Jihočeská univerzita v Českých Budějovicích
Pedagogická fakulta – Katedra fyziky

Multimediální přenosy v síti ethernet

Bakalářská práce

Autor: Stanislav Kalina
Vedoucí práce: Ing. Michal Šerý

České Budějovice 2007

Anotace

Cílem této práce je ucelený pohled na problematiku přenosu multimediálních dat pomocí datových sítí technologie ethernet. Zabývá se především popisem transportních a signalizačních protokolů, vysvětluje jejich použití, popisuje hlavní funkce a uvádí příklady. Další podstatnou část práce věnuji multicastovému vysílání a řízení kvality služeb v síti pomocí QoS.

Abstract

The aim of this BC thesis is a comprehensive view of the problem of multimedia data transmission in ethernet. The thesis deals mostly with the description of the transport and signal protocols, explains their usage, describes their main functions and presents examples. Further substantial part of the thesis has been devoted to multicasting and service regulations in network by means of QoS.

Prohlašuji, že předloženou bakalářskou práci jsem vypracoval samostatně, pouze s použitím pramenů a literatury uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách.

30. listopad 2007 Stanislav Kalina

Obsah

Úvod

Cílem práce je popis technologií, které se využívají pro přenos hlasu a videa v sítích ethernet. Vzhledem k tomu, že o každém dílčím tématu této práce by se dala vydat obšírná odborná publikace, jsou proto v práci popsány pouze nejdůležitější pojmy, vysvětleny základní principy a popisy přenosu multimedií v síti.

V následující kapitole nazvané multimediální přenosy, nastíním problematiku multimediálních přenosů v sítích technologie ethernet.

Další kapitola, pojmenovaná multicast, popisuje jeho adresování, směrování a distribuci. Multicast je dnes ještě často opomíjené všesměrové vysílání, které je vhodné především pro přenosy multimédií v reálném čase.

Kapitola protokolové prostředí se zabývá popisem nejpoužívanějších transportních, signalizačních a řídících protokolů nebo doporučení používaných při přenosu multimédií v počítačových sítích. U jednotlivých protokolů je uvedena jejich syntaxe a nastíněn příklad jejich použití.

Další kapitola seznamuje čtenáře s kvalitou služeb v počítačových sítích, kterou se prioritizací provozu řídí datové toky, čímž se zamezuje zahlcování sítě.

Předposlední kapitolu tvoří diagram MPEG-2 (Motion Picture Experts Group) over Internet Protocol.

V závěrečné kapitole shrnuji problematiku a využití multimediálních přenosů.

Multimediální přenosy

S postupným zvyšováním kapacit datových sítí, se začal měnit charakter přenášených dat a tím narůstaly nároky na vlastnosti sítě až k dnešním požadavkům na přenos multimediálních dat v reálném čase.

Nejdůležitějšími vlastnostmi při přenosu multimédií v reálném čase jsou šířka pásma, rozptyl zpoždění (jitter) a zpoždění, které především při potřebě zpětné vazby, tj. při videokonferenci nebo při telefonním spojení, musí být maximálně v řádu stovek milisekund. Pokud jsou tyto parametry zhoršené, mají za následek nežádoucí trhaný obraz nebo zvuk. Jejich vliv a způsob eliminace jsou popsány v dalších kapitolách této práce.

Přenos hlasu (VoIP – Voice over IP)

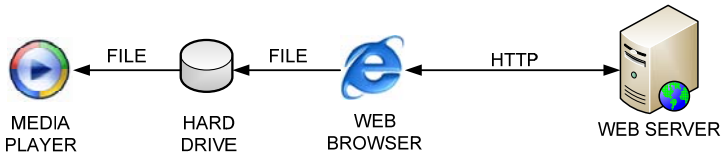
Pro přenos hlasu pomocí IP protokolu je v současné době k dispozici transportní protokol RTP (Realtime Transport Protocol), řada kompresních algoritmů např. G.729, G.723 a několik signalizačních protokolů H.323, SIP (Session Initiation Protocol), MGCP (Media Gateway Control Protocol).

Cílem signalizačního protokolu H.323 je jako v telefonním světě navázání spojení mezi dvěma telefonními čísly bez ohledu na další identifikační (adresářové) údaje. SIP se na druhou stanu snaží o navázání komunikace mezi dvěma účastníky bez ohledu na to, u kterého telefonního terminálu zrovna jsou. U H.323 je tedy hlavním identifikátorem číslo, u SIP ekvivalent e-mailové adresy, ve které ale může být číslo zakomponováno. MGCP nebo nově vyvíjený Megaco se od obou předchozích liší v tom, že je ideální pro centrální řízení jednoduchých koncových přístrojů, kdy řídící servery mezi sebou dále komunikují prostřednictvím H.323 nebo SIP.

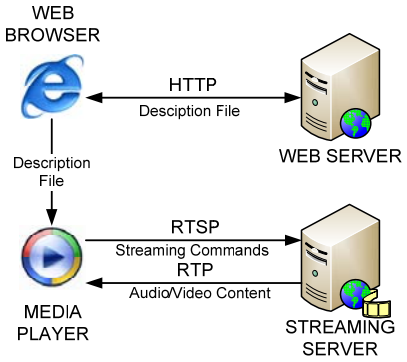
Aby byl obrázek IP telefonie úplný, je třeba na něm vidět jednak samotnou síťovou infrastrukturu s podporou kvality služeb, telefonní terminály a řídícími servery s maximální podporou otevřených standardů a rozšiřující aplikace, které jsou díky integraci datové a hlasové sítě schopny přinést větší funkčnost při vynaložení menšího úsilí a investičních nebo provozních nákladů.

Přenos videa

Způsobů jak přenášet multimediální obsah z internetu je několik. Ne zrovna vhodný způsob je nejprve celý multimediální soubor stáhnout a pak jej přehrát. Což vylučuje využití aplikaci pracujících v reálném čase.



Alternativou je přenášet média proudově – streaming, kdy klient přehrává stahovaná data průběžně a nemusí tak čekat na stažení celého, často dosti objemného, multimediálního souboru.

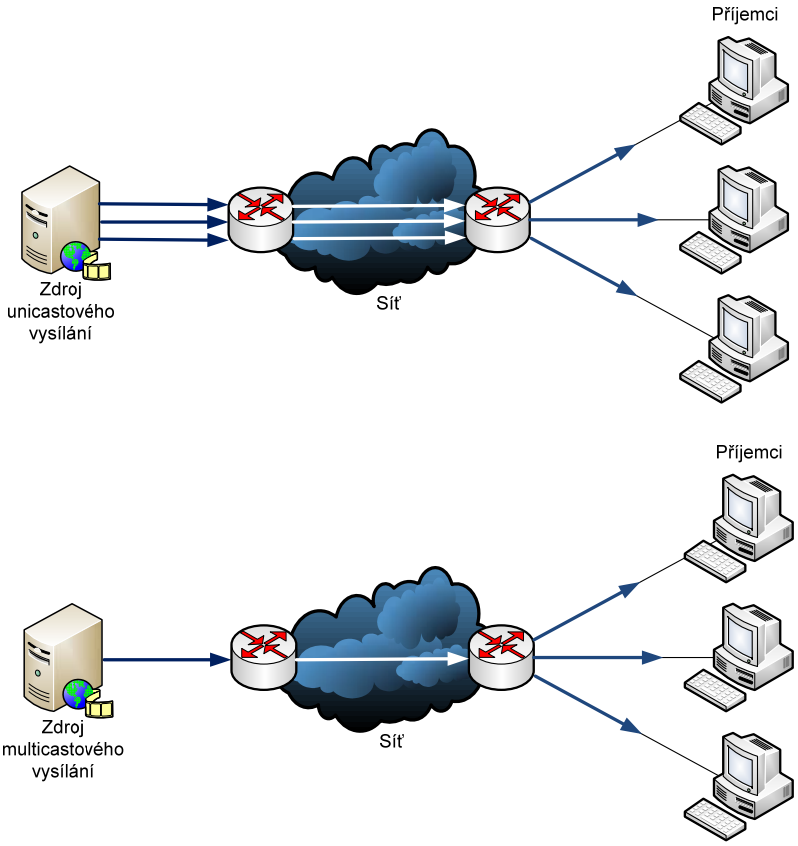


Streamování multimédií, lze ještě dále rozdělit na VoD (Video on Demand), kdy je celý mediální obsah umístěn na serveru a klient ho přehrává unicastově nebo VoL (Video on Line), kdy se multimediální obsah v reálném čase na serveru vytváří a současně je přenášen k příjemcům. Zatímco první způsob je vhodný především pro přehrávání záznamů, druhý způsob je vhodný a v kombinaci s multicastovým vysíláním i velice efektivní např. pro konference nebo přenos televizního a rádiového vysílání.

Většina streamovacích technologií disponuje tzv. bandwidth negotiation, kdy klient serveru pošle dostupnou šířku pásma, a server mu pak posílá obsah v nejbližší nižší kvalitě. Protože všechny streamovací systémy načítají několik sekund vysílání do mezipaměti (odstraňují tak částečně i problém se zpožděním a s jeho rozptylem), nelze proto nikdy získat opravdu přímý přenos vysílané akce.

Multicast

Pro zajištění přenosu datagramů určených pro více uzlů umístěných mimo broacastovou doménu[1], se v poslední době začal ve velké míře využívat i multicast. Pro tento typ přenosu je zdrojový uzel nakonfigurován tak, že vysílá data z předem určené adresy, kterou je dáno multicastové vysílání. Podle zvolené zdrojové IP adresy je určen dosah daného vysílání. Vlastní vysílání se šíří většinou v broadcastové doméně a až hraniční prvek, který zajišťuje směrování paketů a určuje, jakým způsobem bude s daným datagramem zacházeno. Za předpokladu, že bude od klientů požadován příjem daného vysílání, směrovač zajistí replikaci multicastového vysílání na všechna rozhraní, z nichž přišly požadavky. Registrací požadavků vysílání od klientů, směrovač zajišťuje vysílání paketů pouze tam, kde existují určití příjemci. Tato technologie se nazývá sparse mode a je jí zajištěna ochrana sítí před zahlcením. V případě složité topologie sítě směrovač zajišťuje přenos dat nejlépe zvolenou cestou. Pro zvolení nejvýhodnější cesty se používají link state multicastové protokoly. Multicasová cesta sítí nemusí být vždy shodná s nejvýhodnější cestou pro unicast.



[1] Broadcastová doména je poslední adresa v určeném segmentu sítě a používá se pro odeslání rámce všem uzlům v dané síti. MAC (Media Access Control) adresa broadcastu je vždy ff:ff:ff:ff:ff:ff a pokud je nějaký rámec takto označen, pak je jen na síti, aby vytvořila kopie a rozeslala je na každý uzel v daném segmentu sítě.

Adresové schéma

Hlavní rozdíl mezi multicastovým a unicastovým paketem spočívá v tom, že cílová adresa je u multicastového paketu z rozsahu adres třídy D. U těchto adres pak začíná první oktet v binárním vyjádření na 1110, a adresy tudíž leží v rozsahu 224.0.0.0 až 239.255.255.255. Adresy z tohoto adresového prostoru IANA (Internet Assigned Numbers Authority) dále rozdělila:

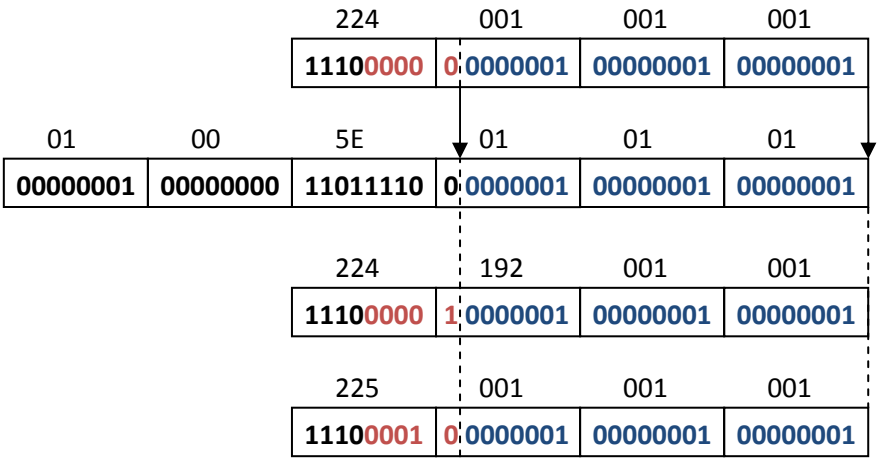
224.0.0.0/24	Local Network Control Block	pakety posílané na adresy z tohoto rozsahu nesmí být směrovány dále – mají nastaveno TTL (Time To Live – RFC791) na hodnotu jedna. Používají je hlavně směrovací protokoly ke komunikaci mezi sousedními směrovači.
224.0.1.0/24	Internetwork Control Block	tyto adresy mají přiděleny významné síťové služby (např. Network Time Protocol má přidělenu adresu 224.0.1.1)
224.0.1.0 až 238.255.255.255	Globally Scoped Address	adresy z tohoto rozsahu přiděluje IANA a forwardují se běžně
239.0.0.0/8	Administratively Scoped	adresy z toho rozsahu se využívají v privátních sítích (mají stejný význam jako neveřejné síťové rozsahy)

Multicastová adresa může být uvedena pouze v cílové adrese paketu, zdrojová adresa je vždy unicastová.

Mapování IP adresy multicastového paketu na adresu multicastového rámce se provádí s menšími komplikacemi. Adresa multicastového rámce vždy začíná 25 bitovým prefixem 01:00:5e v šestnáctkové soustavě. Protože v nejvyšším čtvrtém bajtu adresy rámce musí být nula, zbývá pro mapování IP adresy do adresy rámce 23 bitů. Jelikož ale IP adresa z třídy D začíná vždy prefixem 1110, zůstává pro mapování 28 bitů. Z toho plyne, že mapování nelze provést beze ztráty, a proto se pouze posledních 23 bitů z IP adresy zkopíruje do posledních 23 bitů adresy multicastového rámce. Z toho plyne nejednoznačnost těchto adres. Jelikož se pět bitů IP adresy nemapuje, tak je do jedné multicastové adresy rámce mapováno 2^5 IP adres. Proto musí IP vrstva kontrolovat doručené datagramy a zahazovat datagramy určené pro jiný uzel.

Příklad

Na následujícím obrázku je naznačeno mapování multicastové adresy paketu 224.1.1.1 do ethernetové adresy 01:00:4e:01:01:01 – stejnou MAC adresu má i 224.192.1.1, 225.1.1.1 apod.



