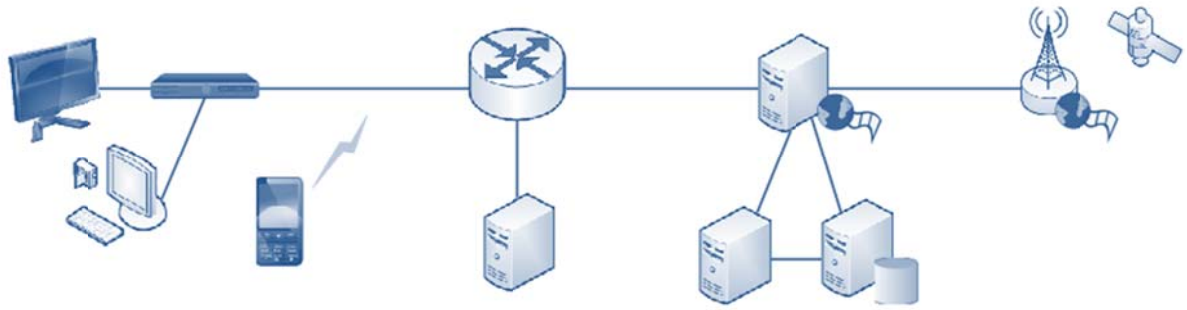
Projekt č. 688503
NEWTON – Networked Labs for Training in Sciences and Technologies for Information and Communication

Sieťové architektúry, služby a aplikácie



Autori: Podhradský Pavol, Medvecký Martin, Trúchly Peter, Vargic Radoslav, Londák Juraj, Kadlic Radovan, Schumann Sebastian, Salazar Jordi, Silvestre Santiago, Levický Dušan, Polakovič Adam

Editori: Podhradský Pavol, Trúchly Peter

SPEKTRUM STU

SIEŤOVÉ ARCHITEKTÚRY, SLUŽBY A APLIKÁCIE

Podhradský Pavol, Medvecký Martin, Trúchly Peter, Vargic Radoslav, Londák Juraj, Kadlic Radovan, Schumann Sebastian, Salazar Jordi, Silvestre Santiago, Levický Dušan, Polakovič Adam

Recenzenti: doc. Ing. Ľubomír Doboš, PhD.
Ing. Tomáš Zeman, Ph.D.

Vydala Slovenská technická univerzita v Bratislave vo Vydavateľstve SPEKTRUM STU, Mýtna 30, Bratislava, v roku 2020.

ISBN 978-80-227-5000-4

Táto publikácia bola vytvorená s podporou Európskej komisie v rámci projektu H2020 „NEWTON“.

Obsah

1. Úvod

Vzájomnou spoluprácou rôznych typov sietí a ich postupnou integráciou do jednej univerzálnej širokopásmovej multimediálnej siete - siete budúcnosti (***Future Network***, **FN**) sa postupne vytvárajú podmienky pre prenos všetkých typov médií a poskytnutie širokého spektra multimediálnych služieb a aplikácií. Koncepcia **NGN** (***Next Generation Networks*** – siete ďalšej generácie) sa vyvíjala niekoľko rokov, hlavne v rámci pracovných skupín štandardizačných inštitúcií ITU a ETSI.

V oblasti informačných a komunikačných technológií prebieha kontinuálny proces evolúcie, vrátane evolúcie technológií NGN smerom k budúcim sieťam. Existuje niekoľko aspektov, ktoré ovplyvňujú aktuálnu architektúru NGN založenú na IMS, s cieľom rozšíriť ju o ďalšie funkcie pre podporu implementácie a poskytovania multimediálnych služieb a aplikácií ďalšej generácie.

Tento študijný materiál ponúka vybrané témy pokrývajúce rôzne technológie, ktoré môžu byť integrované v rámci sietí novej (budúcej) generácie (FN), t.j. nové informačné a komunikačné technológie, ako aj nové služby a aplikácie.

Koncepcia a štruktúra študijného materiálu je navrhnutá tak, že je možné ho využiť jednak pre prezenčnú formu vzdelávania, ale aj on-line formou na báze e-vzdelávania (e-*learning*). Študijný materiál využíva nové vzdelávacie metodiky a nové informačné a komunikačné technológie (IKT), ako:

- „*Self directed learning*“ (autonómne učenie/vzdelávanie), kde študent si sám riadi proces učenia, s možnosťou prístupu k rôznym vzdelávacím zdrojom, hlavne cez internet (vzdelávacie portály, e-knižnice, konzultácie s lektorom/tútorom, diskusné skupiny, sociálne siete, experimenty vo virtuálnych/fab laboratóriách, atď.).
- „*Gamification*“ (vzdelávacie hry: 2D, 3D), s možnosťou využitia 3D VR aplikácií - virtuálna realita alebo 3D AR – rozšírená (*augmented*) realita.
- Realizácia praktických laboratórnych experimentov vo virtuálnom laboratóriu na báze vzdialeného prístupu.

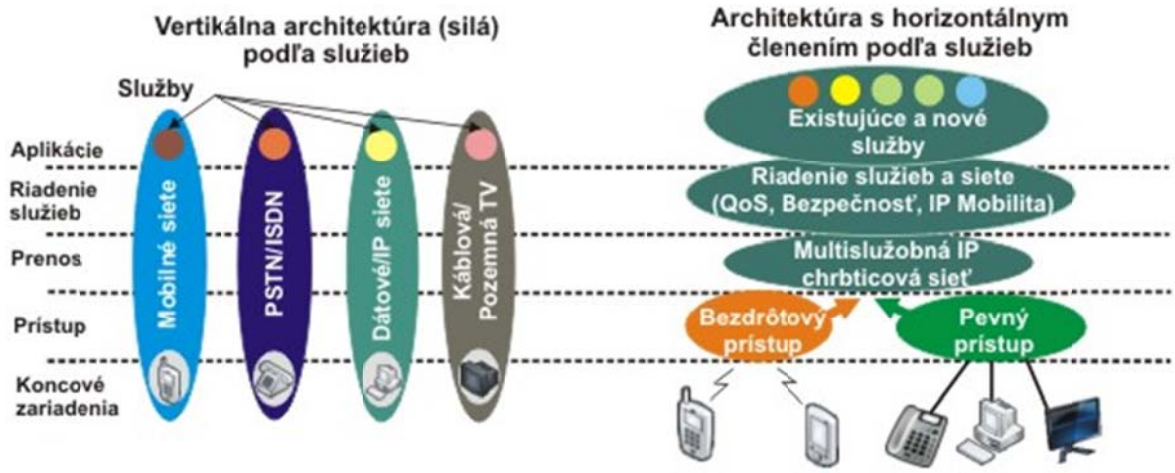
2. Evolúcia NGN architektúr smerom k sieťam budúcnosti (Future Network)

Rýchly vývoj internetových služieb a služieb na poskytovanie obsahu v heterogénnych sieťach mení požiadavky z rôznych aspektov, ako sú: mobilita, virtualizácia a zdieľanie zdrojov, bezpečnosť (sieťová a informačná), zjednodušenie architektúry a flexibilita v modeloch riadenia siete, atď. To všetko kladie nové požiadavky na evolúciu NGN architektúr smerom k FN (Future Networks – Siete budúcnosti).

2.1. Multimediálne služby a aplikácie v prostredí NGN a sietí budúcnosti

Nové koncepty a architektúry novej generácie **IKT** (***Informačné a komunikačné technológie***), založené na konvergovaných IKT a NGN, ponúkajú operátorom nové príležitosti pre implementáciu a poskytovanie širokého spektra multimediálnych služieb a aplikácií [1].

Preto operátori môžu zanechať vertikálnu štruktúru architektúry, kde každý typ služby má preddefinovanú prístupovú, transportnú, riadiacu a aplikačnú infraštruktúru pre danú službu a prejsť na horizontálne orientovanú architektúru, nezávislejšiu od poskytovanej služby (**Obr. 1**).



Obr. 1 Od vertikálnej k horizontálnej NGN architektúre [2]

2.2. Architektúry a koncepcie NGN

Hlavné princípy NGN (siete ďalšej generácie) vznikli, keď sa objavila myšlienka NGN. Ďalšie dve definície od ETSI a ITU-T opisujú podstatu NGN. ETSI opisuje NGN ako koncepciu definovania a vytvárania sietí, ktorá umožňuje formálne rozdelenie funkcií do samostatných vrstiev a rovín s využitím otvorených rozhraní. Koncepcia NGN poskytuje nové podmienky pre tvorbu, implementáciu a efektívne riadenie inovatívnych služieb. ITU-T opisuje NGN ako sieť založenú na prenose paketov, ktorá umožňuje poskytovať služby, vrátane telekomunikačných služieb a je schopná využívať niekoľko širokopásmových prenosových technológií

umožňujúcich zaručiť QoS. Funkcie súvisiace so službami sú zároveň nezávislé od základných prenosových technológií. NGN poskytuje neobmedzený prístup používateľov k rôznym poskytovateľom služieb. Podporuje všeobecnú mobilitu, ktorá poskytuje používateľom konzistentnosť a dostupnosť služieb.

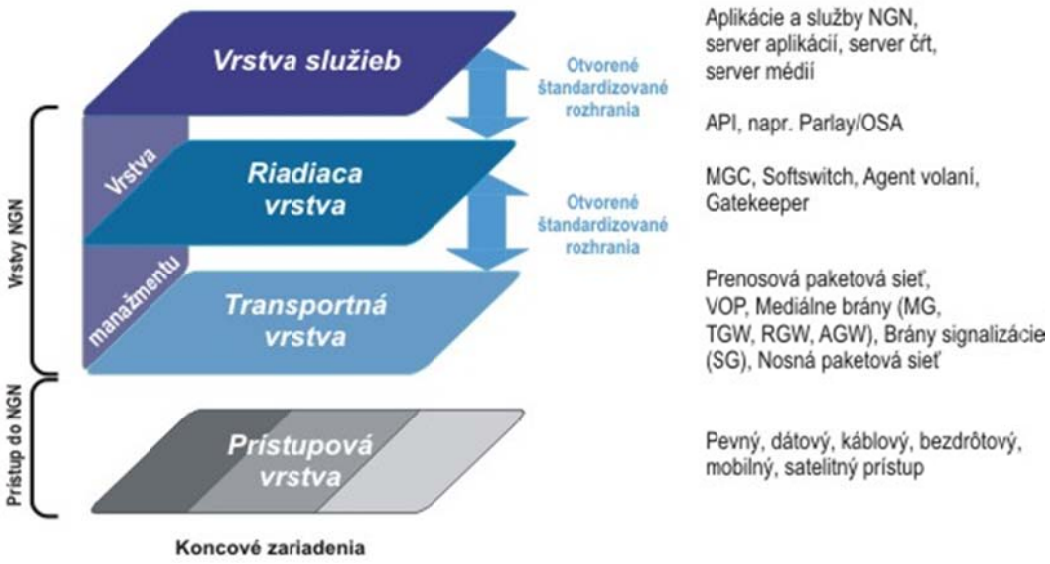
Ďalej sú uvedené niektoré požiadavky na NGN, ktoré by mali spĺňať [3]:

- vysokokapacitný prenos paketov v rámci prenosovej infraštruktúry,
- oddelenie riadiacich funkcií od funkcií prenosu,
- podpora širokého spektra služieb a aplikácií,
- možnosti širokopásmového pripojenia, pričom spĺňajú požiadavky na kvalitu služieb (**QoS**, ***Quality of Service***),
- rôzne typy mobility (používatelia, terminály, služby),
- rôzne identifikačné schémy a adresovanie,
- konvergované služby medzi pevnými a mobilnými sieťami (ako aj konvergencia hlasu, údajov a videa),
- súlad s požiadavkami na reguláciu, ako sú tiesňové volania a bezpečnostné požiadavky,
- lacnejšie a efektívnejšie technológie.

V rámci koncepcií NGN normalizačné inštitúcie tieto problémy riešili z pohľadu:

- migrácie existujúcich sietí smerom k NGN,
- rozvoja v oblasti prístupových technológií,
- prepojenia iných sietí so sieťami **IP** (***Internet Protocol***),
- poskytovania služieb a vývoja nových služieb a aplikácií,
- spolupráce v oblasti adresovania,
- prepojenia signalizačných systémov,
- roamingu a mobility.

Existuje mnoho koncepčných modelov a referenčných architektúr pre konvergované siete aj architektúry **VoIP** (***Voice over IP***). **Obr. 2** zobrazuje koncepčný model pre NGN. Cieľom koncepčného modelu je určiť funkčné vrstvy (pokrývajúce podobné funkcie), ich entity, referenčné body (rozhrania) a informačné toky medzi nimi. Takýto model potom možno ľahšie zmapovať do fyzickej referenčnej architektúry (ktorý je nezávislý od fyzických entít, t.j. komponentov architektúry). Vo väčšine analyzovaných prípadov sú vrstvy konceptuálneho modelu NGN, z hľadiska funkcií, rozdelené do nasledovných nezávislých častí: prístup (niektoré referenčné architektúry ho nezahŕňajú priamo do modelu NGN, alebo ho nahradia adaptérom), prenos (prenos, prepínanie), ovládanie / riadenie (ovládanie / riadenie hovorov / relácií) a aplikácie (služby).



Obr. 2 Koncepčný model a funkčné vrstvy NGN [4]

Vrstvy koncepčného modelu

Prístupová vrstva poskytuje infraštruktúru, napríklad prístupovú sieť medzi koncovým používateľom a transportnou sieťou.

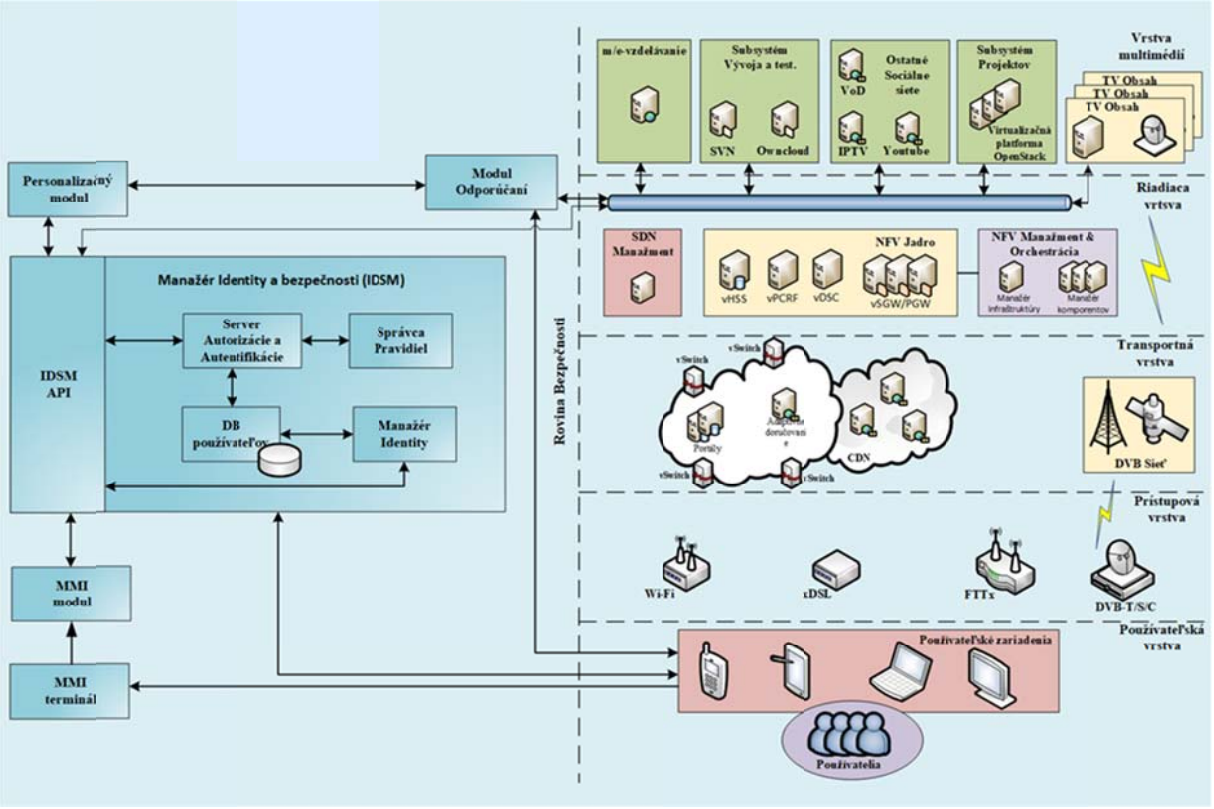
Transportná vrstva zabezpečuje transport (prenos) medzi jednotlivými uzlami (bodmi) siete.

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

Vrstva služieb ponúka základné servisné funkcie, ktoré môžu byť použité na vytvorenie zložitejších a sofistikovanejších služieb a aplikácií.

3. Systémová architektúra sietí budúcnosti

Architektúra siete budúcnosti je znázornená na **Obr. 3**. Pozostáva z niekoľkých vrstiev a rovín.



Obr. 3 Bloková schéma architektúry siete budúcnosti

3.1. Používateľská vrstva

Sieť bude využívaná koncovými používateľmi na vzájomnú komunikáciu alebo získavanie informácií a multimediálneho obsahu zabezpečovaného prostredníctvom Aplikačnej (Multimediálnej) vrstvy. Koncoví používatelia môžu na vzájomnú komunikáciu využívať rôzne typy koncových zariadení ako sú telefóny, počítače, herné konzoly, TV prijímače a to s rôznym stupňom funkčnosti (od obyčajných telefónnych prístrojov až po chytré (*smart*) telefóny s podporou AV/VR) alebo mobility (ako PC alebo TV využívajúce pevné pripojenie v domácnosti až po prenosné notebooky a mobilné telefóny). Okrem ľudí bude sieť využívaná aj na komunikáciu medzi rôznymi zariadeniami ako sú inteligentné samojazdiace autá, rôzne zariadenia v domácnosti (*smart home*), mestách (*smart city*) a priemysle (Industrie 4.0). Predpokladá sa, že v budúcnosti bude k sieti pripojený oveľa väčší počet zariadení ako ľudí a objem dát prenášaný pri komunikácií medzi zariadeniami mnohonásobne prevýši objem dát prenášaný pri komunikácií ľudí.

3.2. Prístupová vrstva

Prístupová vrstva zabezpečuje konektivitu koncových účastníkov a zariadení k sieti. Podobne, ako tomu bolo v prípade NGN, sa v prístupovej vrstve predpokladá využitie viacerých progresívnych širokopásmových technológii a to ako pre pevné optické, alebo metalické pripojenie (FTTx, xDSL), tak aj pre bezdrôtové (WiFi, DVB-T/S) a mobilné (3G/4G/5G) pripojenie.

3.3. IP/Transportná vrstva

Úlohou transportnej vrstvy je zabezpečenie prenosu dát medzi koncovými zariadeniami alebo medzi koncovými zariadeniami a servermi. Sieť bude využívať optické, metalické, mikrovlnné alebo satelitné linky a rôzne transportné technológie (DWDM, OTH, MPLS a pod.). Zjednocujúcim prvkom bude použitie IP protokolu ako jednotného formátu pre výmenu dát.

Významnými črtami sietí budúcnosti sú programovateľnosť a virtualizácia. Sieť bude tvorená na princípoch **SDN** (***Software Defined Networking***). Sieť SDN využíva sieťové prvky, ktoré majú oddelenú dátovú a riadiacu vrstvu. Funkcionalita riadiacej vrstvy je centralizovaná do tzv. SDN kontroléra, ktorý riadi smerovanie paketov v sieti. Samotné smerovanie paketov sa vykonáva v prepínačoch, ktoré sú optimalizované na výkon z hľadiska preposielania (*forwardingu*) paketov a majú obmedzenú funkcionalitu riadiacej časti. Z uvedeného dôvodu môžu byť jednoduchšie a lacnejšie. Uvedená koncepcia umožňuje flexibilné a efektívne softvérové vytváranie sietí a pravidiel pre smerovanie. Okrem princípov SDN môžu byť súčasťou architektúry aj ďalšie koncepcie, ako napr. koncepcia **CDN** (***Content Delivery Network***) používaná pre distribúciu digitálneho obsahu.

Je snaha, aby čo najväčší počet sieťových funkcií (pre smerovanie, riadenie prístupu a pod.) nebol realizovaný prostredníctvom špeciálnych, na daný účel vyrobených hardvérových zariadení ale softvérovo, prostredníctvom aplikácií emulujúcich dané sieťové funkcie v prostredí cloudu. Tento koncept sa nazýva **NFV** (***Network Function Virtualization*** – Virtualizácia sieťových funkcií).

3.4. Riadiaca vrstva

Riadiaca vrstva siete zabezpečuje funkcie riadenia SDN siete ako aj riadenia jednotlivých telekomunikačných služieb (napr. IMS). Jednotlivé funkčné bloky zabezpečujúce riadenie sú chápané ako sieťové funkcie a môžu byť preto realizované prostredníctvom virtualizácie formou NFV. Neoddeliteľnou súčasťou riadiacej vrstvy je tiež funkcia manažmentu a orchestrácie NFV infraštruktúry a služieb.

3.5. Multimediálna vrstva

Multimediálna (aplikačná) vrstva obsahuje aplikačné a dátové servery poskytujúce funkčnosť a dáta pre jednotlivé služby. Oddelenie funkčnosti služieb do samostatnej vrstvy umožňuje efektívne a lacnejšie poskytovanie existujúcich služieb a zavádzanie nových služieb. Podobne,

ako v prípade predchádzajúcich dvoch vrstiev a v prípade multimediálnej vrstvy, je aj pri zabezpečovaní funkcií multimediálnej vrstvy možno využiť výhody virtualizácie a cloudifikácie.

3.6. Bezpečnostná rovina

Hlavným komponentom bezpečnostnej roviny je Manažér Identity a bezpečnosti (IDSM), ktorý tvorý komplexný centralizovaný subsystém, preberajúci zodpovednosť v úlohách súvisiacich so zabezpečením systému, identity používateľa, dát a prístupu k nim. Ako pomocné funkcie, ktoré sa opierajú práve o identitu používateľa sú v tejto rovine umiestnené moduly personalizácie a odporúčaní, ktoré používateľovi sprostredkovávajú prostredie a obsah viac vyhovujúci jeho vkusu a požiadavkám. IDSM k svojej plnohodnotnej funkcií potrebuje dostať spoľahlivé dáta o tom, kto sa pri koncovom zariadení nachádza. Tieto dáta mu sprostredkujú a pomôžu spracovať **MMI** (***Multi-Modal Interface***) terminál a modul. Tieto komponenty zároveň pomáhajú rozpoznávať riadiace pokyny zadané gestami rúk prípadne hlasom.

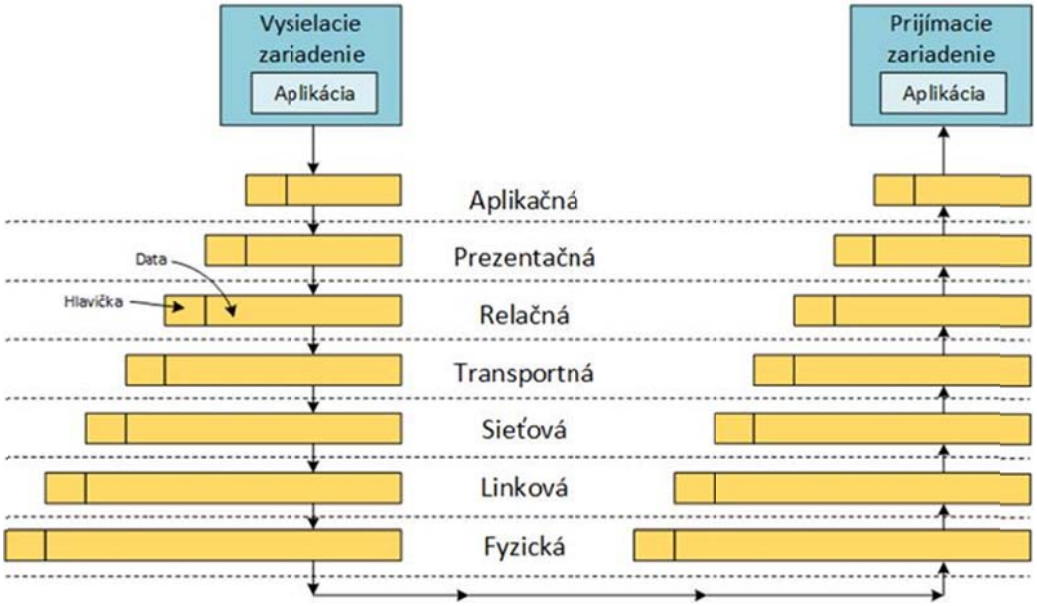
IDSM komunikuje so svojím okolím prostredníctvom API rozhrania. Hlavným výkonným komponentom je Modul Autorizácie a Autentifikácie, ktorý prostredníctvom Správy pravidiel a databázy používateľov rozhoduje o tom, či daný používateľ má požadované oprávnenie pre službu.

4. Základná charakteristika sieťových modelov

V tejto kapitole budú uvedené charakteristiky dvoch sieťových modelov, z ktorých prvý sa používa v súčasnosti ako referenčný model (**RM OSI**, ***Open Systems Interconnection Reference Model***), pričom druhý je základným sieťovým (protokolovým) modelom súčasného Internetu (TCP/IP model).

4.1. RM OSI model

Referenčný model OSI je štandardom Medzinárodnej organizácie pre normalizáciu (**ISO**, ***International Organization for Standardization***) definovaným v ISO/IEC 7498-1 [5]. Používa sa ako univerzálny model pre diskusiu alebo opis toho ako počítače navzájom komunikujú prostredníctvom siete. Jeho sedemvrstvový prístup k prenosu údajov rozdeľuje mnohé operácie na špecifické súvisiace skupiny akcií na každej vrstve (**Obr. 4**). Vrstva slúži vrstve vyššie a je podávaná vrstvou pod ňou.



Obr. 4 Tok dát v OSI modeli

Princípom OSI modelu je delenie komunikačného systému na abstraktné vrstvy. Pôvodná verzia modelu definovala sedem vrstiev. Na každej úrovni si dve komunikujúce entity vymieňajú protokolové dátové jednotky (**PDU**, ***Protocol Data Unit***) prostredníctvom protokolov dostupných v tejto vrstve. Každá PDU obsahuje užitočnú záťaž, nazývanú služobnou dátovou jednotkou (**SDU**, ***Service Data Unit***), spolu s hlavičkou prípadne pätou, ktoré súvisia s protokolom.

Spracovanie údajov dvoma komunikujúcimi zariadeniami kompatibilnými s OSI prebieha takto:

1. Dáta, ktoré sa majú prenášať, sa skladajú na vrchnej vrstve vysielacieho zariadenia (vrstva N) do protokolovej dátovej jednotky (PDU).

2. PDU prechádza do vrstvy N-1, kde sa použije ako služobná dátová jednotka (SDU).
3. Na vrstve N-1 sa SDU zlučuje s hlavičkou vytvárajúcou vrstvu N-1 PDU. Potom sa prenesie do vrstvy N-2.
4. Proces pokračuje až do dosiahnutia spodnej úrovne, z ktorej sa údaje prenášajú na prijímacie zariadenie.
5. Na prijímacom zariadení sa údaje prenášajú z najnižšej na najvyššiu vrstvu ako séria SDU, zatiaľ čo sa postupne odoberajú hlavičky alebo päty každej vrstvy, kým sa nedosiahne horná vrstva, kde sa spotrebuje posledná z údajov.

4.2. TCP/IP model

TCP/IP (***Transmission Control Protocol/Internet Protocol***) bol vyvinutý v šesťdesiatych rokoch minulého storočia ako súčasť úsilia o vybudovanie celonárodnej paketovej dátovej siete v rámci rozvojovej agentúry Ministerstva obrany (**DoD**, ***Department of Defense***) pre pokročilé výskumné projekty (**ARPA**, ***Advanced Research Projects Agency***). Prvýkrát sa použil v počítačoch so systémom UNIX na univerzitách a vládnych zariadeniach. Dnes je to hlavná paradigma používaná vo všetkých prevádzkach Internetu.

Obr. 5 Súvis OSI vrstiev a TCP/IP vrstiev

TCP/IP je tiež vrstvový model, ale nepoužíva všetky vrstvy OSI, hoci niektoré z vrstiev sú ekvivalentné v prevádzke a funkcii (**Obr. 5**). Vrstva prístupu k sieti je ekvivalentná 1. a 2. OSI vrstve. Vrstva IP je porovnateľná s 3. vrstvou v modeli OSI. Transportná vrstva je ekvivalentná 4. vrstve OSI. Jedná sa o funkcie protokolu TCP a UDP. Nakoniec aplikačná vrstva je podobná vrstvám OSI 5, 6 a 7 v kombinácii.

4.3. TCP/IP protokoly

V tejto kapitole budú stručne charakterizované protokoly na sieťovej, transportnej a aplikačnej vrstve modelu TCP/IP sietí (**Obr. 6**).

RM OSI	TCP/IP	Protokoly
Aplikačná	**Aplikačná**	HTTP, DNS, FTP, DHCP, SSH, SOAP, RTP, SIP, RTCP, XMPP, Telnet, NETCONF, RIP, IS-IS, BGP, SMTP, POP3, IMAP
Prezentačná		
Relačná		
Transportná	**Transportná**	TCP, UDP, RSVP
Sieťová	**Sieťová**	IPv4, IPv6, ARP, RARP, ICMP, ICMPv6, IGMP
Linková	**Linková**	Ethernet, 802.3x(WiFi)
Fyzická	**(hardware)**	

Obr. 6 Protokoly na jednotlivých vrstvách sieťového TCP/IP modelu

4.3.1. Sieťové protokoly

Táto časť pojednáva o nasledovných sieťových protokoloch: IPv4, IPv6, ICMP, ICMPv6, IGMP a IPsec.

IPv4

IPv4 (***Internet Protocol version 4***) je štvrtá verzia internetového protokolu (IP) [6]. Jedná sa o jeden z hlavných protokolov potrebných pre fungovanie Internetu. V súčasnosti stále prebieha väčšina internetovej komunikácie prostredníctvom IPv4 napriek pokračujúcemu nasadeniu zdokonaleného protokolu IPv6. IPv4 je popísaný v dokumente RFC 791.

IPv4 je protokol bez spojenia používaný v sieťach s prepájaním paketov.

Pracuje na princípe „najlepšieho úsilia“, pretože nezaručuje dodávku, ani nezabezpečuje správne zoraďovanie alebo vyhýbanie sa duplicitnej dodávke. Tieto aspekty, vrátane integrity údajov, sú riešené prenosovým protokolom vyššej vrstvy napríklad protokolom riadenia prenosu (**TCP**, ***Transmission Control Protocol***).

IPv4 používa 32-bitové adresy, ktoré obmedzujú adresný priestor na 4 294 967 296 (2^{32}) adries. IPv4 rezervuje špeciálne bloky adries pre privátne siete (~ 18 miliónov adries) a adresy multicast (~ 270 miliónov adries).

Adresy IPv4 môžu byť reprezentované v akejkoľvek notácii vyjadrujúcej 32-bitovú celočíselnú hodnotu. Najčastejšou formou je bodkovo-desiatková notácia, ktorá sa skladá zo štyroch oktetov adresy, vyjadrených jednotlivo v desiatkových číslach a oddelených bodkami.

Revidovaný systém adresovania IPv4 definuje päť tried (**Obr. 7**). Triedy A, B a C mali rozdielne dĺžky bitov pre identifikáciu siete. Zvyšok adresy sa používa na identifikáciu hostiteľa v sieti, čo znamenalo, že každá sieťová trieda mala inú kapacitu na adresovanie hostiteľov. Trieda D je rezervovaná pre adresovanie multicastov a Trieda E je vyhradená pre testovacie účely.

Trieda	Rozsah adries	Prvý oktet	Poznámka
A	**0**000000 - **0**1111111	1 - 127	16 777 214 zariadení na podsieť
B	**10**000000 - **10**111111	128 - 191	65 534 zariadení na podsieť
C	**110**00000 - **110**11111	192 - 223	254 zariadení na podsieť
D	**1110**000 - **1110**1111	224 - 239	Rezervované pre multicast
E	**1111**000 - **1111**0111	240 - 255	Rezervované pre experim. využitie

Obr. 7 Triedy IPv4 adries

Z približne štyroch miliárd adries definovaných v protokole IPv4 sú pre súkromné (privátne) siete vyhradené tri rozsahy (**Obr. 8**). Adresy v týchto rozsahoch nie sú smerovateľné vo verejnom Internete, pretože sú ignorované všetkými verejnými smerovačmi. Používatelia s privátnymi adresami preto nemôžu priamo komunikovať s verejnými sieťami, na tento účel vyžadujú preklad sieťových adries (**NAT**, ***Network Address Translation***).

Názov	Rozsah adries	Počet adries
24-bitový blok	10.0.0.0 – 10.255.255.255	16 777 216
20-bitový blok	172.16.0.0 – 172.31.255.255	1 048 576
16-bitový blok	192.168.0.0 – 192.168.255.255	65 536

Obr. 8 Vyhradené rozsahy pre privátne adresy

Vysielacia adresa (*broadcast*) je adresa, ktorá umožňuje odosielať informácie na všetky rozhrania v danej podsieti, namiesto konkrétneho zariadenia.

Vo všeobecnosti je vysielacia adresa vypočítaná získaním bitového doplnku masky podsiete a vykonaním bitovej operácie OR s identifikátorom siete. Inými slovami, adresa vysielania je posledná adresa v rozsahu adries podsiete.

IPv6

Internetový protokol verzie 6 (IPv6) je najnovšia verzia internetového protokolu (IP), ktorý bol štandardizovaný v **IETF** (***Internet Engineering Task Force***) [7] a určený pre riešenie dlho očakávaného problému vyčerpania adresy IPv4.

IPv6 používa 128-bitovú adresu, ktorá teoreticky umožňuje 2^{128} alebo približne $3{,}4 \times 10^{38}$ adries. Skutočné číslo je o niečo menšie, pretože viaceré rozsahy sú vyhradené pre špeciálne použitie alebo úplne vylúčené z používania. Celkový počet možných adries IPv6 je viac ako $7{,}9 \times 10^{28}$ krát viac ako IPv4, ktorý používa 32-bitové adresy a poskytuje približne 4,3 miliardy adries.

Adresy IPv6 sú reprezentované ako osem skupín so štyrmi hexadecimálnymi číslicami, pričom skupiny sú oddelené dvojbodkami, napríklad 2001:0db8:0000:0042:0000:8a2e:0370:7334, ale existujú metódy na skrátenie tohto plného zápisu.

IPv6 má nahradiť protokol IPv4 a tieto dva protokoly nie sú navrhnuté tak, aby boli interoperabilné (t.z., aby dokázali vzájomne spolupracovať).

IPv6 poskytuje ďalšie technické výhody okrem väčšieho adresného priestoru. Umožňuje najmä hierarchické metódy prideľovania adries, ktoré uľahčujú agregáciu trasy na internete a tým obmedzujú rozširovanie smerovacích tabuliek. Použitie multicastového adresovania je rozšírené a zjednodušené a poskytuje dodatočnú optimalizáciu pre poskytovanie služieb. Aspekty mobility, bezpečnosti a konfigurácie boli zohľadnené už pri samotnom návrhu protokolu.

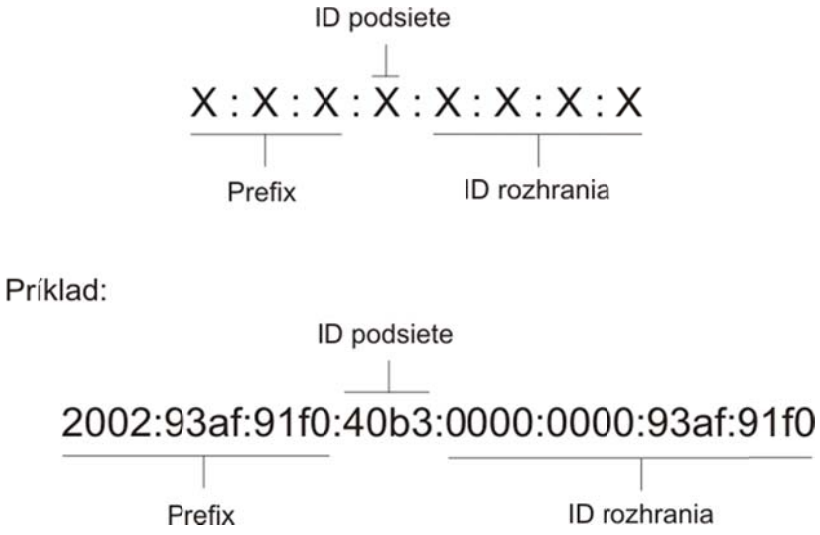
IPv6 adresovanie

Adresy IPv6 sú priraďované k rozhraniam, nie k uzlom, pretože uzol môže mať viac ako jedno rozhranie. Okrem toho môže byť rozhraniu priradená viac ako jedna adresa IPv6.

IPv6 definuje tri typy adries:

- **unicast** - identifikuje rozhranie jednotlivých uzlov.
- **multicast** - identifikuje skupinu rozhraní, zvyčajne na rôznych uzloch. Pakety, ktoré sa odosielajú na adresu multicast, idú všetkým členom multicast skupiny.
- **anycast** - identifikuje skupinu rozhraní, zvyčajne na rôznych uzloch. Dáta, ktoré sa odosielajú na anycast adresu, idú do člena skupiny, ktorý je fyzicky najbližšie k odosielateľovi.

Adresa IPv6 má dĺžku 128 bitov a pozostáva z ôsmich, 16-bitových polí, pričom každé pole je ohraničené dvojbodkou. Každé pole obsahuje hexadecimálne číslo, na rozdiel od adresy IPv4. Tri ľavé polia (48 bitov) obsahujú predponu lokality. Predpona opisuje verejnú topológiu, ktorú zvyčajne priraďuje ISP alebo Regionálny Internetový Register (**RIR**, ***Regional Internet Registry***). Ďalších 16-bitov je identifikátor podsiete, ktorý si používateľ vyhradil pre svoju lokalitu. Identifikátor podsiete opisuje súkromnú topológiu, známu aj ako topológiu lokality. Pravé štyri polia (64 bitov) obsahujú ID rozhrania, ktoré sa tiež označuje ako token. Identifikátor rozhrania je buď automaticky konfigurovaný z **MAC** (***Medium Access Control***) adresy rozhrania, alebo manuálne nakonfigurovaný vo formáte EUI-64. Štruktúra a príklad IPv6 adresy je zobrazený na **Obr. 9**.



Obr. 9 Štruktúra a príklad IPv6 adresy

ICMP

ICMP (***Internet Control Message Protocol***) [8] je podporným protokolom. Sieťové zariadenia používajú ICMP na odosielanie chybových hlásení a prevádzkových informácií, ktoré naznačujú, že požadovaná služba nie je k dispozícii, alebo že hostiteľa alebo smerovač nie je možné dosiahnuť. ICMP sa líši od transportných protokolov, ako sú protokoly TCP a UDP, pretože sa zvyčajne nepoužíva na výmenu údajov medzi systémami, ani nie je pravidelne využívaný sieťovými aplikáciami pre koncových používateľov (s výnimkou niektorých diagnostických nástrojov, ako je ping a traceroute).

ICMPv6

ICMPv6 (***Internet Control Message Protocol verzia 6***) [9] je implementácia protokolu ICMP pre IPv6. Na rozdiel od originálneho ICMP je ICMPv6 integrálnou súčasťou IPv6 a vykonáva hlásenia chýb a diagnostické funkcie (napr. Ping) a má rámec pre rozšírenia na implementáciu budúcich zmien.

IGMP

IGMP (***Internet Group Management Protocol***) [10] je komunikačný protokol používaný hostiteľmi a priľahlými smerovačmi v sieťach IPv4 na vytvorenie členstva v multicast skupine. IGMP je integrálnou súčasťou IP multicastu. IGMP sa môže používať na vytváranie sieťových aplikácií typu one-to-many, ako je on-line streamovanie videa a hier, a umožňuje efektívnejšie využívanie zdrojov pri podpore týchto typov aplikácií.

IGMP je zraniteľný niektorými útokmi a preto firewally obyčajne umožňujú používateľovi jeho zakázanie, ak nie je potrebný.

Existujú tri verzie IGMP. Tieto verzie sú spätne kompatibilné, preto smerovač podporujúci IGMPv3 môže podporovať klientov s IGMPv1, IGMPv2 a IGMPv3.

- IGMPv1 používa model odpovede dotazu. Dotazy sa posielajú na adresu 224.0.0.1. Správy o členstve sa posielajú na adresu multicast skupiny.
- IGMPv2 urýchľuje proces opustenia skupiny a upravuje ďalšie časové limity. Správy zanechávajúce skupiny sa posielajú na 224.0.0.2. Zaviedol sa špecifický dotaz pre skupinu. Skupinové dopyty sa posielajú na adresu multicast skupiny.
- IGMPv3 zavádza multicastové funkcie špecifické pre zdroj. Správy o členstve sa posielajú na 224.0.0.22.

IPsec

IPsec (***Internet Protocol Security***) je sieťová protokolová sada, ktorá autentifikuje a šifruje pakety dát odosielaných cez sieť. IPsec obsahuje protokoly na vytvorenie vzájomnej autentifikácie medzi agentmi na začiatku relácie a vyjednávanie kryptografických kľúčov, ktoré sa majú používať počas relácie.

IPsec môže chrániť toky údajov medzi dvojicou hostiteľov (hostiteľ-hostiteľ), medzi dvojicou bezpečnostných brán (sieť-sieť) alebo medzi bezpečnostnou bránou a hostiteľom (sieť-hostiteľ). IPsec používa kryptografické bezpečnostné služby na ochranu komunikácií prostredníctvom IP sietí.

IPsec je schéma zabezpečenia typu end-to-end, ktorá funguje v Internetovej vrstve balíka Internetových protokolov, zatiaľ čo niektoré ďalšie internetové bezpečnostné systémy

s rozšíreným používaním, ako napríklad **TLS** (***Transport Layer Security***) a **SSH** (***Secure Shell***) pracujú na transportnej (TLS) a aplikačnej vrstve (SSH). Preto iba IPsec chráni všetky aplikácie cez IP sieť. IPsec dokáže automaticky zabezpečiť aplikácie na vrstve IP.

4.3.2. Protokoly transportnej vrstvy

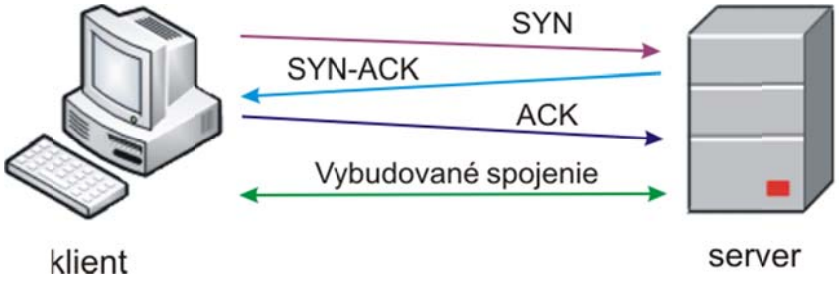
Táto časť pojednáva o nasledovných transportných protokoloch: TCP, UDP, SCTP a RSVP.

TCP

TCP (***Transmission Control Protocol***) [11] je jeden z hlavných protokolov TCP/IP balíka. TCP je protokol orientovaný na spojenie, čo znamená, že sa vytvára a udržiava spojenie, až kým programy na oboch koncoch komunikácie nedokončia výmenu správ. TCP je zodpovedný za to, ako rozdeliť aplikačné dáta do segmentov tak, aby mohli byť v sieti doručené, zabezpečuje riadenie toku a spracováva retransmisiu stratených alebo skomolených paketov ako aj potvrdenie všetkých prijatých paketov.

Kvôli jeho orientácií na presné viac než včasné doručenie, môže spôsobiť relatívne dlhé oneskorenia (v rádoch sekúnd), kým čaká na nevybavené správy alebo opätovné prenosy stratených správ. Preto nie je vhodný na aplikácie v reálnom čase, ako napríklad Voice over IP.

Na vytvorenie TCP spojenia sa používa trojcestná výmena (*handshake*). Skôr ako sa klient pokúsi spojiť so serverom, tento sa musí najprv pripojiť a počúvať na určenom porte, aby ho otvoril pre spojenie - toto sa nazýva pasívne otvorenie. Po vytvorení pasívneho otvorenia môže klient iniciovať aktívne otvorenie (**Obr. 10**).



Obr. 10 Ukážka trojcestnej výmeny na vytvorenie TCP spojenia

UDP

UDP (***User Datagram Protocol***) [12] používa jednoduchý prenosový model bez spojenia s minimálnym protokolovým mechanizmom. Používa kontrolné súčty pre kontrolu integrity údajov a čísla portov na adresovanie rôznych funkcií na zdroji a cieľovej stanici. Nemá implementované žiadne mechanizmy dohadovania spojení. Preto neposkytuje žiadnu kontrolu správnosti doručených dát zároveň neexistuje žiadna záruka dodávky, objednávky alebo duplicitnej ochrany. Vďaka tejto jednoduchosti je UDP vhodným protokolom pre streamovanie médií a prenosy dát v reálnom čase.

SCTP

SCTP (***Stream Control Transmission Protocol***) [13] je protokol transportnej vrstvy, ktorý slúži podobne ako protokoly TCP a UDP. SCTP poskytuje podobné funkcie ako UDP a TCP. SCTP je správovo orientovaný ako UDP, ale zároveň zabezpečuje spoľahlivý prenos správ s riadením

preťaženia ako TCP. Na rozdiel od uvedených dvoch protokolov však poskytuje funkciu viacnásobných a nadbytočných ciest na zvýšenie odolnosti a spoľahlivosti.

Pri absencii natívnej podpory SCTP v operačných systémoch je možné tunelovať SCTP cez UDP, alebo využiť mapovanie volaní TCP API na SCTP.

RSVP

RSVP (***Resource Reservation Protocol***) [14] je protokol prenosovej vrstvy určený na rezervovanie zdrojov v sieti používajúci model integrovaných služieb. RSVP pracuje pomocou IPv4 alebo IPv6 protokolov a poskytuje nastavenie rezervácie zdrojov iniciované prijímačom pre multicast a unicast toky. Samotný protokol neprenáša aplikačné dáta, ale je podobný kontrolnému protokolu ako ICMP alebo IGMP.

RSVP môže byť použitý na vyžiadanie alebo dodanie špecifických úrovní kvality služieb (**QoS**, ***Quality of Service***) pre rôzne aplikácie. RSVP definuje spôsob, akým aplikácie umiestňujú rezervácie a ako môžu zrušiť vyhradenie zdrojov po ukončení ich potreby. Prevádzka RSVP zabezpečuje rezerváciu zdrojov v každom uzle pozdĺž cesty.

