhé, napr. viď príklad [22].
- Ekonomicky životaschopný a rentabilný – Siete budúcnosti by mali byť ziskové pre poskytovateľov sieťových služieb.
- Rozvíjajúci sa - Architektúra Internetu budúcnosti by mala predbežne predpokladať, že sa bude meniť a vyvíjať v priebehu času.
- Predvídateľný - Používateľ by mal vedieť, čo očakávať od siete a tá by mala byť schopná poskytnúť predvídateľné a opakovateľné služby.
- Podpora anonymity, kedy sú potrebné opatrnosť a zodpovednosť.

5.3 Redizajn internetových technológií



Ako už bolo spomenuté, počet pripojených zariadení na Internete má tendenciu konštantného a nezastaviteľného rastu, pričom sa tento rast rok po roku neúmerne násobí.

Ak chceme získať stabilnú, bezpečnú, flexibilnú a agilnú sieť, už nemôžeme zostať v normách šesťdesiatych a sedemdesiatych rokov, ale sme nútení k pohybu vpred a otvoreniu dverí pre nové technológie. Ako možno nádejným sa zdá byť prepojenie softvérovo definovaných sietí a virtualizácie sieťových služieb. Taká novovytvorená architektúra sľubuje nielen prepojenie nesporných výhod oboch technológií, ale aj vznik nových vylepšení.



Prelomová myšlienka je určite architektúra pre automatizované poskytovanie sieťových služieb vo virtualizovanej forme. Softvérovo definované siete môžu vytvoriť perfektné automatizované sieťové prostredie, ktoré automaticky konfiguruje siete spoločností, ako aj zákaznicke prostredie. Okrem toho bude aplikácia na vrchu SDN. Riadiaca jednotka bude schopná dynamicky generovať a hodnotiť kvalitu siete. V prípade potreby zmeniť cestu k sieti, aby parametre siete zostali zachované, ale aj zasiahnuť v prípade poruchy určitého sieťového spojenia.

V kontexte automatizácie môžeme uvažovať o konkrétnych šablónach alebo pravidlách pre konkrétne virtualizované služby, ale tiež o zmieňovaných pravidlách pre konkrétneho klienta. Prostredníctvom softvérovo riadeného prístupu sme schopní udržať požadovanú konfiguráciu napriek počtu sieťových služieb, ktoré sú ešte v súlade - to zamedzí nekonzistencii, ktorá môže vyplynúť z ľudského faktoru.

Najväčšou výzvou je centralizácia a prevod vlastných služieb, takzvané "cestovanie s mojimi sieťovými službami". To znamená, že služby už nie sú viac v podobe veľkých fyzických a ťažko prenosných zariadení. Každý klient je schopný cestovať so svojimi službami, konfigurovanou sieťou bez nutnosti prenášať niečo fyzicky.



Vďaka flexibilitě týchto sietí budúcnosti je oveľa lepšie sledovať a upravovať ponúkaný produkt (službu rovnako ako aj ponuku nových vylepšení), ktorý doteraz nebolo možné aplikovať vďaka výhradne účelovým zariadeniam.



Všetky tieto myšlienky znejú lákavo, ale nasadenie architektúry prepojujúcej technológie SDN a NFV vyžaduje výmenu existujúcej zastaranej infraštruktúry, čo nie je také jednoduché. Ako možný prechod môže byť integrácia a testovanie architektúry SDN a NFV v existujúcom prostredí a následná výmena zastaraných zariadení.

Softvérovo definované siete sú nový prístup, ktorý by nám mal umožniť riadiť, meniť a kontrolovať sieť dynamicky pomocou dobre definovaných rozhraní. Centralizované riadenie zaručí všetku inteligenciu a spravuje dohľad nad dátovými elementmi ciest a linkami medzi nimi. Tento moderný centralizovaný pohľad robí

riadiacu jednotku vhodnú na plnenie funkcií pre správu siete a zároveň umožňuje jednoduché zmeny sieťových funkcií prostredníctvom centralizovanej riadiacej roviny. SDN umožňuje riadiť celú sieť cez inteligentné zariadenia a poskytuje systém, ktorý umožňuje alokáciu zdrojov na vyžiadanie.

Základné predpoklady novej sieťovej architektúry [22]:

- Rozpoznávanie tokov – vedci v článku [22] veria, že prvou dôležitou vecou je rozpoznávanie tokov.
- Sieťové adresovanie – adresovanie by malo byť viac intuitívne, odkazujúce sa na služby a ľudí, nie na rozhrania.
- Smerovacie protokoly – smerovacie protokoly by mali byť spoľahlivejšie a stabilnejšie.
- Využitelná štruktúra.
- Dynamické prepínanie okruhov.
- Dizajn chrbticovej siete – dizajn chrbticovej siete by mal byť predvídateľnejší, odolnejší voči zlyhaniu a stabilný.
- Modely princípu end-to-end.
- Medzivrstvový dizajn - Niet pochýb o tom, že vrstvený model má mnoho výhod, ale má aj veľa neefektívnosti.
- Sieťová virtualizácia - sieťová infraštruktúra by sa mala vyvíjať v priebehu času.

V tejto časti boli prezentované niektoré základné predstavy o Internete budúcnosti.



V súčasnej dobe existuje mnoho projektov bežiacich súbežne, snažiacich sa vytvoriť čistý koncept Internetu. Tento výskum je stále ešte v plienkach, takže je ťažké o tom hovoriť a zaviesť presnú architektúru siete, trendy, atď. Pracuje na ňom mnoho vedcov z celého sveta a každá výskumná skupina o ňom hovorí z vlastného uhla pohľadu. Ale jedna vec je jasná. Pretože aktuálne Internet založený na IP, je tu viac ako 40 rokov, už v súčasnej dobe čelíme jeho obmedzeniam. Nový koncept Internetu s čistým štítom bude veľmi dôležitý a jeho nasadenie je len otázkou času.