černě – jsou označeny multicastové prefixy
modře – 23 přenášených bitů
červeně – 5 nepoužitých bitů

Jednodušší ethernetové přepínače, většinou přepínače bez managementu, neumí pracovat s multicastovými rámci a tak je rozešlou podobně jako broadcast na všechny své porty mimo příchozího. Sofistikovanější přepínače rozesílají multicastové rámce pouze na porty, na kterých jsou očekávány. Zda jsou na portech příjemci multicastového vysílání přepínače zjišťují pomocí protokolu IGMP a monitoringu MAC adres stanic, které si zprávy protokolu IGMP vyměňují. Přepínači pak stačí zjistit, na které unicastové MAC adresy stanic má poslat příchozí rámec s každou jednotlivou multicast MAC adresou. Čísla portů, na které jsou stanice s těmito MAC adresami připojeny, si najde v přepínací tabulce.

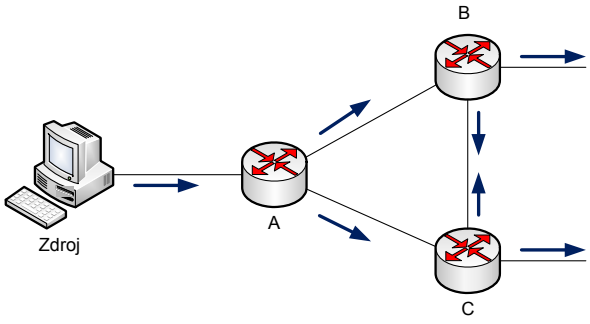
Reverse Path Forwarding – RFC3684

Jakmile přijde unicastový datagram na libovolné rozhraní směrovače, sníží se mu parametr TTL o jedna, a když je i nadále vyšší než nula, zjistí si z unicastové směrovací tabulky, co má s tímto datagramem udělat (přeposlat dále na příslušný interface následujícímu uzlu – Next Hop nebo datagram zahodit). Problémy nastávají v případě multicastu, kde se v datagramy v síti často replikují a mění se multicastové cesty.

Proto je při směrování multicastových datagramů nejdůležitější zajistit, aby v síti nedocházelo k zacyklení, nebo aby na směrovačích nedocházelo ke zbytečnému replikování, a tím i zbytečnému zatěžování sítě a stanic duplikátními datagramy.

Mechanismus TTL sice zaručuje, že bude paket jednou zahozen, ale nezabrání zbytečným replikacím. Proto byl vyvinut RPF (Reverse Path Forwarding).

RPF funguje tak, že si směrovač z multicastového datagramu zjistí zdrojovou adresu a poté podle své unicastové směrovací tabulky otestuje (RPF-Check), jestli by stejným rozhraním poslal i unicastový paket, který by měl cílovou adresu stejnou jako je zdrojová adresa multicastového datagramu. Pokud test projde, datagram je dále zpracováván, pokud ne, je zahozen.



Zdroj multicastového vysílání pošle paket na směrovač A, který paket replikuje na své downstream porty. Jakmile přijde paket na upstream port směrovače B, je opět replikován na své downstream porty. Paket, který přijde na směrovač C ze směrovače B je zahozen, protože neprojde při RPF-Check.

Multicastové směrovací protokoly přiřazují ke každému distribučnímu stromu upstream rozhraní (vedoucí ke kořenu distribučního stromu) a i množinu rozhraní downstream (rozhraní vedoucí do segmentů sítě, kde se vyskytují další uzly dané multicastové skupiny). Datagramy vyhovující RPF-Check se pak pouze odesílají na downstream rozhraní. Distribuční stromy spolu s upstream a downstream rozhraními tvoří multicastové směrovací tabulky, které obsahují pro:

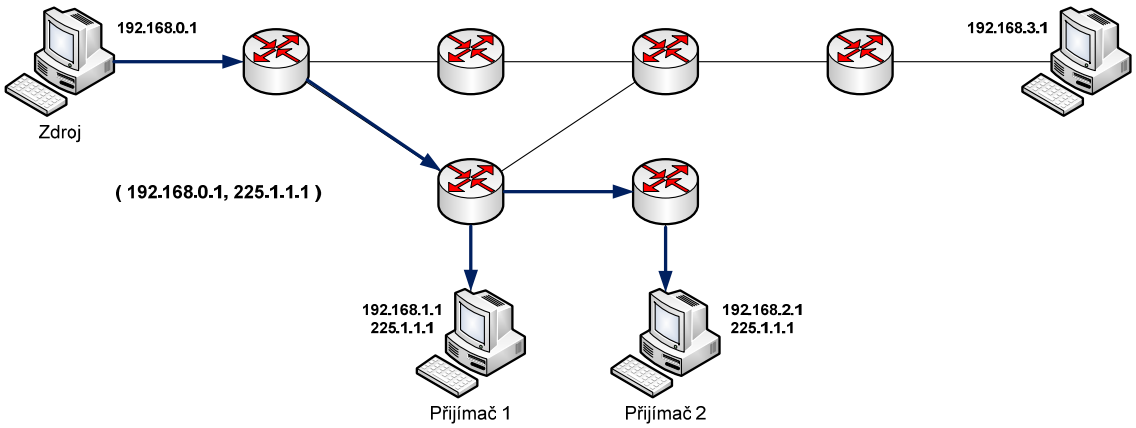
Source Trees – multicast adresu, adresu zdroje, upstream rozhraní, downstream rozhraní
Shared Tress – multicast adresu, upstream rozhraní, downstream rozhraní

Pro Source Trees je záznamů v multicastové směrovací tabulce tolik, kolik je ve skupině vysílačů.

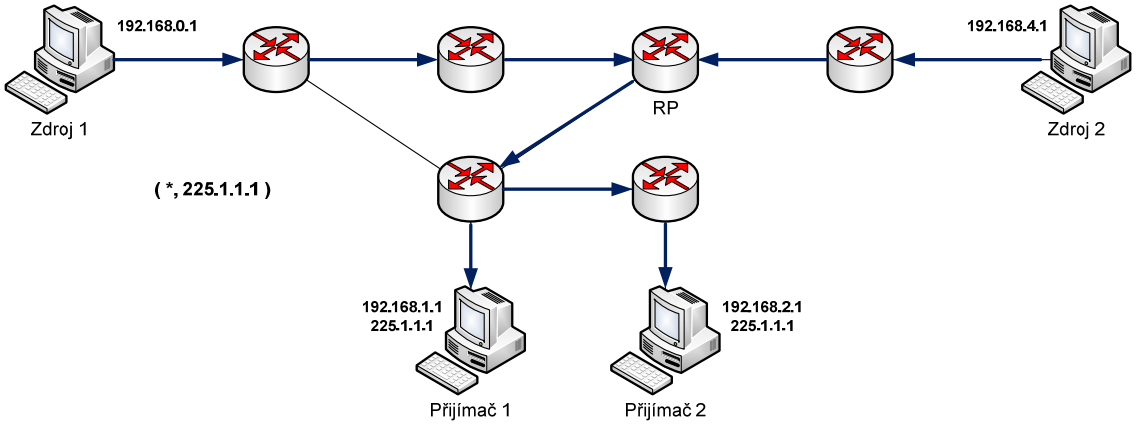
Distribuční stromy

Multicastové distribuční stromy vytváří topologii sítě a spojují zdroj multicastových dat (kořen), přes multicastové směrovače, s příjemci vysílání (listy stromu). S přihlašováním a odhlašováním příjemců vysílání, se ke stromu připojují další nové větve nebo se odstraňují nepotřebné.

Zdrojový strom (Source Tree) – často označovaný jako SPT (Shortest Path Tree). Označuje se (S, G), kde S je adresa zdroje a G je adresa multicastové skupiny. Pokud budou dva zdroje vysílat do jedné multicastové skupiny, bude síť udržovat dva nezávislé distribuční stromy, proto se označuje jako SSM (Source Specific Multicast).



Sdílený strom (Shared Tree) – obsahuje pro všechny zdroje ve skupině jeden distribuční strom, který má kořen vždy na jednom vhodně zvoleném směrovači. Tento kořen se často označuje jako Core nebo RP (Randesvous Point), strom se pak značí (*, G), kde hvězdička znamená stejný strom pro mnoho zdrojů vysílajících do multicastové skupiny G. Tento strom se dělí na jednosměrný, kde zdroje posílají data unicastem ke kořenu, který se postará o jejich distribuci a na obousměrný, kde zdroje vysílají muticast nejen ke kořeni, ale současně také po směru stromu k příjemcům vysílání. Protože ať vysílá v rámci skupiny kdokoliv a strom je vždy stejný, označuje se tento způsob jako ASM (Any Source Multicast).



Směrovací protokoly

Dělí se do tří základních skupin: dense mode, sparse mode a link state. První dvě uvedené metody se používají pro směrování v rámci lokálních sítí, dense mode pro hustý a sparse mode pro řídký výskyt příjemců v jednotlivých větvích sítě. Protokoly link state, se zejména používají pro směrování v rámci internetu mezi jednotlivými operátory.

Dense mode

Tato metoda využívá pro distribuci zdrojové stromy a dala by se nazvat – paketový spam, protože pracuje na tzv. push modelu, který předpokládá v každé větvi příjemce multicastového vysílání, a proto toto vysílání defaultně směruje do všech segmentů sítě. Pokud směrovač nemá na žádném rozhraní příjemce, pošle směrovači na vyšší úrovni distribučního stromu časově omezenou prune zprávu, která větev odřízne. Pokud se z odříznutého směru připojí nový zájemce o příjem dané skupiny, pošle směrovač zprávu graft a multicastový provoz se obnoví. Vysílání se obnoví i v případě, že vyprší platnost prune zprávy, kterou směrovač neaktualizuje.

DVMRP (Distance Vector Multicast Routing Protocol – RFC1075)
PIM-DM (Protocol Independent Multicast Dense Mode – RFC3973)

Sparse mode

Tato metoda k distribuci multicastového vysílání využívá sdílený strom a tzv. pull model, který defaultně předpokládá, že ve větvích nejsou žádní příjemci a multicastové pakety tedy neposílá nikam. Pokud se na segmentu objeví zájemce o příjem multicastové skupiny, pošle směrem ke kořenu časově omezenou join zprávu, kterou žádá o zasílání paketů z RP. Z prvního přijatého paketu zjistí směrovač zdroj multicastového vysílání a může si zažádat o příjem přímo od zdroje, čímž zruší příjem z RP. Pokud už v daném segmentu není žádný příjemce, směrovač zprávou graft oznámí, že už o multicast nemá zájem. Větev odřízne i v případě, že nedojede k obnovení join zprávy.

PIM-SM (Protocol Independent Multicast Sparse Mode – RFC2362)
CBT (Core Based Trees – RFC2189)

Link state

Protokoly této metody využívají k distribuci multicastového vysílání zdrojové stromy. Jednotlivé směrovače si vyměňují informace o stavu a rychlosti linek, které pak ukládají do vlastních databází, z kterých sestavují pro každou multicastovou skupinu distribuční strom.

MOSPF (Multicast Open Shortest Path First – RFC1584)
MSDP (Multicast Source Discovery Protocol – RFC3618)
BGMP (Border Gateway Multicast Protocol – RFC3913)
MBGP (Multiprotocol Border Gateway Protocol – RFC2858)

Internet Group Management Protokol

IGMP (Internet Group Management Protokol) protokol využívají příjemci multicasového vysílání k přihlášení a od verze 2 i k odhlášení od multicastové skupiny u nejbližšího směrovače, který také používá tento protokol k zjišťování trvání zájmu o příjem dané multicastové skupiny a k registraci svého segmentu sítě do multicasového distribučního stromu.

IGMPv1 – RFC998

Tento protokol ve verzi 1 obsahuje pouze dvě zprávy – Membership Report a Membership Query.

Zprávu Membership Repost s vyplněnou adresou skupiny posílá stanice, která se chce přihlásit k příjmu multicastového vysílání, na adresu 224.0.0.2 (všechny směrovače v síti). Protože členství je dynamické posílá směrovač každých 60 vteřin zprávu Membership Query na adresu 224.0.0.1 (všechny systémy v síti), aby zjistil, zdali je o příjem dané multicastové skupiny stále zájem. Pokud stanice na výzvu neodpoví zprávou Membership Report třikrát za sebou, směrovač přestane tímto směrem multicast posílat. Protože se obě zprávy šíří multicastem, mohlo by docházet ke zbytečnému zatěžování sítě, proto stanice neodpovídají na Membership Repost ihned, ale každá si zvolí náhodné číslo v rozmezí 0 až 10, určující za kolik vteřin odpoví. Stanice i nadále naslouchá na síti, a pokud jiná během tohoto času neodpoví, vyšle sama zprávu Membership Query, kterou uslyší i ostatní stanice a své zprávy zruší. To znamená, že směrovač neví kolik má daná skupina posluchačů, ví jen, že je v segmentu minimálně jeden.

IGMPv2 – RFC2236

U protokolu verze 2 je přihlášení do skupiny stejné jako u IGMPv1. Navíc je zde ale proces opuštění skupiny, kdy klient odesílá zprávu Leave Group, kterou se zkrátí doba, kdy je segment zbytečně zahlcován multicastovým vysíláním, které již nikdo neposlouchá. Pokud směrovač obdrží zprávu Leave Group, vyšle do dané skupiny zprávu Group-Specific Query. Pokud na ní někdo do jedné vteřiny odpoví, směrovač pokračuje dál v posílání dat, pokud ne posílání dat ukončí.

Další novinky se týkají Membegship Query. Kromě toho, že se prodloužil čas odesílání na jednou za 125 vteřin, změnil se formát na specifický dotaz pouze na konkrétní skupinu a ne na jakoukoliv skupinu jako u verze 1. Nová je i volba směrovače rozesílajícího tyto zprávy. Vybrán je ten s nejvyšší IP adresou a ostatní jen poslouchají a jsou připraveni převzít jeho roli.

IGMPv3 – RFC3378

IGMP verze 3 je především rozšířen o možnost filtrování požadovaného provozu. Člen multicastové skupiny již nemusí přijímat vysílání ode všech, ale jen od vybraných zdrojů. Toho se docílí tak, že se člen nepřihlašuje do skupiny (*, G), ale přihlašuje se přímo ke kořeni v dané skupině (S, G). Membership Report se odesílá na adresu 224.0.0.22.

Spolehlivý multicast

Multicast používá pro šíření nespolehlivý protokol UDP (User Datagram Protocol), který neobsahuje opravné mechanismy, které jsou využívány u protokolu TCP (Transmission Control Protocol). Z toho plyne, že v případě výpadku, nedojde k doručení dat až ke koncovému uzlu.

Zajistit spolehlivý proud multicastových datagramů podobný unicastovému TCP proudu není snadné, protože při multicastovém vysílání z více zdrojů nelze zajistit správné pořadí příchozích datagramů, proto lze o spolehlivém multicastu mluvit pouze při vysílání s jedním zdrojem.