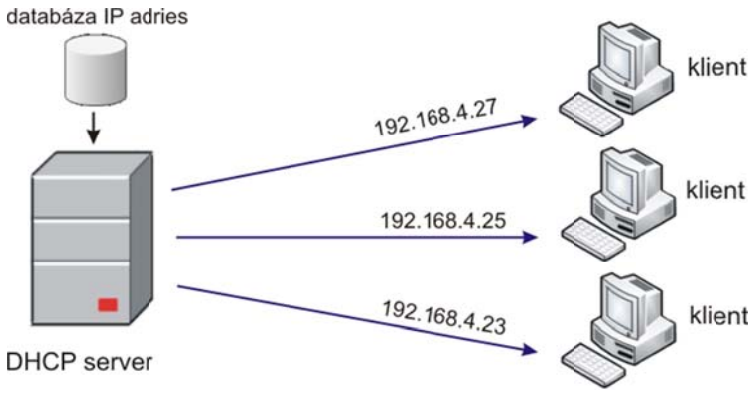
RSVP nie je smerovací protokol a bol navrhnutý tak, aby spolupracoval so súčasnými a budúcimi smerovacími protokolmi. Samotný RSVP sa v dnešných telekomunikačných sieťach používa zriedkavo, ale rozšírenie RSVP alebo RSVP-TE v premávke sa v súčasnosti v mnohých sieťach s orientáciou na kvalitu siete prijíma čoraz viac.

4.3.3. Aplikačné protokoly

Táto časť pojednáva o nasledovných aplikačných protokoloch: DHCP, DNS, TLS/SSL, Telnet, FTP, HTTP, POP, IMAP, SMTP, XMPP, SOAP, RIP, SIP, OSPF, IS-IS, RTP, RTCP, RTSP, SNMP a NETCONF.

DHCP

DHCP (***Dynamic Host Configuration Protocol***) [15] je sieťový protokol umožňujúci automatizované nastavenie TCP/IP parametrov (IP adresy, predvolenej brány, doménového mena, menných serverov a časových serverov) pre zariadenia v sieti. DHCP používa model klient - server. DHCP server spravuje rozsah IP adries a informáciu o klientskej konfigurácií. Keď sa počítač alebo iné zariadenie pripojí k sieti, DHCP klient pošle požiadavku na zaslanie potrebných konfiguračných informácií na DHCP server. Svoju žiadosť pošle na všesmerovú (*broadcast*) adresu danej podsiete, čo je spravidla adresa 255.255.255.255. Na žiadosť môže odpovedať každý DHCP server v danej sieti. DHCP server po prijatí žiadosti o priradenie IP adresy od klienta zarezervuje klientovi IP adresu a zašle mu ponuku, ktorá obsahuje MAC adresu klienta, ponúkanú IP adresu, masku podsiete, dobu platnosti priradenia adresy a IP adresu DHCP servera, ktorý ponuku klientovi poslal (**Obr. 11**). Klient môže prijať ponuky od viacerých serverov, ale môže akceptovať iba jednu z nich. Klient v odpovedi pre DHCP server, ktorú pošle na všesmerovú adresu podsiete, požiada o nim vybranú ponúkanú adresu. DHCP server po prijatí žiadosti od klienta pošle klientovi správu, ktorou mu pridelenie adresy potvrdí.



Obr. 11 Prideľovanie adries protokolom DHCP

DHCP používa nespojovo orientovaný mód prenosu a UDP port 67 pre server a UDP port 68 pre klienta. DHCP server môže používať niektorý z nasledovných troch spôsobov prideľovania adries:

- *Dynamické pridelenie adries* – DHCP server priraďuje IP adresy na určitý čas a adresy, ktoré neboli obnovené, prideľuje novým záujemcom.
- *Automatické pridelenie adries* – DHCP server si udržiava tabuľku v minulosti pridelených IP adries a klientom prioritne prideľuje rovnaké IP adresy ako v minulosti.
- *Manuálne (statické) pridelenie adries* – DHCP server prideľuje privátne IP adresy podľa pravidiel definovaných administrátorom.

DNS

DNS (***Domain Name System***) [16] je hierarchický, decentralizovaný menný systém pre preklad človeku zrozumiteľných počítačových mien na IP adresy. DNS poskytuje celosvetovú, distribuovanú adresárovú službu pre Internet. DNS protokol definuje dátové štruktúry a dátové komunikačné výmeny používané v rámci DNS. DNS protokol používa dva typy DNS správ - dopyty (*query*) a odpovede (*reply*). Žiadosť o preklad mena na IP adresu spravidla pozostáva z jedného dopytu zaslaného klientom prostredníctvom UDP a jednej UDP odpovedi zaslanej serverom. DNS používa UDP port 53. V špeciálnych prípadoch, keď veľkosť odpovede prekračuje 512 bajtov, sa používa TCP.

TLS/SSL

TLS (***Transport Layer Security***) [17] a jeho predchodca **SSL** (***Secure Sockets Layer***) [18], oba často nazývané "SSL", sú kryptografické protokoly používané na zaistenie bezpečnosti komunikácie v počítačovej sieti. TLS využíva celý rad všeobecne používaných aplikácií ako sú prehliadanie webu, e-mail, rýchle posielanie správ (*instant messaging*) a **VoIP** (***Voice-over-IP***). Napríklad webové stránky používajú TLS na utajenie komunikácie medzi servermi a webovými prehliadačmi.

Komunikácia s využitím TLS má tri fázy: dohodu účastníkov na podporovaných algoritmoch, výmenu kľúčov a šifrovanie prenášaných dát. TLS podporuje viacero rôznych spôsobov výmeny kľúčov, šifrovania dát a overenia integrity dát.

Telnet

Telnet [19] je komunikačný protokol typu klient - server používaný na obojsmernú interaktívnu textovo orientovanú komunikáciu medzi virtuálnym terminálom a serverom. Telnet sa používal na prístup k príkazovo orientovanému rozhraniu (**CLI**, ***Command Line Interface***) na vzdialenom zariadení. Z dôvodu absencie podpory utajenia komunikácie (Telnet nešifruje žiadne prenášané dáta, a to vrátane hesiel) je však pri komunikácií cez verejné siete, ako napr. Internet, nahrádzaný SSH. Telnet používa TCP a port 23.

FTP

FTP (***File Transfer Protocol***) [20] je štandardný sieťový protokol používaný v počítačových sieťach na prenos súborov medzi klientom a serverom. FTP využíva model klient - server, pričom používa oddelené riadiace a dátové spojenia medzi klientom a serverom.

FTP používateľ sa môže pri vytváraní spojenia autentifikovať menom a heslom (ktoré sú prenášané v nešifrovanej podobe), alebo, ak to daný server povoľuje, sa môže prihlásiť anonymne. Pre zvýšenie bezpečnosti prenosu a ochranu prihlasovacích údajov používateľa môže byť FTP prenos zabezpečený prostredníctvom SSL/TLS (FTPS) [21].

HTTP

HTTP (***Hypertext Transfer Protocol***) [22] je aplikačný protokol pre hypermediálny, distribuovaný informačný systém. HTTP tvorí základný kameň dátovej komunikácie v rámci **WWW** (***World Wide Web***). Hypertext je štruktúrovaný text, ktorý používa logické linky (hyperlinky) medzi uzlami, na ktorých sa text nachádza. HTTP je protokol na prenos hypertextu. HTTP zdroje sú v rámci siete identifikované a lokalizované prostredníctvom **URL** (***Uniform Resource Locator***) [23], ktorý definuje doménovú adresu servera, umiestnenie zdroja na serveri a protokol, ktorým je možné k zdroju pristupovať, napr. *https://tools.ietf.org/html/rfc2616*.

POP

POP (***Post Office Protocol***) [24] je aplikačný protokol používaný klientom elektronickej pošty na preberanie e-mailových správ zo serverov. Prenos správ prebieha prostredníctvom TCP spojenia. Existuje niekoľko verzií POP protokolu, aktuálna verzia má označenie POP3. Protokol POP je v súčasnosti často nahrádzaný vyspelejším protokolom IMAP.

IMAP

IMAP (***Internet Message Access Protocol***) [25] je aplikačný protokol používaný na preberanie elektronickej pošty klientmi zo serverov. Na rozdiel od protokolu POP3, ktorý umožňoval len preberanie e-mailov, protokol IMAP umožňuje kompletné manažovanie e-mailového účtu z viacerých e-mailových klientov. E-mailové správy ostávajú uchované na serveri pokiaľ ich používateľ explicitne neodstráni. IMAP server využíva štandardne na príjem port 143, pri komunikácií cez SSL (IMAPS, IMAP over SSL) sa využíva port 993. Aktuálna verzia protokolu je IMAP4.

IMAP a POP3 sú v súčasnosti dva najpoužívanejšie štandardné protokoly na preberanie elektronickej pošty, ktoré sú podporované takmer všetkými e-mailovými klientmi.

SMTP

SMTP (***Simple Mail Transfer Protocol***) [26] je internetový štandard navrhnutý pre výmenu elektronickej pošty (e-mailov) medzi e-mailovými servermi. SMTP je v prípade e-mailových

serverov a iných maily preposielajúcich agentov používaný na odosielanie a prijímanie e-mailových správ. Okrem prenosu správ medzi servermi sa SMTP používa aj na posielanie e-mailových správ z klientov elektronickej pošty na e-mailové servery. (Na príjem správ zo serverov sa používajú IMAP alebo POP3).

XMPP

XMPP (***Extensible Messaging and Presence Protocol***) [27] je komunikačný protokol určený pre výmenu správ a informácií o prítomnosti (*presence*) medzi viacerými sieťovými entitami. XMPP je založený na **XML** (***Extensible Markup Language***) [28]. Sieť XMPP využíva architektúru klient - server. Klienti nekomunikujú navzájom, ale prostredníctvom serverov. Systém má decentralizovanú architektúru podobnú elektronickej pošte, t.j. hocikto si môže vytvoriť svoj vlastný XMPP server. Každý používateľ v sieti má svoju jedinečnú XMPP adresu nazývanú JID, ktorá je podobná emailovej adrese, napr. meno@domena.sk.

SOAP

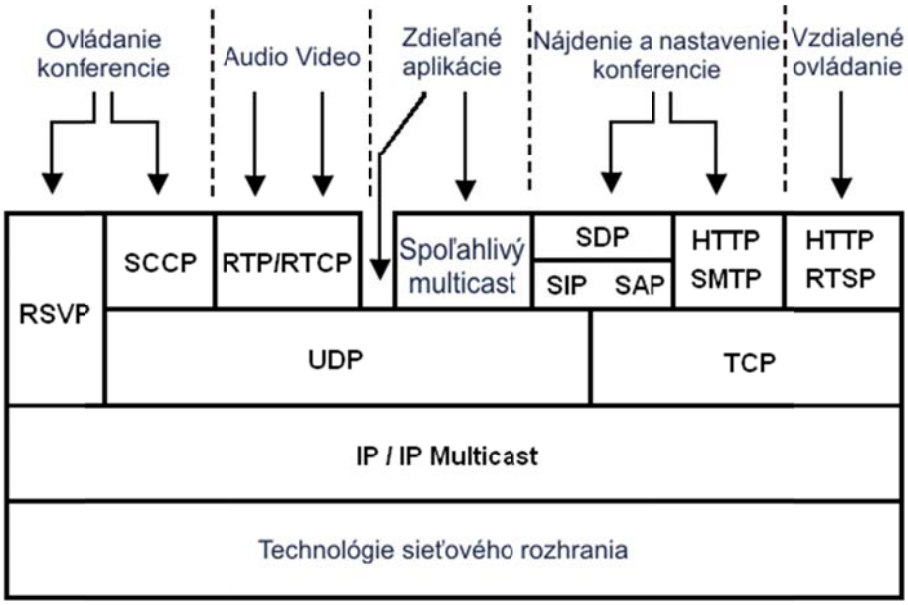
SOAP (***Simple Object Access Protocol***) [29] je protokol na výmenu štruktúrovaných správ pri implementácií webových služieb v počítačových sieťach. SOAP umožňuje navzájom komunikovať procesom bežiacim na rôznych operačných systémoch, ako sú napr. Windows a Linux. SOAP je protokol založený na XML, ktorý sa skladá z troch častí:

1. obálky, ktorá definuje štruktúru správ a spôsob spracovania,
2. súboru kódovacích pravidiel na vyjadrenie inštancií dátových typov definovaných aplikáciou,
3. pravidiel pre reprezentovanie procedurálnych volaní a odpovedí.
4. SOAP používa HTTP ako protokol nižšej vrstvy.

SIP

SIP (***Session Initiation Protocol***) [30] je textovo orientovaný signalizačný protokol pracujúci na aplikačnej vrstve. Je používaný na zostavenie, modifikovanie a ukončenie multimediálnych relácií. SIP je používaný v kombinácii s inými protokolmi určenými na opis parametrov zostavovanej relácie medzi dvomi (alebo viacerými) účastníkmi. SIP je založený na transakčnom modeli typu požiadavka – odpoveď, ktorý je známy z protokolu HTTP. Každá transakcia pozostáva z požiadavky, ktorá vyvolá príslušnú metódu alebo funkciu servera a aspoň jednu odpoveď. SIP podporuje päť hlavných aspektov pre zostavenie a ukončenie multimediálnej komunikácie:

- Lokalita používateľa – určenie konca systému komunikácie,
- Dostupnosť používateľa - zistenie “ochoty”, ale aj schopnosti volaného zapojiť sa do komunikácie,
- Schopnosti používateľa – určenie typu média a parametrov média, ktoré budú použité pre zostavenie komunikácie,
- Zostavenie relácie – “zvonenie”, zostavenie parametrov relácie na oboch stranách, t.j. volajúcej a volanej,
- Manažment relácie – zahŕňa prenos, ale aj ukončovanie relácií, modifikáciu parametrov a vyvolanie služieb.



Obr. 12 Protokolový zásobník

RIP

RIP (***Routing Information Protocol***) [31] je dynamický smerovací protokol patriaci do skupiny smerovacích protokolov smerujúcich podľa dĺžky jednotlivých ciest (*distance vector*), ktorý ako metriku smerovania používa počet skokov. RIP na ochranu pred vznikom smerovacích slučiek limituje počet skokov v rámci cesty na 15 (počet skokov 16 je považovaný za nekonečnú vzdialenosť a daná cesta za nedosiahnuteľnú). Obmedzenie maximálneho počtu skokov limituje použitie protokolu RIP na menšie siete. RIP pre určenie najkratšej cesty v sieti používa Bellman-Fordov algoritmus. RIP má z hľadiska rýchlosti konvergencie a škálovateľnosti všeobecne horšie vlastnosti ako iné smerovacie protokoly (napr. OSPF, IS-IS a pod.), je však ľahko konfigurovateľný, nakoľko nevyžaduje žiadne podrobnejšie nastavenia.

OSPF

OSPF (***Open Shortest Path First***) [32] je smerovací protokol určený pre IP siete. Patrí do skupiny **IGP** (***Interior Gateway Protocol***) smerovacích protokolov určených pre smerovanie v rámci jedného autonómneho systému (AS). OSPF je smerovací protokol, ktorý pri smerovaní využíva topologickú mapu siete vytvorenú na základe informácií o stave liniek (*link state*) získaných z dostupných smerovačov. OSPF dokáže detegovať zmeny v topológii siete (napr. prerušenie linky) a skonvergovať sieťovú topológiu do novej štruktúry v priebehu niekoľkých sekúnd. OSPF počíta pre každý smer najkratšiu cestu pomocou Dijkstrovho algoritmu. OSPF je najpoužívanejším IGP smerovacím protokolom v podnikových sieťach. Aktuálne používanými verziami OSPF sú OSPFv2 pre IPv4 siete a OSPFv3 [33] pre IPv6 siete.

IS-IS

IS-IS (***Intermediate System to Intermediate System***) [34] je dynamický smerovací protokol typu *link state* používaný vo veľkých sieťach poskytovateľov služieb. IS-IS je protokol typu **IGP** (***Interior Gateway Protocol***), t.j. je určený na použitie v rámci administratívnej domény alebo siete. Podobne ako OSPF smeruje podľa stavu liniek a používa Dijkstrov algoritmus na výpočet najlepšej cesty v sieti. Na rozdiel od OSPF, ktorý bol vyvinutý pre smerovanie protokolu IP na 3.

vrstve OSI, bol IS-IS protokol navrhnutý ako ISO štandard pre smerovanie na 2. vrstve OSI a pre prenos smerovacích informácií nepoužíva IP. IS-IS je z hľadiska sieťových adries neutrálny, čo umožnilo jeho jednoduché nasadenie pre smerovanie v sieťach IPv6. Z uvedeného dôvodu býva IS-IS označovaný za de facto štandard v chrbticových sieťach veľkých poskytovateľov Internetu.

BGP

BGP (***Border Gateway Protocol***) [35] je dynamický smerovací protokol typu **EGP** (***Exterior Gateway Protocol***), ktorý je určený na výmenu smerovacích informácií a informácií o dostupnosti medzi autonómnymi systémami (AS) v rámci Internetu. Protokol BGP rozhoduje o smerovaní na základe informácií o cestách, sieťových politikách alebo konfiguračných pravidlách určených sieťovým administrátorom. Pre rozlíšenie jednotlivých podsietí používa čísla autonómnych systémov.

BGP môže byť použitý ako na smerovanie v rámci autonómneho systému, vtedy sa označuje ako **iBGP** (**Interior Border Gateway Protocol**), tak aj na smerovanie medzi autonómnymi systémami, vtedy sa označuje ako **eBGP** (***Exterior Border Gateway Protocol***). Aktuálna verzia je BGP4.

RTP

RTP (***Real-time Transport Protocol***) [36] je sieťový protokol pre prenos audio a video obsahu prostredníctvom IP sietí. RTP sa používa v systémoch vyžadujúcich prenos v reálnom čase, ako sú telefónia, videokonferencie, televízia, systémy typu *push to talk* a pod. RTP prenáša dáta najčastejšie prostredníctvom UDP protokolu. RTP sa používa v spolupráci s protokol **RTCP** (***RTP Control Protocol***), pričom prostredníctvom RTP sa prenášajú mediálne toky (audio a video) a protokolom RTCP sa prenášajú doplnkové informácie pre riadenie relácie. RTP sám o sebe neposkytuje žiadny mechanizmus na zaistenie včasného doručenia dát alebo poskytovania nejakého QoS, zaisťuje však synchronizáciu (pomocou časových značiek), detekciu strát a doručenie segmentov v správnom poradí (pomocou poradových čísel) a identifikáciu prenášaného obsahu. RTP relácie sú spravidla zostavené prostredníctvom signalizačných protokolov ako sú SIP, RTSP, XMPP a pod.

RTCP

RTCP (***RTP Control Protocol***) [37] je sieťový riadiaci protokol, ktorý slúži na riadenie RTP relácie prostredníctvom sledovania kvality toku. Primárnou funkciou RTCP je poskytovanie spätnej väzby o kvalite služby pri prenose mediálnych tokov prostredníctvom periodického posielania štatistických informácií účastníkom príslušnej multimediálnej relácie. RTCP spolupracuje s RTP pri prenose multimediálnych dát, ale sám žiadne mediálne dáta neprenáša. RTCP prenáša štatistiky mediálneho spojenia a informácie ako počet prenesených oktetov a paketov, počet stratených paketov, zmena paketového oneskorenia a jednosmerné oneskorenie. Tieto údaje môžu byť použité na riadenie QoS parametrov, napr. obmedzením toku, alebo použitím iného kodeku. RTCP obvykle používa port o jedno číslo vyšší ako RTP.

RTSP

RTSP (***Real Time Streaming Protocol***) [38] je sieťový riadiaci protokol navrhnutý na riadenie streamovacích mediálnych serverov v oblastiach ako sú komunikácia a zábava. Protokol RTSP sa používa na vytvorenie a riadenie mediálnej relácie medzi koncovými bodmi spojenia. Klienti a mediálne servery používajú príkazy podobné tým, ktoré sa používajú na ovládanie prístrojov na záznam videa (napr. prehrať, nahrať, pozastaviť), ktoré umožňujú v reálnom čase ovládať prenos

mediálneho toku zo servera ku klientovi (video na požiadanie), alebo od klienta na server (hlasové nahrávanie). Protokol RTSP neslúži na prenos streamovaných dát, tie sa zo servera spravidla posielajú prostredníctvom protokolu RTP (v spolupráci s RTCP).

SNMP

SNMP (***Simple Network Management Protocol***) [39] je manažmentový protokol určený na monitorovanie a správu zariadení v IP sieti. SNMP používa architektúru manažér – agent. Manažmentové informácie sú na spravovaných zariadeniach uchovávané v databáze **MIB** (***Management Information Base***) [40]. SNMP agent udržiava stav MIB v zhode s aktuálnym stavom spravovaného zariadenia a riadi prístup SNMP manažérov k údajom v MIB. Existujú a v súčasnosti sa používajú tri verzie protokolu SNMP. Prvá verzia SNMP používa na autentifikáciu jednoduchý reťazec (názov *komunity*), ktorý je prenášaný sieťou nešifrovaný. Novšie verzie prinášajú zvýšenie výkonnosti (SNMPv2c) [41] a bezpečnosti (SNMPv3) [42]. SNMP používa porty 161 a 162.

NETCONF

NETCONF (***Network Configuration Protocol***) [43] je manažmentový protokol, ktorý, na rozdiel od SNMP, poskytuje mechanizmy na inštalovanie, manipulovanie a odstraňovanie konfiguračných dát na sieťových zariadeniach. Jednotlivé operácie sú vykonávané prostredníctvom vzdialeného volania procedúr (**RPC**, ***Remote Procedure Call***). NETCONF využíva architektúru klient-server, keď klient špecifikuje požadovanú operáciu a jej parametre a NETCONF server túto operáciu vykoná a vráti odpoveď. NETCONF kóduje konfiguračné dáta a protokolové správy pomocou XML a prenáša ich pomocou transportných protokolov SSH alebo TLS.

5. Sieť doručovania obsahu (CDN)

Sieť doručovania obsahu CDN (*Content Delivery Network*) je sieť, ktorá sa skladá z veľkého počtu distribučných miest (tzv. uzlov). Táto sieť je spustená v rámci siete internet a môže priniesť obrovské množstvo obsahu k obrovskému množstvu príjemcov. Je to sieť určená na distribúciu obsahu.

Najobľúbenejšie využitie týchto sietí je distribúcia softvérových aktualizácií.

Sieť CDN je vo vlastníctve poskytovateľa CDN, ktorý je zodpovedný za distribúciu obsahu ku koncovému zákazníkovi CDN.

Výhodou CDN je zdieľanie zdrojov, pretože ak by každý softvérový poskytovateľ chcel distribuovať aktualizácie k svojim zákazníkov, musel by vybudovať systém serverov, ktoré by musel udržiavať v prevádzke. Takéto riešenie by vytváralo paralelné systémy, čo by v konečnom dôsledku spôsobovalo zvyšovanie cien za distribúciu.

Moderné CDN dokážu zvládnuť množstvo IT úloh, ktoré napomôžu:

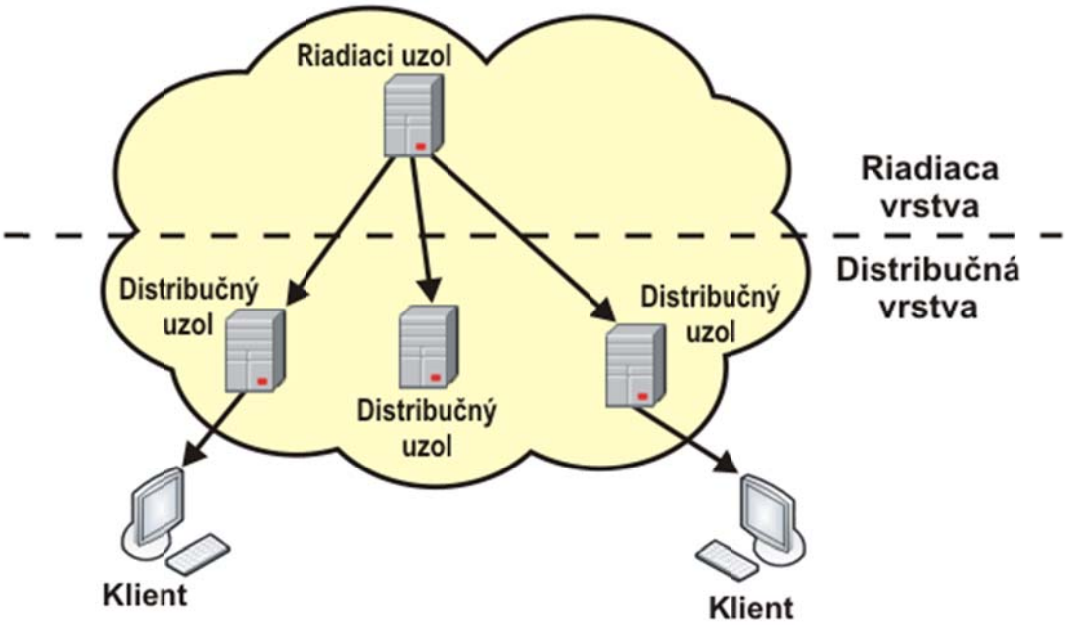
- zlepšiť rýchlosť načítania stránky,
- zaobchádzať s vysokým zaťažením,
- blokovať spamerov, robotov,
- zabezpečiť pokrytie bez nákladov,
- znížiť spotrebu pásma,
- udržovať rovnováhu medzi viacerými servermi,
- chrániť webové stránky pred útokmi **DDoS** (***Distributed Denial-of-Service***),
- zabezpečiť aplikácie.

Sieť CDN je organizovaná v dvoch vrstvách (**Obr. 13**):

- Riadiaca vrstva - väčšinou ide o centrálny uzol, ktorý sa používa na riadenie prijímania a distribúcie obsahu cez distribučnú vrstvu. Je zodpovedný aj za autentifikáciu a autorizáciu.
- Distribučná vrstva - farma uzlov, je rozložená na mnohých miestach.

Distribúcia obsahu CDN sa delí na dve metódy:

1. priama - podobne ako pri skupinovom prenose všetci príjemcovia dostanú rovnaký obsah, v tom istom čase. Dobrým príkladom je športové podujatie, keď každý zákazník chce vidieť zápas s minimálnym oneskorením (prípustná hodnota je najviac 10 sekúnd)
2. nepriama – obsah, ktorého tvorba začala a skončila v minulosti. Nepriamu distribúciu možno rozdeliť do dvoch typov prenosových metód: *sťahovanie, postupné sťahovanie*. Príkladom môže byť dobre známe postupné sťahovanie videí (YouTube) alebo distribúcia aktualizácií.



Obr. 13 Architektúra CDN

Medzi základné stavebné bloky sietí CDN patria (**Obr. 14**):

- **POPs** (***Points of Presence***) - sú strategicky umiestnené dátové centrá zodpovedné za komunikáciu s používateľmi v ich geografickej blízkosti. Ich hlavnou funkciou je zníženie koncového (obojsmerného) oneskorenia tým, že sa obsah približuje návštevníkovi webovej stránky. Každý CDN PoP typicky obsahuje množstvo serverov uchovávajúcich obsah do vyrovnávacích pamätí.
- **Servery uchovávajúce obsah** vo vyrovnávacich pamätiach (caching servers) **-** sú zodpovedné za ukladanie a odovzdávanie uložených súborov. Ich hlavnou funkciou je urýchlenie času načítania webových stránok a zníženie spotreby šírky pásma. Každý server na ukladanie údajov do vyrovnávacej pamäte CDN typicky obsahuje viacero úložných jednotiek a veľké množstvo pamätí RAM.
- **Vnútorné servery** CDN s vyrovnávacími pamäťami – obsah je ukladaný do vyrovnávacích pamätí na pevných diskoch (SSD a HDD) alebo v pamäti s náhodným prístupom (RAM), pričom častejšie používané súbory sú umiestnené na rýchlejšom médiu. Ako najrýchlejšia sa RAM zvyčajne používa na ukladanie najčastejšie požadovaných položiek.

Obr. 14 Základné stavebné bloky sietí CDN

5.1. Dnešné CDN vo svete

CDN sú v súčasnej dobe implementované len ako samostatný komerčný produkt. Pre zabezpečenie jedinečnej funkcionality a efektivity prevádzkovatelia CDN zaviedli svoje vlastné algoritmy a prenosové protokoly. Existujú aj rôzne typy komerčného softvéru pre tvorbu CDN vo vlastnej réžii pre spoločnosti, ktoré vyžadujú vlastné prevedenie siete CDN. Takýmto poskytovateľom je napríklad EdgeCast [44].

Open source Projekty otvorených zdrojov sú založené na aktivite jednotlivých projektov, ktoré vyvinuli svoje vlastné siete CDN založené na voľne dostupnom softvéri. Každý dobrovoľník sa môže zapojiť k tejto sieti s jeho vlastným serverom, prípadne skupinou serverov (clusterom). Tento nový server sa tak stane novým uzlom otvorenej siete CDN, ktorý bude zabezpečovať aj celkový manažment tejto siete.

5.2. Tok obsahu

V súčasnej dobe sa služby internetového obsahu rozdelili do týchto hlavných častí: *obsah, služba, sieť (transport), spotrebiteľ (zákazník)*. Všetky tieto subjekty majú medzi sebou jasne vymedzené vzťahy, ktoré definujú spôsob toku obsahu od jeho tvorcu (autora) až ku zákazníkovi. Jednotlivé časti toku sú poskytované definovanými subjektmi. Obsah je vytvorený autorom. Potom prechádza obsah s právami na poskytovateľa obsahu. Poskytovateľ obsahu potom poskytne obsah prevádzkovateľovi služieb. Prevádzkovatelia služieb ponúkajú služby distribúcie obsahu ku koncovému zákazníkovi prostredníctvom siete. Sieť je poskytovaná prevádzkovateľom siete. Nemusí isť vždy len o autonómne subjekty, napríklad poskytovateľ služby môže byť aj poskytovateľom siete alebo poskytovateľ obsahu tiež prevádzkuje službu.

5.3. Riadiaca vrstva

Táto vrstva je zodpovedná za riadenie distribúcie obsahu, prijímania obsahu, ohlasovanie, záznam, funkciu smerovania požiadaviek.

Každá sieť CDN má implementované metódy distribúcie, prispôsobenia a zabezpečenia obsahu. Všetky tieto informácie sú veľmi dôležité pre prenos obsahu od zdroja ku konečnému zákazníkovi.

- Distribučné metódy – pod týmito metódami rozumieme rôzne metódy na prenos obsahu z distribučného uzla konečnému zákazníkovi.
- Prispôsobenie obsahu - je súbor metód, ktoré môžu byť použité na zmenu formy pôvodnej informácie na formu, ktorá je vhodnejšia pre prenos v reálnom čase.
- Zabezpečenie obsahu - je súbor pravidiel a mechanizmov určených na ochranu obsahu, vrátane oprávnenia a prístupu, správy digitálnych práv, ochrany proti kopírovaniu, vodotlače, ...

Je veľmi dôležité mať zmapované, ktorý distribučný uzol alebo sieť môže obsluhovať danú oblasť. V IP sieti je na takéto mapovanie určená smerovacia tabuľka, kde je každý bod popísaný sieťovou adresou a maskou siete. V sieťach CDN sú adresa a veľkosť definované v jednom parametri s nazývanom stopa (footprint). Stopa môže obsahovať informácie o pokrytí zemepisnej oblasti [45], poskytovateľovi internetu [46], atď. Stopy sú uložené v tabuľke, ktorá obsahuje zoznam všetkých stôp s ich distribučnými uzlami.

5.4. Distribučná vrstva

Táto vrstva je zodpovedná za poskytovanie obsahu pre zákazníkov. Skladá sa z veľkého počtu prenosových uzlov, ktoré môžu byť organizované aj v skupinách (cluster). Tieto uzly alebo skupiny môžeme nazývať distribučné body. Každý distribučný bod obsahuje veľkú úložnú kapacitu na lokálnych alebo externých diskových poliach, tento priestor sa využíva na ukladanie distribuovaného obsahu.

Obsah založený na súboroch

Obsah založený na súboroch je postupnosť bajtov, ktorá sa začala a skončila v minulosti. Možno ho stiahnuť bez QoS, ale takmer vždy vyžaduje nulovú toleranciu voči zmenám alebo úpravám na akejkoľvek úrovni obsahu. Práve väčšina dát prenesených internetom alebo sieťami CDN je tohto typu. Pre tento účel je ideálny protokol HTTP, ktorý sa v súčasnosti bežne používa.

Obsah založený na toku

Obsah založený na toku je postupnosť bajtov, ktorá sa začala a skončila v minulosti. Obsahuje užitočné informácie po častiach, takže môže byť prenášaná priebežne, počas prenosu môže byť tiež spotrebovávaná. Postupné sťahovanie takéhoto obsahu je väčšinou citlivé na QoS prenosového kanála, a to najmä na oneskorenie a jitter.

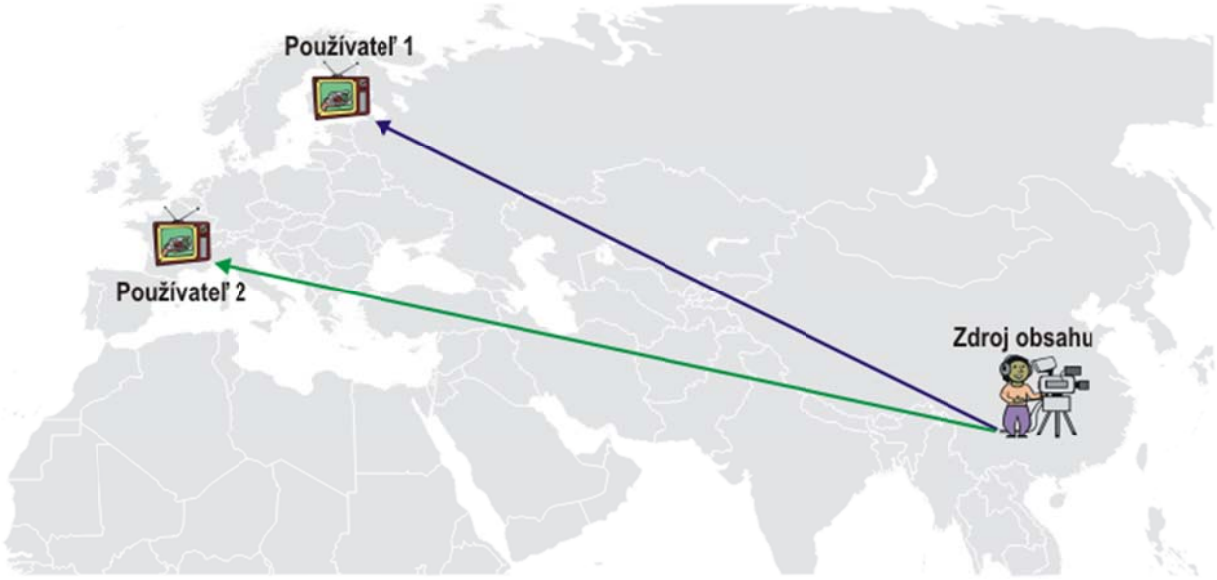
Typickým obsahom tohto typu je multimediálny tok. V porovnaní s dátovým prenosom sa video a audioobsah stáva stále viac a viac populárnym. CDN ako súčasť internetu pomáha plniť tieto požiadavky šírením obsahu rozložením zaťaženia na viac miest a distribučných bodov.

Používatelia multimediálneho obsahu sú citliví na zvukové informácie, pretože každá krajina používa iný jazyk. Ak chceme znížiť záťaž siete, je efektívne prenášať len zvukový záznam v požadovanom jazyku. Na zabezpečenie takéhoto prenosu musí distribučný bod disponovať videozáznamom s viacerými zvukovými stopami. K spotrebiteľovi je prenášaná iba jedna audiostopa (elementárny tok). Každý elementárny tok môže byť prenášaný rôznymi cestami od

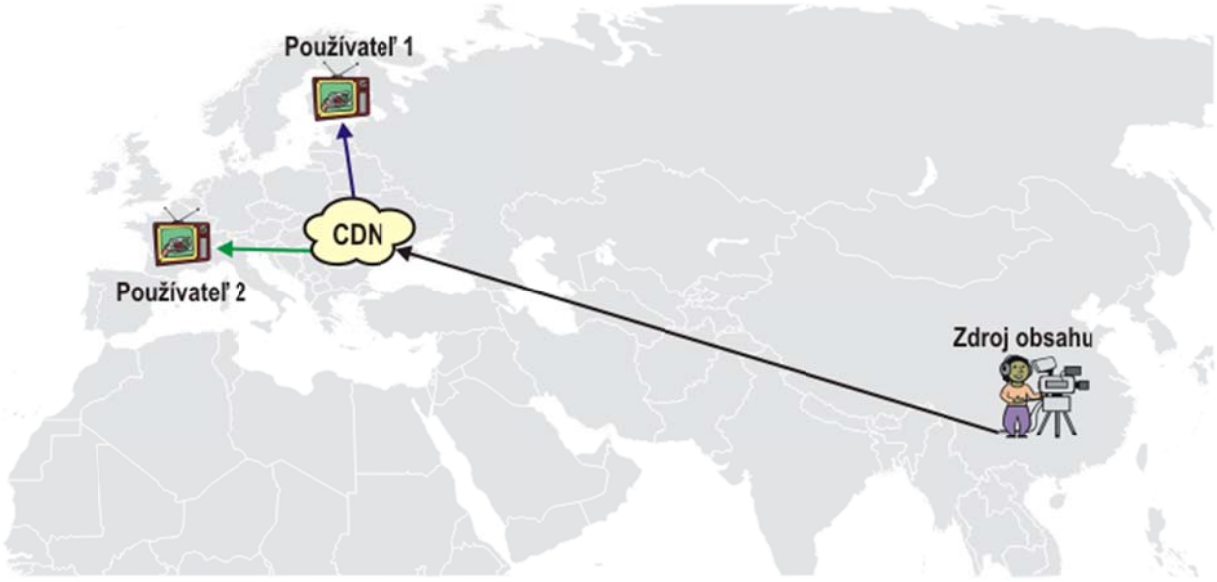
zdroja k cieľu. Rovnaký koncept môže byť použitý pre obsah z viacerých uhlov pohľadu, kde je obsah zaznamenaný viacerými kamerami z rôznych uhlov (pohľadov). V tomto prípade prenášame len video z distribučného bodu k zákazníkovi.

Obsah založený na živom toku

Takýto tok je postupnosť bajtov, ktorá začala v minulosti a ešte neskončila. Pretože tento tok je živý, nemôže byť uložený pre ďalšie postupné sťahovanie. Preto musí byť prenášaný a prijímaný v reálnom čase.



Obr. 15 Distribúcia živého toku bez CDN



Obr. 16 Distribúcia živého toku s CDN

Najjednoduchšie na pochopenie bude, ak si to ukážeme na nasledujúcom príklade: predstavte si, že dvaja diváci v Európe chcú vidieť živé vysielanie z olympijských hier v Číne. V normálnej

sieti individuálneho prenosu, ktorou aj internet v podstate je, by tok musel byť v Číne duplicitne prevedený do tvaru vhodného na postupné sťahovanie a prenášaný ku účastníkom dvomi samostatnými tokmi (**Obr. 15**).

Presmerovaním účastníkov do CDN môže byť tento videotok z čínskeho servera na postupné sťahovanie prenesený do príslušnej lokality v Európe (**Obr. 16**). Tok je zdvojený až v tomto distribučnom bode a prenášaný k účastníkom iba v rámci európskej siete. Takýmto spôsobom môžeme ušetriť internetové prepojenie z Európy do Číny. V tomto prípade potrebujeme o polovicu menšiu šírku pásma, ak by boli traja diváci potrebovali by sme len tretinu, atď.

5.5. Federácia sietí CDN

Je veľmi ťažké nasadiť globálnu medzinárodnú sieť, ktorá je rozmiestnená po celej zemeguli. CDN ťaží z obrovského množstva prenášaného obsahu (bajtov). Čím viac prenesených bajtov určitou platformou, tým viac sa zvyšuje využívanie siete, a preto je cena jedného preneseného bajtu nižšia. Nižšia cena za bajt prináša viac účastníkov, čo nám opäť prináša viac preneseného obsahu. Viac obsahu bude využívať viac bajtov pre prenos. Ako môžeme vidieť proces cenotvorby sa pohybuje v slučke. Táto slučka je "zodpovedná" za vyprofilovanie sa veľkých hráčov CDN na trhu, ktorí ovládajú súčasný trh.

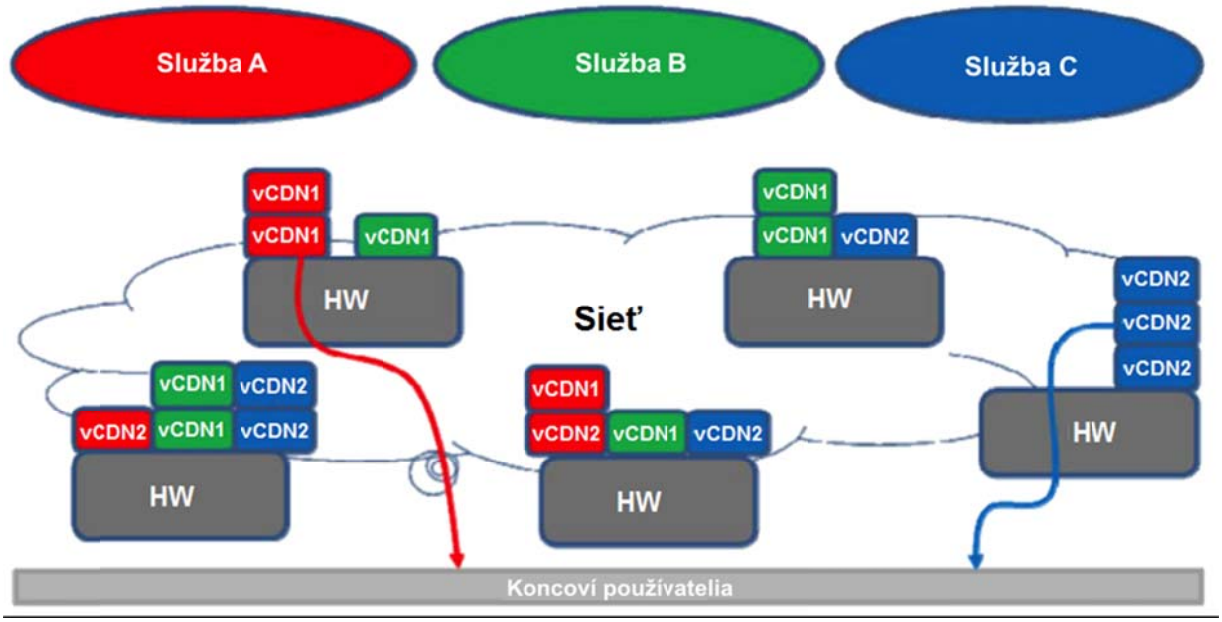
Telekomunikační operátori strácajú podiel na trhu deň po dni, zatiaľ čo medzinárodní celosvetoví poskytovatelia služieb (Akamai, Globix, Limelight ...) ho získavajú. Telekomunikační operátori sú tlačení do úlohy prevádzkovateľa siete ako "vlastníka kábla". Táto situácia je samozrejme pre nich nežiaduca, a preto sa snažia investovať aj v tejto oblasti.

Za vytvorením federácie v oblasti sieti CDN stojí množstvo vlastníkov CDN, hlavne ale telekomunikačných operátorov [47], [48]. Federácia je spôsob prepojenia CDN, kde obsah môže byť kopírovaný z jednej CDN siete do druhej. V konečnom dôsledku môže byť koncový používateľ obsluhovaný oboma sieťami, tou ktorá obsah vytvorila a aj tou, ktorá je s ňou vo federácii.

O federácii sietí CDN hovoríme vtedy, keď sa niekoľko sietí CDN navonok tvári a správa ako jedna.

5.6. Virtualizácia CDN

Potenciál pre využitie funkcií virtualizácie siete (NFV) v rámci sietí CDN je značný. Z dôvodu, že v rámci Internetu sa čoraz viac do popredia dostáva streamovanie videí s vysokým rozlíšením, alebo posielanie veľkokapacitných súborov, tak segregácia na viacero virtuálnych častí je vhodná. Dnes si už môžeme vytvoriť samostatnú logicky izolovanú sieť v rámci už existujúcich fyzických sietí, čo otvára novú cestu či už poskytovateľom sietí CDN alebo poskytovateľom internetových služieb. V rámci **Obr. 17** môžeme vidieť, že koncový používateľ ani nevie o tom, že využíva viaceré virtuálne CDN.



Obr. 17 Aplikácia virtuálnych CDN

Požiadavky na CDN pre telekomunikačné siete možno rozdeliť do dvoch skupín. Prvou skupinou sú koncoví používatelia, ku ktorým možno zahrnúť aj poskytovateľov multimediálnych služieb. Dané požiadavky môžu byť:

- Štatistika v reálnom čase o využití CDN.
- Rýchlosť nahrávania súborov napríklad pomocou FTP.
- Jednoduchý prístup napríklad aj pomocou rozhrania pre programovanie aplikácií API.
- Rýchlosť prepisovania dočasných súborov, ktorý odosiela hlavný server.

Z hľadiska majiteľa CDN siete je jeden hlavný problém, ktorým je rýchlosť. Keďže rýchlosť je kľúčová pre CDN siete, je nutné vedieť, ako rýchlo dokážeme odoslať súbor koncovému používateľovi. Čiže hlavnými kľúčovými ukazovateľmi výkonnosti sú:

- oneskorenie v [ms]
- priepustnosť v [kbit/s]

Pre všetky ukazovatele sú k dispozícii minimálna, maximálna a priemerná hodnota pre dostatočne dlhú periódu, preferujúc v normálnej prevádzke a/alebo špičke prevádzkových hodín. Okrem oneskorenia treba zvážiť aj výkon serverov. Servery môžu byť síce blízko používateľov a tým pádom by mali mať nízke oneskorenie, ale môžu byť pomalé z rôznych dôvodov:

- server nedokáže zvládať viacero simultánnych spojení od používateľov, z čoho vyplývajú čakacie rady,
- hardvér môže byť zastaralý a pomalý,
- server môže byť za zariadením realizujúcim vyrovnávanie zaťaže, ktorý má zníženú kapacitu,
- server môže byť pripojený k Internetu pomocou nedostačujúcej linky.

Pre budúcnosť CDN je dôležité nájsť rolu, ktorú dané siete CDN budú zastávať. Už teraz sú rôzne spoločnosti, ktoré ponúkajú mimo CDN iné služby, ale pre jednoduchosť si môžeme zobrať situáciu, kedy bude jedna spoločnosť poskytovať sieť CDN a druhá multimediálne služby. Keď si predstavíte, ako doteraz fungovali siete CDN, tak mnoho z nich už aj teraz zahŕňa virtualizačné technológie.

Ak teda máme sieť CDN, ktorá sa má postupne rozrastať a v rámci nej sú využívané kapacity rôznymi telekomunikačnými a multimediálnymi operátormi, tak musí prísť otázka aj na operátorov, či vlastne potrebujú využívať siete CDN. Žiaľ staršie siete a architektúry využívané operátormi nie sú také flexibilné alebo škálovateľné na to, aby zvládli dnešný nápor dát, preto sa hľadajú iné riešenia. To je jeden z hlavných dôvodov, že sieťová virtualizácia vo forme SDN a NFV sa stala v posledných rokoch jednou z popredných tém. SDN a NFV môžu dodať telekomunikáciám všeobecne potrebnú flexibilitu, agilitu a škálovateľnosť pre zvládnutie záplav dát v budúcnosti bez nutnosti utrácania bohatstva na zväčšovanie kapacít.

Z týchto dôvodov je potrebná spolupráca medzi poskytovateľmi služieb respektíve telekomunikačnými operátormi a poskytovateľmi sietí CDN. Keď viacerí operátori budú využívať „jednu“ sieť CDN, tak je treba zabezpečiť prístup každému z nich k ich dátam a štatistikám, ktoré využívajú ich koncoví zákazníci, za čo ich ďalej môžu účtovať. Zároveň je treba zabezpečiť kvalitu služieb, ktoré sú poskytované v rámci sietí CDN. Vďaka týmto problémom sa do popredia dostáva SDN a NFV, keďže sa môžu vytvoriť virtuálne CDN pre každého v rámci sietí CDN.

6. Cloud Computing

Podľa **NITS** (***National Institute of Standards and Technology***) je cloud computing model navrhnutý pre umožnenie pohodlného prístupu k zdieľaným konfigurovateľným výpočtovým zdrojom (sieťam, serverom, úložiskám, aplikáciám, službám), ktoré môžu byť okamžite zabezpečené a poskytnuté s minimálnym manažmentom alebo potrebou zásahu poskytovateľa tejto služby [49]. Definícia podľa RAD Lab na univerzite v Berkeley hovorí [50], že cloud computing zodpovedá aplikáciám dostupným cez Internet a taktiež hardvéru i softvéru v datacentre, ktorý tieto služby poskytuje. Cloud computing je v podstate distribuovaná počítačová forma, ktorá poskytuje svoje prostriedky širokému spektru používateľov na škálovanie, virtualizáciu hardvérovej a/alebo softvérovej infraštruktúry cez Internet. Cloud computing povoľuje zdieľať svoje výpočtové zdroje cez Internet. Pozostáva zo súboru technológií, ktoré ponúka poskytovateľ vo forme služieb samotným zákazníkom. Napríklad ukladací priestor, výpočtový výkon za použitia hardvérovej/softvérovej distribuovanej virtualizovanej siete. Poskytovateľ týchto služieb môže vlastniť alebo hosťovať hardvér alebo softvér potrebný pre používanie rôznych domovských alebo biznis aplikácií. Cloud computing je kompletný a rýchlo sa vyvíjajúci koncept. Cloud computing môže byť považovaný za distribuovaný systém, ktorý ponúka výpočtový výkon cez počítačovú komunikačnú sieť, zvyčajne cez Internet. Zdroje v cloude sú jasne definované pre používateľa a používateľ nepotrebuje vedieť, kde presne sa tieto zdroje nachádzajú. Tie môžu byť zdieľané medzi väčším počtom používateľov, ktorí sú schopní pristupovať k aplikáciám a dátam kedykoľvek a odkiaľkoľvek. Jednoduchým príkladom cloud computingu je e-mail. Poskytovateľ e-mailovej služby spravuje server a poskytuje k nemu prístup. Používateľ jednoducho zadá iba adresu do prehliadača a používateľské údaje na prihlásenie. Softvér a úložisko nie sú na jeho osobnom počítači, ale existujú ako služba na cloude. Hlavným cieľom cloud computingu je vytvorenie lepšieho využitia distribuovaných zdrojov. Rieši tiež problémy veľkého škálovania výpočtového výkonu. Slovo "cloud - mrak" je metafora, ktorá znázorňuje web ako priestor, kde sú výpočtové zdroje predinštalované a existujú ako služba [49]. Operačný systém, aplikácie, ukladací priestor, dáta a kapacita spracovania dát, to všetko existuje ako webová služba, ktorá je pripravená byť zdieľaná medzi používateľmi. Používanie cloudových služieb má výhody využívania veľkého množstva výpočtového výkonu alebo diskového priestoru, ktorý je zároveň poskytovaný ako internetová služba. Nie je potrebné fyzicky vlastniť servery v rámci korporátnej siete, postačí mať osobný počítač a softvér. Všeobecne sú tieto služby poskytované transparentným spôsobom, kde platforma zjednodušuje celú zložitosť infraštruktúry cloudu pred používateľmi a aplikáciami. V cloud computing modeloch sú výpočtový výkon, softvér, úložiská a platformy na vyžiadanie poskytované zákazníkom cez Internet. Všetky typy aplikácií od textových editorov po softvér na úrovni administrácie môžu pracovať v cloude. Prístup, ktorý táto technológia poskytuje k zdrojom a službám, môže byť zväčšovaný alebo zmenšovaný podľa požiadaviek. Za cloud computing sa účtuje poplatok podľa množstva využívaných zdrojov. Zatiaľ čo výhod cloud computingu je mnoho, jeho nevýhod je len niekoľko. Ak je cloud computing vhodne použitý, je vhodný pre každý typ biznisu. Hlavnými výhodami cloud computingu sú samoobslužné služby na vyžiadanie, všadeprítomný prístup k sieti, združovanie zdrojov nezávisle na umiestnení a prenos rizika. Ďalšími výhodami sú nízke prevádzkové náklady, jednoduchá správa, kvalita služieb, spoľahlivosť, žiadne veľké investície do infraštruktúry, lepšie prispôsobovanie a škálovateľnosť a lepší manažment (riadenie preťaženia dopytu). V dnešnej dobe sú najväčšími výzvami cloud

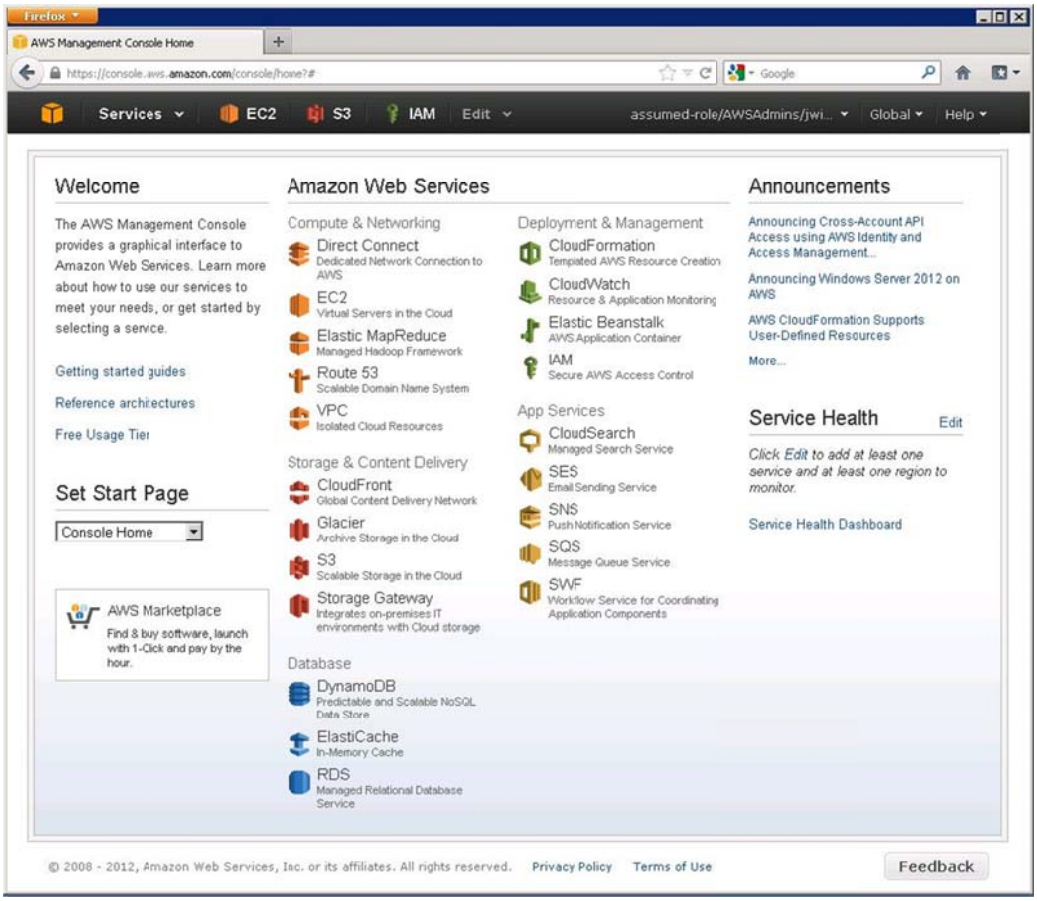
computingu súkromie a bezpečnosť. Nevýhodami sú nedostatočná alebo limitovaná kontrola, priama závislosť na poskytovateľovi, ktorá je známa ako "vendor lock-in". Je ťažké migrovať technológiu od jedného poskytovateľa k druhému. Vivek Kundra, Federal CIO a kedysi technologický riaditeľ pre oblasť Kolumbia povedal: "Cloud bude robiť pre vládu to, čo Internet v 90-tych rokoch," [51].

6.1. História

Informačné technológie boli vždy považované na hlavný kameň úrazu podnikových organizácií z pohľadu nákladov a manažmentu. Informačný priemysel získal mnoho skúseností a výrazne sa posunul v posledných desaťročiach. Faktory ako komoditizácia hardvéru (značka hardvéru už nie je dôležitá), open-source softvér, virtualizácia, globalizácia pracovnej sily a agilné IT procesy podporovali vývoj nových technológií a biznis modelov. Cloud computing je prirodzenou evolúciou virtualizácie, architektúry orientovanej na služby s užitočným výpočtovým výkonom. V skutočnosti je cloud computing novým výrazom pre dlho udržiavaný sen computingu ako prospešného nástroja, ktorý sa do komerčnej reality prepracoval pred nedávnom. Táto evolúcia začala v 50-tych rokoch, kedy bolo umožnené viacerým používateľom pristupovať k centrálnemu počítaču cez veľmi limitované terminály. Neskôr v 70-tych rokoch bol vytvorený koncept virtuálnych strojov. Vývoj cloud computingu sa zrýchlil v 90-tych rokoch, kedy Internet začal poskytovať značné šírky pásma a telekomunikačné spoločnosti začali ponúkať virtualizované privátne siete.

Niektorí experti pripisujú koncept cloudu Johnovi McCarthymu, profesorovi na Univerzite Stanford a vynálezcovi programovacieho jazyka Lisp, ktorý navrhol v roku 1961 myšlienku výpočtového výkonu, ktorý by bol verejne doručiteľný a bol by podobný princípom verejného výpočtového strediska. V roku 1966 Douglas F. Parkhill vydal knihu "The Challenge of the Computer Utility"[52], ktorá obsahovala víziu budúceho computingu predpovedajúc, že počítačový priemysel sa bude podobať verejnému záujmu "v ktorom mnoho vzdialených používateľov je pripojených cez komunikačné linky do centrálneho počítačového zariadenia". V knihe je uvádzaných niekoľko charakteristík cloud computingu (pružné poskytovanie dodávané ako služba, ilúzia/pocit neobmedzeného množstva). A. Regalado v článku "Who coined Cloud Computing" [53] uviedol, že "mnohí veria v prvé nasadenie cloud computingu". Jeho moderný kontext 9.augusta 2006 Google CEO Eric Schmidt predstavil na priemyselnej konferencii." Čo je zaujímavé, že vzniká nový model", povedal Schmidt. "Nemyslím si, že ľudia pochopia aká veľká príležitosť to skutočne je. Začína s predpokladom, že dátové služby a architektúra by mali byť na serveroch. Nazývame to cloud computing - mali by byť niekde v oblakoch (cloude)." Jeden z prvých míľnikov v histórii cloud computingu bol príchod Salesforce.com v roku 1999, ktorá napredovala v koncepte doručovania podnikových aplikácií dostupných z webovej stránky. Táto spoločnosť vydláždila cestu špecializovaným i mainstreamových spoločnostiam so softvérom, ktoré mohli doručovať aplikácie cez Internet a hrala veľmi dôležitú úlohu pri predstavovaní konceptu ***Software as a Service*** (**SaaS**) - softvér ako služba. SaaS model povoľuje spoločnostiam pristupovať k softvéru on-line a platiť len za služby a aplikácie, ktoré používajú. Ďalší krok priniesla spoločnosť Amazon v roku 2002 s Amazon Web Service, ktorá poskytovala súbor cloudovo založených služieb vrátane úložného priestoru a výpočtového výkonu. Stránky tretích strán (iných organizácií) mohli prehľadávať a zobrazovať produkty z webovej stránky Amazon a pridávať položky do nákupného košíka. Prvotná verzia AWS v roku 2002 bola zameraná na tvorbu informácií dostupných z Amazonu smerom k partnerom pomocou modelu

webových služieb s programovou a vývojovou podporou a bola zameraná na Amazon ako maloobchodný predaj. V auguste 2006 Amazon spustil komerčnú webovú službu, svoj Elastic Compute cloud (EC2). Toto riešenie dalo používateľom možnosť ukladať dáta z vonku, prenajímať si výpočtové cykly ako službu a poskytovať on-line služby pre ďalšie webové stránky alebo klientske aplikácie. Pravdepodobne bol EC2 prvý široko prístupný cloud s infraštruktúrou ako služba.



Obr. 18 Konzola od Amazonu pre manažment webových služieb

Spustenie Google App Engine v apríli 2008 bolo vstupom prvej hernej technologickej spoločnosti na trh cloud computingu. Google Apps služby poskytli tejto spoločnosti možnosť začať ponúkať podnikové aplikácie bežiace cez webový prehliadač. Microsoft niekoľko rokov neakceptoval web ako významný trh a pokračoval v zameraní na desktop trhy. V novembri 2009 Microsoft zmenil toto kritérium a spustil Windows Azure cloud computing platformu. Táto platforma poskytuje PaaS aj IaaS služby a podporuje rôzne programovacie jazyky, nástroje a aplikačné štruktúry. V roku 2014 bola premenovaná na Microsoft Azure. V decembri 2013 bol spustený Google Compute Engine. Táto infraštruktúra umožňuje používateľom vytvárať a spúšťať virtuálne stroje na vyžiadanie s rozličnými konfiguráciami. V rokoch 2009-2010 si získal pozornosť open source cloud. Existuje množstvo cloud computing služieb, ktoré sú písané v open source kóde alebo sú začlenené do množstva open source aplikácií. Použitie open source kódu v cloud computingu umožňuje vývojárom tvoriť aplikácie na existujúcej aplikačnej infraštruktúre, využívajúc nízke náklady, väčšiu flexibilitu a pravdepodobne robustnejšie

aplikácie (s menším množstvom chýb) ako tie, ktoré sú vyvíjané individuálne. Naprieč mnohým cloud computing modelom služieb existuje veľké a rozmanité množstvo aplikácií či už v komerčnej alebo open source sfére ako napríklad Apache Cloudstack, Eucalyptus, OpenNebula a OpenStack [54]. Príchod aplikácií od Microsoftu, Google, Amazon, Apple, Cisco a ďalších veľkých IT spoločností má za následok široké prijatie on-line služieb a predstavuje relevantný prínos pre nasadzovanie cloud computingu.

6.2. Vlastnosti cloud computingu

Cloud computing je model pre všadeprítomný, pohodlný sieťový prístup na vyžiadanie k zdieľanému súboru konfigurovateľných výpočtových zdrojov (siete, servery, disky, aplikácie a služby), ktoré môžu byť okamžite vyhradené a poskytnuté s minimálnym manažmentom bez zásahu samotného poskytovateľa. Podľa NIST tento cloud model pozostáva z piatich nevyhnutných vlastností: samoobslužný systém na vyžiadanie, široký sieťový prístup, delenie zdrojov, pružnosť, meranie služby. Ďalej obsahuje niekoľko spoločných vlastností ako škálovateľnosť, virtualizácia, orientácia na služby, pružný výpočtový výkon, zvýšená bezpečnosť, geograficky distribuovateľný, atď. Päť základných vlastností je krátko popísaných nižšie:

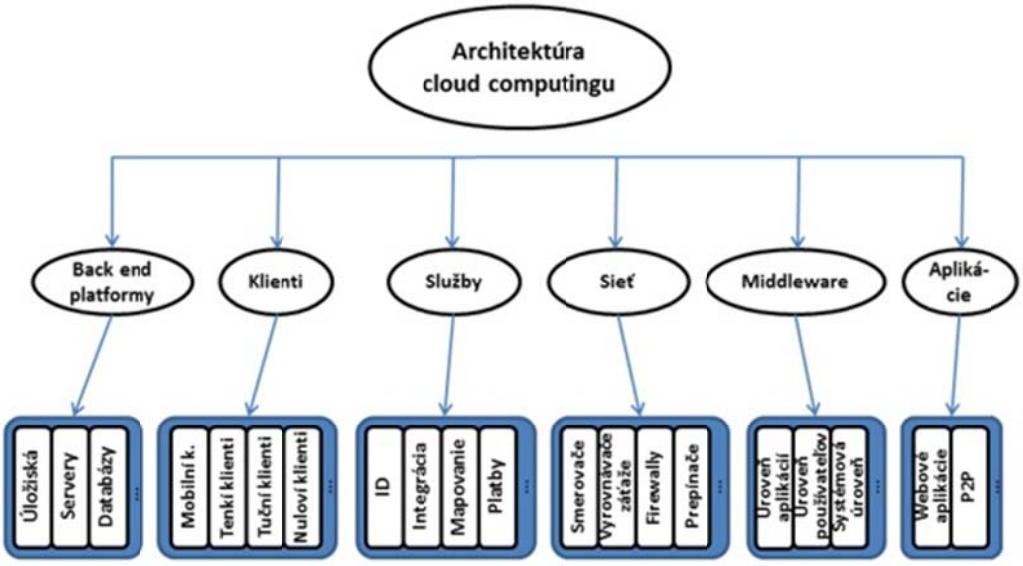
1. Samoobslužné služby na vyžiadanie. Cloud computing poskytuje zdroje ako sú serverový čas a sieťové úložisko na vyžiadanie vtedy, keď to zákazník chce. Zdroje vrátane úložiska, procesora, pamäte a rýchlosti pripojenia. Zákazník môže jednostranne zabezpečovať výpočtové prostriedky. To je možné pomocou samoobsluhy a automatizácie. Samoobsluha znamená, že zákazník vie vykonať všetky potrebné kroky, aby zrealizoval požadované služby. Jeho požiadavky sú automaticky spracované cloud infraštruktúrou bez ľudskej interakcie na strane poskytovateľa. Tieto vlastnosti zahŕňajú vysokú úroveň plánovania, keďže zákazník môže kedykoľvek zmeniť svoje požiadavky a očakáva ich realizáciu do pár minút. Poskytovateľ cloud riešenia by mal sledovať trendy využívania zdrojov a na základe nich plánovať budúce možné situácie.
2. Široký sieťový prístup. Prístup k technológii je umožnený cez sieť pomocou rôznych klientskych platforiem vďaka použitiu štandardných mechanizmov. To nezahŕňa len klasické zariadenia (laptopy, pracovné stanice, atď.) ale tiež mobilné telefóny, tenkých klientov a mnohé iné. Sieť, úložisko a výpočtové zdroje boli obmedzené a veľmi nákladné ešte pred niekoľkými rokmi. Postupom času sa náklady spojené s týmito prostriedkami znižovali dôsledkom škálovateľnosti výroby a komoditizácii súvisiacich technológií. Ako sa zvyšovala prenosová rýchlosť vzrastal sieťový prístup a škálovateľnosť. "Široký sieťový prístup" je vnímaný ako charakteristická črta a ako prístup.
3. Delenie zdrojov. Zdroje poskytovateľa cloudovej služby sú delené medzi niekoľkých používateľov vďaka modelu viacnásobného nájomníka "multi- tenant model" s rozličnými fyzickými a virtuálnymi zdrojmi dynamicky prideľovanými na vyžiadanie zákazníka. Tento koncept je základným predpokladom škálovateľnosti v cloude. Prostredia viacnásobných nájomníkov, kde niekoľkí používatelia zdieľajú takmer rovnaké zdroje v cloude s inými používateľmi sú základom verejnej cloud infraštruktúry. Pri viacnásobnom prenájme je neodmysliteľnou časťou zvyšovanie operačných nákladov, ktoré môžu byť kompenzované istou hardvérovou konfiguráciou a softvérovými

riešeniami ako aplikácie a serverové profily. Delenie zdrojov poskytuje pocit nezávislosti na umiestnení. Vo všeobecnosti používateľ nevie, kde konkrétne sa jeho zdroje nachádzajú. Bez princípu viacnásobného prenájmu a delenia zdrojov by cloud finančne nedával zmysel.

4. Pružnosť. Pružnosť je v zásade pomenovanie škálovateľnosti, ktorá je schopná pridávať alebo odoberať kapacitu, výpočtový výkon a pamäť, keď je to potrebné. Vlastnosť je premenovaná kvôli prostriedkom, ktoré sú vyčlenené a poskytnuté, v niektorých prípadoch automaticky, aby rýchlo upravovali požiadavky na zvyšovanie alebo znižovanie potrebných zdrojov. Pre používateľov sa prostriedky často javia ako neobmedzené a môžu si ich vymedziť v ľubovoľnom množstve a čase. Množstvo implementácií je založených na pridávaní a odoberaní uzlov, serverov alebo inštancií do alebo z fondu ako klaster alebo farma. Dobre známym príkladom je pridávanie kompenzácie záťaže pred farmu webových serverov, ktorá distribuuje požiadavky.
5. Meranie služieb indikuje, že používané zdroje sú monitorované, kontrolované a reportované používateľom. Poskytujú transparentný prehľad pre používateľa i poskytovateľa o spotrebe a nákladoch. Toto je rozhodujúce pre fakturáciu, kontrolu prístupu, optimalizáciu zdrojov, plánovanie kapacít a ďalšie úlohy.

6.3. Komponenty a architektúra Cloud computingu

Mnoho autorov zdôrazňuje použitie a prístup k výpočtovým zdrojom založených na viacnásobných serveroch, kde poukazujú na architektúru cloud computingu. Napriek tomu architektúra cloud riešenia je štruktúra systému, ktorý typicky obsahuje cloudové zdroje (back end platformu, servery, úložiská), služby, sieť, middleware a softvérové komponenty, ich viditeľné vlastnosti z vonku a vzťahy medzi nimi (**Obr. 19**) [55].



Obr. 19 Komponenty cloud computingu

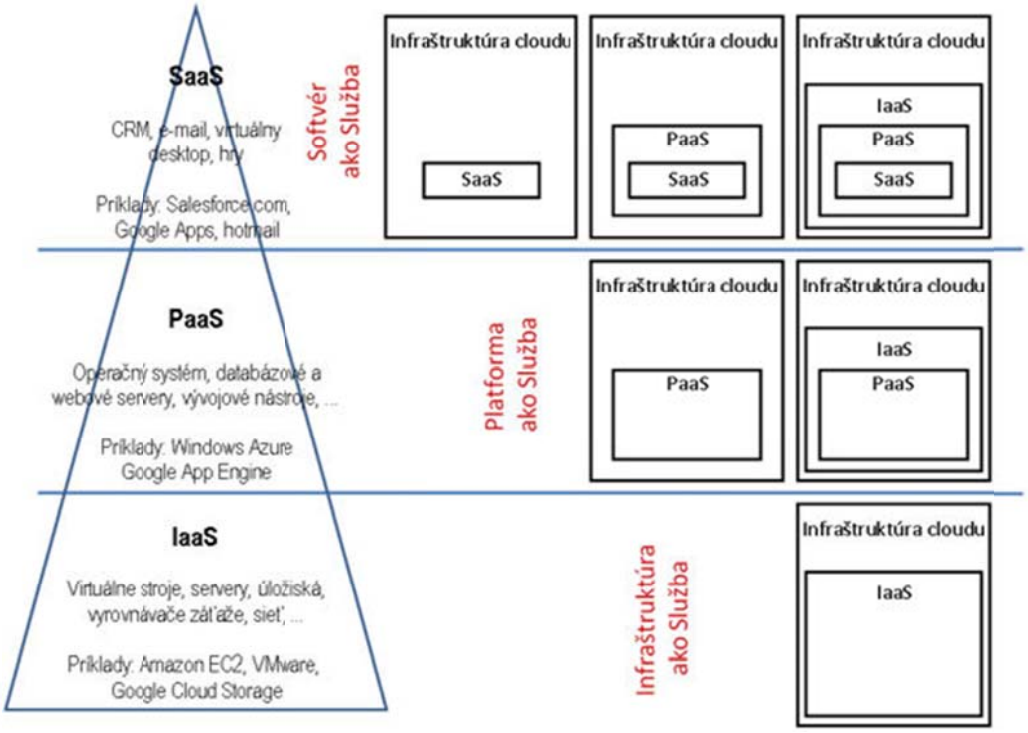
Ďalšie komponenty sú popísané nižšie.

1. Back end platforma. Tieto servery sú veľmi veľké, vedia udržiavať masívne množstvo dát a môžu byť umiestnené kdekoľvek na svete. Častokrát sú servery na rozličných miestach, ale správajú sa ako keby boli vedľa seba. Okrem toho existuje aj centrálny server, ktorý manažuje celý systém, monitoruje prevádzku a požiadavky klientov aby sa uistil, že všetko beží v poriadku.
2. Cloud používatelia môžu pristupovať pomocou klientov ku cloud zdrojom, vrátane tučných klientov, tenkých klientov, nulových klientov, tabletov, mobilných zariadení. Tieto klientske platformy spolupracujú s cloudovým dátový úložiskom cez aplikáciu (middleware), cez webový prehliadač alebo cez virtuálne spojenie.
3. Sieť. Čo sa týka klientskej strany, využívanie cloud computing služieb podnikmi znamená, že IT servery a úlohy serverového manažmentu vymenili za siete a sieťový manažment. Z toho dôvodu je niekoľko požiadaviek na sieť. Na druhej strane v súvislosti s poskytovateľom, podmienky siete musia zabezpečiť, aby celá komunikácia prebiehala hladko, jednoducho a s ohľadom na bezpečnosť. Je dôležité mať inteligentnú, spoľahlivú a funkčnú sieť, ktorá poskytuje inovácie ďalšej generácie.
4. Middleware je softvér, ktorý vytvára spojenie medzi ľubovoľnými dvoma klientmi, servermi databázami alebo dokonca aplikáciami. Cloud middleware poskytuje používateľom niekoľko funkcionalít, ktoré im pomáhajú pri tvorbe biznis aplikácií: podporujú súčinnosť, transakcie, paralelizáciu činností a výmenu správ.
5. Služby. Cloudové služby sú služby, ktoré podporujú riešenia založené na cloude ako manažment identity, integrácia služba-služba, mapovanie, fakturácia/platby, vyhľadávanie, ...
6. Aplikácie. Cloud aplikácia (Cloud App) je aplikačný program, ktorý beží v cloude s niektorými vlastnosťami desktopovej aplikácie a vlastnosťami webovej aplikácie. Zvyčajne sú tieto aplikácie postavené cez high-level integrované prostredie. Príkladom je Google App Engine, ktorý umožňuje používateľom vytvoriť aplikácie na tých istých škálovateľných systémoch ako výkonné Google aplikácie.

6.4. Modely služieb

Cloud computing ponúka nové možnosti podľa toho ako je realizovaná infraštruktúra. Šetrí náklady a deleguje záväzky na stranu poskytovateľa. Stal sa ucelenou časťou technológie a biznis modelu. Núti biznis aby sa adaptoval na nové technologické stratégie. Dopyt po cloud computingu zrýchlil vývoj nových trhových ponúk, reprezentujúcich rozličné cloudové služby a doručovacie modely. Tieto modely významne rozširujú rozsah dostupných možností a organizáciu úloh pri sťažených situáciách, ktoré cloud computing model využíva.

Modely služieb popisujú ako sú cloudové služby dostupné klientom (**Obr. 20**). V súlade s NITS existujú tri modely služieb: SaaS (softvér ako služba), PaaS (platforma ako služba) a IaaS (infraštruktúra ako služba), ktoré sú popísané v nasledujúcich kapitolách. V skutočnosti je najzákladnejší model služieb kombináciou IaaS, PaaS a SaaS. Tieto modely služieb môžu spolupracovať medzi sebou navzájom a byť nezávislé. Ale napríklad PaaS je závislá na IaaS, pretože aplikačné platformy potrebujú fyzickú infraštruktúru.



Obr. 20 Modely služieb [56]

Dnes si spoločnosti viac uvedomujú hodnotu a šetrenie zdrojov softvéru a platformových služieb než infraštruktúry. Z toho dôvodu IaaS model je schopný držať strácajúci podiel na trhu oproti PaaS a SaaS. V blízkej budúcnosti sa očakáva významný počet trhových konsolidácií s niekoľkými významnými hráčmi, ktorí si ponechajú kontrolu až do konca [57].

6.4.1. Softvér ako služba

SaaS (softvér ako služba) je softvérový distribučný model, v ktorom sú aplikácie hosťované samotným predajcom alebo poskytovateľom služieb. Sú sprístupnené zákazníkom cez sieť, typicky cez Internet. Táto vlastnosť eliminuje potrebu inštalovať softvér na strane klienta a môže byť nápomocnou pre mobilných alebo dočasných pracovníkov. E-mail je jednoduchý príklad SaaS. Ak používateľ má poskytovateľa služieb, vyžaduje desktopovú alebo mobilnú aplikáciu na prístup k e-mailom. Môže hosťovať na individuálnom serveri. Je dôležité poukázať na to, že používateľ nemôže riadiť infraštruktúru cloudu alebo dokonca individuálne schopnosti aplikácií s možnou výnimkou pre limitovanú konfiguráciu používateľsky špecifickej aplikácie. Výhody SaaS sú:

1. Šetrenie nákladov: Malé alebo žiadne kapitálové investície.
2. Flexibilita: Ponúkaná ako služba na vyžiadanie.
3. Stabilita: SaaS aplikácie sú inštalované na profesionálnom, zabezpečenom a redundantnom hardvéri.
4. Okamžité nasadenie: Od žiadneho po veľmi malý čas na vyhradenie a nasadenie.
5. Dostupnosť: Jediná potrebná vec je internetové pripojenie.

6. Nové aktualizácie: Poskytovatelia služieb aktualizujú riešenie a je automaticky dostupné pre zákazníkov. Náklady spojené s tým spojené sú oveľa nižšie než pri tradičných modeloch.

Okrem nedostatočnej kontroly jednou z hlavných nevýhod je, že SaaS aplikácie nemusia mať rovnaké vlastnosti ako non-SaaS aplikácie. Funkcionalita nie je často prepracovaná alebo plná. Tento problém bude časom zmenšený. Vývojové nástroje pre SaaS aplikácie sa stávajú oveľa viac spôsobilé. Nakoniec, rýchlosť môže byť aj nevýhodou. Všeobecne SaaS aplikácie sú pomalšie než jej non-SaaS ekvivalenty. Príklady SaaS poskytovateľov:

1. Google Apps poskytuje webové kancelárske nástroje ako e-mail, kalendár a dokumenty.
2. Salesforce.com poskytuje plné **CRM** (***Customer Relationship Management***) aplikácie.
3. Zoho.com poskytuje veľký súbor webovo založených aplikácií, väčšinou pre firemné účely.

6.4.2. Platforma ako služba

PaaS (Platforma ako služba) je kategória cloud computingu, ktorá poskytuje platformu a prostredie aby umožnila vývojárom tvoriť aplikácie a služby cez Internet. PaaS služby sú hosťované v cloude a dostupné cez webový prehliadač. Zvyčajne je to spôsob prenájmu hardvéru, operačného systému, úložiska a sieťovej kapacity cez Internet. Model služieb poskytuje zákazníkom možnosť si prenajať virtualizované servery a príslušné služby pre používanie vlastných aplikácií, ktoré sú vytvorené pomocou programovacích jazykov, knižníc, služieb a nástrojov podporovaných samotným poskytovateľom. Platformy pre vývoj aplikácií povoľujú používateľom tvoriť a hosťovať aplikácie väčších rozmerov než by boli schopní zvládnuť individuálne. PaaS poskytovatelia môžu asistovať vývojárom od konceptu ich originálnej myšlienky až po vytvorenie aplikácií, testovanie a nasadenie. Toto všetko je obsiahnuté v manažovanom mechanizme. Zákazník nemanažuje ani nekontroluje infraštruktúru cloudu vrátane siete, serverov, operačných systémov alebo úložiska, ale kontroluje pomocou aplikácií a možností konfiguračných nastavení samotné prenajaté prostredie. Profituje z nízkych ekonomických nákladov, ktoré vychádzajú zo zdieľania infraštruktúry medzi viacerými používateľmi a tie sa odrážajú v nízkej cene. PaaS služby sú všeobecne platené za odber prostriedkov, ktoré sú v skutočnosti čerpané. Príklady prostriedkov, ktoré sú obsiahnuté v PaaS:

1. Operačný systém
2. Skriptovacie prostredie na servery
3. Systém na správu databáz
4. Serverový softvér
5. Podpora
6. Úložisko dát
7. Sieťový prístup
8. Nástroje na dizajn a vývoj
9. Hosťovanie

Výhody PaaS sú:

1. Pokiaľ ide o vývoj softvéru vývojári môžu používať individuálne PaaS prostredia na každej úrovni procesu vývoja, testovať a nakoniec hosťovať aplikáciu.
2. Tím môže spolupracovať na diaľku. Každý člen je kdekoľvek schopný pracovať na projekte.
3. Flexibilita: Zákazníci majú kontrolu cez rôzne nástroje, ktoré sú nainštalované v rámci ich platformy a môžu vytvoriť platformu, ktorá sa hodí ich špecifickým požiadavkám.
4. Šetrenie nákladov: Netreba investovať do fyzickej infraštruktúry.
5. Maximalizácia prevádzky: PaaS poskytovatelia by mali mať nástroje, technológie a skúsenosti, aby pomohli používateľom predísť neplánovaným výpadkom.
6. Jednoduché škálovanie. Vlastnosti PaaS sa môžu meniť ak to okolnosti vyžadujú.

Jedna z výhod PaaS je, že v závislosti na ponukách spoločnosti poskytuje PaaS možnosť uzavrieť používateľa do špecifického softvérového prostredia, jazyka alebo rozhrania. To môžu zabezpečiť len niektorí poskytovatelia, nie všetci. Príklady PaaS:

1. Google App Engine poskytuje používateľom kompletný vývojársky zásobník a umožňuje im, aby ich aplikácie bežali na Google infraštruktúre.
2. Akamai EdgePlatform poskytuje veľkú distribuovanú počítačovú platformu, na ktorej organizácie môžu nasadzovať ich vlastné webové aplikácie. Majú zameranie na analýzu a monitorovanie.
3. Microsoft Azure poskytuje výpočtový výkon a služby dátového úložiska založené na vývojovej platforme Windows.
4. Yahoo! Open Strategy (Y!OS) poskytuje používateľom prostriedky na vývoj webových aplikácií založených na existujúcej službe Yahoo!

6.4.3. Infraštruktúra ako služba

IaaS (infraštruktúra ako služba) je model poskytovania, v ktorom prenajaté zdroje tvoria operačné systémy, zabezpečenie, sieť, úložisko a servery pre vývoj aplikácií, služieb a pre nasadzovanie vývojových nástrojov, databáz, atď. Poskytovateľ služieb vlastní zariadenie a je zodpovedný za hosťovanie, chod a správu. Klient platí podľa používania. Namiesto pripravených aplikácií a služieb je poskytovaná sieť. Najpoužívanejšie IaaS systémy obsahujú virtuálne servery, kompenzácie preťaženia a sieťové pripojenie. IaaS umožňuje organizáciám a vývojárom rozširovať ich IT infraštruktúru na požiadanie. Poskytovateľ cloud riešenia má súbor virtualizovaných výpočtových zdrojov a diskov, ktoré používateľ môže využívať. Toto je computing na vyžiadanie a stará sa o nepravidelnosti vo výkyvoch. Fyzicky je súbor hardvérových zdrojov ťahaný z veľkého množstva serverov a sietí, zvyčajne distribuovaných medzi niekoľkými dátovými centrami. Za správu všetkých centier je zodpovedný poskytovateľ. Na druhej strane je klientovi daný prístup k virtualizovaným komponentom na zostavenie vlastnej IT platformy. Klient nemanažuje ani neriadi infraštruktúru cloudu, ale má kontrolu operačného systému, disku a nasadených aplikácií a možnosť obmedzenej kontroly vybraných sieťových komponentov (firewally). Výhody IaaS sú:

1. Rýchly a jednoduchý prístup k podnikovým riešeniam.

2. Škálovateľnosť: Zdroje sú stále dostupné a pokiaľ klient chce viac zdrojov, v okamihu ich má k dispozícii. Pokiaľ zdroje nepotrebuje môže požiadavky znížiť.
3. Jednoduchosť: Poskytovateľ má na starosti manažment zdrojov, obstarávanie hardvéru a softvéru, záplaty a všetky komplexné úkony spojené s infraštruktúrou.
4. Žiadne investície do hardvéru: Fyzický hardvér, ktorý podporuje IaaS služby je inštalovaný a spravovaný poskytovateľom cloudových služieb, šetrí čas a náklady klienta.
5. Nezávislosť na umiestnení: Služba môže byť prístupná z ľubovoľného miesta pokiaľ má prístup na Internet a bezpečnostný protokol cloudu to povolí.
6. Fyzická bezpečnosť umiestnenia dátového centra: Služby dostupné cez verejný cloud alebo privátne cloudy hosťované externe u poskytovateľa cloudu, výhody fyzickej bezpečnosti pre servery v rámci dátového centra.
7. Rýchle nasadenie: Malý alebo žiadny čas pre nasadenie.

Vo väčších biznisoch je hlavnou výhodou posledný spomínaný bod. Je spojený so včasným nasadením pri nepredvídaných okolnostiach a potrebách. Hlavnou nevýhodou IaaS je biznis riziko. Aj s veľkým úsilím, auditmi a proaktívnym manažmentom IaaS vyžaduje dôveru v infraštruktúru predajcu s ohľadom dostupnosť, dátovú bezpečnosť, atď. Príklady poskytovateľov IaaS:

1. Amazon Elastic Compute Cloud (EC2) poskytuje používateľom špeciálny virtuálny stroj (AMI), ktorý môže byť nasadený a bežiaci na EC2 infraštruktúre.
2. Amazon Simple Storage Solution (S3) poskytuje používateľom prístup do dynamicky škálovateľného úložiska.
3. Microsoft Live Mesh poskytuje používateľom prístup do distribuovaného súborového systému zameraného na individuálne použitie.
4. IBM Computing on Demand (CoD) poskytuje prístup ku konfigurovateľným serverom a ako pridanú hodnotu služieb dátové úložisko.

Spoločne s ďalšími dvomi formami cloud hostingu môže byť IaaS využívaná firemnými zákazníkmi na tvorbu cenovo výhodných a jednoducho škálovateľných IT riešení. Komplexnosť a výdavky spojené so správou hardvéru sú prenechané poskytovateľovi riešenia. Ak sa škála biznisu zákazníckych operácií mení alebo sa majú rozširovať, môžu zákazníci čerpať cloud zdroje keď potrebujú. Je to výhodnejšie ako by zdroje kupovali, inštalovali a integrovali hardvér svojpomocne.

6.5. Modely nasadenia

Zvyčajne sa používajú štyri modely nasadenia cloudu: privátny, verejný, hybridný a komunitný. Posledný z nich sa používa najmenej.

1. Privátny cloud je vystavaný a spravovaný v rámci jedinej organizácie. Organizácie používajú softvér, ktorý umožňuje funkcionalitu cloudu, napríklad VMware.
2. Verejný cloud pozostáva z výpočtových zdrojov poskytnutých poskytovateľom. Medzi najpopulárnejšie verejné cloudy patria Amazon Web Services, Google AppEngine a Microsoft Azure.

3. Hybridný cloud je kombináciou výpočtových zdrojov poskytnutých privátnymi aj verejnými cloudmi.
4. Komunitný cloud zdieľa výpočtové zdroje medzi viacerými organizáciami a môžu ho spravovať IT zdroje z organizácií, ale aj od iných poskytovateľov.

V budúcnosti bude dominantný verejný model nasadenia cloudu, ktorý sa bude ďalej rozširovať. Privátne a hybridné modely nasadenia zostanú v nasledujúcich rokoch používané, ale ich podiel na trhu bude neustále klesať. Z dlhodobého hľadiska budú privátne a hybridné modely cloudu využívané zrejme iba na špecifické biznis riešenia.

6.5.1. Verejný cloud

Verejné cloudy poskytujú širokej verejnosti poskytovatelia služieb, ktorí spravujú cloudovú infraštruktúru. Vo všeobecnosti verejní poskytovatelia cloudu ako Amazon AWS, Microsoft a Google vlastnia a riadia infraštruktúru a cez Internet ponúkajú prístup na otvorené použitie širokej verejnosti. S takýmto modelom zákazníci nevidia ani neovplyvňujú, kde sa infraštruktúra nachádza. Je potrebné poznamenať, že všetci zákazníci verejného cloudu zdieľajú tú istú čiastkovú infraštruktúru s obmedzenou konfiguráciou, bezpečnostnou ochranou a variantmi dostupnosti. Ako príklady môžeme uviesť služby určené pre širokú verejnosť ako sú služby on-line ukladanie fotiek, e-mailové služby či stránky sociálnych sietí. Vo verejnom cloude však môžu byť poskytované aj služby pre podniky. Vo verejných cloudoch sa zdroje ponúkajú ako služba. Používatelia môžu meniť svoje potreby na požiadanie a nemusia kvôli tomu nakupovať hardvér. Poskytovatelia verejného cloudu spravujú infraštruktúru a rozdeľujú ju podľa kapacitných požiadaviek používateľov. Zákazníci verejných cloudov využívajú ekonomickejšie možnosti rastu, pretože náklady na infraštruktúru sú rozdelené rovnomerne medzi všetkých používateľov. Vďaka tomu môže každý klient fungovať samostatne, nízkonákladovo, systémom "pay-as-you-go". Ďalšou výhodou verejných cloudových infraštruktúr je, že sú oveľa väčšie ako vnútrofiremné podnikové cloudy. Klienti majú k dispozícii možnosť plynulého škálovania na požiadanie. Tieto cloudy poskytujú najvyššiu úroveň efektívnosti zdieľaných prostriedkov. Verejný cloud je jasnou voľbou, ak:

1. je štandardizovaná záťaž pre aplikácie využívaná množstvom ľudí, napr. e-mail,
2. je treba testovať a vyvíjať aplikačný kód,
3. je nutné postupne navyšovať kapacitu (schopnosť pridať výpočtové zdroje počas špičiek),
4. sa pracuje na spoločných projektoch.

6.5.2. Privátny cloud

V privátnom cloude využíva celú infraštruktúru výhradne jediný klient alebo organizácia. Nie je zdieľaná s inými organizáciami, no môže obsluhovať viacero zákazníkov (napr. obchodné jednotky). Infraštruktúra môže byť umiestnená interne alebo externe a môže ju spravovať buď organizácia sama, niekto iný alebo ich kombinácia. Umožňuje organizáciám ukladať dáta a aplikácie v cloude, ktorý je bezpečnejším a lepšie riadeným prostredím v porovnaní s verejným cloudom. Zdroje sú nasadené za firewallom a prístup k nim môže byť zabezpečený pomocou súkromných liniek alebo zabezpečených šifrovaných spojení cez verejné siete tak, aby prístup k nim mali iba konkrétni klienti, ktorí s nimi môžu pracovať. Cieľom týchto mechanizmov je

minimalizovať bezpečnostné riziká a obmedziť prístup len pre vybraných klientov. Podľa umiestnenia cloudu existujú dve varianty privátnych cloudov [58]:

1. Cloud vo vlastných priestoroch: Tento druh cloudu je umiestnený priamo v priestoroch organizácie. Táto možnosť je vhodná pre organizácie, ktoré investovali do značného serverového a ukladacieho hardvéru. Chcú využiť túto investíciu a použiť hardvér na privátny cloud, napríklad pre aplikácie vyžadujúce kompletnú kontrolu a konfigurovateľnosť infraštruktúry a bezpečnosť.
2. Externe umiestnený privátny cloud: Externe umiestnené cloudy sa nachádzajú u organizácie, ktorá sa špecializuje na cloudovú infraštruktúru. Poskytovateľ služieb zriadi vyhradené cloudové prostredie s úplnou zárukou súkromia. Tento formát sa odporúča organizáciám, ktoré preferujú nevyužívanie verejnej cloudovej infraštruktúry z obáv spojených so zdieľaním fyzických zdrojov.

Pustiť sa do projektu privátneho cloudu vyžaduje značnú úroveň a stupeň snahy o virtualizáciu biznis prostredia. Privátne cloudy sú drahšie, ale bezpečnejšie v porovnaní s verejnými. Významná časť ľudí zodpovedných za IT rozhodnutia sa zameriava výhradne na privátny cloud, keďže tieto cloudy poskytujú najvyššiu úroveň bezpečnosti a kontroly. Privátny cloud označiť za najlepšie riešenie, ak:

1. je potreba vysokej miery kontroly,
2. je kriticky dôležitá bezpečnosť dát a súkromie,
3. je vyžadovaná nezávislosť dát spolu s výhodami cloudu.

6.5.3. Komunitný cloud

Komunitný cloud je model cloudovej služby s viacerými vlastníkmi, ktorú zdieľa niekoľko organizácií zo špecifickej skupiny s podobnými nárokmi na službu (napr. ciele, bezpečnostné požiadavky a vzájomný súlad). Tieto organizácie alebo komunity majú podobné nároky na cloud a ich hlavným cieľom je spolupracovať na dosiahnutí ich obchodných cieľov. Komunitný cloud má svoje vlastné úskalia ako je rozvrhnutie nákladov, zodpovednosti, riadenia a bezpečnosti. Náklady sa rozkladajú medzi menší počet používateľov než pri verejnom cloude (ale väčší než pri privátnom cloude), takže potenciál úspory nákladov nie je taký vysoký. Cloud môžu spravovať priamo organizácie alebo iná organizácia a umiestnený môže byť v priestoroch organizácie alebo mimo nich. Vo všeobecnosti sú verejné cloudové služby finančne výhodnejšie a škálovateľnejšie než privátne cloudy, no sú menej bezpečné. Cieľom komunitných cloudov pre zúčastnené organizácie je zlúčenie výhod verejného cloudu s vyššou úrovňou súkromia, bezpečnosti a súladu s vnútrofiremnými pravidlami, ktoré sú zvyčajne doménou privátneho cloudu. Výhody bezpečnosti v prostredí komunitného cloudu využívajú napríklad vládne, zdravotnícke alebo telekomunikačné komunity, organizácie ale aj regulované súkromné podniky. Okrem využívania priestoru vo verejnom cloude môžu organizácie testovať a pracovať v cloudovej platforme, ktorá je bezpečná, vyhradená iba pre ne a dokonca spĺňajúca špecifické predpisy.