Spolehlivost vyžaduje určitý mechanismus potvrzování, ale protože zdroj nemá možnost, jak zvládnout tolik ACK (Acknowledge) paketů a nastane tzv. ACK imploze. Proto se ustanoví hierarchický strom šíření, kde budou po cestě umístěny tzv. potvrzovací body. Datagramy nesou sekvenční čísla, a pokud klient detekuje chybějící datagram, požádá o nový přenos zprávou NACK (Negative ACK), kterou zachytí nejbližší potvrzovací bod a pošle datagram znovu ze své záložní kopie.

Bez dostatku potvrzovacích bodů může lehce dojít k ACK implozi. Protože se ale potvrzovací body dají konfigurovat jen ručně, proto se tato metoda hodí jen do topologicky stálých sítí.

Alternativou k metodě negativního potvrzování může být redundance datagramů. Jednou možností je používání samoopravných kódů, anebo jich místo jednoho datagramu posílat více.

Shrnutí

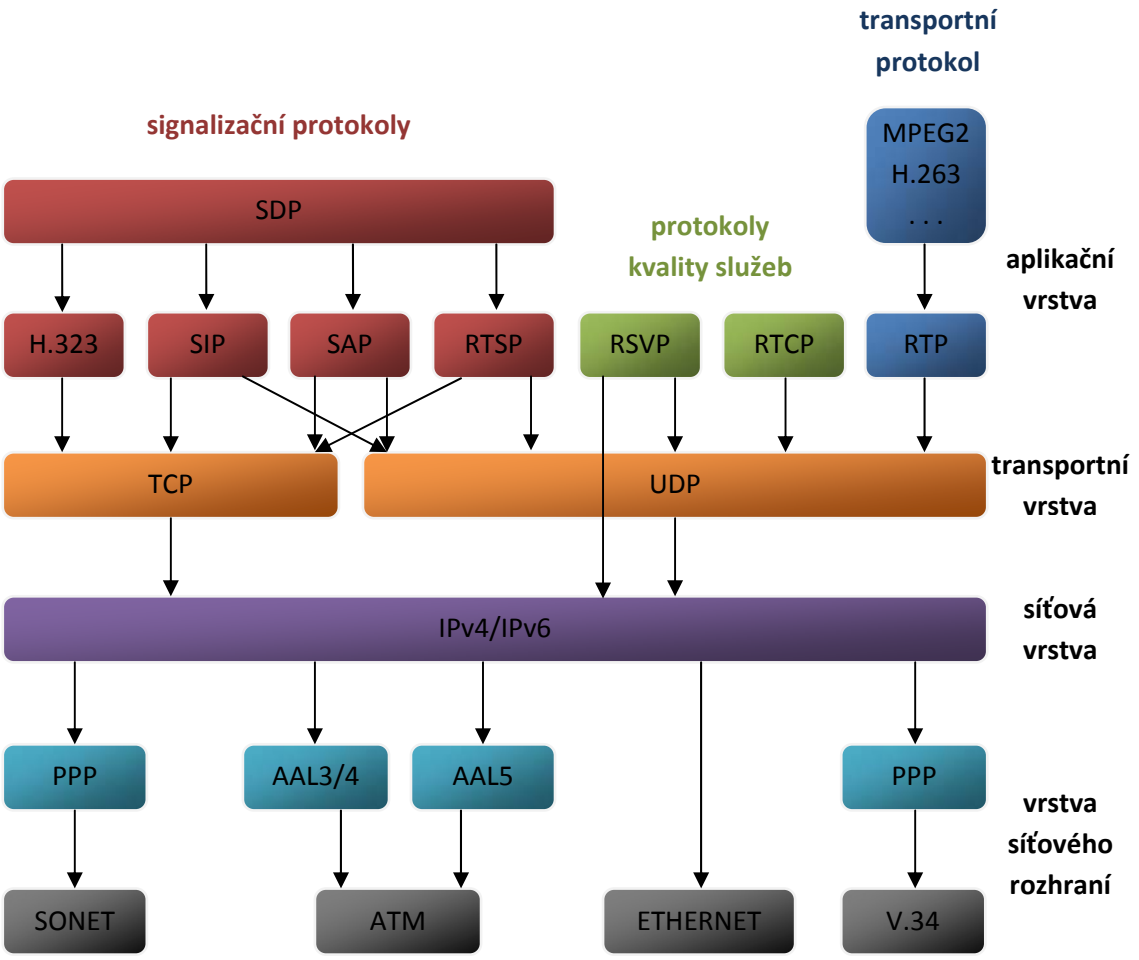
V současné době je nejrozšířenější protokol v lokálních sítích PIM-SM, který je současné době podporován řadou výrobců. Jako příklad je možné uvést výrobky firem Cisco Systems, Nortel Networks, Juniper Networks a mnoha dalších. U uvedených firem je v praxi ověřena kompatibilita směrování u jednotlivých poskytovatelů internetu. Je tedy možné předpokládat, že s postupem času a s pomocí směrovacích protokolů MBGP a MSDP budou do akademických sítí připojeni i ostatní poskytovatelé internetu.

Protokoly podporující multimediální služby

Internet, jako sdílená síť pro přenos datagramů, není primárně vhodná pro přenos multimedií. Dnešní hardware sice nabízí dostatečný výkon na multimediální přenos, ale současná technologie nedokáže zajistit požadované parametry zpoždění a stálost toku. Proto je nutné používat protokoly vhodné k řízení sítě s ohledem na vlastnosti datových protokolů.

Protokolová mapa

Na následující protokolové mapě jsou zobrazeny protokoly, které se nejčastěji používají při multimediálních přenosech.



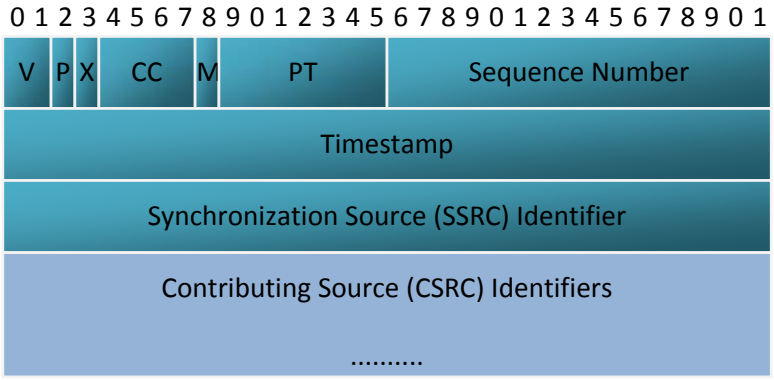
Realtime Transport Protocol (RTP) – RFC3550

Protože základní protokoly rodiny TCP/IP nejsou vhodné pro přenos multimediálních dat v reálném čase, jelikož negarantují dobu, za kterou budou data doručena, byl vyvinut transportní protokol RTP, který je vhodný jak pro jednosměrný přenos – VoD, tak i pro interaktivní služby – IP telefonii, videokonferenční služby apod.

RTP vkládá jednotlivé části multimediálních dat do vlastních paketů a ty následně do klasického UDP paketu nebo do jiného protokolu z transportní vrstvy.

UDP je sice nespojová datagramová služba bez záruky doručení paketů, ale jelikož je RTP primárně navržen pro multicast (vhodný je i pro unicast), nepotřebuje spolehlivost spojení, ale klade důraz především na velikost přenosového zpoždění a na jeho pravidelnost. Proto protokol RTP připojuje k multimediálnímu obsahu záhlaví, obsahující například pořadové číslo paketu, podle kterého aplikace rozpozná ztracené pakety, jeho časovou známku pro rekonstrukci datového proudu a obsahuje také informaci o formátu multimediálního souboru, který je v paketu.

V multimediálních relacích se přenáší každé médium ve zvláštním RTP spojení se svým vlastním RTCP (Realtime Transport Control Protocol) kanálem. Tak lze vysílat zvlášť více audio a video kanálů v různé kvalitě a přijímač se pak rozhodne, ke kterému spojení se přihlásí.



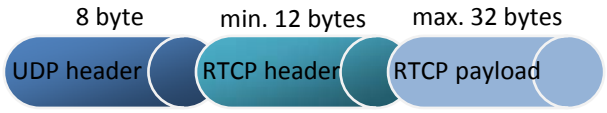
V – Version number – nejnovější je verze protokolu 2
P – Padding Bit – pokud je nastaveno, RTP paket obsahuje i patičku
X – Extension Bit – určuje, zdali je standardní hlavička rozšířena
CC – CSRC Count – počet CSRC za standardní RTP hlavičkou, toto číslo je větší než jedna pokud data RTP paketu obsahují data z několika zdrojů
M – Marker Bit – u videa označuje poslední paket nutný k sestavení jednoho snímku
PT – Payload Type – určuje typ přenášených multimediálních dat
Sequence Number – inkrementálně čísluje pakety od náhodně vybraného čísla – podle tohoto údaje přijímač zjistí ztrátu paketu

Timestamp – tyto informace přijímač používá k rekonstrukci časové posloupnosti nebo k synchronizaci několika datových toků
SSRC – Synchronization Source Identifier – náhodně vybrané číslo rozlišující zdroje uvnitř stejné RTP relace
CSRC – Contributing Source Identifiers – seznam jednotlivých zdrojů dat obsažených v tomto balíčku, může zde být max. 16 identifikátorů a jejich počet je uložen v poli CC

RTP nemá žádný mechanismus zaručující včasné doručení dat, a proto potřebuje ke správnému fungování podporu nižších vrstev. Jelikož byl protokol RTP vyvíjen jako nezávislý, nestará se o vrstvy pod ním a lze jej snadno implementovat i na další protokoly jako jsou ATM-AA5 (Asynchronous Transfer Mode) a IPv6.

Realtime Transport Control Protocol (RTCP) – RFC3550

RTCP je řídící a monitorovací protokol spolupracující s RTP, který pracuje na principu periodického přenosu řídících paketů ke všem účastníkům relace. RTCP pakety především obsahují informace o toku RTP, podle kterých může vysílající strana dynamicky měnit multimediální proud na základě požadavků strany přijímací. Podobně jako RTP pracuje také nad UDP protokolem, ale může také pracovat nad jiným protokolem transportní vrstvy.



Kromě QoS (Quality of Service) RTCP identifikuje zdroj vysílaných dat – tzv. cname, který přijímač používá ke spojování vícenásobných toků dat z jednoho zdroje s odpovídající relací RTP protokolu, např. synchronizace audio a video toků. Mezi další služby poskytované RTCP patří synchronizace samostatně vysílaných audio a video toků – tzv. intermediální synchronizace a přenášení různých identifikačních informací, které mohou být zobrazeny na straně připojeného účastníka.

Obvykle je přenášeno několik RTCP paketů zahrnutých do jednoho UDP paketu – jedna UDP hlavička tak redukuje síťovou režii.

Protože objem RTCP dopravy může převyšovat RTP traffic, např. při konferenční relaci s větším množstvím účastníků, kdy jen jeden mluví a ostatní poslouchají, je proto rychlost odesílání RTCP paketů dynamicky měněna v závislosti na počtu účastníků. Standardně je 20% šířky pásma relace vyhrazeno pro RTCP komunikaci a navíc 5% z šířky pásma RTCP je vyhrazeno pro specifického účastníka – cname.

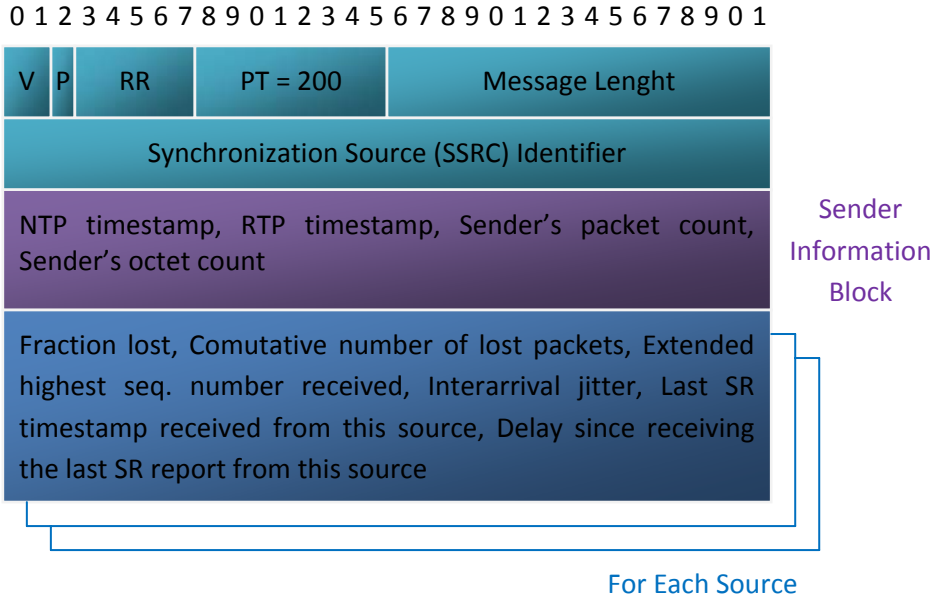
Druhy zpráv

Typ paketu	Zkratka	Popis
192	FIR	Full Intraframe Request
193	NACK	Negative ACK
200	SR	Sender Report
201	RR	Receiver Report
202	SDES	Source Description
203	BYE	Goodbye
204	APP	Application
207	XR	Extension

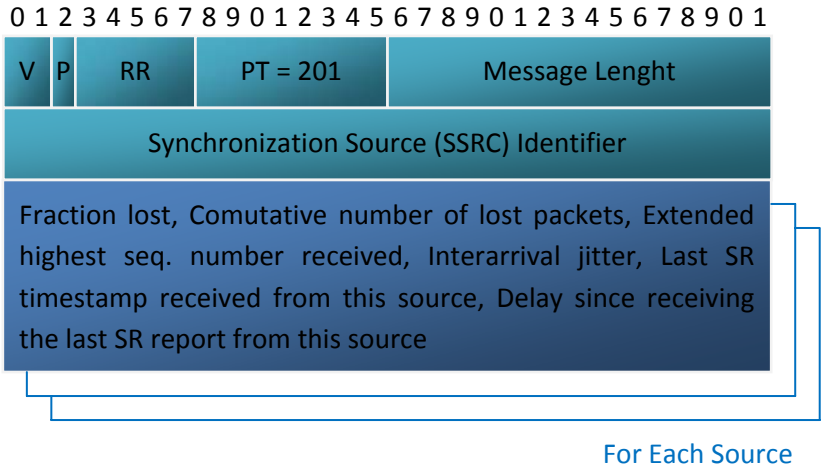
RTCP hlavička

V – Version – stejné jako u RTP
P – Padding Bit – stejné jako u RTP
RR – Reception Report Count
PT – Packet Type – typ RTCP paketu