6.5.4. Hybridný cloud

Hybridný alebo kombinovaný cloud je zmesou rôznych metód riadenia zdrojov, napríklad kombinovanie verejných a komunitných cloudov. Na hybridné cloudy sa možno tiež pozerať ako na kombináciu dvoch alebo viacerých cloudov (privátnych, komunitných alebo verejných), ktoré sú zviazané dokopy a ponúkajú výhody viacerých modelov nasadenia s použitím štandardizovanej alebo proprietárnej technológie. Umožňujú prenositeľnosť dát a aplikácií. Všetky tieto techniky sa môžu použiť aj u externých poskytovateľov cloudových riešení buď úplne alebo čiastočne, čo zvyšuje flexibilitu computingu. Hlavnou myšlienkou hybridného cloudu je skombinovať niekoľko cloudových modelov na vytvorenie riešenia na mieru požiadavkám príslušnej organizácie. Architektúra hybridného cloudu vyžaduje cloudovú infraštruktúru priamo v priestoroch organizácie, ako aj server umiestnený mimo nich. Možno ju implementovať rôznymi spôsobmi. Organizácia môže mať napríklad dáta a aplikácie umiestnené v cloude, ktorý zachováva kontrolu nad topológiou siete organizácie a jej vnútornou politikou. Zároveň si môže zachovať existujúcu fyzickú infraštruktúru (hoci tá sa nedá dynamicky meniť) a zapožičiavať si ďalšie zdroje podľa potreby. Hybridné cloudy umožňujú spoločnosti zachovať všetky časti jej podnikania v tom najefektívnejšom prostredí. Okrem toho sú tieto modely ľahko rozšíriteľné, cenovo efektívne (menej citlivé dáta je možné umiestniť z privátneho cloudu do verejného cloudu), bezpečné a flexibilné. Nevýhodou je, že organizácie musia sledovať viacero cloudových bezpečnostných riešení a zaistiť, aby všetky zložky podniku mohli navzájom komunikovať. Hybridný cloud je vhodnou možnosťou v prípade, že:

1. Spoločnosť chce používať verejný cloud na testovanie a vývoj a hosťovaný privátny cloud v spoločnosti chce využívať na produkčné nasadenie.
2. Spoločnosť používa verejné cloudy pre aplikácie smerujúce externe a hosťovaný privátny cloud využíva na interné aplikácie.
3. Spoločnosť chce používať verejný cloud na kontakt so zákazníkmi, ale ich citlivé údaje chce udržiavať v zabezpečenom privátnom cloude.

6.6. Použitie a aplikácie

Cloud computing môže podporovať prakticky akúkoľvek aplikáciu. Niektoré úlohy sú však vhodnejšie pre nasadenie do cloudu z organizačného alebo technického hľadiska. Dva najlepšie príklady pre využitie cloud computingu:

1. Správa Big dát. Cloud computing je ako stvorený na spracovanie analytiky z Big dát, keďže pružná výpočtová kapacita a poskytovanie výkonu na požiadanie robia analýzu dostupnú pre viacero tímov v organizácii. Okrem toho je cloud užitočné riešenie, ak je potrebné množstvo výpočtov na riešenie zložitých úloh alebo ak je potrebná spolupráca viacerých vývojárov. Cloud computing umožňuje efektívnejšie vykonávanie výpočtov pomocou centralizácie ukladania dát.
2. Testovanie a vývoj v cloude. Vývojové tímy využijú pružnosť tvorby virtuálnych strojov za niekoľko minút. Cloud computing nevyžaduje od organizácií, aby si vývojové prostredie zriaďovali pomocou fyzických zariadení, značnej pracovnej sily a času. Okrem toho môže organizácia dostať aplikácie do produkčného prostredia rýchlo a škálovať ich podľa potreby.

Ďalšie relevantné možnosti použitia:

1. Ukladanie súborov a zdieľanie
2. Zálohovanie a obnovenie po haváriách
3. CRM
4. Hosting web stránok

Typické aplikácie:

1. Sociálne siete
2. E-mailové stránky
3. Vyhľadávače
4. Komunikačné riešenia (napr. Skype)
5. Aplikácie na sledovanie času
6. Správa poznámok (napr. Evernote)
7. Tvorba a zdieľanie kancelárskych dokumentov (napr. Google Apps)

6.7. Výhody a nevýhody cloud computingu

Mnoho používateľov a malých aj veľkých podnikov dnes využíva namiesto tradičných alternatív cloud computing, či už priamo (napr. Google alebo Amazon) alebo nepriamo (napr. Twitter). Cloudy ponúkajú používateľom množstvo rôznych výhod. Jednou z najdôležitejších je zníženie nákladov, problémov z vlastnenia a používania počítačov a sietí. Používatelia cloudu nemusia investovať do informačnej infraštruktúry, kupovať hardvér alebo platiť licencie za softvér. Navyše existujú poskytovatelia cloudu, ktorí sa špecializujú na konkrétne oblasti (ako napr. e-mail), čo môže spoločnostiam priniesť užitočné pokročilé služby. Medzi ďalšie výhody pre klientov patria škálovateľnosť, spoľahlivosť a efektivita. Škálovateľnosť znamená, že cloud computing nie je obmedzený výkonovo ani kapacitne. Cloud je spoľahlivý vďaka tomu, že poskytuje prístup k aplikáciám a dokumentom kdekoľvek na svete prostredníctvom Internetu. Cloud computing sa často považuje za efektívny, pretože dovoľuje organizáciám uvoľniť zdroje a použiť ich na inovácie a vývoj produktov. Navyše sa informácie z cloudu ľahko nestratia. Ďalej uvádzame zoznam niektorých najdôležitejších výhod plynúcich z používania cloud computingu:

1. Dostupnosť a univerzálny prístup. Cloud computing umožňuje vzdialeným zamestnancom prístup k zdrojom a aplikáciám v akomkoľvek čase cez bežné internetové pripojenie.
2. Výber aplikácií. Ten umožňuje pružnosť používateľov cloudu vo výbere a skúšaní toho, čo najviac vyhovuje ich potrebám. Cloud computing taktiež umožňuje podnikom používať, pristupovať a platiť iba za to, čo využívajú s rýchlym časom implementácie.
3. Spolupráca. Používatelia začínajú cloud vnímať ako spôsob súbežnej práce so spoločnými dátami a informáciami.

4. Zníženie nákladov. Model "plať-za-použitie" (pay-per-usage) na rozdiel od vlastného hostingu dovoľuje organizácii platiť iba za zdroje, ktoré potrebuje prakticky bez investícií do fyzických zdrojov, ktoré sú dostupné v cloude.
5. Pružnosť. Poskytovateľ transparentne spravuje klientovo využitie zdrojov na základe dynamicky sa meniacich potrieb.
6. Pružnosť. Cloud computing umožňuje klientom rýchlo a jednoducho si meniť aplikácie tak, aby používali takú ktorá najviac vyhovuje ich potrebám.
7. Potenciál byť ekologickejší a ekonomickejší. Priemerné množstvo energie potrebné na výpočtovú činnosť vykonanú v cloude je oveľa menšie než pri vykonaní vo vlastnom prostredí. Je to vďaka tomu, že viacero organizácií môže zdieľať tie isté fyzické zdroje.
8. Zníženie rizika. Organizácie môžu používať cloud na testovanie nápadov a nových konceptov predtým ako by značne investovali do technológie.
9. Škálovateľnosť. Používatelia majú prístup k veľkému množstvu zdrojov, ktoré sa škálujú podľa ich potrieb.
10. Aktuálny softvér. Poskytovateľ cloudu je schopný aktualizovať softvér pri zachovaní spätnej väzby na predošlé verzie softvéru.
11. Virtualizácia. Každý používateľ má jediný pohľad na dostupné zdroje bez ohľadu na to, ako sú usporiadané z pohľadu fyzických zariadení. Preto poskytovateľ môže obslúžiť väčšie množstvo používateľov s menším množstvom fyzických zdrojov.

Napriek tomu existuje niekoľko problémov, ktoré môžu brániť organizácii v používaní cloud computingu. Tu je zoznam takýchto obmedzení:

1. Interoperabilita. Zatiaľ neboli definované univerzálne štandardy a/alebo rozhrania, čo môže viesť k riziku uzamknutia organizácie u jediného poskytovateľa (vendor lock-in).
2. Latencia. Prístup ku cloudu sa deje cez Internet, čo prináša oneskorenie v každej komunikácii medzi používateľom a poskytovateľom.
3. Obmedzenia platformy alebo jazyka. Niektorí poskytovatelia cloudu podporujú iba vybrané platformy a jazyky.
4. Regulácia. V komunite cloud computingu, najmä v organizáciách spravujúcich citlivé dáta, existujú obavy o súdne spory, ochranu dát, férové narábanie s informáciami a medzinárodný prenos dát.
5. Spoľahlivosť. Mnoho existujúcich cloudových infraštruktúr využíva lacnejší hardvér, ktorý môže nečakane zlyhať.
6. Kontrola zdrojov. Množstvo kontroly, ktoré má používateľ nad poskytovateľom cloudu a jeho zdrojmi sa medzi jednotlivými poskytovateľmi značne mení.
7. Bezpečnosť. Hlavnou obavou je súkromie dát. Používatelia nemajú kontrolu ani vedomosť o tom, kde sú ich dáta skutočne uložené. Napriek tomu, z pohľadu forénznej bezpečnosti, použitie cloud computingu môže poskytnúť (platba-za-použitie) vyhradené forénzne obrazy virtuálnych strojov, ktoré sú dostupné bez odpojenia infraštruktúry. To vedie ku kratšiemu času odpojenia potrebného na forénznu analýzu. Môže tiež poskytnúť

finančne efektívnejší priestor na ukladanie záznamov a dovoliť podrobnejšie záznamy bez ovplyvnenia výkonu [59].

6.8. Bezpečnosť cloudu. Možné riziká súkromia

Aj keď existuje mnoho výhod, existujú aj obavy o súkromie a bezpečnosť. Dáta sú prenášané cez Internet a ukladané na vzdialených miestach. Poskytovatelia cloudu navyše obsluhujú množstvo zákazníkov naraz. Toto všetko môže zvýšiť mieru vystavenia sa možným prienikom do súkromia, či už náhodne alebo cielene. Je nutné zabezpečiť, aby bolo s osobnými informáciami narábané zodpovedne [60]. Obavy o bezpečnosť môže zvýšiť dynamický charakter cloudového prostredia. Jednou z hlavných výhod cloudu je rýchlosť s akou môžu poskytovatelia cloudu upravovať, vyvíjať a meniť svoju ponuku. Medzi požiadavkami na rýchlosť, flexibilitu a úroveň bezpečnosti vždy existuje kompromis. Cloud computing so sebou nesie niekoľko rizík pre zákazníkov aj poskytovateľov cloudu spojených s ochranou dát. V niektorých prípadoch môže byť pre zákazníka cloudu (ako správcu dát) zložité efektívne kontrolovať spôsob, akým poskytovateľ cloudu narába s dátami aby si bol istý, že s dátami sa narába zákonným spôsobom. Tento problém je zjavnejší v prípade viacerých prenosov dát, napr. medzi prepojenými cloudmi. Súkromie, vrátane potreby chrániť informácie o identite je základnou otázkou úspechu nasadenia v cloude. Mnoho organizácií sa necíti dobre, ak majú svoje dáta a aplikácie umiestňovať na systémoch, ktoré sídlia mimo ich interných dátových centier. Riziko vystavenia alebo nepovoleného prístupu k citlivým dátam rastie, keď pracovné činnosti migrujú smerom k zdieľanej infraštruktúre. Vzniklo aj mnoho obáv, že cloud computing môže viesť k "function creep" - použitiu dát poskytovateľmi cloudu, ktoré nebolo plánované počas získavania pôvodných dát a na ktoré nebolo dané povolenie. Keď niekto požiada o odstránenie cloudového zdroja, potom podobne ako pri väčšine operačných systémov to nemusí viesť k skutočnému vymazaniu dát. Tiež nemusí byť možné adekvátne alebo včasné odstránenie dát, pretože existujú ich ďalšie kópie, ktoré sú nedostupné alebo preto, že disk, ktorý sa má zničiť obsahuje dáta iných klientov. V prípade viacerých prenájmov a opätovnom použití hardvérových zdrojov to pre zákazníka predstavuje vyššie riziko ako pri vyhradenom hardvéri. Vzhľadom na lacné ukladanie dát, je malý záujem na tom, aby boli informácie z cloudu odstránené a viac dôvodov na ich ďalšie využitie. Poskytovatelia cloudových služieb musia svojich zákazníkov uistiť a poskytnúť vysoký stupeň transparentnosti ich operácií a zabezpečenia súkromia. Nástroje na ochranu súkromia musia byť vstavané priamo vo všetkých bezpečnostných riešeniach

6.9. Závery

Cloud computing je novo vznikajúci a rapídne sa vyvíjajúci model, kde pravidelne vznikajú nové možnosti a spôsoby použitia. Cloud computing konkrétne predstavuje zvyčajne cloudovú alternatívu k niečomu, čo by organizácie zvyčajne spravovali u seba. Je to alternatíva s použitím dynamicky škálovateľných a často virtualizovaných zdrojov poskytovaných ako služba cez Intenet/Intranet. Napríklad webmail je cloudová alternatíva k hostingu na vlastnom e-mailovom serveri. Väčšina služieb cloud computingu je prístupná pomocou web prehliadača cez akékoľvek pripojené zariadenie (mobil, tablet, osobný počítač...). Preto cloudové služby nevyžadujú, aby používatelia mali sofistikovaný počítač schopný spúšťať špeciálny softvér. Vďaka rozhraniu orientovanému na používateľa je cloudová infraštruktúra a podpora aplikácií pre používateľov transparentná. Cloud computing má potenciál byť prelomovou silou ovplyvňujúcou nasadenie a

využitie technológií. Cloud prakticky mení spôsob, akým množstvo organizácií spravuje informačné technológie. V závislosti od perspektívy a situácie organizácie či jednotlivca to predstavuje príležitosť aj riziko. Takejto zmene možno odolávať, aj keď je to dobrá myšlienka a funguje. Spoločnosti majú mnoho ciest ako pristupovať ku cloudu vrátane jeho infraštruktúry, platforiem a aplikácií, ktoré sú dostupné od poskytovateľov cloudu ako on-line služby. Jednými z hlavných obáv sú bezpečnosť a súkromie. Tieto obavy závisia od typu spoločnosti. V prípade veľkých organizácií so značnými zdrojmi, ktoré môžu vyhradiť na sofistikovaný program informačnej bezpečnosti je potrebné prekonať množstvo výziev v oblasti bezpečnosti, súkromia a spolupráce. V prípade malých a stredných podnikov (SME - SMB - MSP) môže bezpečnosť cloud computingu vyzerať atraktívne v porovnaní so zdrojmi, ktoré si spoločnosti môžu v dnešnej dobe dovoliť minúť na informačnú bezpečnosť.

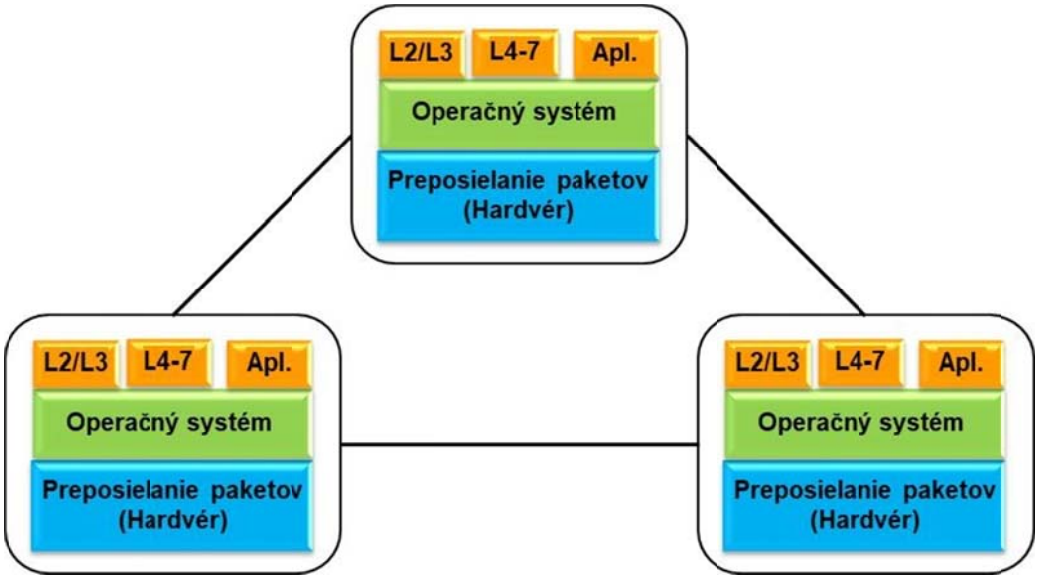
7. Virtualizácia sietí - SDN&NFV

7.1. SDN

Architektúra tradičnej paketovej siete pozostáva z uzlov, z ktorých každý obsahuje funkciu logiky riadenia paketov a hardvér na preposielanie (angl. *forwarding*) paketov. V mnohých smerovačoch (a im podobným sieťových zariadeniam) existuje špecializovaný hardvér pre rýchle preposielanie paketov medzi rozhraniami zariadenia, ktorý tvorí tzv. rovinu preposielania dát. Samotné preposielanie sa riadi pravidlami riadenými lokálnymi procesormi s vlastným operačným systémom, algoritmami smerovania, prekladom adries a ďalšími vyššími funkciami. Pri tradičnom vytváraní sietí sú rovina riadenia a rovina preposielania dát implementované v každom sieťovom uzle. To umožňuje, aby boli všetky zariadenia úplne autonómne a vykonávali všetky rozhodnutia vyššej úrovne, ako napr. smerovanie paketov, nezávisle.

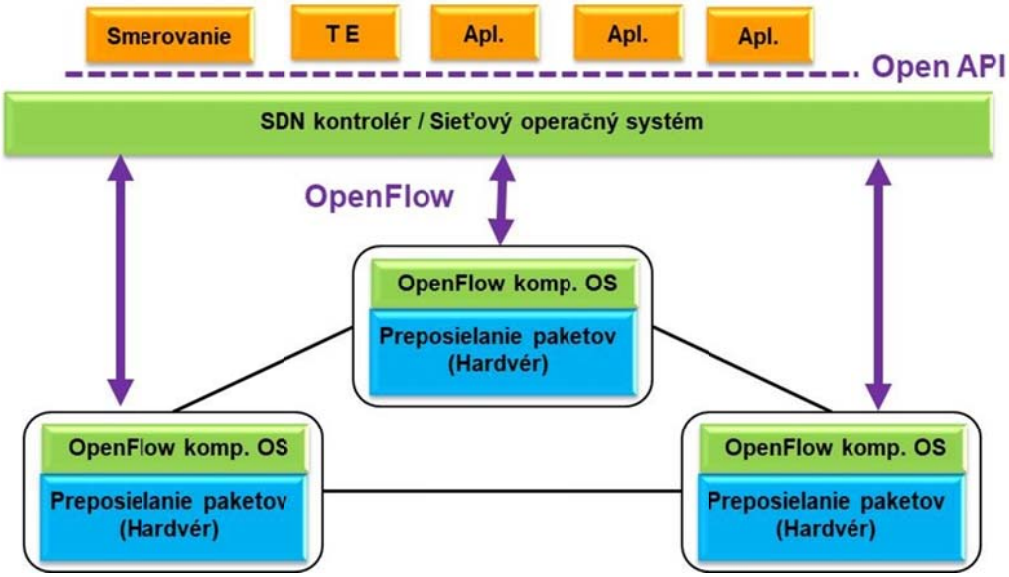
Obr. 21 znázorňuje architektúru tradičnej paketovej siete, v ktorej každý sieťový prvok obsahuje dátovú a riadiacu rovinu. Uvedený model architektúry sieťových prvkov obmedzuje zavádzanie nových funkcií a protokolov a prináša komplexnosť riadiacich mechanizmov a obmedzuje inovácie v IP sieťach.

V moderných sieťových zariadeniach rovina riadenia zbiera informácie o stave susedných prepojení a siete ako celku a poskytuje ich smerovacím algoritmom. Smerovanie sieťovej prevádzky zabezpečujú distribuované smerovacie algoritmy, ale ich nedostatkom je možný problém s konvergenciou. Keďže každé zariadenie zbiera informácie o sieti a rozhoduje o smerovaní samostatne, oneskorenie prenosu informácií o zmenách v sieti môže spôsobiť problémy pri prevádzke siete. Extrémny nárast počtu prepojených zariadení môže tiež limitovať budúci adresný priestor a použiteľnosť, resp. škálovateľnosť súčasných smerovacích protokolov pre veľké, komplexné siete, ako aj ďalšie inovácie, pretože nové funkcie musia byť distribuované do všetkých sieťových uzlov. Uvedené nedostatky rieši SDN.



Obr. 21 Architektúra tradičnej paketovej siete

Softvérovo definovaná sieť (**SDN**, ***Software Defined Networking***) je nový prístup k architektúre IKT siete so zameraním na programové riadenie celej siete. SDN umožňuje správcom siete automatizovane a dynamicky manažovať a riadiť veľký počet sieťových zariadení, služby, topológiu, dátové cesty a politiky pre spracovanie paketov (QoS) prostredníctvom jazykov vyššej úrovne a **API** (***Application Programming Interface***) rozhraní.



Obr. 22 Architektúra SDN siete

Základným princípom SDN je oddelenie roviny riadenia od roviny preposielania dát v sieti, ako je znázornené na **Obr. 22**. Odstránenie 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 umožní tiež znížiť náklady. Navyše, bez potreby distribuovať funkcie smerovania do jednotlivých sieťových uzlov je možné oveľa ľahšie zavádzať nové alebo modifikovať a vylepšovať existujúce algoritmy. Okrem toho konfigurovanie centrálnej roviny riadenia robí riadenie siete jednoduchším, znižuje možnosť nesprávnej konfigurácie a urýchľuje hľadanie problémov. Prídavnou výhodou implementovania softvéru v centralizovanej rovine riadenia je ľahká modifikácia a vývoj nových vlastností.

SDN prináša nasledovné výhody:

- jednoduchšia architektúra - oddelenie roviny riadenia od roviny preposielania dát, možnosť integrovať roviny riadenia pre IP a transportné siete,
- vyššia odolnosť a automatizácia - mechanizmy zotavenia sa z výpadku, škálovateľnosť a vyššia úroveň automatizácie,
- skrátenie doby uvedenia na trh - rýchlejšie zavádzanie nových služieb, možné hosťovanie sieťových služieb v infraštruktúrnom cloude.

7.1.1. Open Flow

Výraz ***OpenFlow*** (**OF**) označuje prvé štandardizované komunikačné rozhranie definované medzi riadiacou rovinou a rovinnou preposielania v rámci architektúry SDN. V súčasnosti je OpenFlow

najpopulárnejší protokol používaný na komunikáciu medzi riadiacou rovinou a rovinou preposielania paketov a stal sa de facto štandardom.

Jadrom OpenFlow špecifikácií je prepínač, t.j. zariadenie spracovávajúce paket. Prepínač spracováva pakety na základe obsahu paketu a nakonfigurovaného stavu prepínača. Na manipuláciu s nastaveniami prepínača bol navrhnutý OpenFlow protokol, pomocou ktorého riadiaca jednotka, ako hlavná časť riadiacej roviny, komunikuje s viacerými prepínačmi a riadi konfigurácie ich stavov.

Špecifikácia OpenFlow popisuje:

- protokol na komunikáciu medzi OpenFlow riadiacou jednotkou a OpenFlow prepínačom,
- činnosť OpenFlow prepínača.

7.1.2. OpenFlow prepínač

OpenFlow prepínač je neoddeliteľnou súčasťou OpenFlow rozhrania. Pre prácu s OpenFlow protokolom existujú dva typy kompatibilných prepínačov:

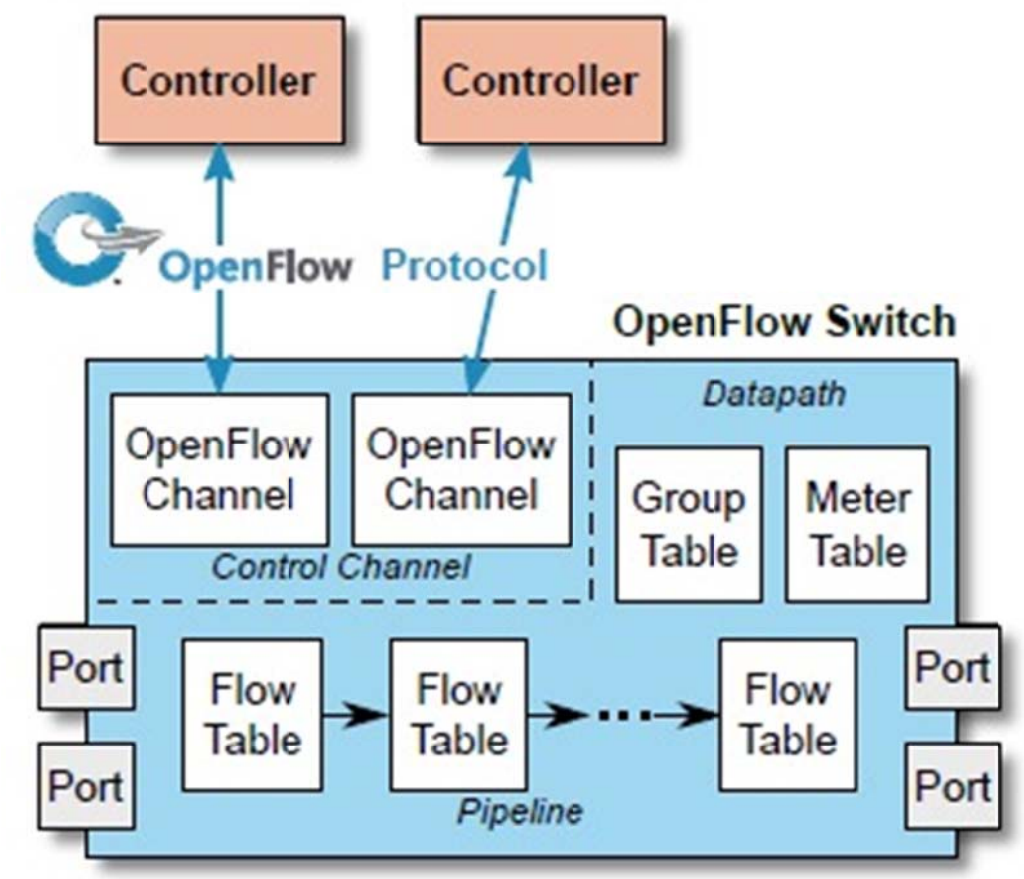
- OpenFlow prepínač - podporuje iba OpenFlow operácie, všetky pakety sú spracovávané podľa OpenFlow pravidiel spracovávania.
- Hybridný OpenFlow prepínač - podporuje OpenFlow operácie aj operácie štandardných eternetových prepínačov. Hybridný prepínač povoľuje prechod paketu z režimu OpenFlow spracovania do režimu normálneho spracovania prostredníctvom portov typu NORMAL a FLOOD.

OpenFlow prepínač používa svoj výstupný port na preposielanie paketov na vstupný port iného prepínača alebo zariadenia. Ako vstupné a výstupné porty sa môžu používať iba štandardné porty, medzi ktoré patria fyzické porty, logické porty a vyhradené porty typu LOCAL (ak sú podporované). Vyhradené porty sa delia na povinné a nepovinné a sú definované v špecifikácii OpenFlow [61].

OpenFlow prepínač pozostáva z viacerých časti (**Obr. 23**) potrebných na spracovanie paketu. Obsahuje jednu alebo niekoľko tabuliek tokov s pravidlami spracovania paketu a tzv. skupinovú tabuľku, ktoré spolu slúžia na vyhľadávanie a spracovanie paketov. Každé pravidlo patrí k určitej podskupine dátovej prevádzky a vykonáva operácie určené pre danú prevádzku. Medzi vykonávané operácie patrí zahodenie paketu, preposlanie paketu alebo preposlanie paketu všetkým dostupným prijímateľom *(tzv. flooding)*.

Podľa pravidiel zavedených riadiacou jednotkou, sa OpenFlow prepínač môže správať ako smerovač, prepínač, firewall, prekladač sieťovej adresy alebo niečo medzi tým.

K ďalším častiam prepínača patrí jeden a viac tzv. OpenFlow kanálov, ktoré sú prepojené s externými riadiacimi jednotkami. Komunikácia medzi prepínačom a riadiacou jednotkou, ako aj riadenie prepínača riadiacou jednotkou, prebieha prostredníctvom OpenFlow protokolu.



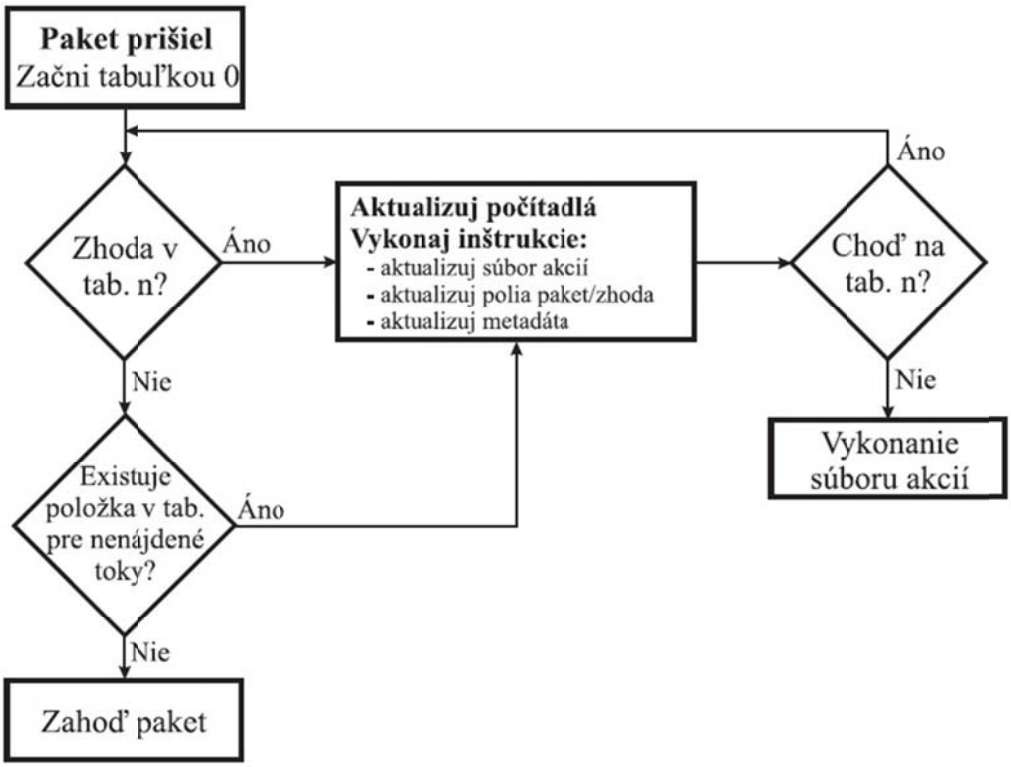
Obr. 23 Bloková schéma OpenFlow prepínača [61]

Každá tabuľka tokov obsahuje niekoľko záznamov o tokoch (tok, angl. *flow*, je výraz používaný v OpenFlow pre spojenie, resp. trasu medzi odosielateľom a príjemcom dát) a každý záznam o toku pozostáva z porovnávacích polí, počítadiel a sady inštrukcií, ktoré sa aplikujú na zhodné pakety. OpenFlow protokol umožňuje riadiacej jednotke pridávať, upravovať a odstraňovať záznamy o tokoch v tabuľkách tokov na základe vlastnej iniciatívy, ako aj v rámci odpovede na zaslaný paket. Záznamy o tokoch môžu presmerovať paket na port, ktorý môže byť fyzický, logický, alebo tzv. rezervovaný. Operácie spojené so záznamami o tokoch môžu presmerovať paket na skupinu (angl. *Group*), ktorá bližšie určí ďalšie spracovanie. Skupiny reprezentujú sady operácií na zaplavenie *(flooding)* alebo na iný spôsob zložitejšieho smerovania *(multipath, fast reroute, link aggregation* a pod.). Zároveň skupiny umožňujú záznamom o tokoch preposielanie na bežný nasledujúci uzol, vďaka čomu môžu byť výstupné operácie na záznamoch o tokoch nemenné.

Skupinová tabuľka *(Group Table)*, ako súčasť OF prepínača, obsahuje skupinové záznamy, v ktorých sú zoznamy operácií, líšiace sa podľa typu skupiny. Operácie v jednom alebo viacerých zoznamoch operácií sú použité na pakety odoslané do danej skupiny.

V tabuľke počítadiel (*Meter Table*) sa nachádzajú záznamy, ktoré určujú počítadlá pre jednotlivé toky. Počítadlá umožňujú implementovať rôzne spôsoby obmedzenia rýchlosti a úrovne kvality služby. Aj keď počítadlá sú úplne nezávislé od čakacích radov na výstupných portov, pre účely

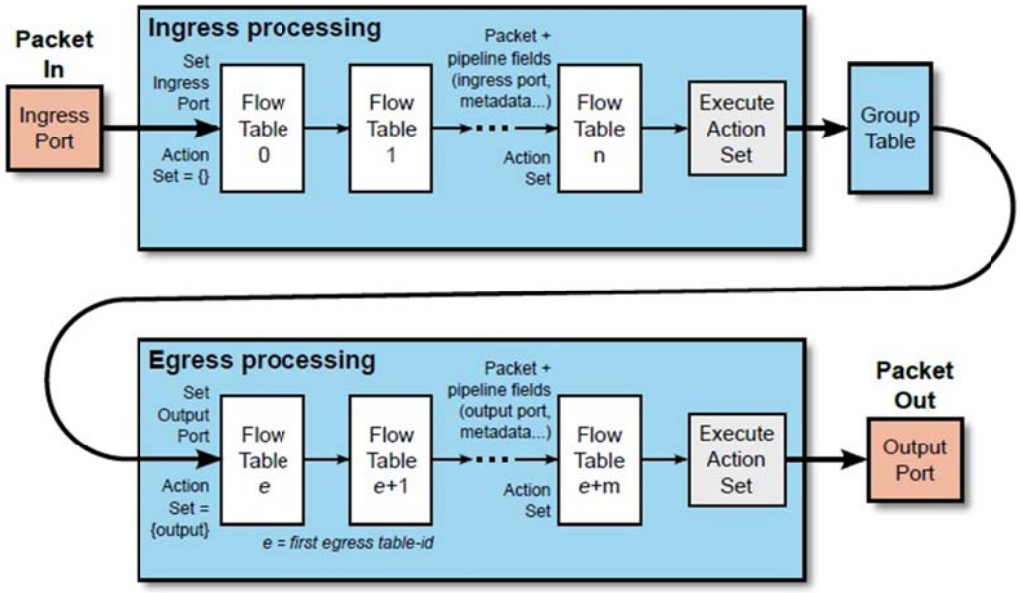
zložitejších meraní môžu byť spolu kombinované. Počítadlo meria a riadi rýchlosť paketov. Každý merací záznam je definovaný svojim meracím identifikátorom, meracími rozsahmi a počítadlami.



Obr. 24 Vývojový diagram spracovania paketov v logickom prepínači OpenFlow

Postup spracovania paketov v logickom OpenFlow prepínači je znázornený na **Obr. 24**. Spracovanie postupnosti polí vždy začína prvou tabuľkou tokov vstupného *(ingress)* spracovania (viď **Obr. 25**). So záznamami o tokoch v prvej tabuľke označenej číslom „0“ je porovnávaný prichádzajúci paket. Použitie ostatných tabuliek tokov vo vstupnom spracovaní závisí od výstupu porovnania paketu s prvou tabuľkou. Po určení výstupného portu preberá prácu s paketom výstupné *(egress)* spracovanie, ktoré nemusí obsahovať žiadnu tabuľku. Vstupné spracovanie začína s prázdnou sadou operácií. Výstupné spracovanie začína so sadou operácií obsahujúcou výstupnú operáciu pre aktuálny port. Výstupné spracovanie je voliteľné, prepínač ho nemusí podporovať. V takom prípade je paket spracovaný a odoslaný von z prepínača výstupným portom.

V rámci spracovania paketu, je paket porovnávaný s tokovým záznamom príslušnej tabuľky tokov. Tokový záznam obsahuje sadu inštrukcií, ktoré sú vykonané na porovnávanom pakete. Jednou z možností inštrukcií je aj priame presmerovanie paketu do nasledujúcej tabuľky tokov, pričom paket je možné presmerovať iba do tabuľky tokov označenej vyšším číslom ako je číslo odosielajúcej tabuľky.



Obr. 25 Postup spracovania paketov v OpenFlow prepínači [61]

V prípade, že prepínač nenájde vo svojich tabuľkách pre daný paket vhodný záznam, môže ho poslať správou *PACKET-IN* na riadiacu jednotku. Riadiaca jednotka môže v svojej odpovedi správou *PACKET-OUT* poslať inštrukcie pre dokončenie spracovania paketu prepínačom a správou FLOW-MOD zadať príkaz na vytvorenie záznamu o novom toku do niektorej z tabuliek na prepínači.

V OpenFlow sú existujú nasledovné tri typy správ:

- z riadiacej jednotky na prepínač - posiela riadiaca jednotka
- asynchrónne - posiela prepínač
- synchrónne - posiela prepínač alebo riadiaca jednotka

Správy posielané z riadiacej jednotky na prepínač:

- ***FEATURES*** - požiadavka o zaslanie zoznamu funkcií podporovaných prepínačom
- ***CONFIGURATION*** - riadiaca jednotka môže nastavovať konfiguračné parametre v prepínači a žiadať o ne. (Prepínač môže iba odpovedať na žiadosti o konfigurácií prijaté od riadiacej jednotky.)
- ***MODIFY-STATE*** - modifikovanie stavu (primárne slúži na pridanie, odstránenie alebo modifikovanie záznamov vo flow/group tabuľkách a pridanie/odstránenie akčných „bucketov“)
- ***READ-STATE*** - umožňuje získanie rôznych informácií z prepínača (aktuálnu konfiguráciu, štatistiky a pod).
- ***PACKET-OUT*** - slúži na poslanie paketu na špecifický výstupný port prepínača a na preposielanie paketov prijatých správou *PACKET-IN*. Správa *PACKET-OUT* musí obsahovať:

    - kompletný paket alebo ID zásobníka obsahujúceho paket uložený na prepínači,

- zoznam akcií, ktoré budú vykonané v poradí, ako sú špecifikované *(ak nie je nič uvedené, paket je zahodený).*

- ***BARRIER*** - správy *Barrier* žiadosť/odpoveď slúžia na overenie závislosti správ a na overenie ukončenia operácií
- ***ROLE-REQUEST*** - umožňuje riadiacej jednotke nastaviť rolu jeho OpenFlow kanála a ID riadiacej jednotky (ak je k prepínaču pripojených viac riadiacich jednotiek)
- ***ASYNCHRONOUS-CONFIGURATION*** - umožňuje riadiacej jednotke nastaviť prídavný filter pre asynchrónne správy

Asynchrónne správy:

- ***PACKET-IN*** - slúži na poslanie paketu z prepínača do riadiacej jednotky. Prepínač si môže uchovávať pakety, v takom prípade sa do riadiacej jednotky posiela iba hlavička paketu a ID zásobníka, kde je paket uložený. Ak si prepínač pakety neuchováva, alebo sa pamäť určená na ukladanie paketov zaplní, posiela riadiacej jednotke celý paket.
- ***FLOW-REMOVED*** - slúži na informovanie riadiacej jednotky, že zápis o toku bol z tabuľky tokov vymazaný.
- ***PORT-STATUS*** - informuje riadiacu jednotku o zmene konfigurácie alebo stavu portu (napr. po reaktivácií portu)
- ***ROLE-STATUS*** - informuje riadiacu jednotku o zmene jeho role (napr. z master na slave)
- ***CONTROLLER-STATUS*** - informuje riadiacu jednotku o zmene stavu OpenFlow kanála. Posiela sa všetkým riadiacim jednotkám (uľahčuje riešenie problému pri strate možnosti vzájomnej komunikácie.)
- ***FLOW-MONITOR*** - informuje riadiacu jednotku o zmene v tabuľke tokov. Riadiaca jednotka môže definovať súbor ukazovateľov na sledovanie zmien v tabuľkách tokov.

Symetrické správy:

- ***HELLO*** - uvítacie správy vymieňané medzi prepínačom a riadiacou jednotkou.
- ***ECHO*** - správy medzi prepínačom a riadiacou jednotkou používané na overenie funkčnosti spojenia, prípadne na meranie oneskorenia a prenosového pásma (prijímacia strana musí vždy poslať potvrdenie)
- ***ERROR*** - informujú o probléme na strane odosielateľa správy. Zvyčajne ju posiela prepínač, ak nemohol vykonať príkaz zaslaný riadiacou jednotkou.
- ***EXPERIMENTER*** - určené na experimentálne účely, resp. implementovanie nových funkčností.

7.2. NFV

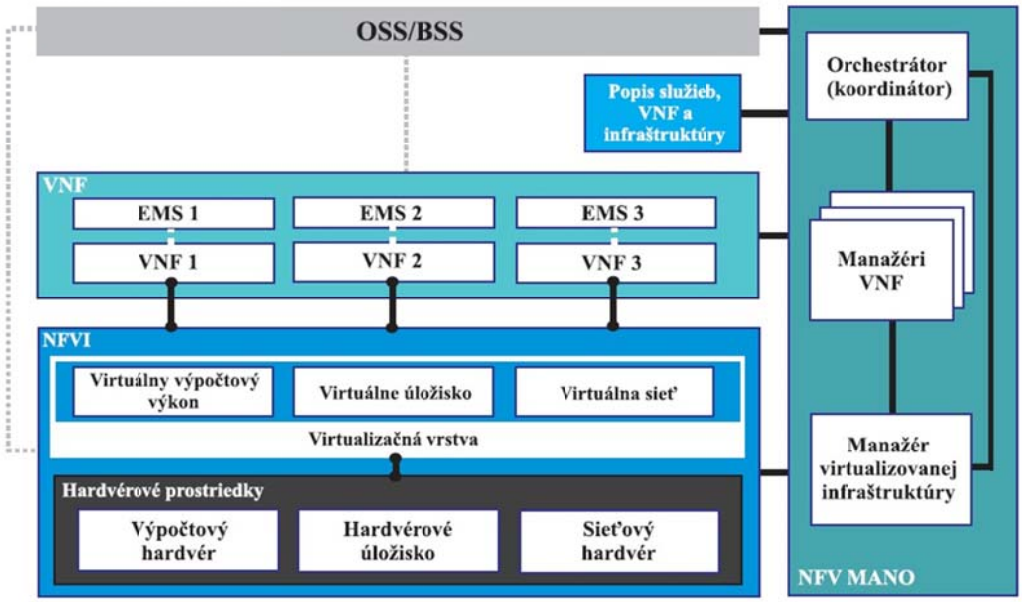
Virtualizácia sieťových funkcií (**NFV**, ***Network Functions Virtualization***) je koncepcia sieťovej architektúry, ktorá využíva IT virtualizačné technológie na virtualizovanie funkcií rôznych sieťových entít do funkčných blokov, ktoré sa môžu navzájom prepojovať alebo zoskupovať s cieľom poskytovania komunikačných služieb. Virtualizácia znamená, že sieťová funkcia a časť infraštruktúry sú implementované softvérovo a preto je softvérová architektúra NFV dôležitou časťou koncepcie NFV.

Prvý návrh NFV bol uverejnený v tzv. Bielej knihe [62] a bol prevažne zameraný na očakávania poskytovateľov služieb. Neskôr sa začali normalizačné aktivity v rámci organizácie **ETSI** (***European Telecommunications Standards Institute***), ktorá vytvorila pracovnú skupinu s názvom ***Network Functions Virtualization Industry Specification Group*** (ETSI **NFV ISG**) pre riešenie úloh spojených s NFV technológiou.

7.2.1. NFV architektúra

Architektúra NFV technológie využíva nasledovné komponenty (**Obr. 26**):

- **NFVI (*NFV Infrastructure*** - NFV infraštruktúra**)** - poskytuje virtuálne zdroje potrebné na podporu virtualizovaných sieťových funkcií - komerčné tzv. *off-the-shelf* hardvérové komponenty a softvér pre virtualizáciu hardvéru.
- **VNF (*Virtualized Network Functions*** - Virtuálne sieťové funkcie**)** - softvérová implementácia sieťových funkcií, ktorá môže byť poskytovaná prostredníctvom NFVI a manažmentových systémom **EMS** (***Element Management System***), ktorý riadi NFV.
- **NFV MANO (*Management and Orchestration*** - Manažment a orchestrácia**)** - pokrýva orchestráciu a životný cyklus manažmentu fyzických softvérových nástrojov, ktoré podporujú virtualizáciu a manažment životného cyklu virtuálnych sieťových funkcií. VNF MANO sa zameriava na virtualizovanie manažmentových funkcií, ktoré sú potrebné pre rámec NFV. Spolupracuje tiež s externými NFV OSS/BSS a umožňuje integráciu NFV do existujúcich sietí.



Obr. 26 Architektúra NFV

7.2.2. NFV infraštruktúra

NFV infraštruktúra je súbor všetkých hardvérových a softvérových komponentov, ktoré vytvárajú prostredie, v ktorom sú NFV poskytované, manažované a vykonávané. NFV

infraštruktúra sa môže rozprestierať na viacerých miestach. Sieť poskytujúca prepojenie medzi týmito miestami sa považuje za súčasť NFV infraštruktúry. Hardvérové zdroje zahŕňajú výpočtové, úložné a sieťové prvky, ktoré poskytujú spracovanie a ukladanie dát a pripojenie k VNF cez virtualizačnú vrstvu (napr. tzv. *hypervízor*) [63], [64]. Ako počítačový hardvér sa predpokladá použitie komerčného, bežne dostupného hardvéru a to hlavne serverov v dátových centrách poskytovateľov služieb. Prostriedky na ukladanie dát môžu byť realizované úložným priestorom, ktorý sa nachádza na samotných serveroch, ako aj zdieľaným **NAS** (***Network Attached Storage***).

Virtualizačná vrstva abstrahuje hardvérové prostriedky a oddeľuje softvér VNF od základného hardvéru, preto môže byť softvér nasadený na rôzne fyzické hardvérové zdroje. Primárnymi nástrojmi na realizáciu virtualizačnej vrstvy je tzv. hypervízor. Použitie hypervízorov je jedným zo súčasných typických riešení pre nasadenie VNF. (Iné riešenie na realizáciu VNF môže zahŕňať softvér, ktorý beží nad nevirtualizovaným softvérom (napr. operačným systémom), napríklad keď nie je k dispozícii podpora hypervízora, alebo VNF je implementované ako aplikácia, ktorá môže bežať priamo na serveri.)

7.2.3. VNF

VNF je softvérový balík, ktorý implementuje sieťovú funkciu s dobre definovaným funkčným správaním a externými rozhraniami. VNF sa môže z dôvodu škálovateľnosti, opätovného využitia alebo rýchlejšej reakcie rozložiť na menšie funkčné moduly, alebo niekoľko VNF môže byť spojených, aby sa zjednodušil manažment a VNF grafy presmerovania.

VNF grafy presmerovania

Sieťová služba môže byť definovaná v rozsahu koniec-koniec prostredníctvom grafu (angl. *forwarding graph*) obsahujúceho sieťové funkcie a koncové body/zariadenia.

Výhody NFV grafov:

- Efektívnosť - výpočtové zdroje priradené k funkčnej a sieťovej kapacite sú nastavené na súčasné zaťaženie a sú zdieľané medzi funkciami.
- Pružnosť - v niektorých prípadoch je možné zdieľať zálohovacie a sieťové kapacity.
- Agilnosť - kratšie časy nasadenia pri inovovaní a zavádzaní nových funkcií, pretože funkcie sú realizované softvérovo.
- Dôraznosť - virtualizované funkcie prepínania a konfigurovanie VNF môže byť vyjadrené grafmi presmerovania jednoduchším a efektívnejším spôsobom.
- Flexibilita - Znižuje zložitosť konfigurácie. Podporuje nové služby a obchodné modely: napr. nasadenie v sieti iných operátorov alebo v dátových centrách tretích strán.

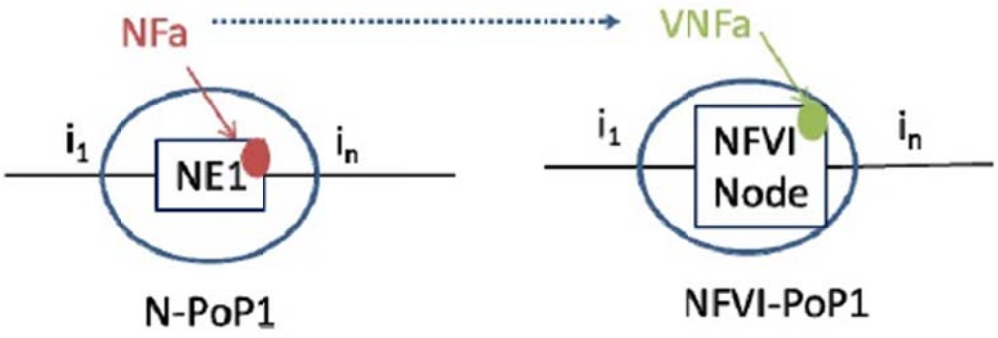
VNF sa môže skladať z viacerých vnútorných komponentov, napr. jedna VNF môže byť rozmiestnená na viacerých virtuálnych počítačoch, kde každý virtuálny počítač je hostiteľom jednej zložky VNF. V inom prípade však môže byť celá VNF umiestnená na jedinom virtuálnom počítači. Veľké VNF môžu pozostávať z viacerých čiastkových VNF, ktoré sú navzájom prepojené formou grafu.

Jednotlivé čiastkové VNF môžu mať nasledujúce prípady rozmiestnenia:

- 1:1 - implementácia sieťovej funkcie jedného sieťového prvku jednou VNF,

- N:1 - v prípade, že existuje N paralelných čiastkových VNF, ktoré implementujú sieťovú funkciu jedného sieťového prvku,
- 1:N - sieťové funkcie N sieťových prvkov sú implementované jednou VNF (napr. virtualizovaná domáca brána).

Obr. 27 zobrazuje mapovanie 1:1 medzi sieťovým prvkom a VNF. V tomto prípade budú externé rozhrania a manažment preferovane kompletné špecifikované prostredníctvom existujúcich štandardných rozhraní sieťového prvku.

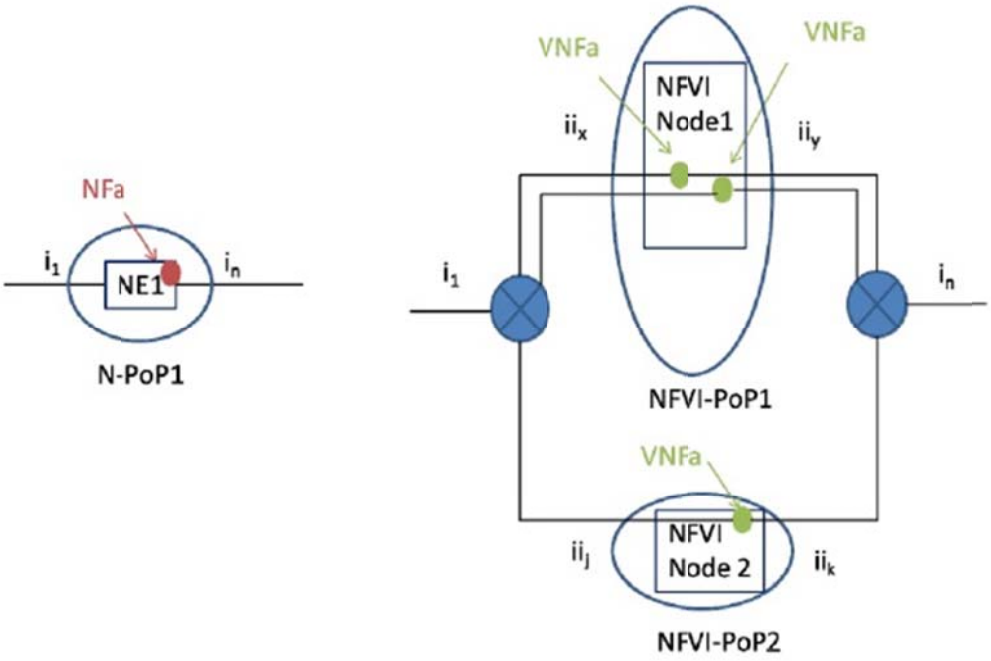


Obr. 27 Príklad 1:1 mapovania NE:VNF [65]

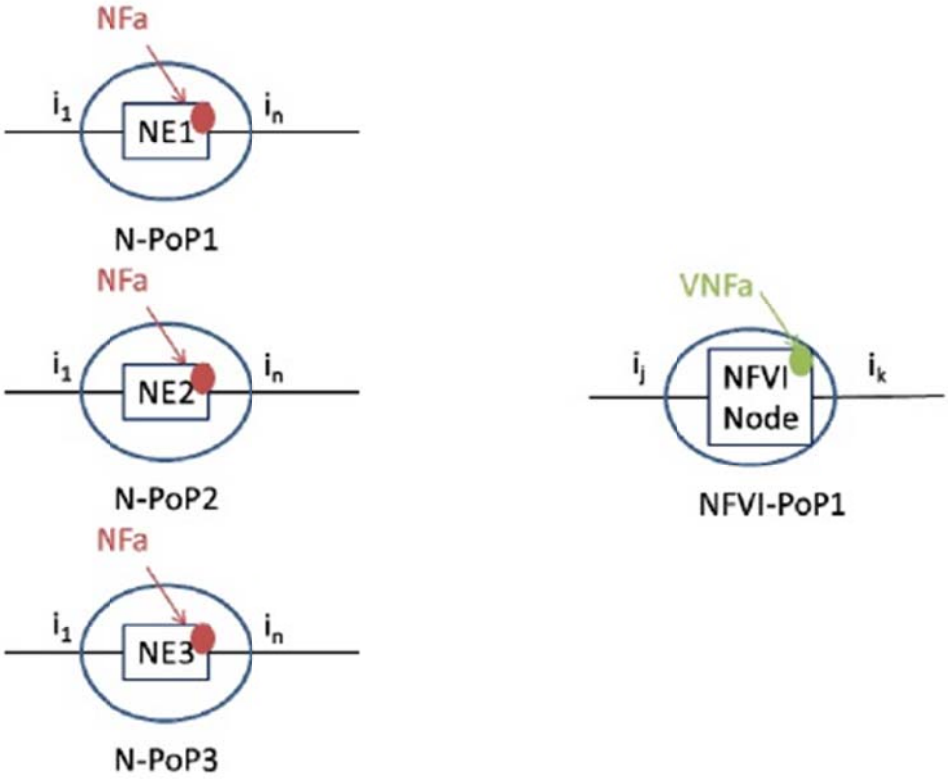
V príklade znázornenom na **Obr. 27** je sieťová funkcia NFa implementovaná v sieťovom prvku NE1 umiestnená na N-POP1 a podporuje rozhrania i_1 až i_n. V uvedenom prípade NE1 neposkytuje žiadnu inú sieťovú funkciu ako NFa. Ekvivalentná virtualizovaná sieťová funkcia VNFa sa vykonáva v uzle NFVI a poskytuje rovnaké rozhrania i_1 až i_n. Ak uzol NFVI neimplementuje žiadnu ďalšiu VNF, potom môže byť považovaný za priamu náhradu NE1. Pre priamu výmenu NE uzlom NFVI s ekvivalentnými VNF je potrebné umiestniť NFVI-PoP1 na rovnaké miesto ako N-PoP1.

Príklad N:1 mapovania sieťovej funkcie NFa implementovanej jedným vysokokapacitným sieťovým prvkom (NE1) prostredníctvom troch inštancií VNFa ja znázornený na **Obr. 28**. Inštancie VNFa môžu byť vo všeobecnosti vykonávané v rôznych VNFI uzloch v rámci rôznych NFVI-PoP. V príklade na **Obr. 28** je funkcia VNFa vykonávaná v dvoch rôznych NFVI uzloch v dvoch rôznych NFVI-PoP. Obidva uzly NFVI Node1 a NFVI Node 2 spolu poskytujú ekvivalentnú množinu externých rozhraní i_1 až i_n. V tomto príklade funkcie rozdelenia a zlúčenia rozdeľujú návštevnosť medzi inštancie rovnakého typu VNF (VNFa). Tento typ funkcie rozdelenia a zlúčenia sa zvyčajne označuje ako rozdeľovanie výkonu *(load balancing)*.

V prípade 1:N mapovania je N sieťových funkcií implementovaných jedinou VNF (napr. virtualizovanou domácou bránou). **Obr. 29** znázorňuje príklad troch identických NF implementovaných v rôznych NE na rôznych miestach. Ekvivalentná VNF (VNFa) podporuje väčší počet rozhraní (i_j až i_k) z jednej inštancie. Jediná VNF tak poskytuje prostriedky, ktoré sú rozdeľované medzi jednotlivé NF - rozdeľovanie použité v tomto scenári je však zvyčajne implementačne špecifické od dodávateľa.



Obr. 28 Príklad N:1 mapovania VNF (NFVI-Node): NE [5]



Obr. 29 Príklad 1:N mapovania VNF:NE [65]

Príkladmi sieťových funkcií, ktoré možno virtualizovať ako VNF, sú napr. prvky siete 3GPP ***Evolved Packet Core*** (**EPC**) ako **MME** (***Mobility Management Entity***), **SGW** (***Serving Gateway***), **PGW** (***Packet Data Network Gateway***), prvky v domácej sieti, napr. domáca brána (Residential Gateway) alebo bežné sieťové funkcie, napr. DHCP server, firewall a pod. Príklady možno nájsť napr. v [66].

NFV MANO (Management and Orchestration)

Riadenie a vzájomná koordinácia (orchestrácia) zahŕňa tri zložky (**Obr. 26**) [67]:

- **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 udalosti), 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 EMS/NMS.
- **Manažér virtualizovanej infraštruktúry VIM** - zodpovedá za riadenie a manažment výpočtových prvkov NFVI, pamäťových a sieťových zariadení v infraštruktúre poddomén jedného operátora, zbieranie a prenos dát z meraní charakteristík a udalostí.

8. Nová generácia multimediálnych služieb a aplikácií

Platformy sietí novej generácie založených na informačných a komunikačných technológiách poskytujú široké spektrum nových služieb a aplikácií. Okrem služieb na báze Internetu vecí, ktoré sú prezentované v samostatnom module sa tento modul sústreďuje na nasledujúce multimediálne služby:

- Internetové multimediálne služby a aplikácie,
- služby hybridného širokopásmového televízneho vysielania (HbbTV),
- eSlužby a mSlužby,
- služby NGN,
- služby na báze WebRTC.

8.1. Internetové multimediálne služby a aplikácie

8.1.1. Softvér ako služba

Softvér ako služba (**SaaS**) sa niekedy prezentuje ako služba poskytujúca softvér na požiadanie. SaaS doručuje a autorizuje softvér pre používateľov. Proces prideľovania licencií je realizovaný na základe poplatku (predplatenia).

Licenčný softvér je centrálne hosťovaný a poskytovaný zákazníkom cez sieť, zvyčajne cez Internet. Používatelia používajú webový prehliadač ako klienta na prístup k tejto službe [68]. SaaS je najviac používaná pre nasledovné účely: obchodné aplikácie (vrátane kancelárskeho softvéru a softvéru na výmenu správ), manažovací softvér, hry, počítačom podporovaný návrh systémov a ekonomický softvér. V prípade bežne predávaného tradičného softvéru používatelia získajú licenciu, ktorá je platná celý ich život. Používatelia platia cenu softvéru vopred plus poplatok za niektoré ďalšie voliteľné služby (podpora).

Model služby SaaS obsahuje nasledovné výhody:

- vo všeobecnosti globálna dostupnosť,
- správa je lacnejšia,
- kompatibilita (rovnaká verzia softvéru u všetkých používateľov),
- jednoduchšia spolupráca (rovnaká verzia softvéru u všetkých používateľov),
- správa automatických aktualizácií a záplat.

Medzi populárne on-line služby v súčasnosti patria **on-line editory videa a fotiek**. Často sú tieto služby prepojené alebo priamo integrované v rámci sociálnych sietí. Poskytujú používateľom možnosť rýchleho a pohodlného zdieľania ich výtvorov na Internete. Ako príklady on-line video editorov možno uviesť: YouTube Video Editor, WeVideo, PowToon, Wideo, Weavly, Kaltura, MIXMOOV, Shotclip, Magisto.

Osobný klaud je platforma, na ktorej je zhromaždený rôzny digitálny obsah a informačné služby a sú dostupné z akéhokoľvek zariadenia na Internete. Pre používateľa sa táto platforma (klaud) nejaví ako hmatateľná entita. Osobný klaud poskytuje používateľom možnosti ako nahrať, uchovať, synchronizovať, kontinuálne prijímať, získať a zdieľať obsah.

8.1.2. Služba postupné vysielanie (sťahovanie) VoD

Video na požiadanie reprezentuje službu ako aj systém, ktorý umožňuje používateľom nájsť, vybrať a potom sledovať alebo počúvať obľúbené video alebo audio. Tento obsah je dostupný používateľom kedykoľvek keď sa rozhodnú. Nemusia sa tak viazať na konkrétny čas vysielania programu.

Používatelia môžu použiť osobné počítače alebo televízory na príjem obsahu na požiadanie, keď sa použije technológia IPTV. Toto je veľmi často používaný scenár. V prípade televíznych systémov s obsahom na požiadanie (VoD) obsah je postupne vysielaný priamo do set-top boxu, počítača alebo iného zariadenia, ktoré má schopnosť ho zobrazovať v reálnom čase. Obsah VoD môže byť tiež stiahnuteľný na zariadenie podporujúce VoD (napr. počítač). Existuje niekoľko spôsobov distribúcie VoD [69]:

- **Transakčné video na požiadanie** - zákazníci platia za každé jedno video (získané na požiadanie, napr. v rámci iTunes, Google Play).
- **Predplatené video na požiadanie** – zákazníci platia mesačný poplatok za neobmedzený prístup k programom (Amazon Video, Hulu Plus, Netflix).
- **Video na požiadanie z programovej ponuky** - televízny program je vysielaný niekoľko krát za sebou v krátkych časových intervaloch (bežne 10 až 20 minút). Diváci sa nemusia prispôsobovať naplánovanému vysielaniu obsahu podľa daného programu.
- **Video na požiadanie s reklamou** - zákazníci neplatia za obsah, ale za to určitý čas strávia sledovaním reklamy (napr. YouTube).

8.1.3. Postupné sťahovanie živého vysielania

Postupné sťahovanie živého vysielania (live streaming) je proces, pri ktorom sú multimédiá doručované klientom (používateľom) cez Internet. *Streaming* znamená, že multimédiá sú kontinuálne (postupne) prijímané zariadením koncového používateľa a potom zobrazované používateľovi. Tento proces je podobný klasickému sťahovaniu, čo je tiež proces doručenia obsahu. Toto doručovanie musí spĺňať špeciálne (pravidelné) podmienky. V prípade sťahovania je obsah dostupný až po stiahnutí posledného bajtu obsahu. V prípade postupného sťahovania (streamingu) obsah (napr. film) môže byť zobrazený prehrávačom používateľovi skôr ako sa stiahne celý (súbor). Proces postupného sťahovania musí byť v prípade multimédií umožnený vhodným audio (MP3, Vorbis alebo AAC) alebo video (H.264 alebo VP8) kodekom.

8.1.4. Služba Cloud gaming alebo Hry/hranie ako služba

Služba *Cloud gaming* (alebo Hry/hranie ako služba alebo hranie na požiadanie) patrí k on-line hraniu hier. V súčasnosti môžeme nájsť dva typy tejto služby:

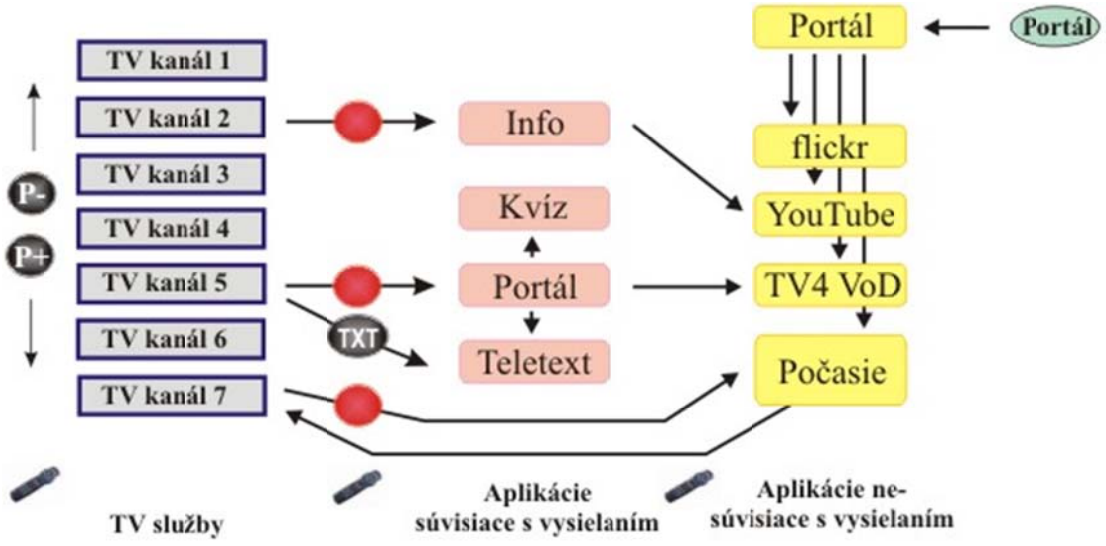
- služba *Cloud gaming* založená na postupnom sťahovaní videa - hry sú postupne vysielané do počítačov, terminálov a mobilných zariadení používateľov ako video s využitím jednoduchého klienta,
- služba *Cloud gaming* založená na postupnom sťahovaní dát (súboru) - zariadenie používateľa spustí a riadi hru. Na začiatku sa malá časť hry stiahne do zariadenia používateľa (hráča) a rýchlo spustí, takže používateľ môže rýchlo začať hrať. Zvyšok hry sa sťahuje do zariadenia počas hrania hry.

8.2. Služby hybridného vysielania širokopásmovej TV

HbbTV (***Hybrid Broadcast Broadband Television*** – Hybridné vysielanie širokopásmovej televízie) reprezentuje konzorcium priemyselných spoločností zameraných na digitálne vysielanie, internetové domény a štandardizáciu. HbbTV je teda medzinárodný štandard (špecifikácia), ktorý definuje doručovanie digitálnej interaktívnej TV používateľom cez spoločné používateľské rozhranie na TV prijímačoch alebo set-top boxoch.

Digitálna TV môže byť distribuovaná pomocou vysielacích technológií (DVB cez kábel, družicu alebo terestriálne) ako aj širokopásmovými technológiami umožňujúcimi prístup do Internetu. HbbTV nie je len digitálna TV, ale prináša používateľom množstvo informačných a zábavných služieb zvyšujúcich zážitky používateľa. HbbTV umožňuje kombinovať to najlepšie z televízie a Internetu. Širokopásmové pripojenie sa používa hlavne na prenos štandardných TV, rozhlasových a dátových služieb (lineárny obsah), prenos a signalizáciu hromadne orientovaných aplikácií a synchronizáciu TV, rozhlasových a dátových služieb a aplikácií. Širokopásmové pripojenie sa používa na doručenie obsahu na požiadanie (napríklad video na požiadanie - VoD), prenos aplikácií a priradených dát, ktoré súvisia alebo nesúvisia s vysielaným obsahom (napríklad teletext). Slúži ako duplexný kanál na výmenu informácií medzi aplikáciami a aplikačnými servermi a na vyhľadanie aplikácií nesúvisiacich s vysielaním.

Práve inteligentná TV technológia ponúka používateľom digitálnu televíziu a veľa interaktívnych služieb. Používatelia môžu pozerať priamo vysielané (TV alebo audio) programy (ľavá časť **Obr. 30**) a môžu tiež aktivovať inteligentnú platformu (napr. Samsung Smart Hub) ponúkajúcu prístup k množstvu atraktívnych aplikácií využívajúcich širokopásmové pripojenie TV prijímača na poskytovanie potrebnej informácie (pravá časť **Obr. 30** - Portál). Tieto aplikácie sa ale označujú ako aplikácie nesúvisiace s vysielaním, t.j. vôbec nesúvisia so službou priameho vysielania (obsahom). **Obr. 30** ukazuje ako môže HbbTV integrovať tieto aplikácie a niektoré z nich previazať so službami, ktoré súvisia s vysielaním [70].



Obr. 30 Koncepcia služieb HbbTV [70]

8.2.1. Služby HbbTV

Na poskytovanie služieb HbbTV koncové zariadenie používateľa spustí príslušnú aplikáciu, aby sa používateľom umožnil prístup ku všetkým funkciám služby. Technológia HbbTV rozširuje funkcie technológie DVB a inteligentných televízorov pre nasledujúce služby [71]: video na požiadanie (catch-Up TV, Start-Over, Push VoD, živé plynulé sťahovanie), informačné služby (správy, počasie, doprava, šport, eGovernment, rozšírený teletext, príručky, EPG), rozšírená TV (doplnkové informácie o TV programoch), hry, kurzy a vzdelávanie, interaktívna reklama, hlasovanie a voľby, prístup do sociálnych sietí, nakupovanie z domu, TV portály, druhá obrazovka, sociálne služby a služby dostupnosti, PVR (personálny videozáznam), personalizácia.

8.2.2. Služba video (obsah) na požiadanie

Služba video (obsah) na požiadanie je veľmi atraktívna služba pre používateľov, nakoľko poskytuje používateľom bezplatne programy z plánovaného vysielania. Aplikácie VoD ponúkajú používateľom široký zoznam filmov, programov, šou a atď., usporiadaných a prezentovaných príťažlivou formou (GUI).

Príkladom služby VoD je **push VoD**, ktorá poskytuje používateľom video obsah na požiadanie. Systém push VoD je založený na tom, že používateľ má lokálne úložisko, ktoré je obyčajne umiestnené vo vnútri set-top boxu. Vybraný obsah sa stiahne do lokálneho úložiska a je používateľom kedykoľvek dostupný bez nutnosti čakať na naplnenie vyrovnávacej pamäte a trpieť kvôli problémom súvisiacim s aktuálnym stavom pripojenia. Systém push VoD využíva personálny videorekordér **PVR** (***personal video recorder***) na uloženie vybratého obsahu, ktorý je často prenášaný v noci (slabá prevádzka) alebo dlhý čas cez deň s malou šírkou pásma.

Služba VoD je vhodná pre vysielateľov a používateľov, ktorí majú nedostatočnú pripojiteľnosť do siete. Tiež pre vysielateľov, ktorí chcú optimalizovať svoju infraštruktúru siete na plynulé sťahovanie videa, lebo najpopulárnejší obsah sa sťahuje do zariadenia odberateľa v predstihu. Ďalšou aplikáciou služby VoD sú aplikácie **catch-up TV**. HbbTV catch-up TV prináša používateľom nové črty voľnosti v porovnaní s priamym pozeraním TV obsahu. Používatelia môžu pozerať obsah TV kanála bez ohľadu na to, kedy bol práve odvysielaný. Služba catch-up TV poskytuje požívateľom prístup do archívu s televíznymi reláciami a iným TV obsahom po dobu niekoľkých dní po ich pôvodnom televíznom odvysielaní.

Služba **start-over** je ďalšia služba HbbTV, ktorá môže byť tiež veľmi zaujímavou a hodnotnou funkciou pre koncových používateľov. Je označovaná aj ako funkcia reštart. Táto funkcia je vhodná hlavne vtedy, keď ste prišli pozerať obľúbený program vtedy, keď vysielanie už začalo pred nejakým časom. Použitím tejto funkcie jednoducho reštartujete vysielanie programu a nikdy nestratíte jeho začiatok. Naviac táto funkcia je aktívna pre daný program počas celého jeho vysielania (napr. od druhej minúty až kým program neskončí). Keď program skončí, používateľ môže použiť službu catch-up na jeho pozeranie z archívu. Funkcia start-over môže byť limitovaná na určitú dobu dňa. Používatelia sa tiež môžu vrátiť späť do živého prenosu

Obr. 31 Kanál ARTE s vlastnosťami catch-up

8.2.3. Iné multimediálne služby HbbTV

Informačné služby poskytované aplikáciami HbbTV sú vybavené atraktívnymi GUI a umožňujú používateľom vyhľadávať rôzne tematicky zamerané informácie (správy, počasie, výmenné kurzy, burza cenných papierov, športy, doprava, eGovernment). Vďaka HTML tieto GUI môžu zobraziť texty, obrázky, grafy, mapy a dokonca videá. Podobne elektronický sprievodca programom môže byť rozšírený o rôzne videošoty.

HbbTV v2 definuje podporu pre aplikáciu spoločné obrazovky **CS** (***companion screens***). Použitím aplikácií HbbTV na TV prístroji môžu používatelia spustiť CS aplikáciu na inom zariadení. Tieto aplikácie môžu komunikovať navzájom medzi sebou. Existuje tiež možnosť pre aplikáciu Spoločná obrazovka bežiacu na inom zariadení nájsť HbbTV terminál a spustiť na ňom aplikáciu CS nesúvisiacu s vysielaním.

8.3. eSlužby a mSlužby

S príchodom informačných a komunikačných technológií (IKT, najmä internetových a webových technológií v poslednom desaťročí) sa začal objavovať nový typ služieb. Tieto služby sa nazývajú elektronické služby (eSlužby). Jedna z niekoľkých jemne sa líšiacich definícií eSlužieb tvrdí [72]:

- eSlužba je akékoľvek aktívum, ktoré je sprístupnené cez Internet aby prinášalo tok príjmov alebo vytváralo nové zefektívnenie činnosti.

eSlužby rozlišujú tri hlavné komponenty: poskytovateľ služby (verejné agentúry, univerzity, komerčné spoločnosti, atď.), prijímateľ služby (obyvatelia, študenti, firmy, atď.) a doručovací kanál (t.j. použitá technológia – Internet, televízia, telefón, rozhlas, CD-ROM). eSlužby môžu napomôcť pri získavaní širšej základne zákazníkov. Môžu byť dostupné denne 24 hodín a dostupné zovšadiaľ. Náklady na inštaláciu a prevádzku môžu byť významne znížené.

E-podnikanie (e-commerce) alebo **elektronické podnikanie** je služba, ktorá pokrýva on-line obchodné činnosti spojené s produktami a službami. Jednoducho povedané, e-podnikanie je o predaji a nákupe tovaru realizovanom cez Internet. To znamená, že príslušné strany vzájomne interagujú väčšinou elektronickým spôsobom (nie priamou fyzickou výmenou). Taktiež pokrýva každú obchodnú transakciu uskutočnenú technológiami IKT a majúcu za následok prevod vlastníctva a práv spojených s používaním rôznych tovarov a služieb [73].

E-obchod reprezentuje komplexnú aplikáciu IKT do všetkých častí a procesov obchodného sveta. Všetky aktivity e-podnikania sú v rámci e-obchodu rozšírené o vnútorné obchodné procesy. Tieto procesy zahŕňajú riadenie zásob, riadenie rizika, produkciu a vývoj produktov, financie, riadenie ľudských zdrojov a znalostí. Príklady aplikácií e-podnikania: on-line nakupovanie (e-nakupovanie), on-line bankovníctvo (Internetové bankovníctvo), platobné systémy, digitálna peňaženka, automatizovaný on-line asistent, on-line rezervácie a elektronické lístky, softvér Nákupný vozík, atď. E-podnikanie môže pracovať v rôznych scenároch:

- **B2B** (***business-to-business***) – spoločnosti predávajú svoje produkty (služby) on-line iným spoločnostiam.
- **B2C** (***business-to-consumer***) – spoločnosti predávajú svoje produkty a služby on-line koncovým používateľom (anonymným klientom). Príkladmi scenára sú Amazon, Zappos, MALL.
- **C2B** (***consumer-to-business***) – zákazníci ponúkajú on-line svoje produkty alebo služby spoločnostiam.
- **C2C** (***consumer-to-consumer***) – spotrebitelia (ľudia, obyvatelia) ponúkajú a predávajú on-line svoj tovar priamo iným zákazníkom (ľuďom). Príkladmi C2C sú eBay, Amazon, BrickLink a využívajú systém PayPal.
- **G2B** (***government-to-business***), **B2G** (***business-to-government***), **G2C** (***government-to-citizen***), **C2G** (***citizen-to-government***), atď. – ďalšie scenáre e-podnikania, kde sú transakcie realizované s vládou.

E-vláda je termín, ktorý zahŕňa používanie rôznych nástrojov, metód a informačných a komunikačných technológií s cieľom poskytnúť a zlepšiť verejné služby pre spoločnosti, firmy a obyvateľov [73]. Je to služba e-podnikanie vo verejnom sektore. E-vláda doručuje služby spoločnostiam (G2B), obyvateľom (G2C), zamestnancom štátnej správy (**G2E**, ***government-to-employee***) a medzi rôznymi vládnymi organizáciami, inštitúciami a oddeleniami (**G2G**, ***government-to-government***). Hlavným cieľom je priniesť verejnú správu bližšie k obyvateľom a spoločnostiam efektívnym a cenovo výhodným spôsobom. Hlavnou myšlienkou je poskytnúť obyvateľom neustály prístup k verejným službám a tiež zlepšiť efektivitu (vnútornej) prevádzky štátnej správy.

Elektronický podpis je elektronická verzia rukou písaného podpisu, ktorý je asociovaný s konkrétnou osobou indikujúci jej súhlas s dokumentom. Môže to byť digitalizovaný obrázok rukou písaného podpisu, symbol, hlasová vzorka a pod., ktorý sa použije na identifikáciu autorov elektronického dokumentu alebo správy. E-podpis je ohrozený kopírovaním a falšovaním a potrebuje proprietárny verifikačný softvér. Na druhej strane **digitálny podpis** sa spolieha na špeciálnu matematickú metódu, ktorá zabezpečí autenticitu dokumentu.

Elektronické bankovníctvo umožňuje zákazníkom prístup do banky odkiaľkoľvek a taktiež môžu získať nižšie poplatky za transakcie.

E-zdravie môže byť definované ako použitie informačných a komunikačných technológií pri poskytovaní správnych informácií pri starostlivosti o zdravie v pravý čas a na správnom mieste, aby sa zlepšil proces starostlivosti o zdravie, kvalita života a splnili nároky občanov a pacientov, zdravotníckych pracovníkov a poskytovateľov zdravotníckej starostlivosti a tvorcov zákonov [74]. Vychádza z digitálnych dát (záznamy o pacientoch), ktoré sú elektronicky prenášané, uchovávané a vyberané pre klinické, vzdelávacie a administratívne účely. Elektronické zdravotníctvo zahŕňa napríklad: konzultácie medzi zdravotníckymi pracovníkmi o zdravotných záznamoch pacienta, e-konzulácie, e-recepty (prístup a tlačenie receptov pacienta), diagnostické testy, diagnózy, liečba a monitorovanie na diaľku, informačné služby, m-zdravie, systém manažovania starostlivosti o zdravie (plánovanie vyšetrení, správa záznamov pacientov).

Elektronické vzdelávanie môže byť charakterizované ako aplikácia IKT do vývoja, distribúcie a manažmentu vzdelávacieho procesu.

E-vzdelávanie obsahuje rôzne formy vzdelávania ako napr. webové vzdelávanie, dištančné vzdelávanie, e-výučba, počítačom podporované vzdelávanie, virtuálne triedy, m-vzdelávanie, spolupráca. Vzdelávací proces je obyčajne realizovaný cez Internet, Intranet, audio alebo video konferencie, pozemné alebo satelitné vysielanie, média ako CD a DVD ROM, USB kľúče. E-vzdelávanie tiež reprezentuje formu samovzdelávania pomocou elektronických vzdelávacích materiálov distribuovaných vyššie spomenutými kanálmi. Môže byť tiež časťou kombinovaného spôsobu vzdelávania. Vzdelávací proces je často poskytovaný, sledovaný a manažovaný systémom **LMS** (***learning Management System***), napr. Moodle.

Telepráca (telework, telecommuting), práca na diaľku, práca doma, e-práca reprezentujú formy práce, pri ktorej pracovník nemusí dochádzať na pracovisko. Hoci veľa pracovníkov pracuje doma, niektorí pracovníci využívajú každé vhodné miesto (mimo pracoviska) na prácu (napr. obchody, reštaurácie v zahraničí). Súčasný pracovník na diaľku využíva na prácu počítač, ktorým je pripojený do siete spoločnosti pre ktorú pracuje. Telepráca znižuje prevádzkové náklady a zlepšuje produktivitu práce a pracovné výsledky. Telepráca má ale aj niekoľko nevýhod. Kladie vyššie nároky na motiváciu pracovníka pracovať. Rušenie v domácnosti môže byť nakoniec kritickejšie ako v práci (napr. deti, domáce zvieratá, susedia). Pracovník na diaľku môže strácať profesionálny kontakt s pracovníkmi pracujúcimi priamo na pracovisku.

8.4. Aplikácie a služby Internetu vecí

Internet vecí (IoT, *Internet of Things*) je novo vznikajúca globálna Internetovo založená technická architektúra zľahčujúca výmenu tovarov a služieb v globálnych dodávateľských sieťach a má vplyv na bezpečnosť a súkromie zúčastnených strán [75]. Počet aplikácií a služieb, ktoré môže poskytovať IoT je prakticky neobmedzený a môže byť prispôsobený mnohým oblastiam ľudskej činnosti. Aplikácie IoT tak môžu uľahčiť a zlepšiť kvalitu života niekoľkými spôsobmi. Niektoré z aplikácií a služieb IoT sú nasledovné:

- Pripojené inteligentné budovy: Zlepšenie účinnosti (manažment spotreby energie a úspory) a bezpečnosti (senzory a alarmy). Domové aplikácie vrátane inteligentných senzorov a akčných členov na ovládanie domácich spotrebičov. Zdravotné a vzdelávacie služby doma. Diaľkové ovládanie liečby pacientov. Káblové/satelitné služby. Systém ukladania/generovania energie. Inteligentné termostaty. Detektory dymu a alarmy. Aplikácia na kontrolu prístupu. Bezpečnosť pre všetkých členov rodiny.

- Inteligentné mestá a doprava: Integrácia bezpečnostných služieb. Optimalizácia verejnej a súkromnej dopravy. Parkovacie senzory. Inteligentná správa parkovacích služieb a premávky v reálnom čase. Inteligentné riadenie semaforov v závislosti od dopravných zápch. Zabezpečenie (kamery, inteligentné senzory, informácie pre občanov). Vodné hospodárstvo. Zavlažovanie parkov a záhrad. Inteligentné popolnice. Kontrola znečistenia. Získavanie okamžitej spätnej väzby a názorov od občanov. Inteligentná správa. Volebné systémy. Monitorovanie nehôd, koordinácia záchranných akcií a tiesňových volaní.
- Vzdelávanie: Prepojenie virtuálnych a fyzických učební na zabezpečenie efektívnejšieho a dostupnejšieho vzdelávania, e-learning. Prístupové služby k virtuálnym knižniciam a vzdelávacím portálom. Výmena správ a výsledkov v reálnom čase. Celoživotné vzdelávanie. Učenie sa cudzích jazykov. Správa účasti.
- Spotrebná elektronika: Inteligentné telefóny. Inteligentná TV. Notebooky, počítače a tablety. Inteligentné chladničky, umývačky a sušičky. Inteligentné domáce kino. Inteligentné spotrebiče. Obojkové (Pet collar) senzory. Personalizácia používateľského komfortu. Osobné lokátory. Inteligentné okuliare.
- Zdravie: Monitorovanie chronických ochorení. Zlepšenie kvality starostlivosti a kvality života pacientov. Sledovače aktivity. Vzdialená diagnostika. Pripojené náramky. Interaktívne pásy. Monitorovanie športovej aktivity. Sledovanie užívania omamných látok (drog). Biočipy. Rozhranie mozog - počítač.
- Automobilový priemysel: Inteligentné autá. Kontrola premávky. Pokročilé informácie o tom čo je pokazené. Inteligentné riadenie a kontrola energie. Samodiagnostika. Akcelerometer. Senzory pozície a priblíženia. GPS sledovače. Riadenie rýchlosti vozidla. Autonómne vozidlá.
- Poľnohospodárstvo a životné prostredie: Meranie a monitorovanie znečistenia prostredia (CO_2, hluk, prvky kontaminujúce okolité prostredie). Predpovede klimatických zmien založené na inteligentných senzoroch. Senzory v paletách výrobkov. Nakladanie s odpadom.
- Energetické služby: Presné údaje o spotrebe energie. Inteligentné meranie. Inteligentné siete. Analýza a predikcia spotreby energie a vzory. Predpovedanie budúcich trendov v spotrebe energie.
- Inteligentné pripojenie: Správa dát a poskytovanie služieb. Prístup k e-mailom, hlasovým a video službám. Interaktívna skupinová komunikácia. Streamovanie v reálnom čase. Interaktívne hranie sa. Rozšírená realita. Sledovanie zabezpečenia siete. Biometrické autentifikačné metódy. Spotrebiteľská telematika. M2M komunikačné služby. Virtuálna realita. Počítačové videnie.
- Výroba: Snímače plynu a prietoku. Inteligentné senzory vlhkosti, teploty, pohybu, sily, zaťaženia, netesnosti, úrovniach. Strojové videnie. Snímanie akustiky a vibrácií. Kompozitné aplikácie. Inteligentné riadenie robotov. Rozpoznávanie vzorov. Strojové učenie.
- Nakupovanie: Inteligentné nakupovanie. Riadenie zásob. Kontrola geografického pôvodu jedla a produktov. Kontrola kvality jedla a bezpečnosti.

8.5. Služby NGN

8.5.1. VoIP

VoIP (***Voice over IP***) alebo IP telefónia, internetová telefónia reprezentuje sadu technológií potrebnú pre poskytnutie hlasovej komunikácie a multimediálnych relácií cez siete na báze **IP** (***Internet Protocol***) – Internet.

Internetová telefónia predstavuje doručenie komunikačných služieb ako hlas, fax, SMS, výmenu hlasových správ cez Internet namiesto siete **PSTN** (***Public Switched Telephone Network***). Proces zostavenia spojenia cez VoIP telefóniu je podobný tradičnej digitálnej telefónii a obsahuje činnosti ako: výmena signalizácie, nastavenie kanála, digitalizácia analógových hlasových signálov a kódovanie hlasových dát. Zakódované hlasové dáta sú vkladané do paketov a prenášané ako IP pakety cez sieť **PSDN** (***Packet-switched Data Network***). Príkladmi aplikácií VoIP sú Skype, Google Talk.

Existuje niekoľko súperiacich prístupov ako implementovať VoIP. Každý je založený na sade protokolov, ktoré zabezpečujú signalizáciu, prenos dát a ďalšie úlohy. Najpoužívanejší protokol vo svete VoIP je SIP [76]. **SIP** (***Session Initiation Protocol***) je komunikačný protokol, ktorý poskytuje prenos signalizácie pre multimediálne komunikačné relácie. SIP je teda riadiaci protokol aplikačnej vrstvy, ktorý zabezpečuje vytvorenie, modifikáciu a zrušenie multimediálnych relácií.

8.5.2. Hostiteľské kontaktné centrá

Za poslednú dekádu kontaktné centrá zažili značný vývoj. Veľa spoločností využíva množstvo kontaktných centier na vybavenie všetkých interakcií so zákazníkmi (či už sú implementované priamo v spoločnosti alebo prenajaté u externého poskytovateľa tejto služby). Hostiteľská (hosťovaná) VoIP telefónia sa rýchlo stáva štandardnou komunikačnou platformou pre organizácie všetkých veľkostí. Hromadný prechod na hostiteľskú VoIP službu (od tradičných telefónnych systémov), ktorá ponúka mnoho funkcií už začal a ponúka značné výhody:

- okamžité šetrenie nákladov,
- nárast spoľahlivosti systému a produktivity pracovníkov.

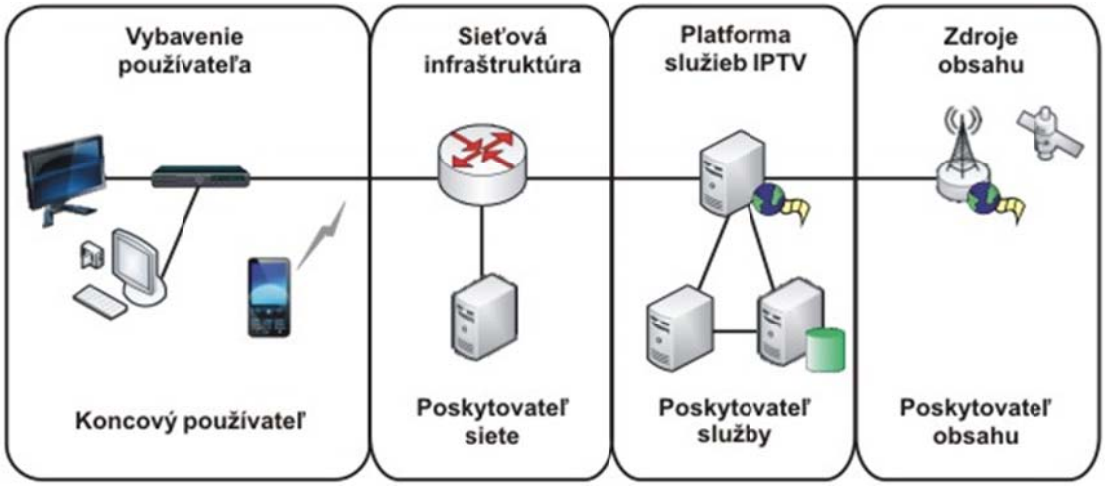
Nasadenie hostiteľskej technológie VoIP vyžaduje nenáročné vybavenie. Vo väčšine prípadov je potrebné vybavenie obmedzené na kvalitný výkonný smerovač, **IADs** (***Integrated Access Devices***) a IP telefóny. V niektorých prípadoch sa môžu použiť aj analógové telefóny ale IP telefóny sú odporúčané, lebo

- ponúkajú viac funkcií,
- vyžadujú menej hardvéru,
- sú jednoduchšie na používanie.

8.5.3. IPTV

ITU-T definuje **IPTV** (***Internet Protocol Television***) nasledovnou definíciou [77]:

IPTV reprezentuje multimediálne služby ako doručenie televízie/audia/videa/textu/grafiky/dát cez siete založené na protokole IP spravované tak, aby poskytli požadovanú úroveň kvality služby a zážitku (QoS/QoE), bezpečnosti, interaktivity a spoľahlivosti. Inými slovami IPTV je systém, ktorý doručuje (metódou streaming) televízne služby IP zásobníkom cez siete PSDN (LAN, Internet) namiesto využitia tradičných pozemných, satelitných a káblových systémov [78]. Celkový komunikačný reťazec na doručenie obsahu IPTV obyčajne obsahuje 4 hlavné oblasti (**Obr. 32**): poskytovateľ obsahu, poskytovateľ služby, poskytovateľ siete a koncový používateľ.



Obr. 32 Domény IPTV

8.5.4. VoIP VPN

VoIP VPN vznikla kombináciou dvoch technológií: hlas cez protokol IP a virtuálne privátne siete, čím dostaneme technológiu, ktorá poskytuje zabezpečené (šifrované) doručovanie hlasu. Ako už bolo spomenuté, VoIP prenáša ľudský hlas ako digitálny dátový tok. Potom je celkom jednoduché uskutočniť šifrovanie hlasu cez tunely VPN jednoduchou aplikáciou šifrovacích algoritmov, ktoré sú prirodzenou súčasťou protokolov použitých na implementovanie tunelov VPN. Nasadením služby VoIP cez VPN získavame ešte ďalší úžitok. Je komplikované prenášať komunikáciu protokolu SIP cez firewall, pretože používa náhodné porty pri výstavbe spojení. VPN je dobré riešenie ako sa vyhnúť tomuto problému, keď sa konfigurujú vzdialení klienti VoIP.

8.5.5. Podporovaná služba (služby emulácie/simulácie ISDN)

Počas evolúcie smerom k NGN má NGN podporovať zastarané terminály (napr. telefóny PSTN/ISDN) a funkcie poskytované sieťami PSTN/ISDN.

Emulácia PSTN/ISDN:

- z pohľadu používateľa sa NGN má javiť, že podporuje rovnaké typy služieb ponúkané existujúcimi sieťami PSTN/ISDN,
- zastarané zariadenia môžu využívať existujúce telekomunikačné služby, keď sú pripojené k NGN.

Simulácia PSTN/ISDN:

- NGN terminály v sieti NGN môžu využívať možnosti služieb sietí PSTN/ISDN,
- zastarané terminály s terminálovou adaptáciou môžu byť tiež používané,
- implementácia cez riadiacu infraštruktúru založenú na protokole IP (napr. použitím SIP).

8.6. WebRTC

WebRTC (***Web Real-Time Communications***) je kolekcia otvorených štandardov pre komunikáciu v reálnom čase vyvinutá najmä pracovnými skupinami WebRTC konzorcia **W3C** (***World Wide Web Consortium***) a **RTCWEB** (***Real-Time Communication in Web-browsers***) komunity **IETF** (***Internet Engineering Task Force***).