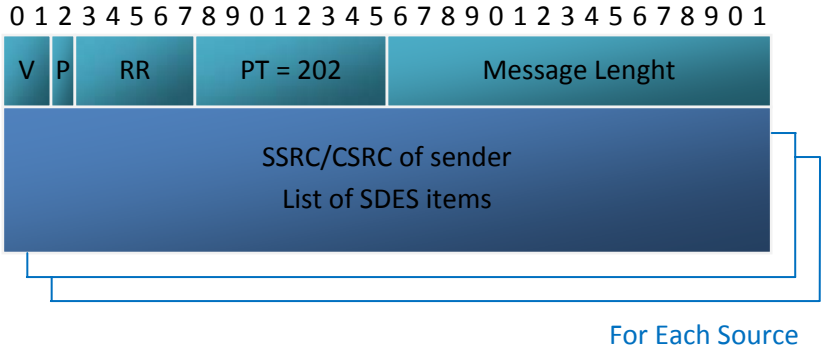
Sender Report



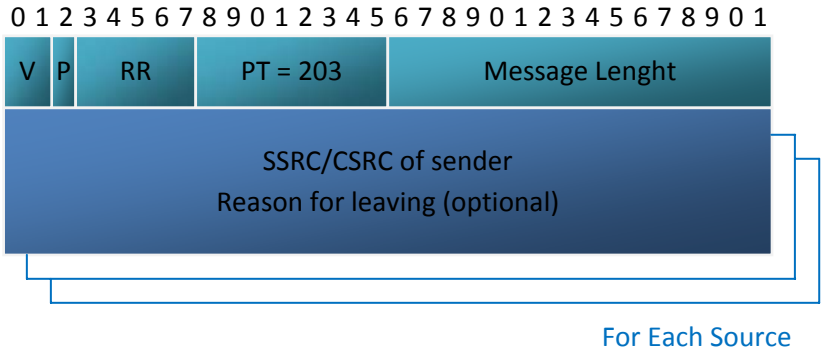
Receiver Report



Source Description



Bye Message



Resource ReSerVation Setup Protocol (RSVP) – RFC2205

Je protokol, pomocí kterého příjemce požaduje od sítě specifickou kvalitu služby pro své datové toky. Aplikace tímto protokolem rezervuje na směrovačích podél přenosové cesty potřebné zdroje, aby bylo požadované pásmo k dispozici při přenosu multimediálních dat.

Způsoby rezervace jsou dva. Oddělená rezervace, kdy se vytváří požadovaný tok pro každý vysílač a každou relaci a sdílená rezervace, kterou současně používá skupina navzájem se neovlivňujících vysílačů.

Datové toky RSVP se dělí podle typu provozu na Best Effort, kdy bude paket doručen nejvhodnější cestou v síti, na Rate Sensitive, který znamená provoz se zaručenou rychlostí v síti a na Delay Sensitive, jenž umožňuje provoz se zaručeným zpožděním.

Aktivace relace protokolu RSVP s použitím adresace multicast:

Příjemce se pomocí protokolu IGMP spojí s cílovou skupinou.

↓

Po navázání spojení začne odesílatel odesílat zprávy RSVP o navržené cestě.

↓

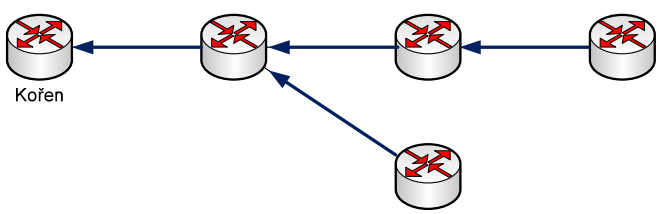
Přijímací aplikace přijme tuto zprávu a začne vysílat zprávy RSVP s žádostí o rezervaci, specifikující požadované atributy toku.

↓

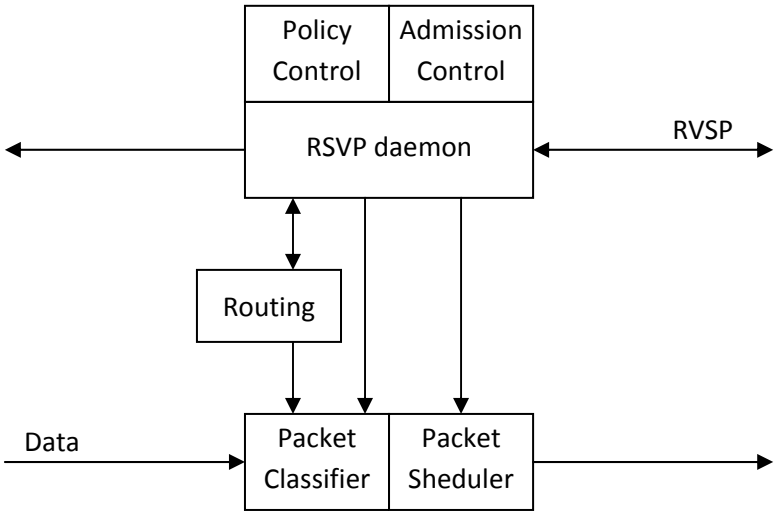
Jakmile odesílající aplikace obdrží tyto zprávy, začne posílat datové pakety.

Protokol RSVP pracuje jak s unicastem tak i s multicastem, nevykonává vlastní směrování, k tomu využívá směrovacích protokolů na nižší vrstvě. Je tedy zodpovědný pouze za sjednání požadovaných parametrů spojení s jednotlivými uzly. Jak budou tyto požadavky zpracovány, záleží na způsobu implementace QoS na těchto uzlech.

Jelikož velká část multimediálních dat má charakter multicastu, cestuje rezervace po multicastovém stromě dokud nenarazí na místo, kde již tato rezervace existuje. Lze tedy připojit mnoho přijímačů bez zvýšení celkového toku dat.



Na každém uzlu běží několik procesů starajících se o nastavení a správu rezervací:



Policy Control – zjišťuje, zda má uživatel administrativní povolení k vytvoření rezervace
Admission Control – určuje, zda má uzel dostatečné zdroje k nastavení požadované kvality
Packet Classifier – rozděluje podle rezervací pakety do jednotlivých tříd QoS
Packet Sheduler – připravuje přenos paketů k dosažení požadované kvality pro každý proud

Zprávy protokolu RSVP

Request Reservation Message – tyto zprávy se žádostí o rezervaci odesílají příjemci k vysílačům a putuje po multicastovém stromě v opačném směru než data od odesílatele. Pokud se změní přenosová cesta tak zajistí na směrovačích vytvoření nové rezervace na změněné cestě.

Path Message – zprávy o cestě periodicky posílají vysílače po multicastovém stromě a obsahují informace o stavu cesty (nalezení datové cesty, rezervace zdrojů po cestě apod.)

Error and Confirmation Message – dělí se na chybovou zprávu s chybou cesty, chybovou zprávu s chybou žádosti o rezervaci a potvrzovací zprávu, která potvrzuje žádost o rezervaci.

Teardown Message – odstraňovací zprávu může vyslat příjemce, vysílač i směrovač a slouží k odstranění záznamu o stavu cesty a rezervace, aniž by došlo k vypršení doby po kterou je rezervace aktivní.

Realtime Transport Streaming Protocol (RTSP) – RFC2326

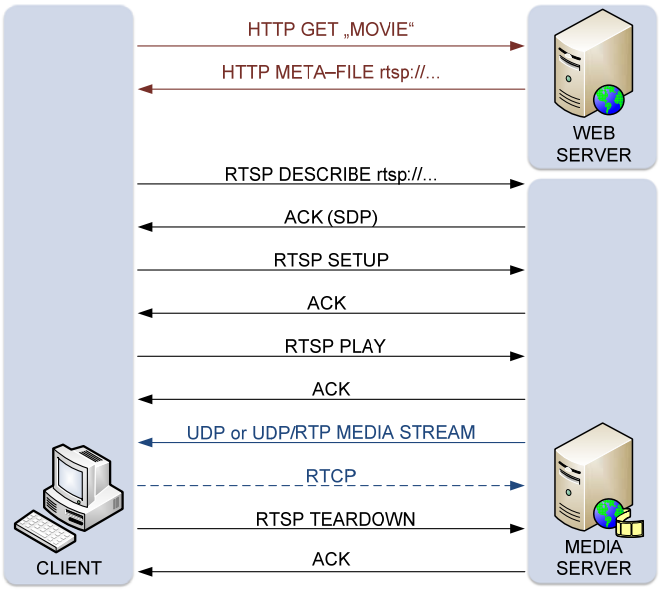
RTSP slouží jako dálkové ovládání, které zajišťuje řízený tok multimediálních dat mezi klientem a serverem. Je to protokol aplikační vrstvy, který umožňuje kompletní přenosové služby, pouze ve spojení s nižšími vrstvami.

Tento protokol umožňuje přehrávači plně ovládat (spustit, pozastavit, přehrát zrychleně apod.) vybrané multimediálních toky ze sítě, aniž by bylo potřeba celá data nejprve stáhnout.

Má podobnou syntaxi, stavové kódy, bezpečnostní mechanizmy, identifikaci pomocí URL (Uniform Resource Locator), jako HTTP (Hyper Text Transfer Protocol), jen na rozdíl od HTTP (bezstavový protokol) musí RTPS server obsluhovat stavy spojení. Kompletní informace (RTSP URL, cílový port, kódování apod.) o multimediálních datech jsou uloženy v tzv. description file.

POŽADAVEK	SMĚR	POPIS
ANNOUNCE	K ↔ S	Změna popisu multimediálního objektu
DESCRIBE	K → S	Poskytuje klientům popis multimediálního objektu
GET_PARAMETER	K ↔ S	Získá hodnoty parametrů proudu specifikovaných v URL
OPTIONS	K ↔ S	Dohodnutí informací o dostupných schopnostech druhé strany
PAUSE	K → S	Dočasné přeruší proud dat bez uvolnění kapacit na serveru
PLAY	K → S	Spustí přenos alokovaný přes SETUP
RECORD	K → S	Nahrávání multimediálních dat
REDIRECT	K ← S	Klient musí použít jiný server, součástí je URL jiného serveru
SET_PARAMETER	K ↔ S	Nastaví hodnoty parametrů proudu specifikovaných v URL
SETUP	K → S	Server přiděluje zdroje pro proud dat a spouští RTSP relaci
TEARDOWN	K → S	Ukončí přenos a zruší na serveru existující RTSP relaci

RTPS požadavky mohou být posílány v obou směrech (od klienta k serveru, a naopak) a posílají se po odděleném kanále mimo datový tok přes port 544.



Příklad

Následující příklad demonstruje, jak klient C žádá film z mediálních serverů A (audio.example.com) a V (video.example.com). Mediální popis je uložen na webovém serveru W a obsahuje popisy prezentace včetně všech jejích proudů, dostupných kodeků, jazykových informací nebo autorských omezení.

Získání popisu multimediálních dat:

```
C->W: GET /twister.sdp HTTP/1.1
      Host: www.example.com
      Accept: application/sdp

W->C: HTTP/1.0 200 OK
      Content-Type: application/sdp
      v=0
      o=- 2890844526 2890842807 IN IP4 192.16.24.202
      s=RTSP Session
      m=audio 0 RTP/AVP 0
      a=control:rtsp://audio.example.com/twister/audio.en
      m=video 0 RTP/AVP 31
      a=control:rtsp://video.example.com/twister/video
```

Začátek relace:

```
C->A: SETUP rtsp://audio.example.com/twister/audio.en RTSP/1.0
      CSeq: 1
      Transport: RTP/AVP/UDP;unicast;client_port=3056-3057

A->C: RTSP/1.0 200 OK
      CSeq: 1
      Session: 12345678
      Transport: RTP/AVP/UDP;unicast;client_port=3056-3057;
                 server_port=5000-5001

C->V: SETUP rtsp://video.example.com/twister/video RTSP/1.0
      CSeq: 1
      Transport: RTP/AVP/UDP;unicast;client_port=3058-3059

V->C: RTSP/1.0 200 OK
      CSeq: 1
      Session: 23456789
      Transport: RTP/AVP/UDP;unicast;client_port=3058-3059;
                 server_port=5002-5003
```

Unicastové přehrávání:

```
C->V: PLAY rtsp://video.example.com/twister/video RTSP/1.0
      CSeq: 2
      Session: 23456789
      Range: smpte=0:10:00-

V->C: RTSP/1.0 200 OK
      CSeq: 2
      Session: 23456789
      Range: smpte=0:10:00-0:20:00
      RTP-Info: url=rtsp://video.example.com/twister/video;
                seq=12312232;rtptime=78712811

C->A: PLAY rtsp://audio.example.com/twister/audio.en RTSP/1.0
      CSeq: 2
      Session: 12345678
      Range: smpte=0:10:00-

A->C: RTSP/1.0 200 OK
      CSeq: 2
      Session: 12345678
      Range: smpte=0:10:00-0:20:00
      RTP-Info: url=rtsp://audio.example.com/twister/audio.en;
                seq=876655;rtptime=1032181
```

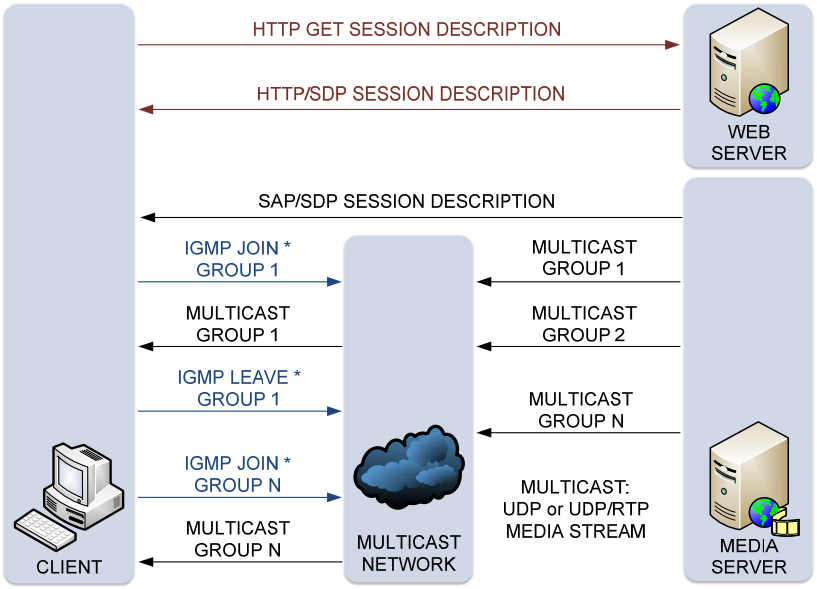
Ukončení relace:

```
C->A: TEARDOWN rtsp://audio.example.com/twister/audio.en RTSP/1.0
      CSeq: 3
      Session: 12345678

A->C: RTSP/1.0 200 OK
      CSeq: 3

C->V: TEARDOWN rtsp://video.example.com/twister/video RTSP/1.0
      CSeq: 3
      Session: 23456789

V->C: RTSP/1.0 200 OK
      CSeq: 3
```

Session Announcement Protocol (SAP) – RFC2974

Protokol SAP se používá pouze pro oznamování multicastových relací.

SAP oznamovatel pravidelně vysílá multicastové skupině na port 9875 oznamovací pakety obsahující SDP (Session Description Protocol) popis relace, která se bude konat. Příjemci, kteří chtějí znát informace o aktivní relaci, jednoduše naslouchají a přijímají tyto pakety ve stejné multicastové skupině.



Protože rychlost rozesílání SAP oznámení je nízká (min. 5 minut mezi opakovanými oznámeními o stejné relaci), proto u konferencí uvidí první příjemce všechny účastníky teprve za několik minut. K tomu, aby se zredukovali časové ztráty související s rozesíláním SAP, se doporučuje využít proxy cache. SAP proxy naslouchá všem skupinám v jejím rozsahu a udržuje tak stále aktuální seznam všech oznámených relací s dobami, kdy bylo oznámení naposledy přijaté.

IANA rezervovala SDP/SAPu multicastový rozsah adres 224.2.0.0/16.

```
 1 Packet Operation: General Service Reply
 2 SAP set #1
 3  Server Type: Unknown
 4  Server Name: NTRADCOM
 5  Network Address: 0x00000017
 6  Node Address: 0x000000000001
 7  Socket Address: 0xE885 (Unknown)
 8  Hops To Server: 1
 9 SAP set #2
10  Server Type: Unknown
11  Server Name: NTRADCOM!!!!!!!A5569B20ABE511CE9CA400004C762832
12  Network Address: 0x00000017
13  Node Address: 0x000000000001
14  Socket Address: 0x4080
15  Hops To Server: 1
```

Session Initiation Protocol (SIP) – RFC3261

Tento signalizační protokol, z aplikační vrstvy, je určen k realizaci jakéhokoliv multimediálního přenosu v IP sítích. Standardizovala organizace IETF (Intenet Emgineering Task Force) a je využívaný k vytvoření, úpravě a ukončení spojení mezi jedním nebo více účastníky. V praxi se využívá především k signalizaci telefonování po IP síti.

Základními prvky SIP systému jsou:

User Agents – jsou uživatelské koncové systémy, které implementují dvě části: klient a server. Klientská část, nazývaná UAC (User Agent Client), se používá k zahájení relace, zatímco severová část, UAS (User Agent Server), se používá pro přijmutí žádostí a vrácení odpovědí.

Network Servers – zprostředkovávají kontakt mezi volajícím a volaným a dělí se na tři typy. Registrar Server přijímá a ukládá zprávy, vztahující se k aktuálnímu umístění uživatelů ze své domény, do své databáze Location Service. Proxy Server přesměrovává přijaté žádosti k next-hop serveru nebo přímo k volanému UA. Redirect Server na přijímané žádosti generuje odpovědi, ve kterých odpovídá klientovi, na jakou alternativní URI má žádosti poslat – dále se signalizace ani hovoru neúčastní. V praxi jsou integrovány všechny tři servery na jenom stroji.

SIP definuje množství textových zpráv tzv. metod, určených ke komunikaci mezi klientem a SIP serverem:

SIP METODA	POPIS
ACK	potvrzení INVITE zprávy příjemcem
BYE	ukončení spojení
CANCEL	ukončí žádost nebo ještě nesestavené spojení
INFO	signalizuje informaci o hovoru
INVITE	žádost o sestavení spojení
MESSAGE	nese obsah právě probíhající zprávy v požadovaném tvaru
NOTIFY	obsahuje informaci o stavu zdroje
OPTIONS	žádá informaci o schopnostech serveru
PRACK	pomocná zpráva
PUBLISH	zveřejňuje stav událostí
REFER	odkazuje příjemce, aby kontaktoval třetí strany
REGISTER	registruje současné uživatelské umístění
SUBSCRIBE	žádá současný stav a aktualizace stavu ze vzdáleného uzlu
UPDATE	aktualizuje parametry spojení

UA odpovídají na tyto metody odpověďmi reprezentovanými následujícími číselnými kódy, rozdělenými do šesti skupin a částečně převzatými z protokolu HTTP:

CODE	DESCRIPTION	EXAMPLE
1XX	Infoprmational	100 – trying, 180 – ringing
2XX	Successful	200 – ok, 202 – accepted
3XX	Redirection	302 – moved temporarily, 305 – use proxy
4XX	Request Failure	403 – forbidden, 404 – not found
5XX	Server Failure	500 – server internal error, 501 – not implemented
6XX	Global Failure	603 – decline, 606 – not acceptable

Volající a volaní nejsou v SIP identifikováni jen podle telefonního čísla, ale používá se především identifikátor URI (Uniform Request Identifier) – sip:user@hostname, sip:group@hostname apod.

SIP zprávy se skládají z následujících tří částí:

1. Start Line – každá SIP zpráva začíná tímto řádkem, který je buď požadavek (Request Line) nebo odpověď (Status Line). Tyto zprávy mají následující formát:
   Request Line = <Method> <Request-URL> <SIP-Version>
   Status Line = <SIP-Version> <Status-Code> <Reason-Phase>
2. Headers – atributy, které poskytují dodatečné informace o zprávách. Mají podobnou syntaxi jako pole hlavičky v HTTP:
   <Field-Name> : <Field-Value>
3. Message Body – SDP, MIME a další definované v ITEF

Příklad zprávy INVITE:

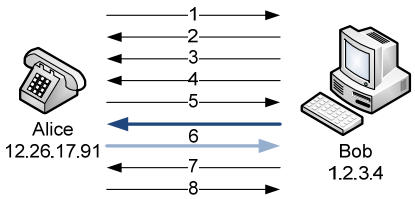
```
 1 INVITE sip:bob@biloxi.com SIP/2.0
 2 Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
 3 Max-Forwards: 50
 4 To: Bob <sip:bob@biloxi.com>
 5 From: Alice <sip:alice@atlanta.com>;tag=1928301774
 6 Call-ID: a84b4c7e66710@pc33.atlanta.com
 7 CSeq: 314159 INVITE
 8 Contact: <sip:alice@pc33.atlanta.com>
 9 Content-Type: application/sdp
10 Content-Length: 142
```

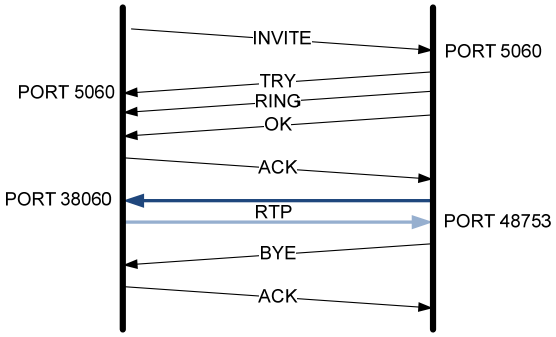
INVITE zpráva obsahuje následující atributy:

CALL-ID – globální jedinečný identifikátor spojení
CONTACT – obsahuje SIP URI volajícího, přes který ho lze přímo kontaktovat
CONTENT-LENGHT – délka zprávy v bytech
CONTENT-TYPE – popisuje tělo zprávy
CSEQ – obsahuje číslo (inkrementované pro každou událost) a název metody
FROM – obsahuje display name a SIP URI volajícího
MAX-FORWARDS – maximální počet směrování, při každém je hodnota snížena o 1, obdoba TTL
TO – obsahuje display name a SIP URI volaného, který přidává tag s náhodně vygenerovaným číslem
VIA – obsahuje IP adresu odesílatele zprávy. Tuto položku se svou IP adresou přidává každý server, který zprávu přeposílá dále

Základní navázání hovoru

Volající SIP klient zná aktuální IP adresu volaného klienta





1	**INVITE**	INVITE sip:bob@1.2.3.4 C=IN IP4 12.26.17.91 M=audio 38060 RTP/AVP 0
2	**TRY**	100 Trying
3	**RING**	180 Ringing
4	**OK**	200 OK C=IN IP4 1.2.3.4 M=audio 48753 RTP/AVP 3
5	**ACK**	ACK
6	**RTP**	Media session over RTP
7	**BYE**	BYE
8	**ACK**	200 OK

SIP response/request (over well known TCP or UDP port 5060)

Media session over RTP and UDP, port 38060, encoding: µLaw audio (AVP0)

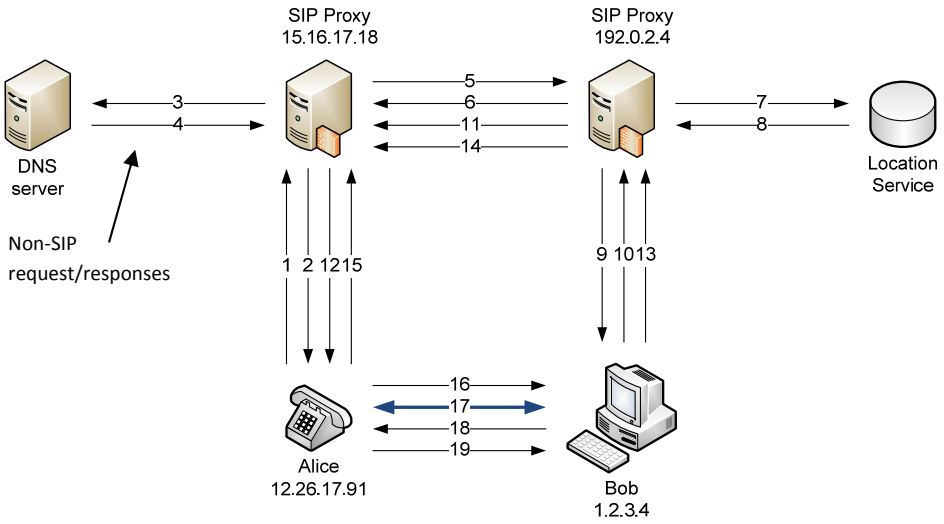
Media session over RTP and UDP, port 48753, encoding: GSM (AVP3)

INVITE metody a odpovědi obsahují SDP, který dohaduje kodeky a porty RTP. Pokud by nedošlo k dohodnutí kodeků, došlo by k ukončení relace.

Pokud se kdokoliv rozhodne změnit parametry existující relace, provede se to pomocí nové INVITE zprávy se stejným Call ID, From, To a jen SDP bude obsahovat nově navrhované parametry. Toto nastavení může druhá strana přijmout nebo odmítnout, pak spojení pokračuje podle původně dohodnutého nastavení.

Navázání hovoru přes SIP proxy servery

Volající SIP klient nezná aktuální IP adresu volaného klienta, který je v jiné doméně než volající.



1	INVITE To: sip:bob@biloxi.com
2	100 Trying
3	DNS Query: biloxi.com
4	Response: 192.0.2.4
5	INVITE To: sip:bob@biloxi.com
6	100 Trying
7	LS Query: sip:bob@biloxi.com
8	Response: sip:bob@1.2.3.4
9	INVITE To: sip:bob@biloxi.com
10	180 Ringing
11	180 Ringing
12	180 Ringing
13	200 OK
14	200 OK
15	200 OK
16	ACK
17	Media session over RTP
18	BYE
19	200 OK

V tomto případě je ukončení spojení realizováno přímo mezi klienty, ale může se provádět i přes proxy servery, kvůli přesnějšímu logování.

Tato situace také předpokládá, že je Bob zaregistrován na Registrar Serveru spravujícím jeho doménu. Registrace je provedena buď staticky, nebo jí Bob provádí dynamicky zasláním zprávy

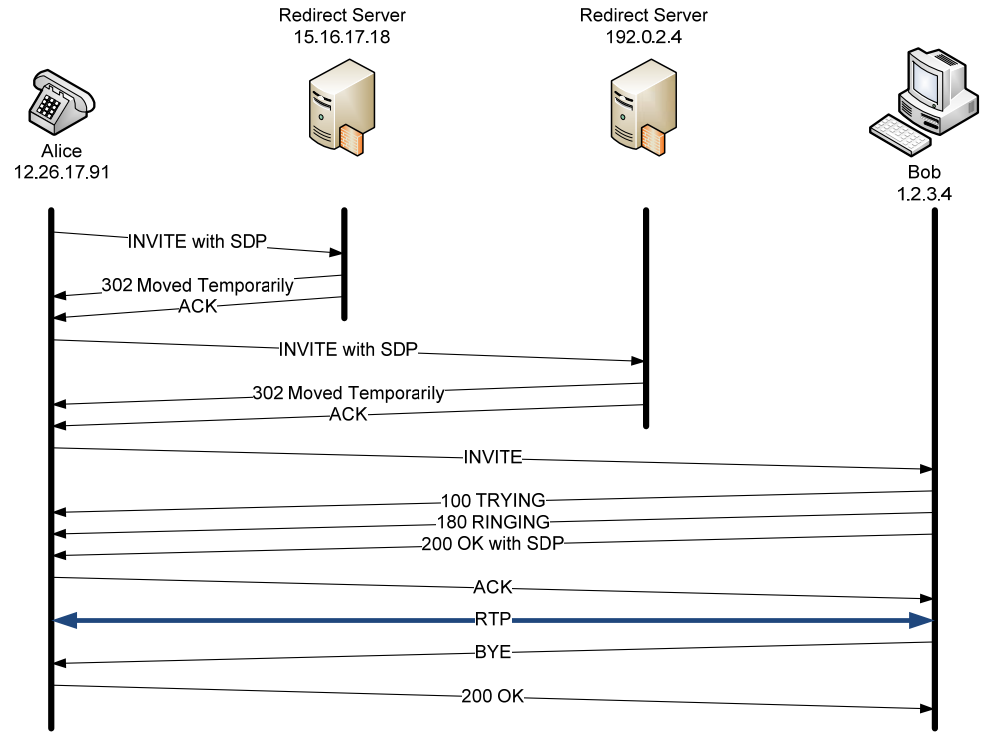
REGISTER na Registrar Server, který si z ní uloží jeho aktuální údaje do databáze Location Service.

```
 1 REGISTER sip:registrar.biloxi.com SIP/2.0
 2 Via: SIP/2.0/UDP bobspc.biloxi.com:5060;branch=z9hG4bKnashds7
 3 Max-Forwards: 70
 4 To: Bob <sip:bob@biloxi.com>
 5 From: Bob <sip:bob@biloxi.com>;tag=456248
 6 Call-ID: 843817637684230@998sdasdh09
 7 CSeq: 1826 REGISTER
 8 Contact: <sip:bob@192.0.2.4>
 9 Expires: 7200
10 Content-Length: 0
```