W3C sústreďuje svoju prácu ohľadne WebRTC najmä na aplikačné programové rozhrania (**API**, ***Application Programming Interface***) prehliadača, aby bolo možné mať prístup k zdrojom videa a audia. IETF vytvorila skupinu RTCweb na definovanie rozhrania medzi prehliadačmi vrátane (signalizačných) protokolov.

WebRTC [79] otvára možnosti pre komunikáciu v reálnom čase, ako napr. audio a video hovory, zdieľanie obrazoviek a video konferencie v rámci webových prehliadačov bez použitia dodatočného softvéru (sú požadované iba moderné webové prehliadače). Toto uľahčuje prácu webovým vývojárom, aby mohli implementovať funkcie WebCRT iba použitím **HTML5** (***Hypertext Markup Language version 5***) a rôznych API jazyka JavaScript.

Okrem poskytovania výkonného decentralizovaného mediálneho nástroja v rámci prehliadačov WebRTC má aj ďalšie výhody ako otvorený zdrojový kód rozhrania API, voľné audio a video kodeky (adaptívne, s vysokým rozlíšením videa) a vstavanou sieťovou podporou (napr. šifrovanie, hľadanie siete). WebRTC nie je technickým návrhom limitovaný iba na použitie v rámci prehliadačov. Môže byť taktiež použitý v aplikáciách a vlastných implementáciách, takže každé moderné pripojené zariadenie – počítače, tablety alebo dokonca televízory – by sa mohli stať rovnocennými entitami WebRTC a tak plne schopnými komunikačnými zariadeniami. V porovnaní s inými komunikačnými systémami v reálnom čase WebRTC nevyžaduje veľkú infraštruktúru, ktorá sa stará o premávku komunikácie medzi jednotlivými (partnerskými) stranami (peers).

8.6.1. Aplikácie

S využitím WebRTC [80] môžu byť vytvorené rôzne aplikácie a použitie nie je obmedzené len na komunikačné účely. WebRTC nie je (iba/najmä) o volaní v rámci prehliadačov ale aj o tom, aby weboví vývojári mohli pristupovať k vstupným audio/video zariadeniam cez JavaScript a tiež, aby sa odstránil problém komunikácie medzi prehliadačmi pre obyčajných webových vývojárov. Ako náhle je problém komunikácie medzi prehliadačmi vyriešený, WebRTC poskytuje dátový kanál pre dátové komunikácie v reálnom čase ale tiež dátový kanál na posielanie akýchkoľvek ďalších dát medzi jednotlivými stranami (partnermi). Všetko toto väčšinou nevyžaduje pluginy, ale je prirodzene podporované v prehliadačoch (v súčasnosti Google Chrome, Mozilla Firefox, Opera, Microsoft Edge).

Aplikácie pre hlasovú komunikáciu a video chat v rámci prehliadačov

Najjednoduchšou aplikáciou WebRTC je audio/video komunikácia medzi prehliadačmi. Vstavané schopnosti WebRTC poskytujú prístup k mikrofónu (audio) a kamere (video). Používateľ si samozrejme môže vybrať zariadenie a udeliť mu právomoc. Dôležité funkcie API pre tento prípad použitia sú: MediaStream/getUserMedia (HTML 5) a RTCPeerConnection. Rozhranie *getUserMedia* pridáva prístup k dynamickým zdrojom ako mikrofóny a kamery. Charakteristiky týchto zdrojov môže meniť ako odpoveď na požiadavky aplikácie. PeerConnection je technológia pre média, ktorá umožňuje dvom používateľom komunikovať priamo medzi dvomi prehliadačmi. Táto komunikácia je riadená cez signalizačný kanál, ktorý je poskytovaný nešpecifikovanými prostriedkami, ale vo všeobecnosti skriptom na webovej stránke, ktorá bola poskytnutá webovým serverom. Príkladom týchto služieb je: appear.in alebo talky.io.

Zdieľanie súborov na báze P2P

Dátový kanál (*RTCDataChannel*) dovoľuje webovej aplikácii posielať a prijímať aplikačné dáta priamo medzi partnermi (peers). Rozhranie dátového kanála reprezentuje obojsmerný dátový kanál medzi dvomi partnermi. Kým PeerConnection je kanál iba pre RTC, DataChannel môže prenášať akýkoľvek typ dát. Príkladom tejto služby je sharefest.me.

Zdieľanie obrazovky

Rozhranie *getUserMedia* nielenže dokáže sprístupniť kameru/mikrofón ako zdroje médií, ale taktiež aj zdieľanú obrazovku. Z bezpečnostných dôvodov je na prístup k obrazovke potrebný zásuvný modul (plug-in). Väčšina služieb, ktoré ponúkajú audio/video komunikáciu tiež ponúkajú aj zdieľanie obrazovky.

Spoločná zdieľaná (elektronická) tabuľa

Okrem audio/video komunikácií a zdieľania obrazovky vytvorený dátový kanál môže byť použitý na prenos nielen súborov ale aj riadiacich informácií. Tieto riadiace informácie môžu byť použité na modifikáciu zobrazeného obsahu prehliadača. Príkladom takejto aplikácie môže byť spoločná zdieľaná tabuľa. Posielaním vstupov z jednej tabule (editora) ku všetkým ďalším tabuliam v rámci rovnakej linky aplikácia prehliadača môže vystupovať ako zdieľanie spoločnej tabule. Webové sídlo podporené takouto WebRTC funkciou môže byť využité napr. v rámci elektronického vzdelávania.

Konferencie

Z pohľadu obyčajného prehliadača WebRTC je koncipovaný ako P2P komunikácia nevyžadujúca dodatočnú infraštruktúru. Tento architektonický prístup ale sťažuje realizáciu relácií s viacerými tokmi pre napr. skupinovú video konferenciu alebo iné scenáre vysielania od N pre M účastníkov. Toto je priestor, kde prichádzajú do úvahy stavebné bloky **konferencie**. Tieto stavebné bloky sa starajú o distribúciu mediálnej premávky ku skupine účastníkov. Táto distribúcia je možná tromi odlišnými spôsobmi, ktoré sa primárne líšia v ich požiadavkách na dodatočné servery.

9. Informačná a sieťová bezpečnosť

Vo všeobecnosti možno definovať bezpečnosť ako kvalitu alebo stav existencie niečoho (napr. systému, informácií), počas ktorej nehrozia žiadne nebezpečenstvá a hrozby. Aby bolo možné dosiahnuť tento cieľ (stav), je nutné aplikovať rôzne bezpečnostné opatrenia. V prípade bezpečnosti IKT systémov sa to bude týkať nasadenia takých opatrení a stratégií, ktoré poskytnú správnu činnosť týchto systémov a ochranu všetkého v nich, čo má svoju hodnotu (napr. informácií). Bezpečnosť IKT systémov bude zahŕňať rôzne oblasti bezpečnosti [81]:

- informačnú (dátovú) bezpečnosť – zabezpečenie informácií (údajov) proti odpočúvaniu a zneužitiu, zničeniu a zmene,
- počítačovú bezpečnosť – bezpečná prevádzka počítačov a ochrana dát spracovávaných a uchovávaných počítačmi (koncovými zariadeniami),
- sieťovú bezpečnosť (prístupovú, komunikačnú a systémovú) – ochrana dát počas ich prenosu komunikačným prostredím a ochrana počítačov pripojených do počítačovej siete.

Je možné sa stretnúť ešte s ďalšími oblasťami bezpečnosti, ako fyzická bezpečnosť (ochrana fyzických objektov), personálna bezpečnosť (kto má pridelenú akú autorizáciu v systéme), softvérová vrátane aplikačnej bezpečnosti (ochrana OS, aplikácií a rôznych nástrojov na poskytnutie napr. informačnej bezpečnosti) alebo internetová bezpečnosť. Tieto oblasti môžu byť úplne alebo čiastočne pokryté vyššie uvedenými typmi bezpečnosti.

V súčasnosti sa stretávame veľmi často aj s pojmom kybernetická bezpečnosť (*cyber security*). Je to bezpečnosť kybernetického priestoru, čo je virtuálny priestor zložený z celosvetovo prepojených komunikačných sietí, informačných systémov a rôznych ďalších podsystémov (riadiacich, výrobných, bezpečnostných a pod.) vrátane hardvéru, softvéru a údajov (t.j. je postavený na reálnom priestore = Internete), v ktorom vzájomne interagujú ľudia, softvér a služby.

9.1. Terminológia informačnej bezpečnosti

V tejto časti si zadefinujeme základné pojmy, ktoré sa využívajú v oblasti informačnej bezpečnosti, a ktoré sa rovnako používajú v štandardoch a normách definovaných pre oblasť IKT.

Ak chceme implementovať bezpečnosť v IKT (samozrejme aj vo všeobecnosti), musíme si uvedomiť, **čo** chceme zabezpečiť. To znamená zadefinovať všetko, čo má hodnotu pre mňa (ako osobu) alebo organizáciu a bude reprezentované spoločným pojmom **úžitková hodnota**, resp. **aktívum** *(asset)*. V spoločnosti alebo organizácii musí byť stanovený súbor pravidiel, ako dosiahnuť požadovanú úroveň zabezpečenia majetku. Spôsob, ako dosiahnuť túto úroveň zabezpečenia, je popísaný v **bezpečnostnej politike** *(security policy)*, ktorá predstavuje súbor noriem, pravidiel a postupov, ktoré definujú spôsob správy, ochrany a šírenia citlivých informácií a iných aktív. Kompromitácia alebo zneužitie **citlivých informácií** *(sensitive information)* môže spôsobiť veľké škody pre jednotlivca, organizáciu alebo spoločnosť.

Úžitkové hodnoty v organizácii zahŕňajú:

- hmotné úžitkové hodnoty (hardvér, budovy a pod.),
- nehmotné úžitkové hodnoty,
    - informácie/dáta,
    - softvér,
    - schopnosť poskytovať produkt, službu, informácie,
- **ľudí** (personál, ktorý prevádzkuje informačný systém)**.**

Zraniteľnosť (*vulnerability*) predstavuje chybu alebo slabé miesto v informačnom systéme, ktoré môže byť využité ohrozením na spôsobenie straty, resp. škody v informačnom systéme. Je dôležité poznamenať, že zraniteľnosť sama o sebe nespôsobuje škody v systéme, ale vytvára podmienky (okolnosti), ktoré môžu byť ohrozením zneužité na spôsobenie straty (škody) v informačnom systéme. Slabé miesta systému sa môžu vyskytovať na všetkých úrovniach informačného systému (fyzická vrstva, hardvér, softvér, organizačná alebo personálna štruktúra, manažment informačného systému). Príkladom môže byť diera v OS, slabé prístupové heslo, chyba v softvéri, nezabezpečený systémový port, nezamknuté dvere, atď.

Nebezpečenstvo, ktoré hrozí úžitkovým hodnotám, označujeme pojmom **hrozba** *(threat).* Predstavuje možnosť využitia zraniteľnosti **IS** (*informačného systému*) k útoku proti IS za účelom spôsobiť škodu alebo zlyhanie IS. Toto poškodenie môže nastať z útoku na informácie, na systém samotný alebo na iné zdroje, ktoré môžu spôsobiť zlyhanie systému.

Ak je zraniteľné miesto systému využité za účelom spôsobenia škody na aktívach systému, hovoríme o **útoku** (*attack*). Existuje úmyselné využitie zraniteľného miesta (cielený útok spôsobujúci škodu) alebo neúmyselné uskutočnenie akcie, ktorej následkom je škoda na aktívach (napr. blesk, ktorý spôsobí škodu na zariadeniach alebo budovách).

Riziko (*risk*) predstavuje pravdepodobnosť, že sa v systéme stane niečo neželané. Reprezentuje potenciálnu možnosť vzniku určitej straty (škody) v informačnom systéme tým, že ohrozenie využije zraniteľnosť niektorých zložiek systému.

V súčasnosti existuje niekoľko dôležitých vlastností aktív (informácií, dát, softvéru, hardvéru, služieb), ktoré by bezpečnosť IKT mala chrániť pred ich narušením. Prvý z najdôležitejších modelov informačnej bezpečnosti definoval tri základné komponenty (požiadavky) [81]:

- **dôvernosť** (*confidentiality*) – aktíva sú dostupné len autorizovaným subjektom,
- **integrita** (*integrity*) – aktíva môžu byť modifikované len autorizovanými osobami,
- **dostupnosť** (*availability*) – aktíva sú dostupné pre autorizované osoby, keď sú potrebné.

Postupom času sa tento model rozširoval o rôzne ďalšie špecifické komponenty, ktoré by mali byť tiež brané do úvahy, ako napr. [81], [82]:

- autenticita (*authenticity*) – pôvod aktív je overený, aktíva nie sú kópiou (podvrhom),
- účtovateľnosť (*accountability*) – možnosť sledovať, čo a kedy daný používateľ, systém alebo proces vykonal,
- nepopierateľnosť (*non-repudiation*) – žiadna strana nemôže neskôr poprieť, že napr. daný dokument podpísala (elektronickým podpisom),
- vlastníctvo (*possession)* – kvalita alebo stav vlastníctva informácie alebo kontroly nad ňou,

- užitočnosť *(utility*) – informácia je v stave (formáte) prospešnom pre používateľa,
- súkromie (*privacy*) – utajenie osobných informácií,
- spoľahlivosť (*reliability*) – zariadenie/systém sa správa konzistentne (dôsledne).

Zo všeobecného hľadiska môžu byť útoky na bezpečnosť rozdelené do nasledovných skupín:

- útoky na dostupnosť – prerušenie prívodu energie, spôsobenie preťaženia systému,
- útoky na dôvernosť – odpočúvanie, analýza toku informácií, kopírovanie údajov z pamäte, krádež údajov alebo zariadenia,
- útoky na integritu – modifikácia softvéru, vírusy, trójske kone, logické bomby, modifikácia uložených dát, modifikácia dát počas prenosu,
- útoky na autenticitu – útoky typu **MITM** (***man in the middle***), útoky opakovaním, vloženie falošného záznamu do databázy.

Je nutné si uvedomiť, že neexistuje absolútne bezpečný informačný systém a bezpečnostné politiky sa len snažia znížiť pravdepodobnosť úspešného útoku proti informačnému systému.

9.2. Mechanizmy bezpečnosti

Služby bezpečnosti sú realizované pomocou mechanizmov bezpečnosti, ktoré podporujú a realizujú špecifické činnosti zamerané na ochranu proti útokom, resp. ich následkom. Medzi základné mechanizmy bezpečnosti (podľa odporúčania X.800), ktoré sa implementujú priamo v niektorej vrstve protokolového (sieťového) modelu, patria [83]:

- **šifrovanie** (*encipherment*) – utajenie informačného obsahu správy; využíva sa špecifická kryptografická transformácia, ktorá prevedie správu do formy, ktorá nie je čitateľná neautorizovaným subjektom.
- **digitálne podpisy** (*digital signature*) – aplikácia kryptografických transformácií na zabezpečenie autentizácie zdroja správy a integrity dát.
- **riadenie prístupu** (*access control*) – na základe autentifikácie alebo inej informácie o entite sa zabezpečuje riadenie a kontrola prístupových práv k systémovým prostriedkom a službám.
- **integrita dát** (*data integrity*) – mechanizmy kontroly či prenášané dáta počas prenosu neboli modifikované.
- **výmena autentizačnej informácie** (*authentication exchange*) – proces výmeny autentizačnej informácie medzi používateľom (entitou) a informačným systémom. Slúži na overenie identity používateľa a jej výsledok ovplyvňuje mechanizmy riadenie prístupu.
- **vypĺňanie medzier** (*traffic padding*) – medzery medzi prenášanými dátami sa vypĺňajú dodatočnými bitmi, aby sa znemožnila analýza toku dát.
- **riadenie smerovania** (*routing control*) – výber zabezpečených (fyzických) prenosových ciest pre špecifické dáta s prípadnou zmenou smerovania, ak sa očakáva narušenie bezpečnosti.
- **osvedčenie tretím subjektom** (*notarization*) – využíva sa tretí subjekt na zabezpečenie určitých vlastností výmeny dát v informačných systémoch.

Okrem týchto mechanizmov existujú aj také, ktoré nie sú naviazané na konkrétnu vrstvu sieťového modelu a môžu byť brané ako prvok manažmentu bezpečnosti. Ako príklad možno uviesť bezpečnostnú značku, detekciu bezpečnostných udalostí, obnovu bezpečnosti atď.

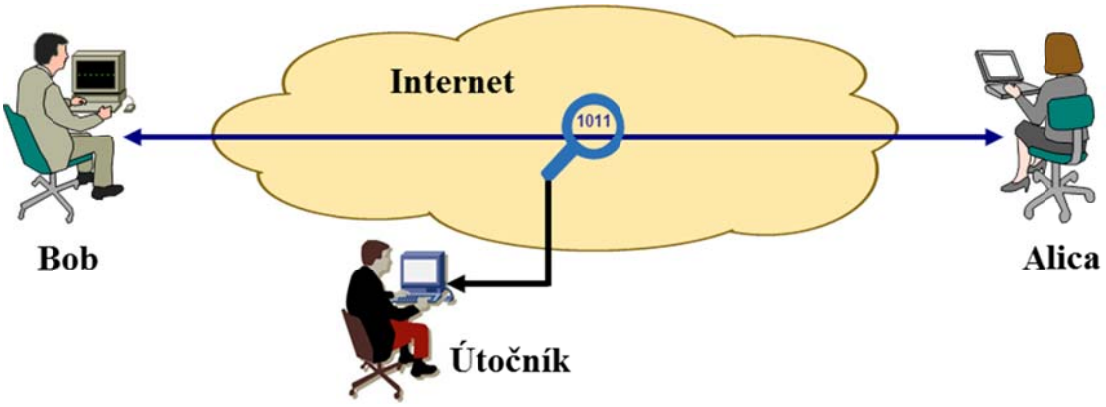
9.3. Útoky na bezpečnosť

Základné delenie útokov na bezpečnosť do dvoch hlavných kategórií je nasledovné [84]:

- **pasívne útoky** (*passive attacks*) **–** cieľom je získať informácie z informačného systému, pričom ale systémové prostriedky informačného systému nie sú ovplyvnené. Preto je veľmi komplikované odhaľovať tento typ útokov a je vhodné aplikovať skôr prevenciu (napr. šifrovanie).
- **aktívne útoky** (*active attacks*) – cieľom je okrem získania informácií aj modifikácia toku dát, čím dochádza aj k ovplyvneniu systémových prostriedkov (prípadne ich činnosti). Preto tento typ útoku sa ľahšie odhaľuje, ale ochrana proti nim je veľmi zložitá, preto cieľom ochrany je skôr detekcia útokov a odstránenie následkov, ktoré spôsobili.

Pasívne útoky na bezpečnosť systémov (**Obr. 33**) využívajú hlavne odpočúvanie alebo monitorovanie premávky aplikovaním dvoch základných prístupov:

- odkrývanie obsahu správ (*release of message content*) – využívajú sa funkcie sledovania (monitorovania), ale sú účinné iba v prípade, že komunikácia prebieha v otvorenej forme. Základným mechanizmom na ochranu (ukrytie informačného obsahu) komunikácie je šifrovanie.
- analýza toku dát (*traffic analysis*) – dômyselné techniky, ktoré sú zamerané na získavanie informácií zo zachyteného toku dát jeho analýzou. Aj v prípade použitého šifrovania útočník stále môže sledovať vzor (profil) komunikácie a získať údaje ako frekvencia a dĺžka prenášaných správ a určiť tak povahu (charakter) komunikácie.

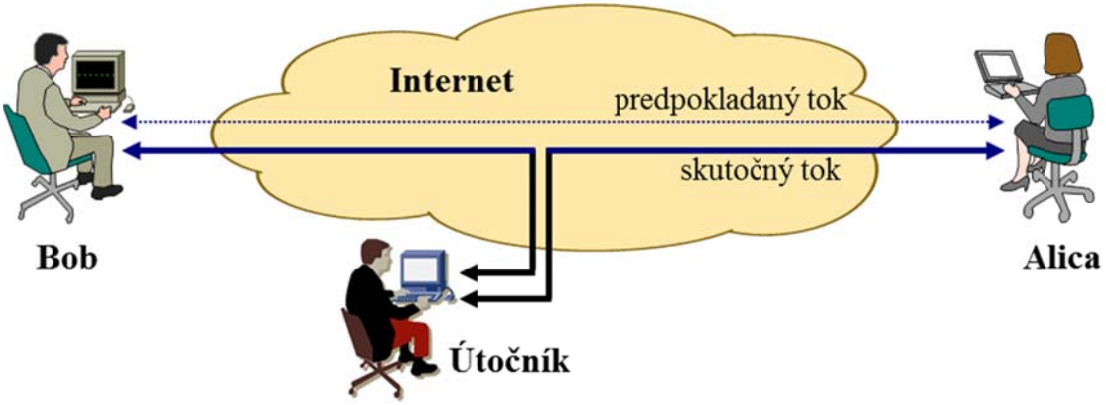


Obr. 33 Princíp pasívnych útokov

Aktívne útoky modifikujú prenášaný tok dát alebo vytvárajú nový (falošný) tok dát (**Obr. 34**). Je ich možné rozdeliť do štyroch kategórií:

- predstieranie identity (*masquerade*) – jeden subjekt predstiera identitu iného subjektu. Výmena autentizačnej informácie autorizovaného subjektu sa zachytí neautorizovaným subjektom, čo mu umožní získať privilégiá pridelené autorizovanému subjektu.

- opakovanie (*replay*) – pri tomto útoku sa zachytia dáta (napr. pakety) a všetky alebo ich časť sa s oneskorením pošle do informačného systému, čo v ňom môže vyvolať nežiaduce (neautorizované) účinky na jeho správanie.
- modifikácia správy (*modification of messages*) – určitá časť originálnej prenášanej správy je útočníkom zmenená alebo správa je oneskorená. Útočník takto získa obsah a súčasne jeho zmenou môže získať aj cudzie privilégiá (právomoci).
- odmietnutie služby (*denial of service*) – cieľom je zabrániť štandardnému používaniu služby alebo manažmentu siete. Útočník tak môže spôsobiť nedostupnosť služby, zariadenia alebo aj celej siete pre ostatných používateľov. Účinnejším variantom tohto útoku je útok realizovaný viacerými počítačmi na jeden server. Označuje sa ako distribuovaný útok **DDoS** (***Distributed Denial of Service***).



Obr. 34 Princíp aktívnych útokov

9.4. Útočníci

Útočník (*intruder*) je subjekt, ktorý realizuje niektorý typ útoku na bezpečnosť informačného systému. Je to osoba, ktorá získa alebo chce získať neautorizovaný prístup alebo neautorizované práva v počítačovom systéme. V súčasnosti útočníkmi nemusia byť iba špičkoví počítačoví odborníci, ktorí sú schopní realizovať veľmi nebezpečné útoky s vážnymi dôsledkami pre počítačové systémy a siete, ale môžu to byť aj amatéri s nižšou úrovňou vzdelania (*wackers*), ktorí s dostupnými nástrojmi z Internetu môžu realizovať menej nebezpečné útoky. Podľa polohy útočníka rozdeľujeme útočníkov na dva typy:

- **vnútorný útočník** (*insider*) – zvyčajne subjekt legitímne pripojený do internej počítačovej siete, ktorý chce získať neautorizovaný prístup k dátam, systémovým prostriedkom a službám.
- **vonkajší útočník** (*outsider*) – zvyčajne subjekt, ktorý nemá autorizovaný prístup do internej počítačovej siete a ktorý chce preniknúť do tejto siete útokom na jej zraniteľné miesta.

Útočníkov je možné rovnako rozdeliť aj na jednotlivcov alebo organizované skupiny. Vo svete informačnej bezpečnosti je možné sa stretnúť s ďalšími názvami útočníkov [85], ako napr.:

- **hacker** (*white hat*) – osoba s veľmi dobrými znalosťami z oblasti IKT. Jeho činnosť sa orientuje na hľadanie zraniteľných miest a bezpečnostných dier navrhovaných alebo existujúcich IKT systémov. Motiváciou je vzrušenie, uspokojenie a uznanie. V prípade oboznámenia vlastníka systému o zistenej zraniteľnosti je jeho činnosť prospešná.
- **cracker** *(black hat)* – osoba, ktorá dokáže obchádzať protipirátske ochrany počítačových programov a svoje vedomosti využíva neeticky. Často sa sústreďuje aj na odhaľovanie prístupových hesiel systémov. Niektoré zdroje uvádzajú, že cracker je hacker s negatívnymi úmyslami.
- **spammer** – osoba, ktorá rozposiela veľké množstvo nevyžiadaných emailových správ (môžu na tento účel využiť aj vírusy).
- **phisher** – s využitím emailu alebo webových stránok sa snaží získať citlivé informácie od používateľov (napr. heslá, čísla kreditných kariet a pod.)
- **scriptkiddies –** používatelia počítačových systémov s nízkou úrovňou znalostí IKT, ktorí svoje útoky realizujú použitím známych skriptov obsahujúcich kód využívajúci zraniteľnosť počítačového systému. Môžu spôsobovať značné škody na systémoch.

9.5. Škodlivý softvér

Škodlivý softvér (*malicious software, malware*) je cieľavedome vytvorený počítačový program, ktorý predstavuje softvérové ohrozenie počítačového systému a môže spôsobiť škody v tomto systéme. Je možné ho rozdeliť do dvoch základných kategórií podľa toho, či na svoje šírenie vyžaduje hostiteľský súbor alebo nie (je nezávislý). Prvá skupina označovaná niekedy tiež ako parazitická obsahuje

- **vírusy** (*viruses*) – sú programy, ktoré sa pripájajú k inému programu (spustiteľnému súboru) a dokážu vykonávať nežiaduce činnosti. Majú schopnosť napádať iné súbory, replikovať a šíriť sa a spôsobovať škody v ďalších počítačových systémoch. Aktivujú sa pri spustení napadnutého programu.
- **logické bomby** (*logic bombs*) – programy tajne a úmyselne integrované do normálnych programov. Aktivujú sa pri splnení určitých podmienok ako napr. spustenie určitej aplikácie, uplynutie určitého času, predvolený čas a iné. Po aktivácii môže zobraziť falošnú správu, zmazať alebo pokaziť údaje, zastaviť prebiehajúci výpočet alebo vykonať iný druh nežiaducej činnosti. Je to najstarší typ škodlivého softvéru (vírusu).
- **trójske kone** (*trojan horses*) – programy, ktoré poskytujú užitočné funkcie, ale okrem toho v sebe obsahujú aj skryté funkcie, ktoré vykonávajú v pozadí nežiaduce a deštrukčné účinky. Využívajú legitímne právomoci danej entity na svoju činnosť a môžu napr. vymazávať údaje alebo zbierať heslá zadávané z klávesnice (*keyloggers*), sledovať činnosť používateľa a odosielať tieto informácie útočníkovi.
- **skryté vstupy** (*trap/back doors*) – sú to vlastne trojské kone, ktoré umožňujú získať útočníkovi prístup do systému obchádzaním mechanizmov bezpečnosti. Môžu byť implementované priamo programátormi a používané pri ladení a testovaní programov. Môžu byť ale implementované aj za účelom naručenia bezpečnosti systému (napr. v hrách a iných užitočných programoch).

Väčšina vírusov má životný cyklus zložený zo štyroch fáz: fáza nečinnosti, fáza šírenia (vírus sa replikuje, klonuje), fáza aktivizácie (pri splnení určitej podmienky) a výkonná fáza (činnosti

vedúce najčastejšie ku škodám v napadnutom počítačovom systéme). Vírusy možno kategorizovať do týchto skupín [81], [84]:

- vírusy šíriace sa pomocou spustiteľných súborov – súborov s koncovkou exe, sys, com, bat,
- makrovírusy – napádajú najčastejšie súbory vytvorené programami v balíku MS Office,
- vírusy šíriace sa cez zavádzacie (*boot*) sektory,
- neviditeľné vírusy – realizujú aktívnu ochranu proti svojmu odhaleniu,
- polymorfné vírusy – vytvárajú mutácie pôvodného vírusu, čo sťažuje ich detekciu,
- rezidentné vírusy – vírusy, ktoré ostávajú neustále bežať v pamäti,
- zašifrované vírusy – časť kódu vírusu je zašifrovaná, čo sťažuje ich detekciu,
- e-mailové vírusy – sú súčasťou prílohy a aktivujú sa po jej otvorení.

Druhú skupinu škodlivého softvéru, ktorý na svoje šírenie nevyžaduje hostiteľský súbor, tvoria:

- **červy** (*worms*) – majú schopnosť sa replikovať a šíriť z jedného počítačového systému na iný počítačový systém, pokiaľ sú tieto systémy pripojené do počítačovej siete. Môžu sa šíriť ako prílohy emailov alebo sa prihlásia na vzdialený systém ako používateľ a po nakopírovaní sa spustia, prípadne využijú inú dieru v systéme na tento účel.
- **zombie** – šíria sa cez počítačovú sieť (Internet) a po úspešnom prieniku do počítačového systému umožňujú prevziať diaľkovú kontrolu nad napadnutým systémom. Niekoľko počítačov napadnutých rovnakým druhom tohto škodlivého softvéru vytvára ***botnet***. Botnety možno riadiť z jedného vzdialeného počítača tak, aby vykonávali napr. útok typu DDoS.

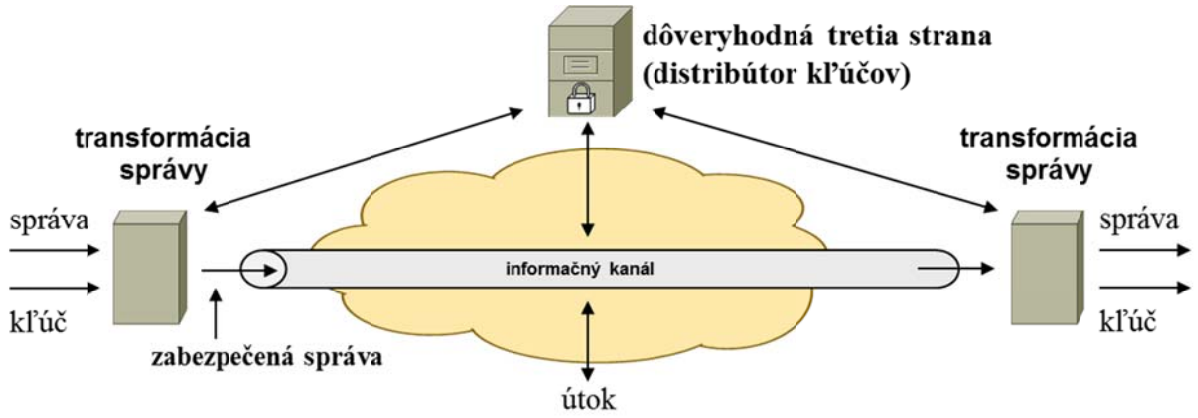
9.6. Modely sieťovej bezpečnosti

Ak sa hovorí o sieťovej bezpečnosti, najčastejšie sa uvádzajú dva základné modely [84]:

- model bezpečného prenosu informácií verejnou sieťou,
- model bezpečného prístupu do siete.

Vo všeobecnosti platí, že verejná sieť, ktorou sme vzájomne všetci poprepájaní v Internete, je sieť nezabezpečená. Ak chceme prenášať touto sieťou citlivé informácie, je potrebné aplikovať model bezpečného prenosu informácií (**Obr. 35**). Tento model je založený na 4 hlavných požiadavkách:

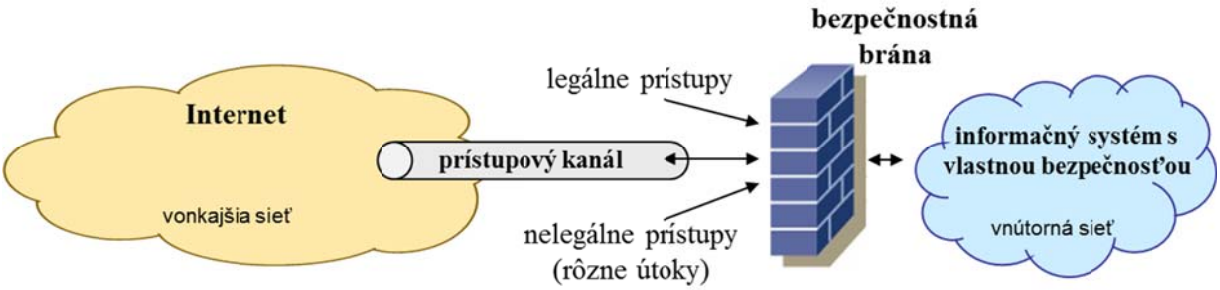
- návrh efektívneho algoritmu pre bezpečnostnú transformáciu prenášanej správy,
- vygenerovanie kľúčov (tajnej informácie), ktoré sa použijú algoritmom,
- vývoj metód, pomocou ktorých sa distribuujú a zdieľajú kľúče (tajná informácia),
- definovanie protokolov pre dosiahnutie požadovaných bezpečnostných služieb.



Obr. 35 Model bezpečného prenosu informácií verejnou sieťou

Model bezpečného prístupu do siete, ktorý je zobrazený na **Obr. 36**, a ktorý chráni informačný systém pred nežiaducimi vstupmi (útokmi), vyžaduje:

- návrh vhodných funkcií bezpečnostnej brány na zabránenie vstupu neautorizovaným subjektom a škodlivému softvéru do bezpečnostnej brány,
- monitorovanie komunikácie cez bránu (analýza, detekcia).



Obr. 36 Model bezpečného prístupu do siete

Prvý model využíva rôzne kryptografické algoritmy a protokoly a môže zakomponovať pri svojej činnosti aj tretiu dôveryhodnú stranu. Jadrom druhého modelu sieťovej bezpečnosti je bezpečnostná brána. V rámci tohto študijného materiálu sa sústredíme ďalej na druhý model a konkrétnejšie na možné realizácie bezpečnostných brán.

9.7. Bezpečnostné brány (firewalls)

Bezpečnostná brána (*firewall*) [84] je zariadenie sieťovej bezpečnosti, ktoré slúži na zabezpečenie vnútornej siete organizácie tým, že oddeľuje vnútornú sieť od zvyšku sveta (Internetu). Ak chce spoločnosť implementovať sieťovú bezpečnosť, musí si zadefinovať bezpečnostnú politiku, čo je súbor pravidiel, ktoré zabezpečia ochranu jej majetku, počítačových systémov, osobných informácií a ďalších citlivých údajov. Podľa tejto politiky budú stanovené bezpečnostné funkcie brány, ktorá môže byť realizovaná hardvérom, softvérom alebo ich kombináciou. Základnou podmienkou je, aby všetka komunikácia do a z vnútornej siete prechádzala cez túto bránu. Potom môže aplikovať dve hlavné funkcie: môže zablokovať alebo

povoliť komunikáciu. Zvyčajne všetka komunikácia z vnútornej siete do vonkajšej siete (Internet) je povolená a na druhej strane sú zvyčajne zakázané všetky žiadosti o spojenia prichádzajúce z Internetu do vnútornej siete. V prvom prípade ale bezpečnostná politika môže aj napr. zabrániť pripojeniu na nedôveryhodné lokality, alebo na iné miesta, ktoré sú považované za bezpečnostnú hrozbu, alebo sú považované za nevhodné pre organizácie. Ako už bolo spomenuté vyššie, bezpečnostná brána musí súčasne byť odolná aj proti útokom na ňu samotnú (musí obsahovať bezpečný operačný systém).

Výhody bezpečnostných brán možno zosumarizovať nasledovne:

- môžu zabrániť vonkajšiemu používateľovi v dosiahnutiu zdrojov vnútornej siete cez nezabezpečený protokol zahodením paketov smerujúcich na konkrétny TCP / UDP port,
- môžu zabrániť určitým IP adresám v dosiahnutí vnútornej siete, môže napríklad zakázať napríklad protokolu FTP príkaz WRITE (umožňuje zapisovať dáta) a tým povoliť iba čítanie obsahu FTP,
- je efektívnejšie použiť jednu alebo viacero brán na zabezpečenie siete, ako zabezpečiť každý počítač a jeho aplikácie,
- je jednoduchšie zabezpečiť bezpečnostnú bránu v porovnaní s koncovým systémom. Majú často zjednodušené operačné systémy a na týchto systémoch nie sú spravidla spustené komplexné aplikácie. Čím je aplikácia menej komplexná, tým menej potenciálnych programových chýb môže aplikácia obsahovať.

Medzi nevýhody bezpečnostných brán možno zaradiť:

- brána (*firewall*) je zvyčajne centrálny bod vystavený útokom. Ak útočník získa kontrolu nad nim, tak môže realizovať útoky priamo z neho do vnútornej ako aj vonkajšej siete alebo zastaviť všetku premávku cez neho a pod.
- tvoria úzke hrdlo v sieti a taktiež predstavujú bod zlyhania. V prípade zlyhania celá sieť stratí pripojenie k Internetu.
- nemôžu ochrániť vnútornú sieť pred vnútornými hrozbami, pričom väčšina útokov na sieť organizácie pochádza z vnútornej siete. Na ochranu proti takýmto útokom je nutné nasadiť iné bezpečnostné systémy.
- nemôžu ochrániť vnútornú sieť pred útokmi cez zle zabezpečenú bezdrôtovú sieť.

9.8. Kategorizácia bezpečnostných brán

Bezpečnostné brány môžu byť rozdelené do nasledujúcich kategórií [81], [84]:

- (bezstavový) firewall s filtrovaním paketov (paketový filter),
- stavový firewall (stavový paketový filter)
- aplikačná brána (proxy server/firewall)

9.8.1. Firewall s filtrovaním paketov (paketový filter)

Paketový filter je najjednoduchším typom firewallov. Pri svojej činnosti využívajú informácie z paketov (ktoré cez ne prechádzajú) týkajúce sa tretej a štvrtej vrstvy referenčného modelu OSI. Ich základnou funkciou je porovnať niektoré hodnoty z hlavičiek paketov s preddefinovanými

hodnotami v konfigurácii (preto sa volajú aj statické firewally). Medzi tieto hodnoty (polia) patria najmä:

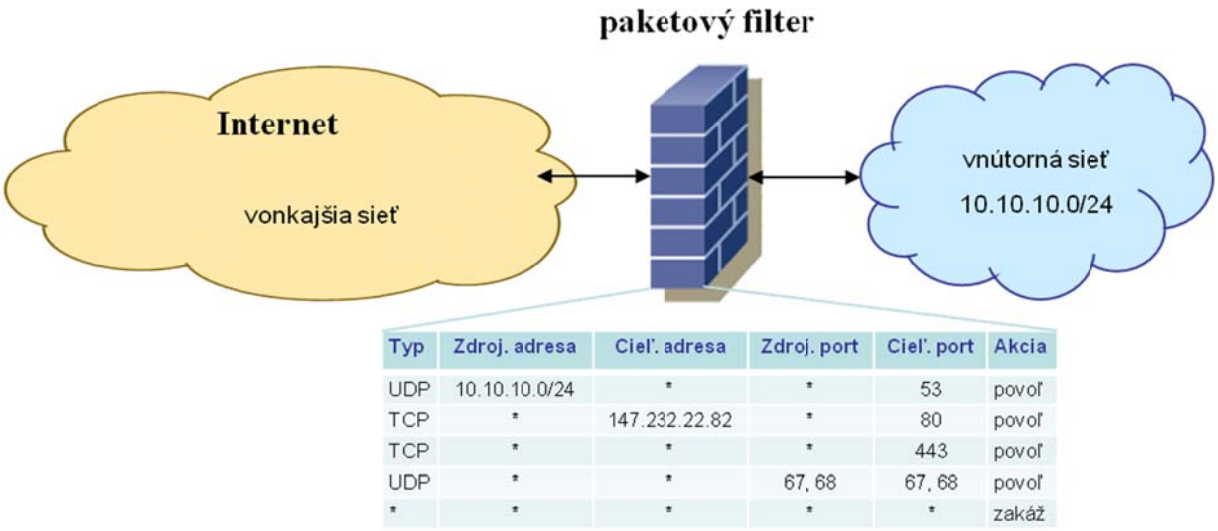
- zdrojová a/alebo cieľová IP adresa,
- zdrojový a/alebo cieľový TCP / UDP port,
- transportný protokol,
- príznaky protokolu TCP: SYN, ACK, RST (len niektoré implementácie ho podporujú).

Výhodou paketových filtrov je ich jednoduchosť a rýchlosť, keďže čítajú údaje iba z hlavičiek protokolov IP alebo TCP / UDP. Táto operácia je ľahko vykonateľná a preto paketový filter má aj menšie požiadavky na výkon zariadenia. Pre používateľov sa javia ako transparentné.

Nevýhodou týchto firewallov je, že sú často zraniteľné útokmi, ktoré napr. falšujú IP adresy, delia pakety na veľmi malé fragmenty, využívajú tzv. zdrojové smerovanie (zdroj špecifikuje cestu paketu sieťou dopredu) alebo využívajú slabé miesta aplikačných protokolov a aplikácií. Paketové filtre neuchovávajú informácie o stave najmä nespojovo orientovanej komunikácie (protokoly UDP a ICMP). Pri komplexnej bezpečnostnej politike môžu nastať aj chyby pri konfigurácii pravidiel.

Na **Obr. 37** je možné vidieť niekoľko pravidiel definovaných pre filtrovanie paketov. Tento firewall má dve rozhrania (vnútorné a vonkajšie). Filtrovacie pravidlá sú aplikované na vnútorné rozhranie a na základe nich bude firewall realizovať napr. nasledovné akcie:

- paket z vnútornej siete poslaný na DNS server vo vonkajšej sieti je prepustený firewallom, lebo DNS protokol posiela správy pomocou protokolu UDP na porte 53 (prvé pravidlo).
- IP adresy z vnútornej siete môžu kontaktovať (vonkajší) webový server IBA s IP adresou 147.232.22.82. Hviezdička (*) v pravidle znamená ľubovoľnú zdrojovú adresu (alebo port). Toto pravidlo ale umožňuje, aby členovia z vnútornej siete podvrhli zdrojovú IP adresu, a takto môžu vykonávať útoky na vonkajšie siete.
- tretie pravidlo povoľuje ľubovoľnej adrese z vnútornej siete kontaktovať akúkoľvek adresu na Internete určenej na cieľový TCP port 443, ktorý patrí štandardne k HTTPS komunikácii.
- akákoľvek komunikácia protokolom DHCP (používa protokol UDP a porty 67, 68) je povolená cez firewall (štvrté pravidlo).
- všetky ostatné komunikácie sú zakázané (posledné pravidlo), lebo pravidlá firewallu sú vyhodnocované sekvenčne najprv prvý riadok, potom druhý, atď., pričom sa skončí pri prvom vyhovujúcom pravidle.



Typ	Zdroj. adresa	Cieľ. adresa	Zdroj. port	Cieľ. port	Akcia
UDP	10.10.10.0/24	*	*	53	povoľ
TCP	*	147.232.22.82	*	80	povoľ
TCP	*	*	*	443	povoľ
UDP	*	*	67, 68	67, 68	povoľ
*	*	*	*	*	zakáž

Obr. 37 Princíp paketového filtra

9.8.2. Stavový firewall (stavový paketový filter)

Stavový firewall pracuje v podstate na rovnakých vrstvách referenčného modelu ISO OSI, ale na rozdiel od statických paketových filtrov nepracujú s každým paketom nezávisle a samostatne. Okrem filtrovania premávky monitorujú komunikáciu, ktorá cez ne prechádza. To znamená, že sledujú pri paketoch aj TCP/UDP porty (pri TCP navyše aj napr. sekvenčné čísla). Informácia o stave komunikácie sa ukladá do špeciálnej dynamickej stavovej tabuľky. Inými slovami stavový firewall sa snaží identifikovať začiatok spojení a tokov v odchádzajúcej premávke (z vnútornej siete do vonkajšej), ktoré sú povolené a informáciu o nich si zapíše do stavovej tabuľky. Tieto informácie najčastejšie obsahujú zdrojovú a cieľovú IP adresu, zdrojový a cieľový port aplikačného protokolu, typ protokolu, čas alebo typ expirácie, poradové čísla a pod.

Na základe týchto informácií vie firewall identifikovať v prichádzajúcej premávke pakety, ktoré patria do povolenej premávky a sú teda pustené do vnútornej siete. Prichádzajúce pakety, ktoré nepatria do žiadneho spojenia (iniciovaného z vnútornej siete), sú zahodené, ak neexistuje výnimočné pravidlo, ktoré by umožnilo firewallu ich pustiť ďalej.

Pri TCP spojeniach vie firewall identifikovať ich začiatok aj koniec podľa príznakov SYN a FIN v hlavičke TCP segmentu. Pri nespojovo orientovaných tokoch (protokolov UDP a ICMP) začiatok toku firewall identifikuje príchodom prvého paketu a koniec sa nastaví uplynutím časovača.

Nevýhodou stavových firewallov je ich vyššia požiadavka na hardvérové zdroje (väčší výkon procesora, väčšie množstvo pamäte, atď.). Keďže musia spracovať a prečítať viac informácií v hlavičke, vnášajú do siete väčšie oneskorenie ako paketové filtre. Rovnako ako paketové filtre nevedia identifikovať protokol aplikačnej vrstvy, takže ak niekto pošle torrent súbor na TCP porte 80, stavový firewall umožní takejto premávke prejsť, aj keď to napríklad nie je povolené bezpečnostnou politikou.

9.8.3. Aplikačná brána (proxy server/firewall)

Ako už bolo spomenuté, paketové filtre (stavové či bezstavové) nie sú veľmi účinné pri filtrovaní aplikačných protokolov. Na tento účel slúžia práve aplikačné brány alebo tzv. proxy servery, ktoré konajú v mene svojich klientov. V ich mene sa pripájajú k Internetu a odosielajú ich dáta (a potom prijímajú odpovede z Internetu a preposielajú ich klientom). Aplikačná brána pracuje na všetkých vrstvách sieťového modelu, to znamená, že rozumejú aplikačným protokolom a môžu potom napr.:

- zakázať flash videá zo známych portálov (napr. youtube), pričom ďalší obsah na stránke ostane povolený.
- sledovať e-mailovú komunikáciu a ak bezpečnostná politika zakazuje prílohy s ".doc" alebo ".pdf" súbormi, aplikačná brána je schopná skontrolovať e-mailový obsah a odstrániť takéto prílohy (dokonca, aj keď sú skomprimované).
- zabrániť podvrhnutiu paketov alebo použitiu nelegálnej aplikácie na povolených portoch (vyššie spomínaný torrent súbor cez TCP port 80 by aplikačná brána zahodila).
- aj čítať šifrovanú komunikáciu.

Na druhej strane takáto hĺbková kontrola kladie zvýšené nároky na výkon hardvéru zariadenia. Keďže dočasne uchovávajú komunikáciu na spracovanie, vnášajú veľké oneskorenia do siete. Činnosti vykonávané na aplikačnej vrstve je možné realizovať iba softvérovo, čo značne zaťažuje procesor a pamäť. Niektoré typy aplikačných brán vyžadujú zásah (úpravu) aj na strane klientov.