Zpráva REGISTER má povinné následující atributy:

CALL-ID – jedinečný identifikátor SIP dialogu
CSEQ – identifikátor žádosti, inkrementující se po každé žádosti
FROM – obsahuje AOR (Address Of Record) uživatele zodpovědného za registraci (bývá shodné s TO)
REQUEST-URI – obsahuje název domény databáze Location Service, u které se provádí registrace
TO – obsahuje AOR uživatele provádějícího registraci

Navázání hovoru přes SIP redirect servery



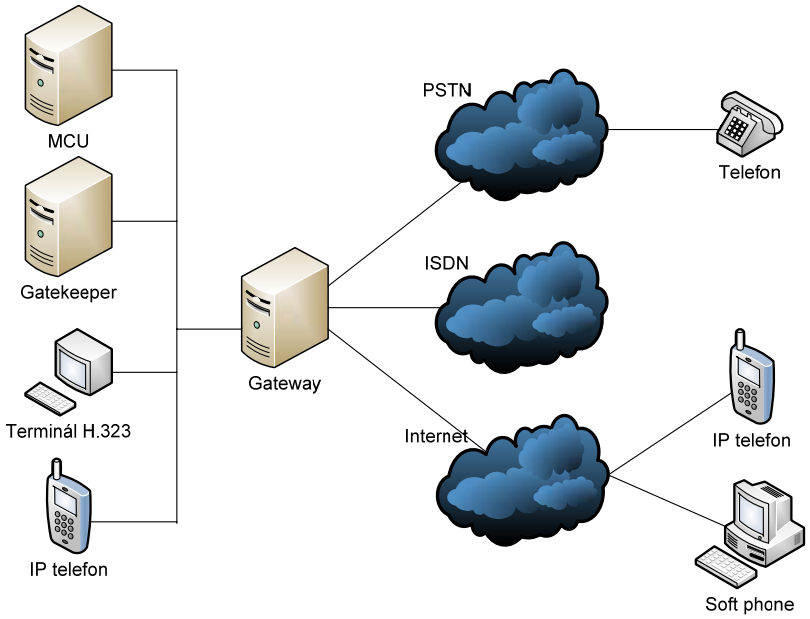
H.323

H.323 je doporučení ITU-T (International Telecommunications Union – Telecommunication Standardization Sector), které definuje protokoly pro audio-vizuální relace komunikace v jakékoli paketové síti. Přizpůsobení k H.323 umožňuje uživatelům aplikací od různých dodavatelů komunikovat, aniž by se zajímali o jejich vzájemnou kompatibilitu.

Toto doporučení poskytuje technické požadavky pro multimediální komunikaci v sítích, které nenabízejí žádné řízení kvality provozu (originální popis H.323 je Visual Telephone System and Equi-pment for Local Area Network which Provide a non Guaranteed Quality of Service). První verze vnikla v roce 1996 a původně byla vyvinuta pro multimediální konference, ale později byla doplněna o VoIP. Od verze 2 tedy navíc definuje např. rychlé navazování spojení, identifikaci volajícího, přesměrovávání hovorů, integraci datových služeb a podporuje také zabezpečení. Každá následující verze obsahuje optimalizace a často i nové protokoly. Zatím poslední verze z června roku 2006 má pořadové číslo 6.

Standard zahrnuje oba druhy komunikace – point-to-point a multipoint.

H.323 definuje čtyři základní logické prvky – Terminals, Gateways, Gatekeepers and MCUs (Multipoint Control Units), z nichž jen Gatekeepers nejsou označovány jako koncové body.



Terminal – je klientské koncové zařízení poskytující v reálném čase obousměrnou komunikaci.

Gateway – hraniční prvek, který umožňuje obousměrnou komunikaci v reálném čase se sítěmi, které nepodporují standard H.323. Umožňuje hromadné připojení k heterogením prostředím jako jsou např. Internet, ISDN, PSTN apod.

MCU – umožňuje třem a více účastníkům účast na multipoint konferencích. Skládá se z povinného MC (Multipoint Controller), který se stará o řídící a kontrolní funkce a z volitelného MP (Multipoint Processor), který zpracovává audio, video a datové toky.

Gatekeeper – chová se jako centrální bod pro všechny koncové body uvnitř jeho zóny, pro které povinně poskytuje Admission Control, Bandwith Control, Zone Management, volitelně pak ještě Address Translation, Call Authorization, Call Management, Call Signaling a Bandwith Management. Tento prvek je v síti nepovinný, pokud ale existuje, jsou terminály povinné přes něj komunikovat.

H.323 zahrnuje především následující signalizační standardy

H.225.0-Q.931 – definuje signalizaci (sestavení, udržování a ukončení spojení) mezi dvěma koncovými body. Jelikož zprávy tohoto protokolu neobsahují všechny potřebné položky VoIP signalizace, využívá se tzv. binárního zapouzdřování. Zprávy tohoto protokolu se využívají k transportu protokol TCP na koncová zařízení naslouchají na portu 1720.

H.225.0-RAS (Registration Admission Status) – určuje signalizaci mezi koncovým bodem a gatekeeprem nebo mezí dvěma gatekeepery. Umožňuje koncovému bodu využívat služby gatekeeperu a gatekeeperu umožňuje řídit terminály. Jako transportní protokol využívá UDP a gatekeeper naslouchá na portu 1719 nebo pro multicast na 1718. Multicastová adresa pro komunikaci mezi gatekeepery je 225.0.1.41.

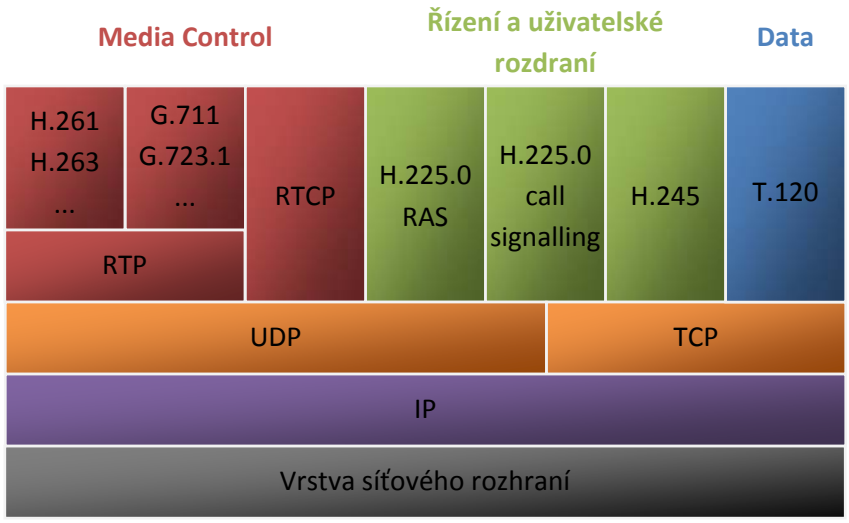
H.245 – zahrnuje signalizaci mezi dvěma koncovými body, vyměňují se jeho pomocí informace o vlastnostech terminálů a umožňuje řízení datového toku. Tento protokol využívá TCP spojení, proto hovorová signalizace mezi dvěma terminály, vyžaduje dva TCP kanály.

T.120 – zahrnuje síťově nezávislé protokoly pro komunikaci v reálném čase s bezchybným přenosem dat. H.323 používá T.120 jen pro datovou komunikaci – přenos souborů a jejich sdílení.

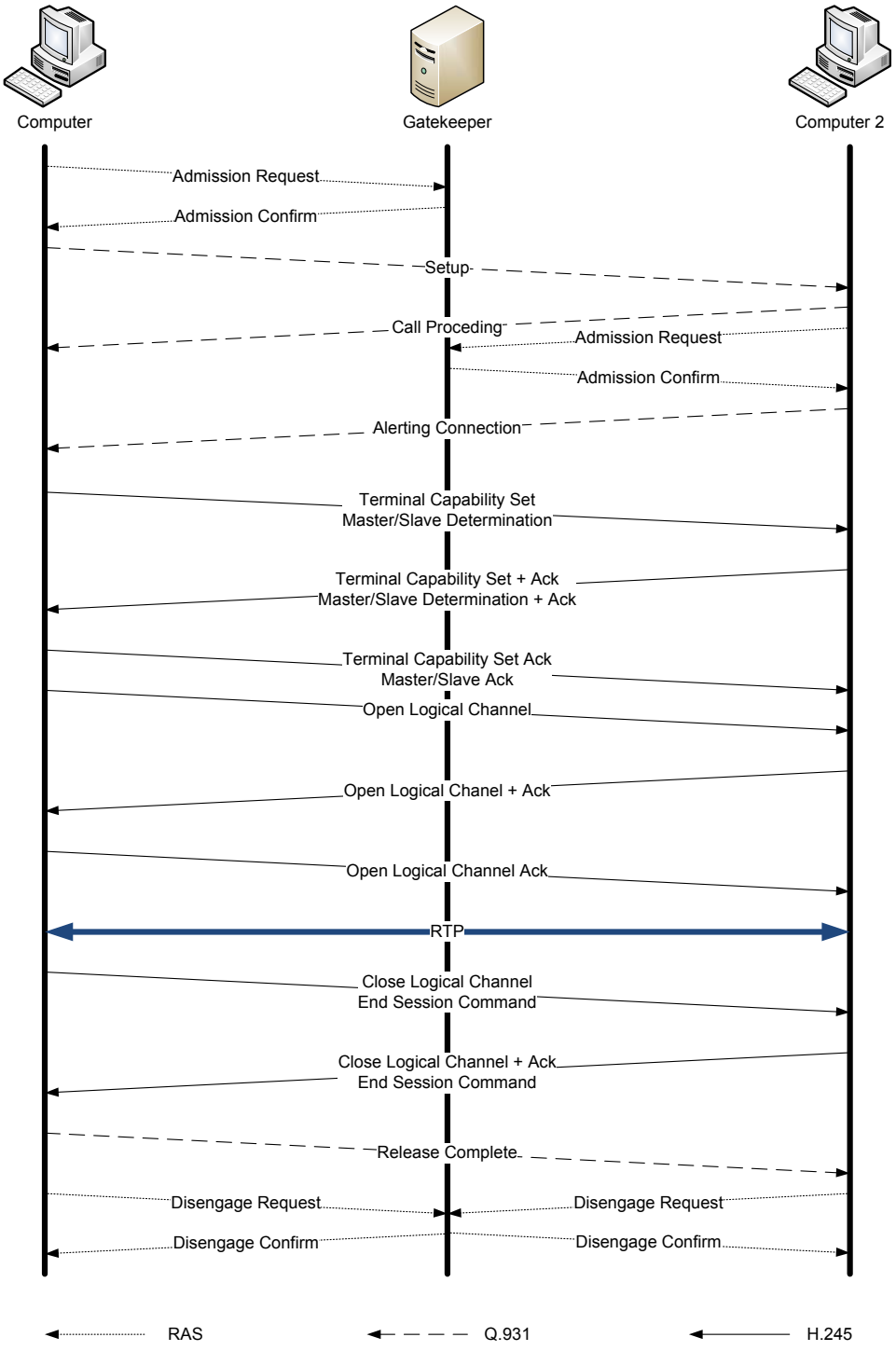
H.711, H.723.1, H.726, H.728, H.729 – zvukové kodeky

H.261, H.263, H.264 – video kodeky

H.323 over IP stack



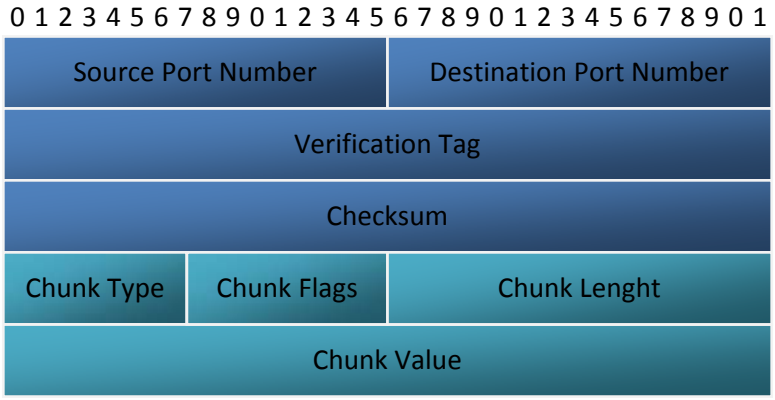
Typické H.323 navázání hovoru



Stream Control Transmission Protocol (SCTP) – RFC2960

Je transportní protokol, který po asociaci spojení, dokáže přenášet řadu navzájem nezávislých streamů. U každého proudu protokol garantuje doručení dat ve správném pořadí. SCTP tedy lze přirovnat k několika souběžným TCP spojením, proto výpadek v jednom proudu neovlivní proudy ostatní.

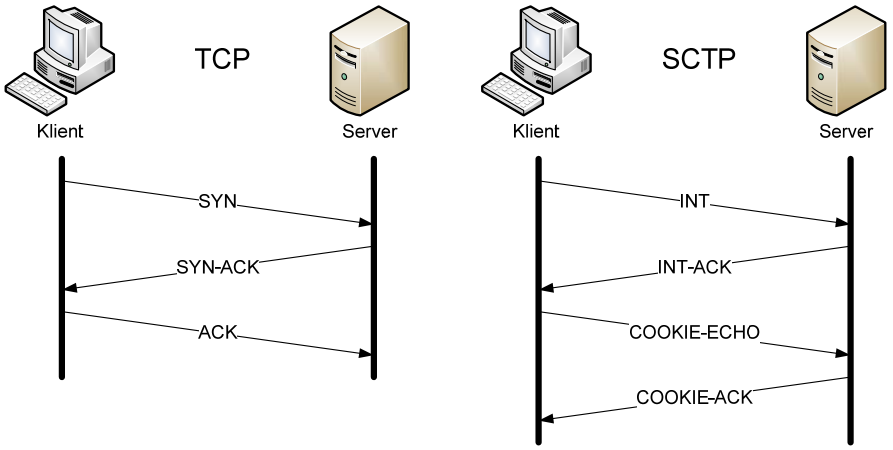
K potvrzování SCTP využívá pořadová čísla TSN (Transmission Sequence Number) k číslování jednotlivých datových kousků (Chunks) a SSN (Stream Sequence Number) určuje číslování v rámci jednoho proudu. Díky potvrzování umí ohlásit a vyžádat si chybějící kusy dat. Slouží k tomu speciální chunk nazvaný selektivní potvrzení, obsahující nejvyšší pořadové číslo přijatého datového kousku a zároveň popisuje chybějící úseky dat.



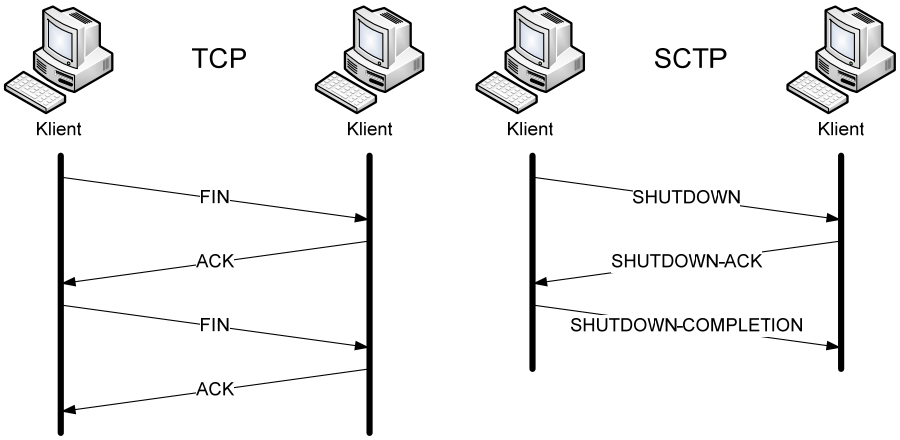
Multihoming – když má komunikující uzel několik IP adres, je pro odesílání dat určena jedna brána jako primárnía na ní jsou pak odesílána data. Pro opakování je vybrána brána jiná, stejně jako když jsou s primární branou častější problémy s dostupností.

SCTP obsahuje ověřovací a potvrzovací mechanismy, které komplikují DoS.

Proces vytvoření SCTP asociace začíná tím, že jeden klient pošle serveru žádost o navázání asociace. Server na jeho základě vytvoří potřebná data, zašifruje je a pošle klientovi jako součást své odpovědi (tzv. cookie). Ještě stále si však nic nerezervuje. Klient vzápětí potvrdí svou žádost a přibalí cookie odeslané serverem, jinak bude žádost ignorována. Teprve pokud se klient prokáže platným cookie, vytvoří server odpovídající datové struktury, prohlásí asociaci za otevřenou a pošle klientovi potvrzení.



Ukončení asociace je podobné TCP. Jedna strana pošle žádost o ukončení – provede tzv. polouzavření. Od této doby již nesmí posílat žádná data, ale musí potvrzovat příjem. Až se protějšek vypovídá, také provede polouzavření a asociace bude ukončena.



Media Gateway Control Protocol (MGCP) – RFC2705

MGCP je signalizační protokol definující komunikaci mezi CA (Call Agents) a MG (Media Gateway). V sítích, kde se používají protokoly H.323 a SIP, protokol MGCP řídí brány a protokoly SIP nebo H.323 řídí hovory.

MGCP realizuje řídící rozhraní MG jako sadu transakcí, které se skládají z příkazu a z povinné odpovědi. Existuje osm následujících typů příkazů:

PŘÍKAZ	SMĚR	POPIS
CreateConnection	MGC → MG	příkaz pro vytvoření spojení s koncovým bodem se specifickou IP adresou a portem. Příkaz posílá i druhý koncový bod. Pokud je žádost branou úspěšně potvrzena, pak je vráceno ConnectionID jedinečně identifikující spojení.
ModifyConnection	MGC → MG	upravuje parametry existujícího spojení, má téměř stejné parametry jako příkaz CreateConnection
DeleteConnection	MGC ↔ MG	ukončuje spojení, odpověď zahrnuje statistiky tohoto spojení
NotificationRequest	MGC → MG	žádá bránu o poslání specifických událostí vyskytujících se v koncovém bodě
Notify	MGC ← MG	odpověď na NotificatoinRequest, zahrnuje seznam vyskytujících se sledovaných událostí
AuditEndpoint	MGC → MG	určuje stav jednoho nebo více koncových bodů
AuditConnection	MGC → MG	zjišťuje parametry související se spojením
RestartInProgress	MGC ← MG	signalizuje, že jeden nebo skupina koncových bodů je nefunkční

Všechny příkazy a odpovědi jsou složeny z nadřazené hlavičky, volitelně následovanými popisem relace. Tyto hlavičky jsou navíc od popisu relace odděleny prázdným řádkem (v příkladu řádek číslo 8).

```
1 Command /Request Message:
2 Header:
3 Command/Request Type: Modify Connection Command
4 Transaction Identifier: ARCH
5 Endpoint Name: *
6 Protocol Version: HTTP/1.1
7 OST: 239.255.255.250:1900
8
```

K sladění příkazů a odpovědí MGCP využívá transakční identifikátor nabývající hodnot 1 až 999 999 999 a nemůže tedy použít stejný transakční identifikátor dříve, než za tři minuty po dokončení předcházejícího příkazu, ve kterém byl identifikátor použit.

MGCP pakety jsou většinou zabaleny v UDP paketu s portem 2427 nebo v TCP paketu.

Session Description Protocol (SDP) – RFC4566

SDP je protokol popisující inicializační parametry multicastových relací.

Relační popis vyjádřený v SDP je krátký uspořádaný popis jména, účelu relace, protokolů, kodeků, časovacích a přenosových informací, které budou požadovány k tomu, aby se účastník rozhodl, zda bude chtít nebo zda se bude moci relace zúčastnit.

SDP obsahuje globální hlavičku, která popisuje vysílání jako celek, každý další řádek popisuje jeden parametr médií. Popisovače médií začínají řádkem m= a pokračují až do následujícího řádku m=

```
 1 v=0
 2 o=jdoe 2890844526 2890842807 IN IP4 10.47.16.5
 3 s=SDP Seminar
 4 i=A Seminar on the session description protocol
 5 u=http://www.example.com/seminars/sdp.pdf
 6 e=j.doe@example.com (Jane Doe)
 7 c=IN IP4 224.2.17.12/127
 8 t=2873397496 2873404696
 9 a=recvonly
10 m=audio 49170 RTP/AVP 0
11 m=video 51372 RTP/AVP 99
13 a=rtpmap:99 h263-1998/90000
```

Na předchozím příkladě je vidět, že SDP je pouze jednoduchý textový popis relace, který musí zprostředkovat dostatek informací k uskutečnění relace. Používá se v SAP, SIP, H.323 i RTSP.

Přehled všech atributů (atributy označené * jsou volitelné, ostatní jsou povinné):

Session description:	v= (protocol version)
	o= (originator and session identifier)
	s= (session name)
	i=* (session information)
	u=* (URI of description)
	e=* (email address)
	p=* (phone number)
	c=* (connection information -- not required if included in all media)
	b=* (zero or more bandwidth information lines)
	z=* (time zone adjustments)
	k=* (encryption key)
	a=* (zero or more session attribute lines)
Time description:	t= (time the session is active)
	r=* (zero or more repeat times)
Media description:	m= (media name and transport address)
	i=* (media title)
	c=* (connection information -- optional if included at session level)
	b=* (zero or more bandwidth information lines)
	k=* (encryption key)
	a=* (zero or more media attribute lines)

Skinny Call Control Protocol (SCCP)

SCCP je signalizační protokol firmy Cisco Systems, který je používán ke komunikaci mezi skinny klientem a softwarovým Cisco CallManagerem, který nahrazuje PBX. Mezi skinny klienty patří jak hardwarové Cisco telefony z řady 7900, tak i softwarové řešení Cisco IP Communicator, ale protokol je podporován i dalšími výrobci.

SCCP definuje jednoduchou a snadno použitelnou architekturu, zatímco systémy vyhovující H.323 doporučení jsou složitější a dražší. I H.323 proxy může komunikovat s klientem používajícím SCCP. Skinny zprávy jsou přenášené protokolem TCP na portu 2000.

Příklad zprávy:

```
1 Message Lenght: 96
2 Message Type: 0x00000000
3 Message ID: 0x00000020 Station Alarm Message
4 Alarm Severity: 2
5 Alarm Message: Name=SEP0010EB004597   Load= 3.00
  Parms=Status/IPaddr.................
6 Parm 1: 2048
7 Parm 2: 1341660332
```

Přehled zpráv SCCP žádostí a odpovědí

Code	Station Message ID Message
0x0000	Keep Alive Message
0x0001	Station Register Message
0x0002	Station IP Port Message
0x0003	Station Key Pad Button Message
0x0004	Station Enbloc Call Message
0x0005	Station Stimulus Message
0x0006	Station Off Hook Message
0x0007	Station On Hook Message
0x0008	Station Hook Flash Message
0x0009	Station Forward Status Request Message
0x11	Station Media Port List Message
0x000A	Station Speed Dial Status Request Message
0x000B	Station Line Status Request Message
0x000C	Station Configuration Status Request Message
0x000D	Station Time Date Request Message
0x000E	Station Button Template Request Message
0x000F	Station Version Request Message
0x0010	Station Capabilities Response Message
0x0012	Station Server Request Message
0x0020	Station Alarm Message
0x0021	Station Multicast Media Reception Ack Message
0x0024	Station Off Hook With Calling Party Number Message
0x22	Station Open Receive Channel Ack Message
0x23	Station Connection Statistics Response Message
0x25	Station Soft Key Template Request Message
0x26	Station Soft Key Set Request Message

```
0x27     Station Soft Key Event Message
0x28     Station Unregister Message
0x0081   Station Keep Alive Message
0x0082   Station Start Tone Message
0x0083   Station Stop Tone Message
0x0085   Station Set Ringer Message
0x0086   Station Set Lamp Message
0x0087   Station Set Hook Flash Detect Message
0x0088   Station Set Speaker Mode Message
0x0089   Station Set Microphone Mode Message
0x008A   Station Start Media Transmission
0x008B   Station Stop Media Transmission
0x008F   Station Call Information Message
0x009D   Station Register Reject Message
0x009F   Station Reset Message
0x0090   Station Forward Status Message
0x0091   Station Speed Dial Status Message
0x0092   Station Line Status Message
0x0093   Station Configuration Status Message
0x0094   Station Define Time & Date Message
0x0095   Station Start Session Transmission Message
0x0096   Station Stop Session Transmission Message
0x0097   Station Button Template Message
0x0098   Station Version Message
0x0099   Station Display Text Message
0x009A   Station Clear Display Message
0x009B   Station Capabilities Request Message
0x009C   Station Enunciator Command Message
0x009E   Station Server Respond Message
0x0101   Station Start Multicast Media Reception Message
0x0102   Station Start Multicast Media Transmission Message
0x0103   Station Stop Multicast Media Reception Message
0x0104   Station Stop Multicast Media Transmission Message
0x105    Station Open Receive Channel Message
0x0106   Station Close Receive Channel Message
0x107    Station Connection Statistics Request Message
0x0108   Station Soft Key Template Respond Message
0x109    Station Soft Key Set Respond Message
0x0110   Station Select Soft Keys Message
0x0111   Station Call State Message
0x0112   Station Display Prompt Message
0x0113   Station Clear Prompt Message
0x0114   Station Display Notify Message
0x0115   Station Clear Notify Message
0x0116   Station Activate Call Plane Message
0x0117   Station Deactivate Call Plane Message
0x118    Station Unregister Ack Message
```

Quality of Service (QoS – RFC2212)

Kvalita služeb je řízení datových toků v síti. Datové sítě byly původně navrženy pro tzv. "best effort" službu, která má nejlepší snahu přenést data nejkratší cestou od zdroje k cíli v nejkratší době a využít pro přenos maximum dostupného pásma. Protože ale nelze předvídat nároky ostatních aplikací, může docházet dlouhodobě i krátkodobě k přetížení sdílených linek. Proto je na síťových prvcích typu směrovač k dispozici klasifikace paketů a jejich prioritizace ve výstupních frontách. Tato služba zamezuje zahlcování sítě, tak že zajišťuje uživatelům jednotlivých služeb definovanou kvalitu, to znamená, že síť rozpoznává typy datového provozu (VoIP, VoD, HTTP apod.) a splňuje jejich požadavky na ztrátovost, zpoždění, pravidelnost apod.

Ztrátovost paketů

Ztrátovost paketů určuje, kolik procent paketů nedorazí od odesílatele k příjemci. Ke ztrátě může dojít při zatížení sítě v důsledku dočasného přetížení některé z komponent komunikační trasy, například po vyčerpání kapacity vyrovnávacích pamětí, přetížení procesoru směrovače a podobně. Důležitá i dynamika ztrátovosti (zda se ztráty vyskytují ve shlucích).

Zpoždění (Latence)

Zpoždění je čas potřebný k přenosu paketu od odesílatele k příjemci.

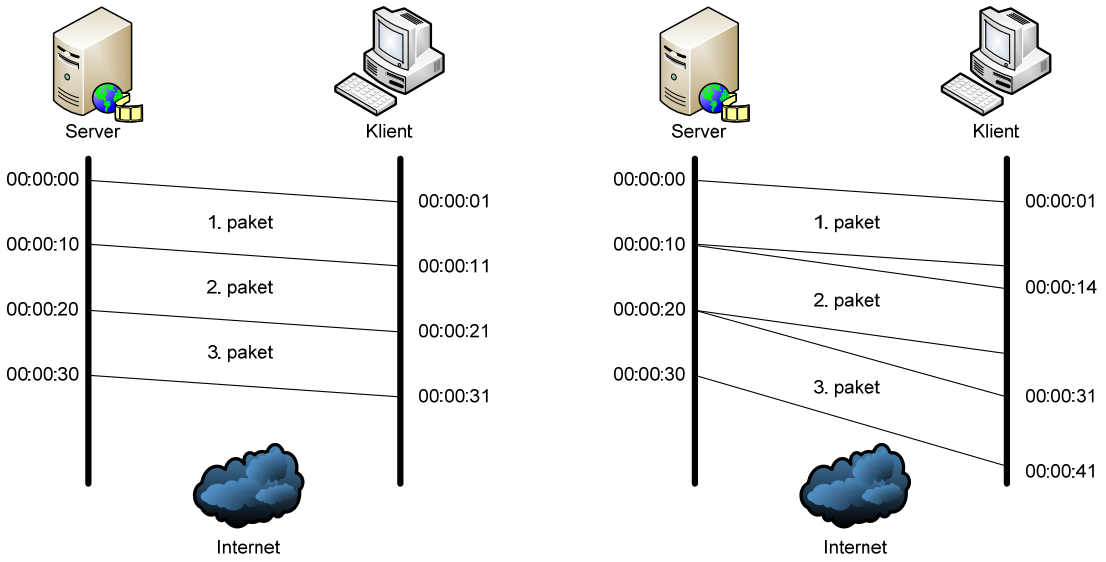
Propagační zpoždění – čas potřebný k cestě dat z jednoho konce sítě na druhý. Je způsobeno konečnou rychlostí šíření signálu po přenosovém médiu.
Paketizační zpoždění – je čas potřebný pro převod analogového signálu do digitálního a do rámců a jeho zpětný převod do analogového signálu.
Jitter buffer zpoždení – zpoždění způsobené přijímačem uložením jednoho nebo více datagramů, tak aby výsledné zpoždění bylo konstantní.