9.9. Systémy na detekciu a prevenciu prienikov

Model bezpečného prístupu do siete založený na aplikácii bezpečnostných brán nie je schopný zabezpečiť vnútornú sieť pred všetkými typmi útokov pochádzajúcich z vonkajšej siete a rovnako pred takmer žiadnymi útokmi vznikajúcimi vo vnútornej sieti. Aby sme mohli zvýšiť úroveň bezpečnosti vnútornej siete, je nutné nasadiť ďalší systém, ktorý sa bude snažiť tieto nedostatky odstrániť. Na tento účel slúžia systémy na detekciu prienikov **IDS** (***Intrusion detection systems***) a prevenciu prienikov **IPS** (***Intrusion prevention systems***). Tieto systémy môžu pracovať na úrovni siete a tiež na úrovni koncových zariadení (počítačov). Všeobecne systém IDS zbiera a analyzuje informácie z rôznych oblastí v rámci počítača alebo siete s cieľom identifikovať možné narušenia bezpečnosti, vrátane zneužitia (útoky v rámci organizácie) a prienikov (útoky zvonku organizácie) ako aj pokusy o narušenie prípadne identifikovať aj zraniteľné miesta systémov [81], [86]. Na tento účel IDS kontroluje všetku prichádzajúcu a odchádzajúcu sieťovú premávku alebo správanie sa používateľov na koncových zariadeniach a identifikuje podozrivé okolnosti. Medzi funkcie IDS patria:

- monitorovanie a analyzovanie činností používateľa a systému,
- analýza systémových konfigurácií a zraniteľností,
- hodnotenie systému a integrity súborov,
- schopnosť rozpoznať typické črty útokov,
- analýza abnormálnej činnosti,
- sledovanie porušovania politiky.

Systémy IDS sa snažia odhaľovať zlomyseľné aktivity (útoky), zatiaľ čo systémy IPS sa snažia chrániť sieť a zariadenia tým, že zahadzujú pakety, zakazujú prístup paketom, blokujú spojenia, posielajú alarmy administrátorom a pod.

10. Adaptácia multimediálneho obsahu

Na adaptáciu multimediálneho obsahu sa môžeme pozerať z rôznych hľadísk. Adaptácia môže byť motivovaná prispôsobením sa špecifickým vlastnostiam prenosovej cesty a zobrazovacieho zariadenia, ako aj preferenciami či požiadavkami konzumenta obsahu. Cieľom adaptácie je spravidla maximalizácia koncovej kvality obsahu vzhľadom na možnosti prispôsobenia sa. Z pohľadu prevádzkovateľa prenosovej cesty sa môže jednať o požiadavku maximálnej kvality prenášaného obsahu pri stanovenej záťaži siete, resp. jej jednotlivých častí. Môže sa aj jednať o optimalizáciu (prispôsobenie sa) pri meniacich sa podmienkach prenosovej cesty: mení sa chybovosť, mení sa latencia, a podobne. Alebo sa mení samotná prenosová cesta (a jej poskytovateľ) v pozadí – prepnutie medzi mobilným pripojením, Wifi a pevných pripojením. Z pohľadu správcu obsahu sa môže jednať o minimalizáciu veľkosti úložiska. Z pohľadu užívateľa sa môže jednať o maximalizáciu kvality obsahu určeného jemu a prispôsobeného vzhľadom na jeho osobné požiadavky a zariadenie, ktoré používa. Tieto požiadavky sú často čiastočne protichodné, majú veľmi veľa stupňov voľnosti ako ich riešiť a riešenia nie sú jednoznačné.

Už len samotné vyhodnotenie kvality multimediálneho obsahu nie je jednoznačné (pre rôznych používateľov) – je horšie video, kde je lepší obraz a horšie audio, alebo naopak? Aj keď zoberieme napr. len audio časť, je kvalitnejšie to, čo ma mierne zníženú kvalitu dlhší čas, alebo veľmi zníženú kvalitu kratší čas? Sú rozpracované predovšetkým metódy, ktoré hodnotia kvalitu každej zložky audio, statický obraz, video zvlášť. Základné delenie týchto metód je podľa toho, či pracujú aj s referenčným signálom (originálom), alebo bez neho, či pracujú objektívne (matematicky stanovená metrika), alebo subjektívne (pomocou ľudských pozorovateľov). Pri videu napr. medzi objektívne metódy s referenciou patria VQM (ITU-T J.147), PEVQ (ITU-T J.246), medzi subjektívne patria metódy podľa odporúčaní ITU-R BT.500 a ITU-T P.910. V týchto testoch sa používa metrika **MOS** (***mean opinion score***), pri ktorej pozorovatelia hodnotia kvalitu videa za kontrolovaných podmienok na stupnici 1 (zle) až 5 (výborne) a výsledky sa pre celú skupinu pozorovateľov priemerujú. Metrika MOS bola pôvodne zavedená na vyhodnocovania kvality hovorového signálu v telekomunikáciách (odporúčanie ITU-T P.800.1). Niektoré štandardizované objektívne metódy vznikli matematickým modelovaním správania sa ľudského pozorovateľa a príslušného vnemového systému, napr. pri audiu je to metóda **PEAQ** (***Perceptual Evaluation of Audio Quality***) – odporúčanie ITU-R BS.1116, pre video napr. vyššie uvedené **PEVQ** (***Perceptual Evaluation of Video Quality***).

Keďže požiadavky individuálneho používateľa sa môžu výrazne líšiť od priemeru a ak má možnosť zasiahnuť parametricky do procesu adaptácie obsahu, mohla by sa výsledná kvalita výrazne zlepšiť. Napr. pri zmenšení prenosovej rýchlosti kanála niektorí používatelia môžu uprednostniť

- zníženie snímkovej frekvencie, zachovanie ostrosti obrazu, zachovanie kvality audia
- zachovanie snímkovej frekvencie, vznik artefaktov v obraze, zachovanie kvality audia
- vypnutie audia a investovať ušetrené bity do obrazu

Toto samozrejme môže byť ešte závislé od zariadenia, na ktorom je obsah sledovaný a ešte aj od samotného obsahu. Podľa odlišných kritérií bude k vyhodnocovaniu kvality pravdepodobne užívateľ pristupovať pri:

- priamom prenose zo športového zápasu

- pri sledovaní akčného filmu
- pri sledovaní televízneho hlásateľa pri predpovedi počasia
- pri sledovaní koncertu

Pri adaptácii poznáme tri základné úrovne ako obsah adaptovať:

- výberom obsahu – vyberajú sa iba relevantné časti (vzhľadom na podmienky, preferencie, atď.) multimediálneho obsahu
- konverzia modality – využívaná sa konverzia jednej zložky multimediálneho signálu na druhý (napr. text na reč)
- škálovanie/prekódovanie obsahu – vykonáva sa napr. zmena formátu obsahu na formát podporovaný zariadením, obsah je doručovaný iba v potrebnom rozlíšení a podobne ...

Potreba adaptácie obsahu vyústila k štandardizácii súborových a prenosových formátov ktoré podporujú možnosť mať uloženú informáciou vo vrstvách, ktoré vylepšujú základnú vrstvu so základnými informáciami.

Jedným z takýchto predstaviteľov je štandard na kompresiou obrazu JPEG. Už ten špecifikoval 2 módy vhodné na využitie v procese adaptácie obsahu (viď **Obr. 38**):

- progresívny mód ([87] v dodatku G): informácie o obraze sú kódované postupne a to tak, že po prijatí časti informácií tieto predstavujú celý obraz, ale s menej detailmi, po prijatí ďalších dávok informácií je obraz postupne vylepšovaný. Pritom platí, že najdôležitejšie informácie, t.j. tie, ktoré najviac zmenšujú chybu rekonštrukcie sú prenášané na začiatku a postupuje sa k menej dôležitým informáciám. Toto sa môže diať dvomi spôsobmi

    - volením koeficientov (spectral selection) – spektrálne koeficienty sú prenášané od dôležitejších k menej dôležitým
    - postupnou aproximáciou (succesive approximation) – hodnoty koeficientov sa prenášajú od najdôležitejších bitových rovín po najmenej dôležité.

- hierarchický mód ([87] v dodatku J) umožňuje lepšie prispôsobenie rozlíšeniu zobrazovacieho zariadenia. Obrázok je prenášaný tak, že najprv sú prenesené informácie potrebné pre rekonštrukciu zmenšenej verzie obrazu, potom postupne zvyšky informácií, ktoré umožnia obrázok kvalitne zobraziť postupne pri väčšom a väčšom rozlíšení.

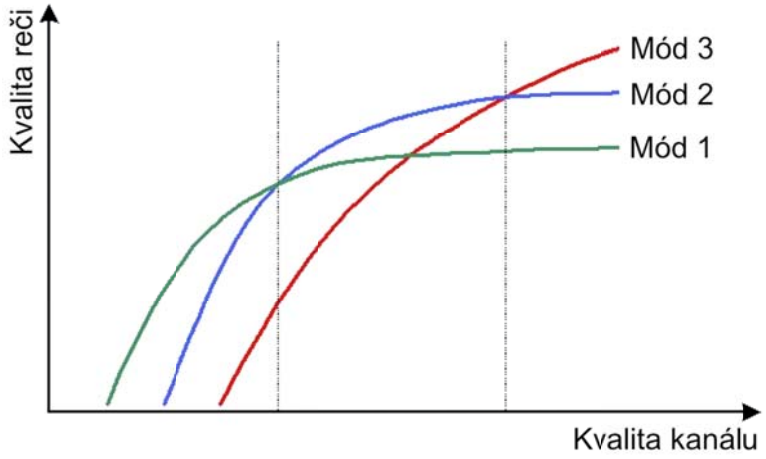
Štandard JPEG2000 [89] na kompresiu a prenos statického obrazu zaviedol paketizáciu pre prenos informácií a najmä zaviedol koncept vrstiev kvality („quality layers“), ktorý umožňuje priamo štruktúrovať údaje na základe prínosu ku kvalite a následne napr. dôležitejšie chrániť viac, nedôležité v prípade potreby ako prvé zahodiť a podobne.

Základný mód	Progresívny mód	Hierarchický mód

Obr. 38 Zobrazenia priebežne dostupnej informácie na prijímacej strane počas prenosu JPEG súboru pri použití rôznych módov (dostupné informácie pribúdajú na obrázku z ľava do prava a potom zhora dole) [88]

V súčasnosti je najefektívnejší štandard na kompresiu obrazu štandard **HEIF** (***High Efficiency Image File***). Je to vlastne časť 12 odporúčania MPEG-H (viď nižšie). Využívajú sa tam algoritmy použité v HEVC pre vnútrosnímkovú predikciu (de facto je to vyňatá časť HEVC vhodná na kódovanie statického obrazu). Tento štandard by mal byť efektívnym nástupcom klasického JPEG algoritmu. HEIF na rozdiel od rozpačite akceptovaného JPEG2000 získal širokú podporu, napr. natívnou súčasťou OS High Sierra. HEIF môže obsahovať viacero tzv. image items, ktoré reprezentujú ten istý obrázok avšak s iným priestorovým rozlíšením, bitovou hĺbkou, gamutom, kódovacím formátom a profilom.

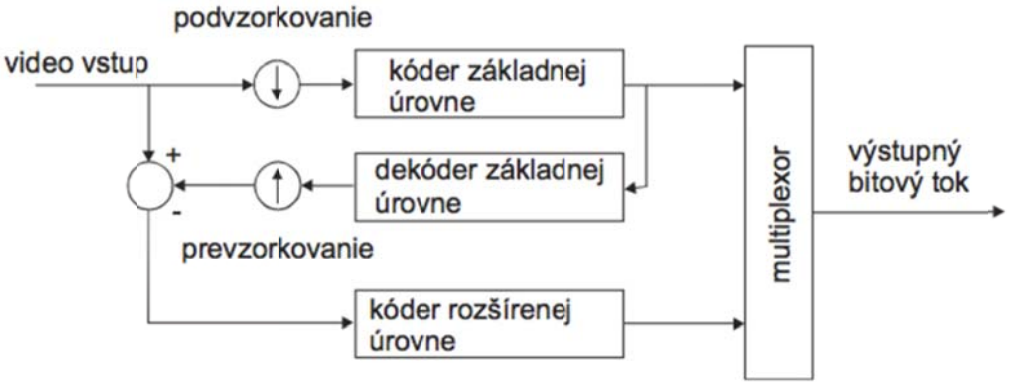
Pri audiu sa etablovala adaptivita obsahu najmä v telekomunikačných systémoch. Napr. **AMR** (***Adaptive Multi Rate***) kodek (odporúčanie 3GPP TS 26.071) resp. jeho vylepšená verzia **AMR WB** (***AMR Wide Band***) (odporúčanie G.722.2 a 3GPP TS 26.190) kódujú 20ms úseky rečového signálu a v závislosti od aktuálnych podmienok v mobilnej sieti sa volí verzia údajov s primerane silným kódovaním. Napr. pri dobrých prenosových podmienkach sa volí verzia, ktorá umožní preniesť maximum užitočných informácií avšak slabo chránených proti chybám, pri zlých podmienkach sa zvolí verzia prenášajúca málo užitočných informácií, avšak oveľa odolnejšia voči prípadným chybám (viď **Obr. 39**).



Obr. 39 Princíp AMR – pri danej kvalite kanálu sa volí mód, ktorý poskytuje najväčšiu kvalitu reči, t.j. pri najväčšej kvalite kanálu sa využije mód 3 (pravá oblasť), pri zníženej sa prepne na mód 2 (stredná oblasť) a pri najnižšej sa prepne na mód 1 (ľavá oblasť).

Pri videu zaviedol pojem škálovateľnosti štandard MPEG-2 [90]. Pri nej je obrazový stream kódovaný v dvoch úrovniach, v prvej, základnej úrovni je prenášaný základ, ktorý môže byť ďalej vylepšený doplnkovou úrovňou, ktorá obsahuje dodatkové informácie k dosiahnutiu plnej kvality videa. Jedny zo základných metód škálovateľnosti sú

- škálovanie na základe **SNR** (***Signal to Noise Ratio***): doplnková úroveň posiela informácie, ktoré vylepšujú kvalitu videa pri danom rozlíšení
- priestorové škálovanie: základná vrstva kóduje video pri nižšom (polovičnom) rozlíšení a rozširujúca úroveň kóduje rozdielové informácie potrebné na zobrazenie v plnom rozlíšení.



Obr. 40 Blokový diagram postupu kódovania pri priestorovej škálovateľnosti v MPEG-2

Pri priestorovom škálovaní (viď **Obr. 40**) je vstupný video signál priestorovo redukovaný horizontálne aj vertikálne, čím sa zníži jeho rozlišovacia schopnosť. Tento obraz je potom štandardným spôsobom zakódovaný kóderom základnej úrovne. Následne je dekódovaný a zväčšený na pôvodný rozmer. Rozdielový obraz je kódovaný pomocou kódera rozšírenej

úrovne. Nakoniec sú výstupy zo základného kódera a z kódera rozšírenej úrovne multiplexované do výstupného bitového toku.

Štandard MPEG-2 nepodporuje škálovateľnosť audia. Ten prináša až štandard MPEG-4, vo forme MPEG-4 **SLS** (***Scalable Lossless Coding***), ktorý umožňuje kódovať zvyškovú informáciu ako ďalšiu vrstvu a dosiahnuť až kvalitu bezstratového kódovania. MPEG-4 zároveň rozširuje škálovateľnosť kódovania obrazovej informácie MPEG-2 tak, že umožňuje využiť viac ako 1 rozširujúcu úroveň. V rámci štandardu MPEG-4 AVC / H.264 [91] sa naviac okrem priestorového a SNR škálovania zavádza aj časové škálovanie. Časové škálovanie je, že v čase existuje viacero sekvencií snímok a teda v prípade potreby je možné doplnkové sekvencie zahadzovať. Toto má za následok redukciu snímkovú frekvencie. V dodatku G štandardu MPEG-4 AVC po názvom **SVC** (***Scalable Video Coding***) sú uvedené doplnkové odporúčania ako škálovateľnosť efektívne využívať [92].

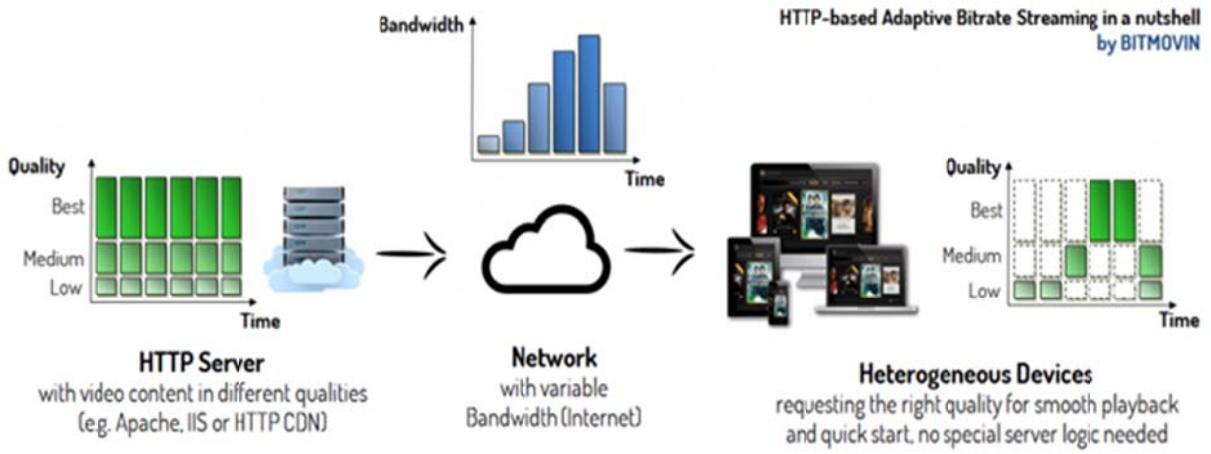
Zatiaľ najnovší kóder H.265 – štandardizovaný v MPEG-H časť 2 ako **HEVC** (***High Efficiency Video Coding***) [93] prináša škálovateľnosť pre videá až s rozlíšením 8K, teda 8192x4320 bodov a o desiatky percent zlepšuje kompresiu oproti MPEG-4 AVC. Časová škálovateľnosť bola prítomná už v prvej verzii štandardu, avšak priestorová, SNR škálovateľnosť a škálovateľnosť na základe bitovej hĺbky a gamutu a ich kombinácie boli pridané až v druhej verzii štandardu vo forme SHVC (rozšírenia **Š**kaľovateľnosti **HEVC**) v októbri 2014. Zároveň boli možnosti rozšírené o efektívny prenos 3D (stereoskopický, s mapou hĺbky) resp. multiview (MV) videa.

V štandarde MPEG21, ktorý bol finalizovaný v roku 2003 a definuje otvorený framework pre multimediálne aplikácie, sa v časti 7 venuje otázke adaptácie obsahu vo forme ***Digital Item Adaptation*** (**DIA**) [94]. Pojem Digital item zahŕňa nejaký multimediálny obsah spolu s jeho všetkými potrebnými metadátami. DIA špecifikuje množinu popisných nástrojov na optimalizáciu adaptácie multimediálneho obsahu. Špecifikuje ako by malo byť popisované prostredie pri adaptácii a to popisom charakteristík siete, zariadenia, užívateľských preferencií a okolia užívateľa:

- schopnosti zariadenia: dostupné kódeky, vstupno-výstupné možnosti (displej, audio, mikrofón, ...)
- charakteristiky siete: schopnosti siete (max. kapacita, minimálna garantovaná šírka pásma, ...), podmienky - oneskorenie, jitter, chybovosť, dostupná šírka pásma
- charakteristiky užívateľa: užívateľské preferencie, história používania, všeobecné informácie o užívateľovi, preferencie na prezentovanie jednotlivých modalít – napr. pri audiu preferovaná hlasitosť a nastavenie ekvalizátora, pri obraze rozlíšenie, teploty farieb, saturácia, kontrast.
- prístupnosť: charakteristiky pre ľudí s postihnutím napr. vizuálneho systému (napr. stupeň a typ poruchy farebného videnia) sluchového systému (obmedzenie sluchu pri rôznych frekvenciách)
- fyzické okolie užívateľa: miesto a čas používania, audiovizuálne vlastnosti prostredia (napr. úroveň a charakteristika hluku), úroveň osvetlenia

Štandard sa venuje aj škálovateľnému obsahu v MPEG-4 SVC a poskytuje generický nástroj na popis syntaxe bitového streamu a použitie tohoto popisu na vytvorenie adaptovanej verzie obsahu. Okrem využitia škálovateľnosti popisuje aj možnosti konverzie modality obsahu (modality translation), napr. audio na text a naopak.

V roku 2012 bol štandardizovaný MPEG-**DASH** (***Dynamic Adaptive Streaming over HTTP***) - ISO/IEC 23009-1, ktorý popisuje interakciu klienta so serverom pri adaptívnom doručovaní obsahu cez HTTP protokol [95]. MPEG-DASH je agnostický od kódeku, môže sa použiť s ľubovoľným moderným kódovacím postupom na kódovanie videa, ako napr. H.264, H.265, VP9 atď. Princípom je, že na strane servera je obsah rozdelený na segmenty a každý segment je zakódovaný pri rôznych bitových náročnostiach, resp. má rôznym spôsobom optimalizovaný obsah. Informácia o segmentoch a ich verziách je dostupná prostredníctvom tzv. **MPD** (***Media Presentation Descriptor***) súboru. Klientské zariadenie si najprv stiahne MPD súbor, na základe toho začne sťahovať video, pričom v závislosti od aktuálnych podmienok na prenosovom kanáli môže optimalizovať akú verziu stiahne pre ďalšie segmenty videa (viď **Obr. 41**). Samozrejmé kritérium je aby stihol včas stiahnuť čo najkvalitnejšiu resp. najvhodnejšiu verziu pre konzumenta. MPEG-DASH používajú napr. Netflix a Youtube pri distribúcii obsahu a to aj pri streamovaní priamych prenosov. Existujú systémy, ktoré vedia efektívne využiť škálovateľnosť MPEG-4 SVC pri použití MPEG-DASH (napr. [96]). Príklady údajov (MPD súbory, video súbory atď.) pri využití SVC sú uvedené napr. v [97].



Obr. 41 Princíp doručovania obsahu pomocou MPEG-DASH [98]

V súvislosti s MPEG-DASH vyvstáva otázka, prečo klient, keď sú dobré podmienky nestiahne celý stream k sebe, aby keď sa zhoršia podmienky prenosu, nemusel zhoršovať kvalitu. Odpovede sú viaceré, napr.:

- obmedzenie dostupných prostriedkov klienta (pamäť)
- načo sťahovať dáta, ktoré si užívateľ možno ani nepozrie
- prečo zbytočne zaťažovať prostriedky siete v čase, keď ich možno urgentnejšie potrebujú iní

MPEG-DASH teda umožňuje riadiť doručovanie obsahu pri rôznych podmienkach prenosového kanálu a optimalizovať kvalitu a prenesený objem dát resp. iné aj kritéria (napr. nepriamo výdrž zariadenia na batériu) z pohľadu jednotlivých užívateľov. Optimalizácii rozhodovania v klientovi (ktorú štandard MPEG-DASH nepredpisuje) je v súčasnosti venovaného veľa úsilia, napr. [99].

Pri komunikačných sieťach 5. generácie je dôraz nielen na rastúcu kapacitu siete, ale aj na to, rastúcou inteligenciou siete túto kapacitu ďalej zvyšovať [100]. V súvislosti s tým boli navrhnuté viaceré rozšírenia siete, ktoré zavádzajú oproti MPEG-DASH aj inteligenciu na strane siete,

napr. použitím vyrovnávacej pamäte (cache), a to čo najbližšie k užívateľom [101] [102]. ETSI tento komponent nazýva **MEC** (***mobile edge computing***) [103] a typicky sa nachádza na okraji mobilnej siete, t.j. napr. v NODE-B. Takto sa dá zmenšiť záťaž zbytku siete, keďže viac zaťažená bude iba časť prístupovej siete medzi cache a koncovými užívateľmi [104].

Pri MPEG-DASH v súčasnosti prebieha výskum a štandardizačné úsilie ako rozšíriť adaptivitu pre doručovanie VR obsahu (DASH-VR). Hlavná motivácia je založená na tom, že zvyčajne pri sledovaní 360° videa vidíme naraz iba 1/12 celkovej obrazovej informácie, zbytok je mimo nášho pohľadu - **FOV** (***Field Of View***). Predpokladajú sa 3 úrovne [105]:

- základná úroveň – doručované celé 360°video
- SRD (spatial relationship description) – poskytuje techniku delenia na oblasti (tiles) aby užívateľ dostával len ten obsah na ktorý sa aktuálne pozerá (predstavuje druhý dodatok MPEG-DASH) plus nejaká oblasť naokolo.
- SRD kombinované so SVHC – pri kombinácii SRD so škálovateľným rozšírením HEVC sa pri delení videa na priestorové oblasti dá efektívne škálovať kvalita pre jednotlivé oblasti. Príklad takéhoto škálovania je uvedený na **Obr. 42**.

Na realizáciu adaptácie na strane siete sa dá s výhodou použiť architektúra **SDN/NFV** sietí (***Software-Defined Networking / Network Function Virtualization***). V jej moduloch VNF (Virtualised Network Functions), ktoré môžu byť v pozícii **EC** (***Edge Computing***), t.j. poskytovať výpočtový výkon na hranici siete, sa dá efektívne budovať adaptivita na strane siete v sieťach 5 generácie.

<table>
<tr><td colspan="2">Príklad delenia videa na oblastí a ich verzie na strane serveru</td><td rowspan="2">Výber oblastí VR klienta na základe toho, kam sa pozerá pozorovateľ</td></tr>
<tr><td>Pri plnom rozlíšení</td><td>Pri polovičnom rozlíšení</td></tr>
<tr><td>  </td><td>  </td><td>  </td></tr>
</table>

Obr. 42 Príklad pre doručovanie VR obsahu - SRD kombinovaného so SVHC – výber oblastí pri zvolenom na základe toho, kam sa pozerá pozorovateľ [106]

11. 5G sieťové architektúry, služby a aplikácie

Výraz 5G sieť je označenie pre 5. generáciu mobilných sietí, ktoré predstavujú ďalší evolučný stupeň vo vývoji mobilných sietí. Požiadavky na 5G siete boli špecifikované Medzinárodnou telekomunikačnou úniou (ITU) v rámci štandardu IMT-2020 [107] a sú rozpracované v rámci organizácie (konzorcia) **3GPP** (The ***3rd Generation Partnership Project***) v jej vydaniach: Release 15 (5G fáza 1) [108] a Release 16 (5G fáza 2) [109].

5G siete budú schopné poskytovať najširšiu škálu služieb a aplikácií v histórii mobilnej a bezdrôtovej komunikácie pokrývajúcich potreby mobilného širokopásmového pripojenia (**eMBB**, ***enhanced Mobile Broadband***), masívnej komunikácie počítačového typu (**mMTC**, ***massive Machine-Type Communication***) a ultra-spoľahlivej komunikácie s nízkym oneskorením (**URLLC**, ***Ultra-Reliable and Low-Latency Communications***).

Odporúčania ITU [107], [110] definujú nasledovné požiadavky na 5G siete:

- 1000x väčší objem mobilných dát na pokrytie určitej oblasti (napr. 0,75 Tbit/s pre štadióny),
- 1000x väčší počet pripojených zariadení (max. hustota ≥ 1 miliónov terminálov/km^2),
- 100x vyššie prenosové rýchlosti (špičkovo ≥ 1 Gbit/s pre cloudové aplikácie v rámci kancelárií),
- koncové (end-to-end) oneskorenie menšie ako 1 ms,
- Prenosová rýchlosť garantovaná používateľovi ≥ 50 Mbit/s,
- Podpora IoT terminálov ≥ 1 bilión (10^{12}),
- Dostupnosť ≥ 99,999% (pre niektoré špecifické služby),
- Podpora mobility do rýchlosti ≥ 500 km/h pre pozemnú dopravu.

Podrobnejšie výkonnostné požiadavky pre scenáre s vysokou prenosovou rýchlosťou a intenzitou prevádzky, ako aj pre scenáre s nízkym oneskorením a vysokou spoľahlivosťou sú uvedené v [111].

Pre splnenie uvedených požiadaviek prinášajú 5G siete nové koncepty a vylepšenia v oblasti architektúry siete. Okrem podpory pre viaceré prístupové technológie prinášajú aj modulárnu a flexibilnú sieťovú architektúru. 5G siete budú umožňovať integráciu viacerých sietí patriacich do rôznych domén. Budú tiež umožňovať vytváranie tzv. sieťových vrstiev (angl. *network slices*) pokrývajúcich viacero domén a technológií, ktoré budú vytvárané pre špecifických nájomcov alebo služby. Jednotlivé logické sieťové vrstvy sa môžu rozprestierať cez rôzne technické domény (napr. prístupové, transportné a jadrové siete) ako aj administratívne domény (napr. rôznych operátorov mobilných sietí) a to vrátane roviny riadenia a orchestrácie.

Bezpečnosť 5G sietí je zabezpečená prostredníctvom bezpečnostnej architektúry, ktorá tvorí súčasť architektúry 5G siete a umožní splnenie požiadaviek aplikácií a služieb kritických z hľadiska bezpečnosti.

11.1. Architektúra 5G siete

Architektúra systému 5G je definovaná tak, aby podporovala dátovú konektivitu a služby umožňujúce pri nasadzovaní používať techniky virtualizácie sieťových funkcií (**NFV**, ***Network Function Virtualization***) a softvérovo definovaných sietí (**SDN**, ***Software Defined Networking***).

Pre architektúru 5G sietí je charakteristické:

- Oddelenie funkcií používateľskej roviny (**UP**, ***User Plane***) od funkcií riadiacej roviny (**CP**, ***Control Plane***).
- Modularizácia funkčného návrhu, ktorá umožňuje flexibilné a efektívne rozčlenenie siete na logické sieťové vrstvy a definuje procedúry (súbor interakcií medzi sieťovými funkciami) ako služby, čo umožňuje ich opätovné použitie.
- Priama komunikácia medzi sieťovými funkciami.
- Minimalizovanie závislosti medzi prístupovou sieťou a jadrovou sieťou. Architektúra 5G siete obsahuje konvergovanú jadrovú sieť a jednotné rozhranie medzi prístupovou sieťou a jadrovou sieťou, ktoré podporuje rôzne typy prístupu.
- Podpora súbežného prístupu k lokálnym aj centralizovaným službám. Pre lepšiu podporu služieb s nízkym oneskorením a prístupu do lokálnych dátových sietí môžu byť niektoré funkcie používateľskej roviny nasadené v blízkosti prístupovej siete.

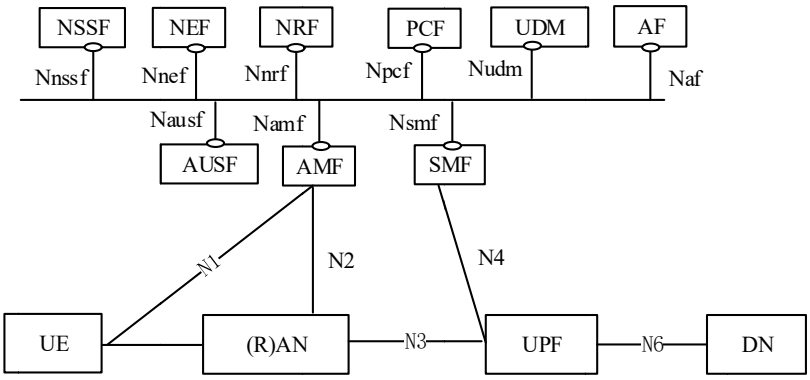
Architektúra 5G je definovaná ako architektúra založená na službách. Interakcia medzi sieťovými funkciami je reprezentovaná dvomi spôsobmi a to prostredníctvom:

- **referenčných bodov** (**Obr. 43**) - zobrazuje interakcie medzi sieťovými službami prostredníctvom referenčných bodov (napr. N4) definovaných medzi dvomi sieťovými funkciami (napr. UPF a SMF).
- **služieb** (**Obr. 44**) – prostredníctvom ktorých sieťové funkcie v riadiacej rovine (napr. AMF) umožňujú ostatným autorizovaným sieťovým funkciám prístup k ich službám.

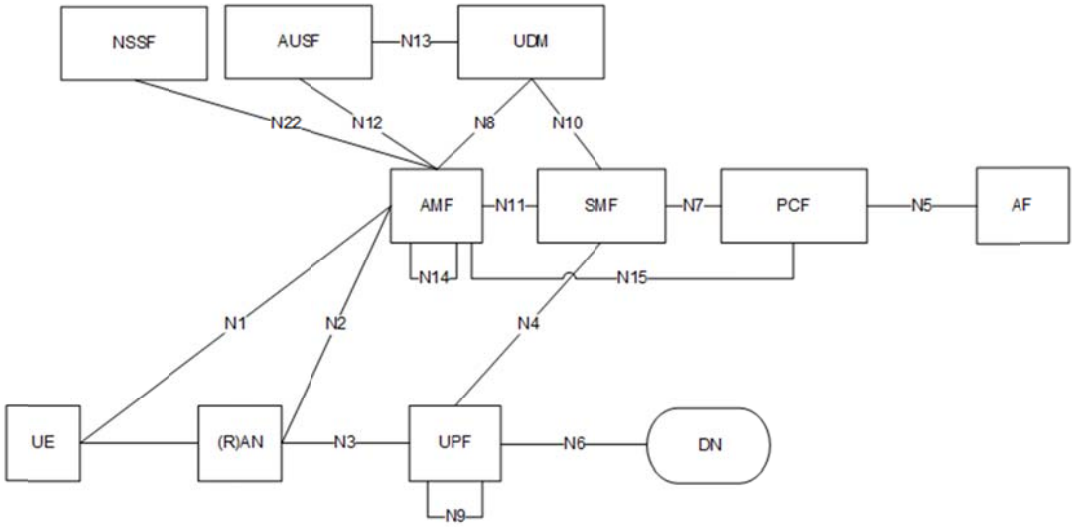
Sieťové funkcie v riadiacej rovine 5G siete používajú na vzájomnú komunikáciu iba rozhrania založené na službách.

Architektúra 5G siete obsahuje nasledovné sieťové funkcie:

- funkcie koncového (používateľského) zariadenia - **UE** (***User Equipment***), funkcie rádiovej prístupovej siete - **R(AN)** (***Radio (Access Network)***), funkcie používateľskej roviny - **UPF** (***User Plane Function***) a dátovej siete - **DN** (***Data Network***),
- funkcie manažmentu prístupu a mobility - **AMF** (***Access and Mobility Management Function***) a manažmentu relácií - **SMF** (***Session Management Function***),
- funkcia výberu sieťovej vrstvy - **NSSF** (***Network Slice Selection Function***), funkcia sieťového repozitáru - **NRF** (***Network Repository Function***), funkcia autentifikačného servera - **AUSF** (***Authentication Server Function***), funkcia unifikovaného manažmentu údajov - **UDM** (***Unified Data Management***), funkcia riadenia politík - **PCF** (***Policy Control Function***), aplikačné funkcie - **AF** (***Application Function***), funkcia uchovania neštrukturovaných údajov - **UDSF** (***Unstructured Data Storage Function***), funkcia jednotného skladu údajov - **UDR** (***Unified Data Repository***), funkcia zverejnenia v sieti - **NEF** (***Network Exposure Function***), funkcia registra identít 5G zariadení - **5G-EIR** (***5G-Equipment Identity Register***),



Obr. 43 Referenčná architektúra 5G siete s rozhraniami sieťovými službami [112]



Obr. 44 Ukážka architektúra 5G siete s referenčnými bodmi (rozhraniami) umožňujúcimi interakciu medzi sieťovými funkciami [112]

Sieťové funkcie môžu byť implementované ako prvok siete na pre tento účel vyhradenom hardvéri, ako inštancia softvéru spustená na vyhradenom hardvéri, alebo ako virtualizovaná funkcia implementovaná na vhodnej platforme, napr. na cloudovej infraštruktúre.

Podrobnejší popis jednotlivých sieťových funkcií 5G siete je možno nájsť v [112], [113], [114].

11.1.1. Network slicing

Network slicing je jedna z najvýznamnejších inovácií 5G sietí, ktorá umožňuje vytváranie špecializovaných vrstiev siete, ktoré majú funkčné architektúry prispôsobené príslušným telekomunikačným službám, ako napr. eMBB, URLLC, mMTC, **V2X** (***Vehicle-to-everything***) a pod.

Network slice (ďalej sieťová vrstva) je vo všeobecnosti špeciálne vytvorená logická sieť slúžiaca určenému obchodnému účelu alebo zákazníkovi, ktorá pozostáva zo všetkých požadovaných sieťových prostriedkov nakonfigurovaných pre daný účel. Je vytvorená, modifikovaná

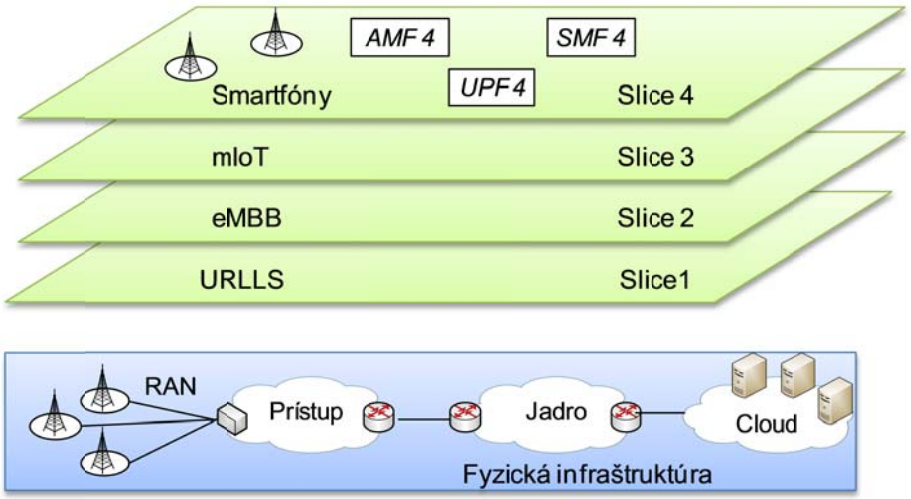
a odstránená prostredníctvom manažmentových funkcií. Pri vytváraní sieťovej vrstvy manažmentová rovina vytvorí skupinu sieťových zdrojov a prepojení medzi ich fyzickými, virtuálnymi a službovými funkciami a vytvorí inštancie všetkých sieťových a službových funkcií priradených do danej sieťovej vrstvy. Pri operáciách so sieťovou vrstvou riadiaca rovina preberá riadenie všetkých sieťových zdrojov, sieťových funkcií a službových funkcií priradených k danej vrstve. Podľa potreby ich konfiguruje alebo rekonfiguruje aby boli zabezpečené požadované služby. Priradenie prevádzky do príslušnej sieťovej vrstvy sa realizuje spravidla prostredníctvom vhodne nakonfigurovaného vstupného smerovača.

Vytváranie sieťových vrstiev môže byť motivované:

- **obchodne** – sieťové vrstvy sú vytvorené pre účely podpory rôznych typov služieb alebo obchodných prípadov,
- **technologicky** – sieťové vrstvy sú vytvorené zoskupením fyzických alebo virtuálnych zdrojov (sieťových, výpočtových, úložných), ktoré môžu pracovať ako podsieť alebo cloud.

Z obchodného hľadiska sieťová vrstva zlučuje všetky relevantné sieťové zdroje, sieťové funkcie a funkcie služby (fyzické alebo virtuálne) vo všetkých segmentoch siete (prístup, jadro a okraj), ktoré sú potrebné na splnenie konkrétneho obchodného prípadu alebo služby a to vrátane OSS a BSS.

Princíp sieťových vrstiev je znázornený na **Obr. 45**.



Obr. 45 Princíp sieťových vrstiev

Poznámka: Vzhľadom na zložitosť technológie network slicing a úroveň stavu technológie budú prvé reálne implementácie 5G využívať len 5G RAN v kombinácií s existujúcimi EPC (Evolved Packet Core) sieťami.

11.1.2. RAN (Radio Access Network)

Rádiová prístupová sieť **RAN** (***Radio Access Network***) je dôležitá časť 5G siete, ktorá zabezpečuje vysoké prístupové rýchlosti dosahované v 5G sieťach. Podobne ako ostatné časti

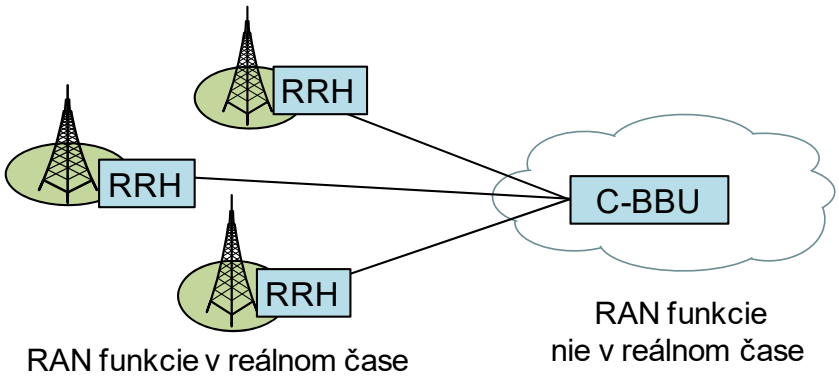
siete, aj 5G RAN prináša určité vylepšenia oproti predošlým verziám mobilných sietí. Okrem použitia iných frekvencií a kódových schém je to využitie cloudovej technológie.

5G RAN zabezpečuje tzv. RAN funkcie v reálnom čase a RAN funkcie nie v reálnom čase.

Funkcie RAN v reálnom čase zahŕňajú plánovanie prístupových sietí, adaptáciu prepojení, riadenie výkonu, koordináciu interferencie, retransmisiu, moduláciu a kódovanie. Tieto funkcie vyžadujú vysoké zaťaženie v reálnom čase a výpočtové zaťaženie. Ich nasadenie vyžaduje špeciálny hardvér s vysokým výkonom, ktorý je umiestnený v tesnej blízkosti poskytovania služieb.

Funkcie RAN nie v reálnom čase zahŕňajú odovzdávanie medzi bunkami, výber a opätovný výber buniek, šifrovanie na úrovni používateľa a spájanie viacerých spojení. Tieto funkcie vyžadujú minimálny výkon v reálnom čase, požiadavky na oneskorenie sú rádovo v desiatkach milisekúnd a sú vhodné pre centralizované nasadenie. Na rozdiel od predošlého prípadu je možné pri nasadení použiť univerzálne procesory.

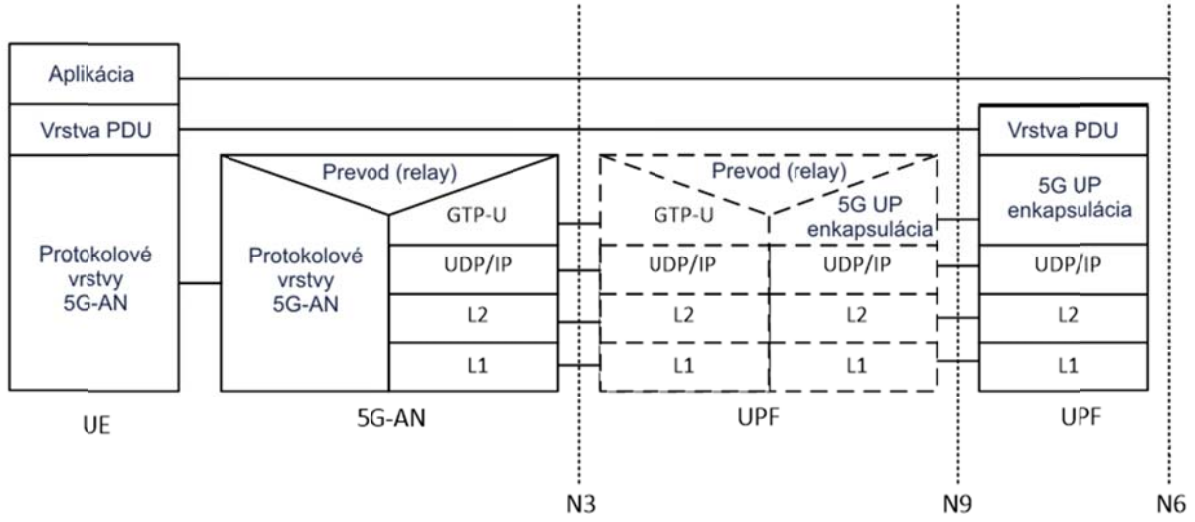
Ďalšou možnosťou je použitie architektúry Cloud RAN, ktorá umožňuje distribuovať implementovanie RAN funkcie v reálnom čase a centralizovať zdroje na vyžiadanie zabezpečujúce funkcie nie v reálnom čase (**Obr. 46**). V prípade Cloud RAN je tak možné využiť výhody plynúce z použitia univerzálnych procesorov pri nasadení C-BBU v prostredí cloudu.



Obr. 46 Architektúra Cloud RAN

11.1.3. Jadrová sieť

Transportná sieť pozostáva z SDN riadiacich jednotiek a nimi riadených SDN uzlov. SDN riadiace jednotky riadia vytváranie ciest, ktoré slúžia na smerovanie dát, pričom zohľadňujú topológiu siete a požiadavky jednotlivých služieb. Riadiaca rovina abstrahuje a analyzuje možnosti siete za účelom optimalizácie siete alebo otvorenia sieťových funkcií prostredníctvom API rozhrania. Siete implementujú politiky pomocou dynamických politík, polo-statických používateľov a statických sieťových dát uložených v zjednotenej databáze na strane jadrovej siete.



Obr. 47 Protokoly používateľskej roviny [112]

Obr. 47 znázorňuje súbor protokolov použitých v používateľskej rovine transportnej vrstvy súvisiacich s PDU (Protocol Data Unit) reláciami.

PDU vrstva korešponduje s PDU prenášanými v rámci PDU relácie medzi koncovým zariadením **UE** (***User Equipment***) a dátovou sieťou. Hodnota PDU Session Type IPv6 znamená, že sú prenášané v rámci relácie IPv6 pakety, hodnota Ethernet, že sú prenášané ethernetové rámce a pod.

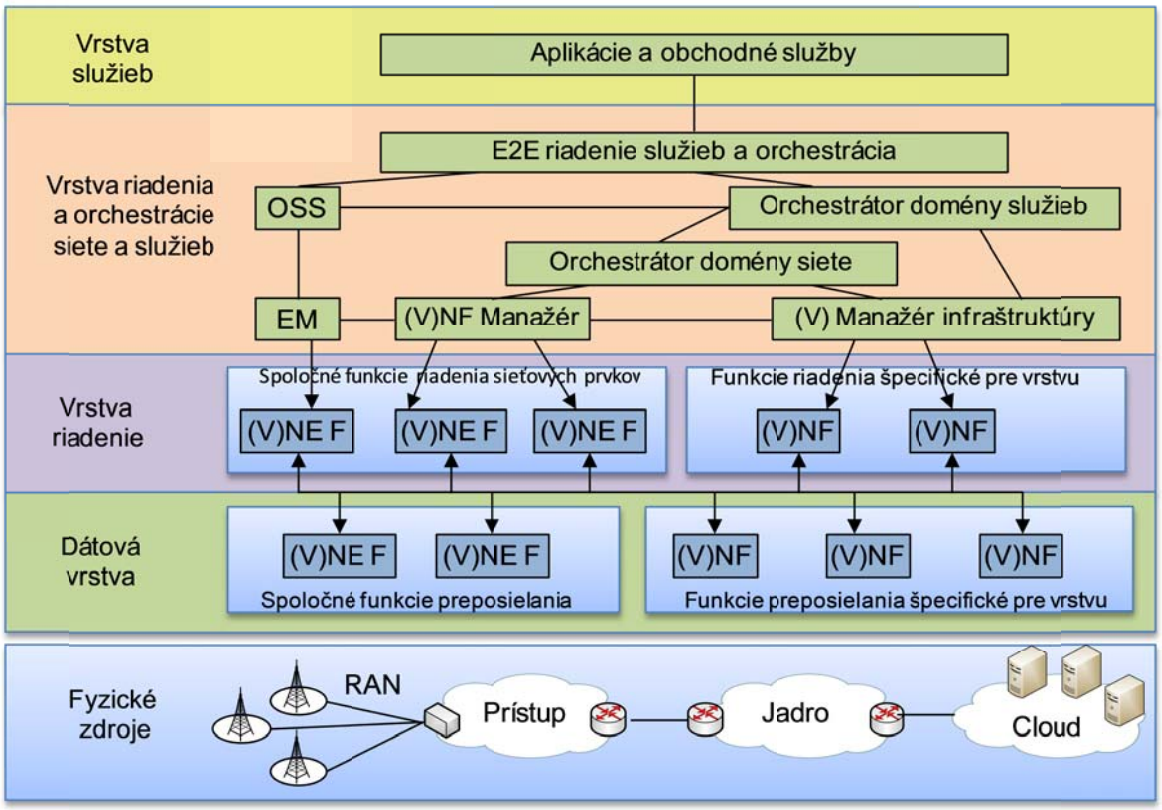
Protokol **GTP-U** (***GPRS Tunnelling Protocol for User plane***) [115] podporuje multiplexovanie viacerých PDU relácií formou tunelovania používateľských dát cez N3 rozhranie medzi 5G-AN uzlom a UPF na chrbticovej sieti. GTP enkapsuluje všetky PDU koncového používateľa.

5G Enkapulácia: Táto vrstva podporuje multiplexovanie prevádzky rôznych PDU relácií cez N9 rozhranie (t.j. medzi rôznymi UPF 5G jadrovej siete). Poskytuje enkapsuláciu na úrovni PDU relácie.

11.1.4. Manažment a orchestrácia

Najvyššia vrstva sieťovej architektúry zabezpečuje automatizované vytváranie a správu vrstiev siete a riadenie sieťových zdrojov. Riadiace roviny pre sieťové komponenty a programovateľné používateľské roviny umožňujú orchestráciu sieťových funkcií s cieľom zabezpečiť, že siete môžu, podľa rôznych požiadaviek na služby, zvoliť zodpovedajúce funkcie riadiacej roviny alebo používateľskej roviny.

Manažment a orchestrácia 5G sietí sú založené na rozšírenej ETSI/NFV **MANO** (***Management and Orchestration***) architektúre (**Obr. 48**) [116]. Pri riadení a orchestrácií sú brané do úvahy aj špeciálne aspekty, ako sú existencia viacerých vrstiev siete, multi-nájomnosť (multi-tenancy) či viacero domén alebo operátorov.



Obr. 48 Manažment a orchestrácie 5G siete

11.1.5. Bezpečnosť

Bezpečnostná koncepcia 5G je založená na použití troch prvkov: domén, vrstiev a bezpečnostných tried.

Doména je zoskupenie sieťových entít podľa fyzických alebo logických aspektov, ktoré sú relevantné pre 5G sieť [117]. Existujú tri rôzne typy domén:

- ***Infraštruktúrne domény*** – sú zamerané na relevantné aspekty fyzickej siete, t. j. obsahujú "hardvér" v sieti.
- ***Nájomné domény*** **-** sú to logické domény vykonávajúce sa v infraštruktúrnych doménach,
- ***Zlúčené domény*** - pozostávajú z kolekcie iných domén zoskupených podľa niektorých relevantných aspektov 5G, napr. vlastníctva. Jedným z dôležitých typov zlúčených domén sú domény vrstiev *(slice domains)*.

Vrstva *(Stratum)* je zoskupenie protokolov, údajov a funkcií súvisiacich s jedným aspektom služieb poskytovaných jednou alebo viacerými doménami. Podľa 5G PPP [118] sú to:

- Aplikačná vrstva – reprezentuje aplikačný proces poskytovaný koncovému používateľovi.
- Domáca vrstva - obsahuje protokoly a funkcie súvisiace s manipuláciou a ukladaním údajov o predplatnom a špecifických službách v domácej sieti.

- Obslužná vrstva - skladá sa z protokolov a funkcií zabezpečujúcich smerovanie dát generovaných používateľom alebo sieťou a to od zdroja až po miesto určenia.
- Transportná vrstva - podporuje prenos používateľských dát a sieťovej signalizácie iných vrstiev cez sieť.
- Prístupová vrstva - je podvrstvou transportnej vrstvy. Nachádza sa medzi okrajovým uzlom obsluhujúcej sieťovej domény a UE doménou.
- Manažmentová vrstva – zahŕňa štandardné aspekty riadenia siete (konfigurovanie, aktualizácie softvéru, spravovanie používateľských účtov, vytváranie/analyzovanie logov atď.) a tiež aspekty riadenia bezpečnosti (audity monitorovania bezpečnosti, správa kľúčov a certifikátov atď.).

Posledným prvkom podľa [118] sú bezpečnostné triedy (*Security Control Classes*). Medzi Security control classes patria autentifikácia, utajenie, integrita a pod..

11.2. 5G služby

5G siete sú navrhované pre veľký počet nových spôsobov použitia, ktoré boli opísané a analyzované organizáciami 3GPP a ITU. Väčšina týchto prípadov použitia sú však len variáciami malého počtu základných tried služieb ponúkaných 5G sieťami, ako:

- **Rozšírenie mobilného širokopásmového pripojenie (eMBB)** – ktoré bude podporovať gigabitovú šírku pásma pre 4K video, stereoskopické 360° video, virtuálnu realitu atď.
- **Masívna komunikácia počítačového typu (mMTC)** – ktorá bude schopná spojenia s miliardami senzorov a zariadení s hustotami do 200 tisíc zariadení na kilometer štvorcový, čo umožní vybudovanie inteligentných miest.
- **Ultra-spoľahlivá komunikáciá s nízkym oneskorením (uRLLC)** – ktorá umožní okamžitú spätnú väzbu s vysokou spoľahlivosťou a umožní vykonávať diaľkové operácie v reálnom čase, alebo tiež diaľkovú kontrolu robotov vo výrobe a autonómne jazdenie áut [118].

Staršie služby

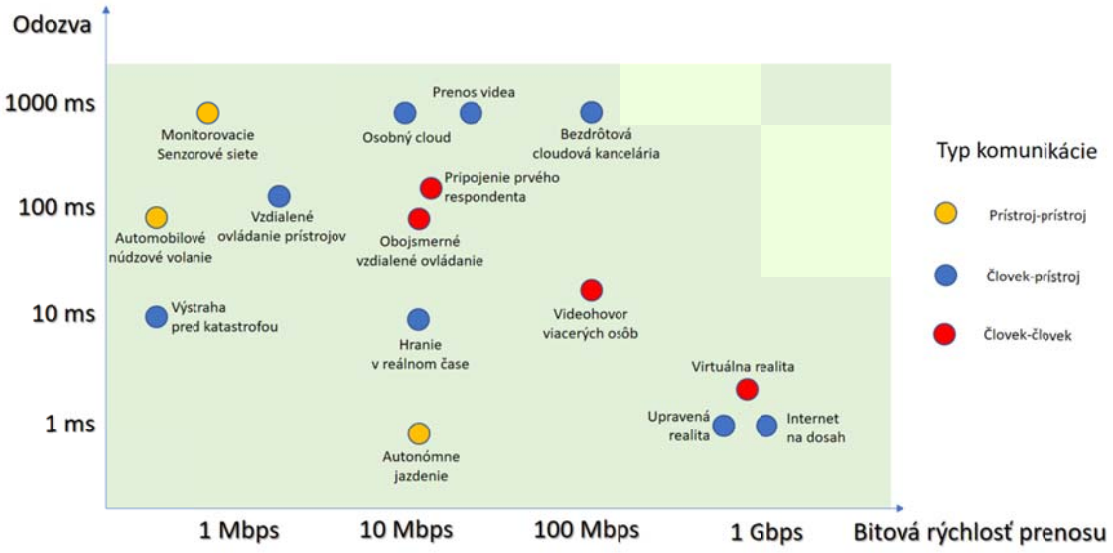
5G siete budú taktiež podporovať staršie služby, teda služby ponúkané predošlými generáciami mobilných sietí. Niektorými z nich sú:

- **IMS (IP multimediálny podsystém)** – IP multimediálny podsystém obsahuje všetky základné sieťové prvky pre doručovanie multimédií. Služby podsystému využívajú protokoly **IETF** (***Internet Engineering Task Force***) tam kde je to možné, čím využívajú konektivitu sietí prístupných cez IP. IP multimediálny podsystém umožnuje operátorom ponúkať multimediálne služby, napr. hlasové služby, video, správy, dáta a webové technológie [119].
- **SMS** – Služba krátkych správ bude realizovaná ako SMS cez NAS (dátové uložisko na sieti) [113].
- **Systém verejnej výstrahy** – Služby mobilného vysielania môžu byť využité na prenášanie správ súvisiacich s verejnou výstrahou. Doručovanie výstražných správ je podobné ako pri službách mobilného vysielania [120].
- **Lokalizačné služby** – Lokalizačné služby identifikujú a hlásia aktuálnu informáciu o lokalizácii používateľa použitím viacerých metód určovania pozície (napr. GPS,

GLONASS...). Informácia o lokalizácii pozostáva z geografickej polohy (geografické súradnice) a rýchlosti (veľkosť rýchlosti a smer rýchlosti zariadenia) [121].

11.3.5G aplikácie

Predošlé generácie mobilných sietí zvyšovali bitovú rýchlosť prenosu, znižovali odozvu a riešili masívnu šírku pásma. Technológia 5G sietí bude zameraná aj na vysokú prenosovú rýchlosť a zníženú odozvu, ale taktiež na zariadenia, ktoré potrebujú malú prenosovú rýchlosť a senzory pre **IoT** (skratka z anglického ***Internet of Things*** – Internet vecí). Na **Obr. 49** sú zhrnuté hlavné aplikácie, ktoré budú podporované v prostredí 5G sietí s ich požadovanou bitovou rýchlosťou prenosu a odozvou.



Obr. 49 Aplikácie, ktoré budú podporované 5G sieťami [122]

Širokopásmový zážitok

Vďaka rozšírenej šírke mobilného pásma, 5G siete budú poskytovať lepšiu konektivitu pre zákazníkov vnútri aj vonku s vyššími rýchlosťami prenosu dát a nižšou odozvou aj v preplnených oblastiach, napríklad pri rôznych udalostiach, verejnej doprave a na futbalových štadiónoch.

Médiá kdekoľvek

Masívne zvýšenie požiadaviek na šírku mobilného pásma v posledných rokoch je spôsobené dopytom po médiách. 5G siete poskytnú možnosti pre živý prenos televízie, prenos videa na požiadanie, hranie hier v reálnom čase, alebo nakupovanie vo virtualnej alebo upravenej realite. Médiá budú poskytované v 8K kvalite s vysokým dynamickým rozsahom a vysokým počtom snímkov za sekundu a stereoskopické 360° video s hmatovou odozvou.

- **Online hry vo VR** – virtuálna realita je scenár generovaný počítačom, ktorý simuluje realistické zážitky, pričom je možná interakcia s objektami a ďalšími hráčmi v reálnom čase. Online virtuálna realita bude potrebovať spoľahlivé pripojenie s nízkou odozvou

pod 20 milisekúnd, aby presvedčila používateľovu myseľ, že sa nachádza na inom mieste čo tiež zamedzí nevoľnostiam. Ďalšími kľúčovými súčasťami AR (upravenej reality) a VR zážitku sú rozlíšenie displeja a rýchlosť dátového prenosu videa. Pre 360° VR zážitok s nízkym rozlíšením je potrebná prenosová rýchlosť minimálne 25 Mbit/s. Pre VR zážitok, ktorý je kvalitou porovnateľný s HDTV je potrebná prenosová rýchlosť 80 až 100 Mbit/s. Najkvalitnejší VR zážitok je možné dosiahnuť pri 8K*8K rozlíšení s frekvenciou snímkov 120 snímkov za sekundu, čo potrebuje prenosovú rýchlosť do 1 Gbit/s [123].

- **3D 360° video –** 360° video zaznamenáva scénu vo všetkých smeroch. Zatiaľ čo štandardné monoskopické video je premietané na plochu gule, stereoskopické (3D) video pridá ďalšiu úroveň ponorenia sa do deja – hĺbku medzi pozadím a stredobodom pozornosti. Typické formátovanie 360° videa je monoskopický alebo stereoskopický tok dát s použitím ekvidištančnej valcovej projekcie zošitej z viacerých kamier zaznamenávajúcich scénu. Pre porovnanie, 360° video potrebuje typicky 3 až 5 krát vyššie prenosové rýchlosti ako bežné video s jednym pohľadom, zatiaľ čo 3D video potrebuje zvyčajne o 30 až 60% väčšiu prenosovú rýchlosť ako monoskopické video. [124].

Internet vecí (IoT)

Internet vecí je sieť fyzických zariadení, napr. monitorovanie teploty, domáce spotrebiče, nositeľné technológie, vozidlá a atď. Tieto prístroje majú vstavanú elektroniku, senzory a softvér na kontrolu a tiež majú konektivitu, ktorá im umožňuje výmenu dát. 5G siete budú podporovať hustotu pripájajúcich sa zariadení do 200 000 na kilometer štvorcový. Internet vecí umožní pristrojom aby boli na diaľku objaviteľné a bolo ich možné diaľkovo ovládať cez infraštruktúru siete [125]. Toto zahŕňa technológie ako napríklad:

- **Inteligentné vozidlá** – V posledných rokoch sa prikladá veľký dôraz na umožnenie autonómnej jazdy. Vývoj prepojených áut a ďalších inteligentných vozidiel je zámerom firiem ako Uber, Google a Volvo. 5G poskytne sieťovú časť tejto technológie. Očakáva sa, že do roku 2020 bude jazdiť približne 10 milónov samojazdiacich áut a ďalších 250 inteligentných vozidiel (áut pripojených do 5G siete), ktoré budú s nimi zdieľať cestu. Inteligentné vozidlá budú pracovať spolu s navigáciou a vysielacími satelitmi. Ako súčasť vývoja inteligentných miest budú inteligentné vozidlá komunikovať so smartfónmi a vysielačmi umiestnenými popri ceste (**RSU, *roadside unit***), čo z nich robí dôležitú súčasť Internetu vecí. Takéto prepojenie umožní autám aby upozornili vodičov v prípade reťazovej kolízie iba niekoľko áut pred nimi, alebo ak sa niekto chystá prejsť na červenú [126]. Taktiež budú posielané informácie v reálnom čase o vozidlách, ktoré brzdia vpredu a o vozidlách v slepých bodoch. Informácie o ostatných autách a prostredí okolo nich budú posielané anonymne ako komunikácia vozidlo-vozidlo (V2V) a vozidlo-infraštruktúra (V2I). Množstvo moderných áut má nástroje používajúce radarovú alebo ultrazvukovú detekciu prekážok a vozidiel, ale dosah týchto prístrojov je limitovaný iba niekoľko desiatok metrov okolo vozidla a tiež nevidí cez okolité prekážky. Výstrahy pre vodičov cez sieť budú rýchle a intuitívne, budú používať svetlá a zvuky aby varovali vodičov okolitých áut na potencíalne nebezpečenstvo. Vysielané informácie z ostatných vozidiel budú spracované palubným počítačom vozidla a zakaždým bude prepočítaná pravdepodobnosť možnej kolízie. Táto technológia by mohla predísť mnohým nehodám a úmrtiam, a taktiež znížiť čas strávený na cestách [127].

- **Inteligentné mestá** – je potrebné aby mesto prevzalo zodpovednosť za svoju digitálnu infraštruktúru, tak ako predtým prevzalo zodpovednosť za analógovú infraštruktúru a jej služby, a zabezpečilo aby tieto služby spolu efektívne fungovali. Toto umožní mestu aby malo pod kontrolou určité odvetvia a ich vývoj. Inteligentné mestá budú mať vysoký dopyt na objem prenesených dát vo viacerých sektoroch, ako napríklad verejná doprava, pohotovostné služby a systém vodného hospodárstva. Integrácia týchto sektorov s informačným systémom povedie k lepšiemu plánovaniu a prevádzke, čo bude mať za následok automatizované reakcie na zmenené podmienky. Aplikácie inteligentných miest potrebujú byť integrované so senzormi zapojenými do sietí. Je potrebné, aby existoval jednotný proces pre pripájanie týchto senzorov do siete a sieť schopná podporovať rôznorodé požiadavky na výkon a funkcionalitu [128].
- **Inteligentné domácnosti** – Inteligentná domácnosť je štruktúra používajúca technológie, ktoré asistujú alebo automatizujú každodenné aktivity a umožnujú vzdialenú kontrolu inteligentných zariadení, ktoré sú súčasťou domácnosti. Vo všeobecnosti je možné pristupovať k týmto zariadeniam z jedného centrálneho zariadenia, čo môže byť napríklad smartfón, tablet alebo laptop, ktorý v dnešnej dobe vlastní skoro každý. S týmito zariadeniami je možné kontrolovať bezpečnostný prístup do domu, nastavenia termostatu, alebo zatiahnuť závesy. Inteligentná domácnosť a jej zariadenia sú prepojené cez Internet a vedia si vymieňať informácie. Štruktúra inteligentnej domácnosti môže byť navrhnutá tak, aby efektívne menila spotrebu energie a ušetrila množstvo času a peniaze [129].
- **Inteligentná pošta** – Inteligentná pošta implementovaná do Internetu vecí pomôže ušetriť čas strávený vyberaním prázdnej poštovej schránky. Nové poštové schránky budú používať senzory, ktoré budú pripojené do siete NB-IoT (úzkopásmového Internetu vecí) a budú poskytovať informáciu o stave ich naplnenia. Využitím tejto informácie v reálnom čase budú schránky vyprázdňované podľa potreby, čo by sa mohlo ukázať prospešné počas sezóny. Senzory budú posielať dáta priamo spravodajskému systému, čo umožní centrálne monitorovanie pošty v reálnom čase. Tieto informácie budú ďalej zaslané poštárom a vodičom pre plnenie ich pracovnej náplne [130].
- **Inteligentné nositeľné technológie** – Nositeľné prístroje ako športové náramky, alebo inteligentné hodinky sa stávajú súčasťou každodenného života. Tieto prístroje zahŕňajú elektroniku a softvér spolu so senzormi a bezdrôtovým pripojením. Využiteľnosť týchto prístrojov stúpa vo viacerých odvetviach, akými sú domácnosť, zdravotníctvo a výstavba [122]. Dnes sú tieto prístroje využité najmä pre zábavu a monitorovanie fyzickej aktivity, ale ich využiteľnosť sa rozširuje aj do zdravotníctva (napríklad nositeľné **EKG** (***elektrokardiogram***), **EEG** (**elektroencefalogram**), tlak krvi, pulz, respiráciu, spánok a monitorovanie pohybu. Inteligentné nositeľné technológie budú klinicky vhodné pre dlhodobé monitorovanie fyziologických a patologických procesov v reálnom čase, čo môže pomôcť lepšie pochopiť vývoj chronických chorôb akými sú kardiovaskulárne ochorenia a poruchy spánku. Výskum v oblasti nositeľných technológií je založený na klinických veľkých dátach a umelej inteligencii pre vybudovanie robustnejších techník na identifikáciu chorôb [131].
- **Kritické ovládanie vzdialených zariadení** – Jedným z hlavných cieľov a vylepšení 5G sietí bude poskytovanie lepšieho pripojenia pre ťažké stroje, inteligentné energetické siete a vzdialené chirurgie, čo bude užitočné pre výrobcov, baníkov a zdravotníkov. Kritické ovládanie zahŕňa najmä komunikáciu prístroj-prístroj, pri ktorej je nevyhnutná nízka odozva a vysoká spoľahlivosť siete. Toto obsahuje komunikáciu medzi robotmi

v továrňach a medzi robotmi v teréne (napríklad zbieranie jabĺk [132]), a taktiež komunikáciu medzi dronmi [133]. Ultra-spoľahlivá komunikácia s nízkou odozvou (uRLLC) bude rozhodujúca pri napríklad vzdialenej chirurgii [134].

12. Skratky

3GPP	3rd Generation Partnership Project
5G-EIR	5G-Equipment Identity Register
AAC	Advanced Audio Coding
AF	Application Function
AMF	Access and Mobility Management Function
AMR WB	AMR Wide Band
AMR	Adaptive Multi Rate
API	Application Programming Interface
ARPA	Advanced Research Projects Agency
AUSF	Authentication Server Function
AV/VR	Augmented and Virtual Reality
B2B	business-to-business
B2C	business-to-consumer
B2G	business-to-government
BGP	Border Gateway Protocol
BSS	Business Support Systems
C2B	consumer-to-business
C2C	consumer-to-consumer
C2G	citizen-to-government
CDN	Content Delivery Network
CLI	Command Line Interface
CP	Control Plane
CRM	Customer Relationship Management
CS	Companion screens
DASH	Dynamic Adaptive Streaming over HTTP
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DIA	Digital Item Adaptation
DN	Data Network
DNS	Domain Name System
DoD	Department of Defense
DVB-S	Digital Video Broadcasting - Satellite
DVB-T	Digital Video Broadcasting - Terrestrial
DWDM	Dense Wavelength Division Multiplexing
eBGP	Exterior Border Gateway Protocol
EC	Edge Computing
EGP	Exterior Gateway Protocol
eMBB	enhanced Mobile Broadband
EMS	Element Management System
EPC	Evolved Packet Core
EPG	Electronic programme guide
ETSI	European Telecommunications Standards Institute
FN	Future Network
FOV	Field Of View

FTP	File Transfer Protocol
FTTx	Fiber to the “x”
G2B	government-to-business
G2C	government-to-citizen
G2E	government-to-employee
G2G	government-to-government
GTP-U	GPRS Tunnelling Protocol for User plane
GUI	Graphical User Interface
HbbTV	Hybrid Broadcast Broadband Television
HDTV	High Definition television Systems
HEIF	High Efficiency Image File
HEVC	High Efficiency Video Coding
HTML	Hypertext Markup Language
HTML5	Hypertext Markup Language version 5
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IAD	Integrated Access Device
iBGP	Interior Border Gateway Protocol
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
IDS	Intrusion detection system
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IKT	Informačné a komunikačné technológie
IMAP	Internet Message Access Protocol
IMS	IP multimedia subsystem
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion prevention system
IPsec	Internet Protocol Security
IPTV	Internet Protocol Television
IPv4	Internet Protocol version 4
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System to Intermediate System
ISO	International Organization for Standardization
JPEG	Joint Photographic Experts Group
LAN	Local Area Network
LMS	Learning Management System
MAC	Medium Access Control
MANO	Management and Orchestration
MEC	Mobile edge computing
MIB	Management Information Base
MITM	man in the middle
MME	Mobility Management Entity
MMI	Multi-Modal Interface
mMTC	massive Machine Type Communications

MOS	mean opinion score
MP3	MPEG (Motion Picture Experts Group) Layer-3
MPD	Media Presentation Descriptor
MPLS	Multiprotocol Label Switching
MSP	Malé a stredné podniky
NAS	Network Attached Storage
NAT	Network Address Translation
NEF	Network Exposure Function
NETCONF	Network Configuration Protocol
NFV ISG	Network Functions Virtualization Industry Specification Group
NFV	Network Functions Virtualization
NFVI	NFV Infrastructure
NGN	Next Generation Network
NITS	National Institute of Standards and Technology
NRF	Network Repository Function
NSSF	Network Slice Selection Function
OF	OpenFlow
OS	Operating System
OSPF	Open Shortest Path First
OSS	Operational Support Systems
OTH	Optical Transport Hierarchy
PaaS	Platform as a Service
PCF	Policy Control Function
PDU	Protocol Data Unit
PEAQ	Perceptual Evaluation of Audio Quality
PEVQ	Perceptual Evaluation of Video Quality
PGW	Packet Data Network Gateway
POP	Post Office Protocol
POPs	Points of Presence
PSDN	Packet-switched Data Network
PSTN	Public Switched Telephone Network
PVR	Personal video recorder
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
RIP	Routing Information Protocol
RIR	Regional Internet Registry
RM OSI	Open Systems Interconnection Reference Model
RSU	Roadside unit
RSVP	Resource Reservation Protocol
RTCP	RTP Control Protocol
RTCWEB	Real-Time Communication in Web-browsers
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
SaaS	Software as a Service
SCTP	Stream Control Transmission Protocol
SDN	Software Defined Networking

SDN/NFV	Software-Defined Networking / Network Function Virtualization
SDU	Service Data Unit
SGW	Serving Gateway
SHVC	Scalable High Efficiency Video Coding
SIP	Session Initiation Protocol
SLS	Scalable Lossless Coding
SMB	Small and Medium Business
SME	Small and Medium Enterprise
SMF	Session Management Function
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNR	Signal to Noise Ratio
SOAP	Simple Object Access Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
SVC	Scalable Video Coding
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UDM	Unified Data Management
UDP	User Datagram Protocol
UDR	Unified Data Repository
UDSF	Unstructured Data Storage Function
UE	User Equipment
UP	User Plane
UPF	User Plane Function
URL	Uniform Resource Locator
URLLC	Ultra-Reliable and Low-Latency Communications
V2X	Vehicle-to-everything
VIM	Virtualized Infrastructure Manager
VNF	Virtualized Network Functions
VoD	Video on Demand
VoIP	Voice over IP
VQM	Video Quality Metric
W3C	World Wide Web Consortium
WebRTC	Web Real-Time Communications
WWW	World Wide Web
xDSL	"x" Digital Subscriber Line
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

13. Literatúra

[1] 3GPP TS 29.163; V6.7.0 „Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched CS) networks“ (2005-06)

[2] Mikóczy, E., Podhradský, P.: Evolution of IPTV Architecture and Services towards NGN, in Recent Advantages in Multimedia Signal processing and Communications, Springer-Verlag, 2009, pp. 315-339

[3] Dúha, J., Galajda, P., Kotuliak, I., Levický, D., Marchevský, S., Mikóczy, E., Podhradský, P. at al.: Multimedia ICT technologies network platforms and multimedia services, Vydal: STU Bratislava, 2005, ISBN 80-227-2310-X

[4] Ferkl, L., Šmejkal, L., Sládek, O., Podhradský, P., Dúha, J.: Teleinformatics in Industrial Automation, LdV ELefANTC, Educational publication, Vydal: AGROGENOFOND Nitra, 2007, ISBN 978-80-89240-14-2

[5] ITU-T Recommendation X.200 (11/93) [ISO/IEC 7498-1:1994], Open Systems Interconnection - Basic Reference Model.

[6] Postel, J.: RFC 791 - Internet Protocol, IETF, September 1981.

[7] Deering, S., Hinden, R.: RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification, IETF, December 1998.

[8] Postel, J.: RFC 792 - Internet Control Message Protocol, IETF, September 1981.

[9] Conta, A., Deering, S., Gupta, M.: RFC 4443 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, IETF, March 2006.

[10] Deering, S., E.: RFC 1112 - Host extensions for IP multicasting, IETF, August 1989.

[11] Postel, J.: RFC 793 - Transmission Control Protocol, IETF, September 1981.

[12] Postel, J.: RFC 768 - User Datagram Protocol, IETF, August 1980.

[13] Stewart, R., Ed.: RFC 4960 - Stream Control Transmission Protocol, IETF, September 2007.

[14] Braden, R., Ed., Zhang, L., Berson, S., Herzog, S., Jamin. S.: RFC 2205 - Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification, IETF, September 1997.

[15] Droms, R.: RFC2131 - Dynamic Host Configuration Protocol, IETF, March 1997.

[16] Mockapetris, P.: RFC 1034 - Domain names - concepts and facilities, IETF, 1987.

[17] Dierks, T., Rescorla, E.: RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2, IETF, August 2008.

[18] Freier, A., Karlton, P., Kocher, P.: RFC 6101 - The Secure Sockets Layer (SSL) Protocol Version 3.0, IETF, August 2011.

[19] Postel, J., Reynolds. J.: RFC 854 - Telnet Protocol Specification, IETF, May 1983.

[20] Postel, J., Reynolds. J.: RFC 959 - File Transfer Protocol, IETF, October 1985.

[21] Ford-Hutchinson, P.: RFC4217 - Securing FTP with TLS, IETF, October 2005.

[22] Fielding. R., T., Gettys, J., Mogul, J., C., Nielsen, H., F., Masinter, L., Leach, P., J., Berners-Lee, T.: RFC2616 - Hypertext Transfer Protocol -- HTTP/1.1, IETF, June 1999.

[23] Berners-Lee, T., Fielding, R., T., Masinter, L.: RFC3986 - Uniform Resource Identifier (URI): Generic Syntax, IETF, January 2005.

[24] Myers, J., G., Rose, M., T.: RFC 1939 - Post Office Protocol - Version 3, IETF, May 1996.

[25] Crispin, M.: RFC 3501 - Internet Message Access Protocol - Version 4rev1, IETF, March 2003.

[26] Klensin, J.: RFC 5321 - Simple Mail Transfer Protocol, IETF, October 2008.

[27] Saint-Andre, P.: RFC 6120 - Extensible Messaging and Presence Protocol (XMPP): Core, IETF, March 2011.

[28] Extensible Markup Language (XML) 1.0 (Fifth Edition). W3C Recommendation, November 2008.

[29] SOAP Version 1.2 Part 1: Messaging Framework (Second Edition). W3C Recommendation, April 2007.

[30] Rosenberg, J., Schulzrinne, H. et al.: RFC 3261 - SIP: Session Initiation Protocol, IETF, June 2002.

[31] Hedrick, C.: RFC 1058 - Routing Information Protocol, IETF, June 1988.

[32] Moy, J.: RFC 2328 - OSPF Version 2, IETF, April 1998.

[33] Coltun, R., Ferguson, D., Moy, J., Lindem, A.: RFC 5340 - OSPF for IPv6, IETF, July 2008.

[34] ISO/IEC 10589:2002 Information technology -- Telecommunications and information exchange between systems -- Intermediate System to Intermediate System intra-domain routing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473). Second edition. ISO standard. November 2002, p.201.

[35] Rekhter, Y., Li, T., Hares, S., A.: RFC 4271 - Border Gateway Protocol 4 (BGP-4), IETF, January 2006.

[36] Schulzrinne, H., Casner, S., Frederick, R., Jacobson, V.: RFC 3550 - RTP: A Transport Protocol for Real-Time Applications, IETF, July 2003.

[37] Huitema, C.: RFC 3605 - Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP), IETF, October 2003.

[38] Schulzrinne, H., Rao, A., Lanphier, R.: RFC 2326 - Real Time Streaming Protocol (RTSP), IETF, April 1998.

[39] Case, J., Fedor, M., Schoffstall, M., Davin, J.: RFC 1067 - Simple Network Management Protocol, IETF, August 1988.

[40] McCloghrie, K., Rose, M., T.: RFC 1213 - Management Information Base for Network Management of TCP/IP-based internets: MIB-II, IETF, March 1991.

[41] Case, J., D., McCloghrie, K., Rose, M., T., Waldbusser, S.: RFC 1901 - Introduction to Community-based SNMPv2, IETF, January 1996.

[42] Harrington, D., Presuhn, R., Wijnen, B.: RFC 3411 - An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, IETF, December 2002.

[43] Enns, R., Bjorklund, M., Schoenwaelder, J., Bierman, A.: RFC 6241 - Network Configuration Protocol (NETCONF), IETF, June 2011.

[44] EdgeCast Eyes CDN Federation, http://www.lightreading.com/document.asp?doc_id=216113

[45] Level 3 Communications expands CDN capacity in Asia, CBR Networking, 2008, http://networking.cbronline.com/news/level_3_communications_expands_cdn_capacity_in_asia_311008

[46] Draft-previdi-cdni-footprint-advertisement, IETF/CDNI WG,2012 http://www.potaroo.net/ietf/idref/draft-previdi-cdni-footprint-advertisement/

[47] MediaCloud Connect for Telcos, ISPs and MSOs, http://www.mediamelon.com/isp-mediacloud.html

[48] Insight for Federated CDNs, http://www.skytide.com/products/insight-federated-cdns

[49] U.S. National Institute of Standards and Technology (NIST) The NIST Definition of Cloud Computing. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Sept. 2011. http://www.nist.gov/itl/cloud

[50] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia "Above the Clouds: A Berkeley View of Cloud Computing" University of California at Berkeley. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS

[51] Cary Landis, Dan Blacharski Cloud Computing Made Easy: An Easy to Understand Reference About Cloud Computing. Virtual Global Inc, 2013, ISBN 978-1482779424

[52] Douglas F. Parkhill The Challenge of the Computer Utility. Addison-Wesley Publishing Company, (1966), ASIN: B000O121OS, ISBN : 0240507177

[53] Antonio Regalado, Who coined "Cloud Computing"? MIT Technology Review, USA, Oct. 2011

[54] M. N.O. Sadiku, S. M. Musa, O.D. Momoh "Cloud computing: Opportunities and challenges" IEEE Potentials 02/2014; 33(1):34-36

[55] Jinesh Varia Architecting for the Cloud: Best Practices, January 2010

[56] Peter Mell, Tim Grance "Effectively and Securely Using the Cloud Computing Paradigm"

[57] Eugene Gorelik Cloud Computing Models, January 2013

[58] The cloud tutorial http://thecloudtutorial.com

[59] D. Catteddu and G. Hogben, "Cloud Computing: Benefits, Risks and Recommendations for Information Security," ENISA, 2009;

www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport.

[60] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," http://www.cloudsecurityalliance.org/csaguide.pdf.

[61] OpenFlow Switch Specification. Version 1.5.1. Open Networking Foundation. March 26, 2015. p. 283

[62] Network Functions Virtualisation - Introductory White Paper. SDN and OpenFlow World Congress, Darmstadt-Germany, October 22-24, 2012. p.16. https://portal.etsi.org/nfv/nfv_white_paper.pdf

[63] ETSI GS NFV-INF 003 V1.1.1 (2014-12), Network Functions Virtualisation (NFV); Infrastructure; Compute Domain. ETSI, December 2014

[64] ETSI GS NFV-INF 004 V1.1.1 (2015-01), Network Functions Virtualisation (NFV); Infrastructure; Hypervisor Domain. ETSI, January 2015

[65] ETSI GS NFV-INF 001 V1.1.1 (2015-01), Network Functions Virtualisation (NFV); Infrastructure Overview. ETSI, January 2015

[66] ETSI GR NFV 001 V1.2.1 (2017-05), Network Functions Virtualisation (NFV); Use Cases. ETSI, May 2017

[67] ETSI GS NFV-MAN 001 V1.1.1 (2014-12), Network Functions Virtualisation (NFV); Management and Orchestration. ETSI, December 2014

[68] Guo, P. A Survey of Software as a Service Delivery Paradigm. TKK T-110.5190 Seminar on Internetworking, 2009

[69] Kaysen, M. Understand the "SVOD", "TVOD" and "AVOD" terms and business models of streaming services like Netflix. 2015. https://www.linkedin.com/pulse/understand-svod-tvod-avod-terms-business-models-streaming-mads-kaysen

[70] ITU. ZDF - Hybrid Broadcast Broadband Television (HbbTV). Document WP 6B/[ZDF], 2012

[71] HbbTV Forum Nederland. Overview of Interactive Television services according to the HbbTV standard in Europe. 2014. http://hbbtv.nu/wp-content/uploads/2014/05/HbbTV_in_Europe_v5b_English.pdf

[72] Chen, J., Yuan, L., Mingins, C. Extending the Definition of E-Services and Its Implications to E-Services Development. International Joint Conference on Service Sciences, 2012, pp. 211-216

[73] Mehdi K.-P. Encyclopedia of E-Commerce, E-Government, and Mobile Commerce. Idea Group Inc., 2006. p. 1260. ISBN 1-59140-799-0

[74] Tarmo, K. and Ain, A. The Development of eServices in an Enlarged EU: eGovernment and eHealth in Estonia. EC JRC Technical Report, 2008. ISSN 1018-5593

[75] R. H. Weber, (2010). "Internet of Things - New Security and Privacy Challenges". Computer Law & Security Review 26: 23-30.

[76] 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

[77] ITU-T Recommendation Y.1910 (09/2008), IPTV functional architecture, ITU-T, 2008

[78] Mikóczy, E. Advanced Multimedia Architecture for Next Generation of Internet Protocol Television Systems. Dissertation theses, FEI STU Bratislava, 2010

[79] W3C. WebRTC 1.0: Real-time Communication between Browsers. W3C Editor's Draft 22 December 2015. http://w3c.github.io/webrtc-pc/

[80] WebRTC homepage. https://webrtc.org/

[81] U. H. Rao, U. Nayak, The InfoSec Handbook – An Introduction to Information Security, Apress Media, New York, 2014, ISBN 978-1-4302-6382-1

[82] H. Moghaddasi, S. Sajjadi, M. Kamkarhaghighi, Reasons in Support of Data Security and Data Security Management as Two Independent Concepts: A New Model, The Open Medical Informatics J., Vol. 10, 2016, pp 4-10

[83] ITU Recommendation X.800 – Data communication networks: Open systems interconnection (OSI) Security, structure and applications – Security architecture for open systems interconnection for CCITT applications, Geneva, 1991

[84] W. Stallings, Cryptography and network security – Principles and practice, 5th ed., Pearson Education, New York, 2011

[85] A. Rufi, Network Security 1 and 2 Companion Guide (Cisco Networking Academy), Cisco Press, 2006, ISBN: 978-1587131622

[86] M. Soriano, Information and Network Security, Czech Technical University in Prague, Techpedia project study material, 2017, ISBN 978-80-01-05297-6

[87] JPEG, ITU odporúčanie T.81, 09/92

[88] Ghanbari, M., Standard Codecs: Image Compression to Advanced Video Coding, Institution of Electrical Engineers, 2003, 407 pages, ISBN:0852967101

[89] JPEG 2000 štandard, ISO/IEC 15444-1, 15444-2

[90] MPEG-2, ISO/IEC 13818 štandardy, časti, ISO/IEC 13818-1 až ISO/IEC 13818-11

[91] MPEG-4 AVC štandard, ISO/IEC 14496–10, ITU-T H.264

[92] H. Schwarz, D. Marpe, and T. Wiegand, "Overview of the scalable video coding extension of the H.264/AVC standard," IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, no.9, pp 1103-1120, 2007

[93] MPEG-H standard časť 2, ISO/IEC 23008

[94] MPEG-21 Digital Item adaptation, ISO/IEC 21000-7:2004 - Part 7: Digital Item Adaptation

[95] Sodagar, I., The MPEG-DASH Standard for Multimedia Streaming Over the Internet. IEEE MultiMedia 18, 4 (October 2011), 62-67. DOI=http://dx.doi.org/10.1109/MMUL.2011.71

[96] Sieber, C., et al., "Implementation and User-centric Comparison of a Novel Adaptation Logic for DASH with SVC," Proc. IFIP/IEEE International Symposium on Integrated Network Management, 2013, pp. 1318-1323.

[97] Príklady DASH SVC datasetov, dostupné online (8.12.2017) na http://concert.itec.aau.at/SVCDataset/

[98] Mueller, Ch., MPEG-DASH (Dynamic Adaptive Streaming over HTTP, ISO/IEC 23009-1), dostupné online (8.12.2017) na https://bitmovin.com/dynamic-adaptive-streaming-http-mpeg-dash/

[99] Online Learning Adaptation Strategy for DASH Clients, MMSys 2016 Klagenfurt, Austria 2016, ACM.ISBN978-1-4503-2138-9. DOI: 10.1145/1235

[100] G. Xylomenos, C. N. Ververidis, V. A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K. V. Katsaros, and G. C. Polyzos. A survey of information-centric networking research. IEEE Communications Surveys Tutorials, 16(2):1024-1049, 2014.

[101] Chang Ge, Ning Wang, Severin Skillman, Gerry Foster, and Yue Cao. 2016. QoE-Driven DASH Video Caching and Adaptation at 5G Mobile Edge. In Proceedings of the 3rd ACM Conference on Information-Centric Networking (ACM-ICN '16). ACM, New York, NY, USA, 237-242. DOI: https://doi.org/10.1145/2984356.2988522

[102] J. O. Fajardo, I. Taboada, and F. Liberal. Improving content delivery efficiency through multi-layer mobile edge adaptation. IEEE Network, 29(6):40-46, Nov. 2015.

[103] ETSI White Paper No. 11, Mobile Edge Computing A key technology towards 5G dostupné online (8.12.2017) na http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf

[104] Yan Ye, Yong He, Ye Kui Wang, Hendry, SHVC, the Scalable Extensions of HEVC, and Its Applications, http://www.cnki.net/kcms/detail/34.1294.TN.20160122.1848.004.html, published online January 22, 2016, ZTE COMMUNICATIONS February 2016 Vol.14 No.1

[105] Weil, N., The State of MPEG-DASH 2017, dostupne online (8.12.2017) na http://www.streamingmediaglobal.com/Articles/Editorial/Featured-Articles/The-State-of-MPEG-DASH-2017-116505.aspx

[106] Skupin, R., Sanchez, Y., Podborski, D., Hellge, C., Schierl, T., HEVC tile based streaming to head mounted displays, Consumer Communications & Networking Conference (CCNC), 2017 14th IEEE Annual, DOI: 10.1109/CCNC.2017.7983191

[107] Recommendation ITU-R M.2083-0 (2015-09), IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond. ITU-R, September 2015

[108] 3GPP Release 15: http://www.3gpp.org/release-15

[109] 3GPP Release 16 http://www.3gpp.org/release-16

[110] DRAFT NEW REPORT ITU-R M.[IMT-2020.TECH PERF REQ], Minimum requirements related to technical performance for IMT-2020 radio interface(s). ITU-R, February 2017

[111] 3GPP TS 22.261 V16.2.0 (2017-12), Service requirements for the 5G system; Stage 1 (Release 16), 3GPP, December 2017

[112] 3GPP TS 23.501 V15.0.0 (2017-12), System Architecture for the 5G System; Stage 2 (Release 15), 3GPP, December 2017

[113] 3GPP TS 23.502 V15.0.0 (2017-12), Procedures for the 5G System; Stage 2, (Release 15), 3GPP, December 2017

[114] 3GPP TS 23.503 V15.0.0 (2017-12), Policy and Charging Control Framework for the 5G System; Stage 2 (Release 15), 3GPP, December 2017

[115] 3GPP TS 29.060 V15.1.0 (2017-12), GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface (Release 15). 3GPP, December 2017

[116] ETSI GS NFV-MAN 001 V1.1.1 (2014-12) Network Functions Virtualisation (NFV); Management and Orchestration. ETSI, December 2014

[117] ETSI TS 123 101 V14.0.0 (2017-05), General Universal Mobile Telecommunications System (UMTS) architecture. ETSI, May 2017

[118] 5G PPP Architecture Working Group, View on 5G Architecture (Version 2.0). https://5g-ppp.eu/wp-content/uploads/2017/07/5G-PPP-5G-Architecture-White-Paper-2-Summer-2017_For-Public-Consultation.pdf

[119] 3GPP TS 22.071 V14.1.0 (2015-09), IP Multimedia Subsystem (IMS); Stage 2 (Release 15), 3GPP, December 2017

[120] 3GPP TS 22.268 V15.1.0 (2017-06), Public Warning System (PWS) requirements; (Release 14), 3GPP, June 2017

[121] 3GPP TS 23.228 V15.1.0 (2017-12), Location Services (LCS); Stage 1 (Release 14), 3GPP, September 2017

[122] 5G, the Internet of Things (IoT) and Wearable Devices. GSMA. https://www.gsma.com/publicpolicy/wp-content/uploads/2017/10/5g_iot_web_FINAL.pdf

[123] Huawei - SDN / NFV Innovation Workshop, Nir Halachmi, Network Research Product Management

[124] Rendering Omnidirectional Stereo Content. Google Inc. https://developers.google.com/vr/jump/rendering-ods-content.pdf

[125] ITU-T: Overview of the Internet of things. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-E&type=items

[126] Internet of Vehicles – Technologies and Services Third International Conference, IOV 2016, Nadi, Fiji, December 7–10, 2016, Proceedings

[127] A new kind of smart car. https://newsroom.cisco.com/feature-content?articleId=1724437

[128] Smart Cities The importance of a smart ICT infrastructure for smart cities. https://www.stokab.se/Documents/Nyheter%20bilagor/SmartCityInfraEn.pdf

[129] Deploying 5G-Technologies in Smart City and Smart Home Wireless Sensor Networks with Interferences. https://rd.springer.com/article/10.1007/s11277-015-2480-5

[130] Telia delivers smart mailboxes to Finnish postal service. https://internetofbusiness.com/telia-makes-postboxes-smarter-finnish-posti/

[131] Smart Wearables in Healthcare: Signal Processing, Device Development, and Clinical Applications. https://www.hindawi.com/journals/jhe/si/389732/cfp/

[132] 5G Cellular Networks Are the Future of Robotics. https://eu.mouser.com/applications/robotics-and-5g/

[133] 5G network slicing enables safer “eye in the sky” for drones. http://www.telecomtv.com/articles/5g/5g-network-slicing-enables-safer-eye-in-the-sky-for-drones-15873/

[134] Applications and use cases of 5G for IoT solutions, AR and VR. https://medium.com/@patelnisha121/applications-and-use-cases-of-5g-for-iot-solutions-ar-and-vr-37072a2a1711

SIEŤOVÉ ARCHITEKTÚRY, SLUŽBY A APLIKÁCIE

Podhradský Pavol, Medvecký Martin, Trúchly Peter, Vargic Radoslav, Londák Juraj, Kadlic Radovan, Schumann Sebastian, Salazar Jordi, Silvestre Santiago, Levický Dušan, Polakovič Adam

Vydala Slovenská technická univerzita v Bratislave vo Vydavateľstve SPEKTRUM STU,

Mýtna 30, Bratislava, v roku 2020.

ISBN 978-80-227-5000-4