Rychlost linky (kbps)	Velikost fragmentu (B)					
	64	128	256	512	1024	1500
64	8	16	32	64	128	187,5
128	4	8	16	32	64	93,8
256	2	4	8	16	32	46,9
512	1	2	4	8	16	23,4
1024	0,5	1	2	4	8	11,7

Z tabulky je vidět, že z hlediska velikosti zpoždění jsou výhodné malé velikosti fragmentů, které ale způsobují větší zatížení sítě (menší rozdíl mezi velikostí hlavičky a daty, které paket obsahuje). Rychlost linky také ovlivňuje hodnotu patetizačního zpoždění.

Pravidelnost (Jitter)

Pravidelnost určuje, jak se mění zpoždění jednotlivých datagramů během přenosu. Tato vlastnost je pro multimediální přenosy často důležitější než absolutní hodnota zpoždění. Vysílač posílá datagramy v pravidelných intervalech. V ideálním případě by přijímač dostával datagramy také v pravidelných časových okamžicích (velikost jitteru by byla nulová).



Protože různá zařízení datagramy v datové síti zpomalují (vyrovnávací paměti na směrovačích, různé cesty sítí), proto některé datagramy přijdou dříve jiné později. Možnost jak potlačit proměnlivost příchodu datagramů je vložit na straně přijímače, mezi síťovou vrstvu a multimediální aplikaci, jitter buffer.

Implementace QoS

V současné době existují dvě hlavní implementace QoS v počítačových sítích – integrované služby (Integrated Services – INTSERV) a rozlišované služby (Differentiated Services – DIFFSERV).

Intserv – RFC1633

Aplikace oznámí počítačové síti své požadavky na přenos dat, například určitou minimální průchodnost a určité maximální zpoždění. Počítačová síť ověří, zda je k dispozici dostatek prostředků pro uspokojení požadavku a rozhodne, zda požadavkům vyhoví. V případě, že síť nemůže požadavkům vyhovět, spojení není provedeno a aplikace se může rozhodnout, zda požádá o méně náročné QoS počítačové sítě. Pokud požadavkům vyhoví, přes rezervační protokoly (např. RSVP) počítačová síť informuje ostatní komponenty (směrovače, přes které bude probíhat spojení), aby mohly pro dané spojení rezervovat odpovídající objem prostředků.

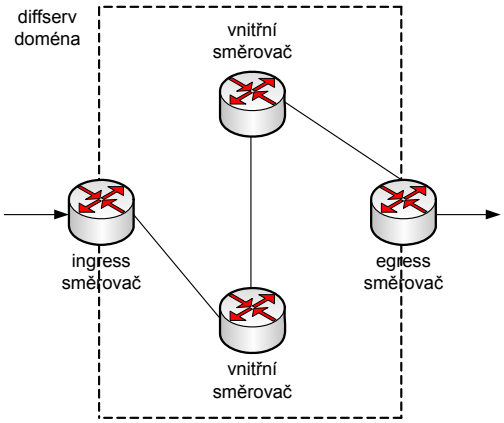
Při stále se zvyšujících rychlostech průchodu paketů směrovači je třeba maximálně zjednodušit zpracování těchto paketů a minimalizovat objem stavové informace (rezervace určité QoS), kterou musí směrovače o jednotlivých spojeních udržovat.

Protože mnoho interaktivních aplikací nepotřebuje nutně zajistit určitou konkrétní průchodnost nebo minimální zpoždění (často stačí zajistit, že parametry nebudou výrazně zhoršeny vlivem jiné současně probíhající komunikace), a protože je tento přístup příliš restriktivní a jeho implementace přináší velkou časovou režii, proto se v poslední době spíše prosazuje druhá implementace QoS – rozlišované služby.

Diffserv – RFC2475

V tomto případě aplikace neoznamuje předem počítačové síti své požadavky na QoS a směrovače tudíž neudržují žádnou stavovou informaci o jednotlivých spojeních. U této implementace QoS je každý paket vstupující do počítačové sítě označen značkou, která určuje následné zacházení s tímto paketem. Toto označování probíhá pouze na vstupu do počítačové sítě. Během přenosu sítí si další směrovače jen přečtou tuto značku, která určí následné zacházení s paketem. Počet těchto značek je relativně malý (obvykle jednotky, maximálně desítky).

Rozlehlé počítačové sítě tvoří obvykle sítě menšího rozsahu a jsou řízeny jiným subjektem (různé možnosti zpracování paketů s ohledem na požadované QoS). Proto je taková rozlehlá síť rozdělena na oblasti se samostatnou správou rozlišovaných služeb – diffserv domény. Pakety vstupují do diffserv domény přes tzv. ingress směrovače, prochází přes vnitřní směrovače diffserv domény a vystupují přes tzv. egress směrovače.



Jsou-li dvě diffserv domény propojeny jedním směrovačem, pracuje egress směrovač jedné diffserv domény zároveň jako ingress směrovač druhé diffserv domény a plní i opačné funkce pro pakety procházející v opačném směru.

Klasifikace paketů (označení značkami) probíhá na ingress směrovači a to jak při vstupu paketů do sítě, tak i při přechodu z jedné diffserv domény do jiné. Výběr značky při vstupu paketu do sítě může být proveden na základě protokolu, IP adresy odesílatele a adresáta, čísel portů a dalších kriterií, včetně výsledků měření dynamických vlastností přicházejících dat. Pakety mohou být klasifikovány již aplikací posílající pakety do sítě a první ingress směrovač může tuto klasifikaci zachovat nebo ji změnit.

Nejčastější je implementace diffserv je na úrovni síťové vrstvy IP protokolu, kde je značka obsažena v osmibitovém poli označeném DS (Differentiated Services – RFC2474), které je uloženo v místě určeném pro pole ToS (Type Of Service) hlavičky protokolu IPv4.

Pole DS se skládá ze dvou částí – šestibitové DSCP (Differentiated Services CodePoint) a dvoubitové CU (Currently Unused).

DSCP může obsahovat až 64 tříd (2^6) a má tři rozsahy:
- xxxxx0 – standardní akce
- xxxx11 – experimentální užití
- xxxx01 – EXP/LU – budoucí využití

Pokud je hodnota QoS uložena v tříbitovém poli precedence v ToS, pak obsahuje osm následujících tříd:

000 – Route	100 – Flash Override
001 – Priority	101 – CRITIC/ECP
010 – Immediate	110 – Internetwork Control
011 – Flash	111 – Network Control

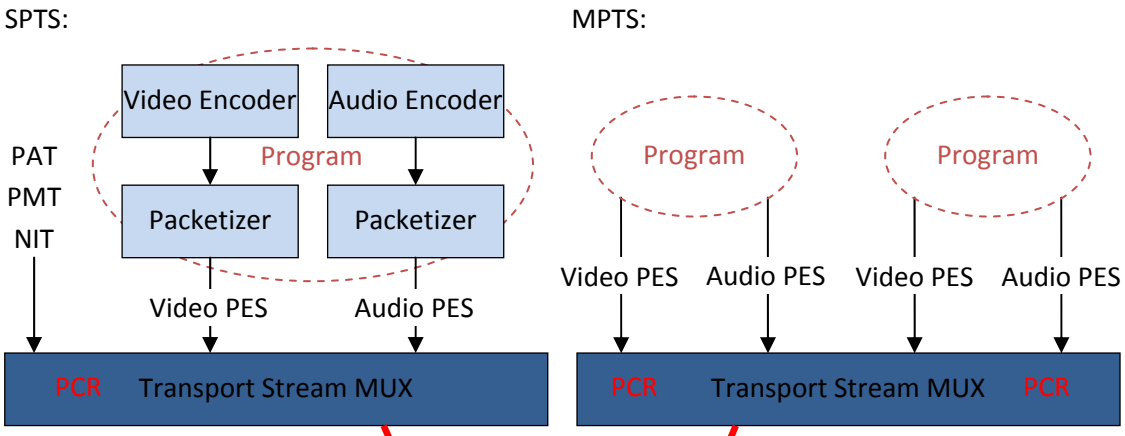
MPEG-2 over IP protokol

Single Program Transport Stream (SPTS)

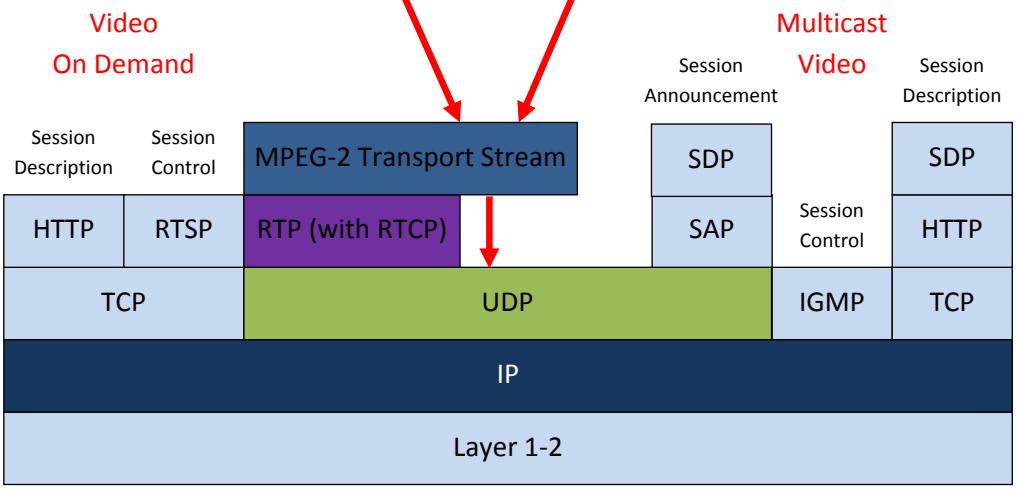
Jednotlivý multimediální tok nebo televizní program se skládá ze základních proudů (ES – Elementary Steram) audio-video toků se společnou časovou základnou. Tato časová základna je vložená v PCR (Program Clock Reference) poli základních streamů (obvykle video ES).

Multiple Program Transport Stream (MPTS)

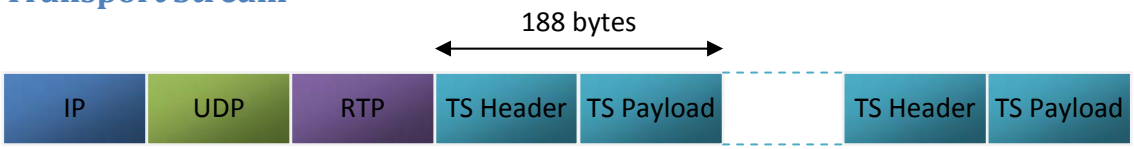
Dva nebo více SPTS proudů jsou společně slučovány a posílány jako jeden transportní stream. Každý SPTS může mít vlastní časovou základnu a výsledný MPTS nese PCR pole pro každý stream – každý stream je oddělen PID polem.



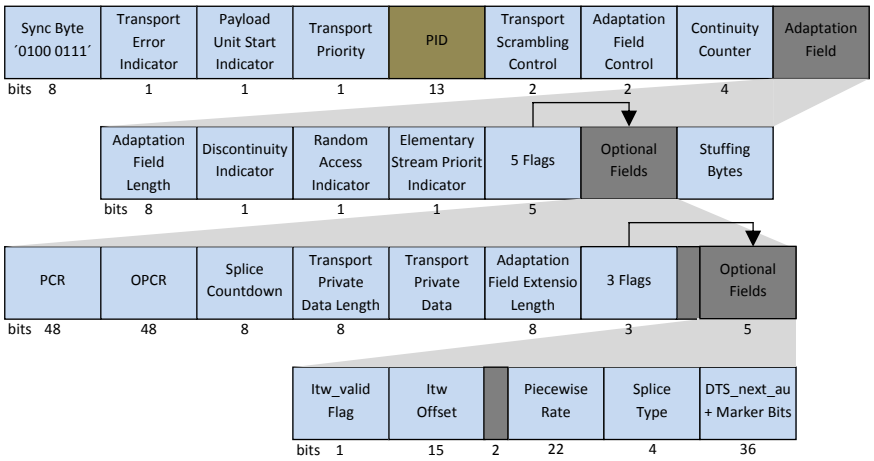
Protocol Stack



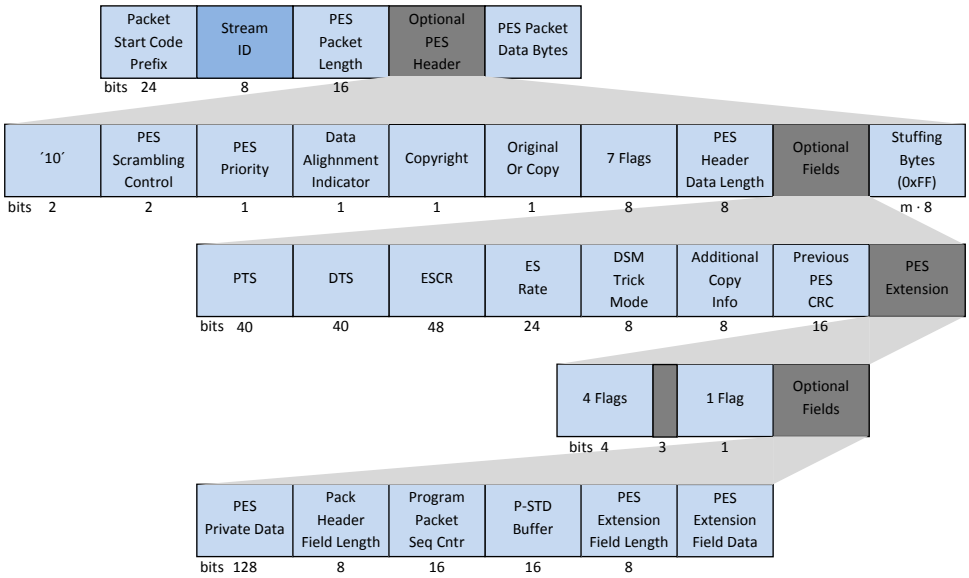
Transport Stream



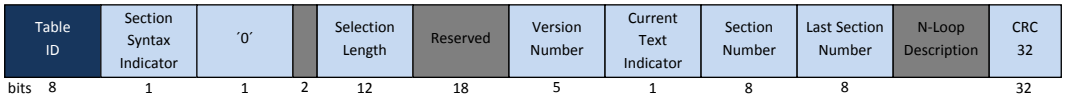
Transport Stream Packet Header



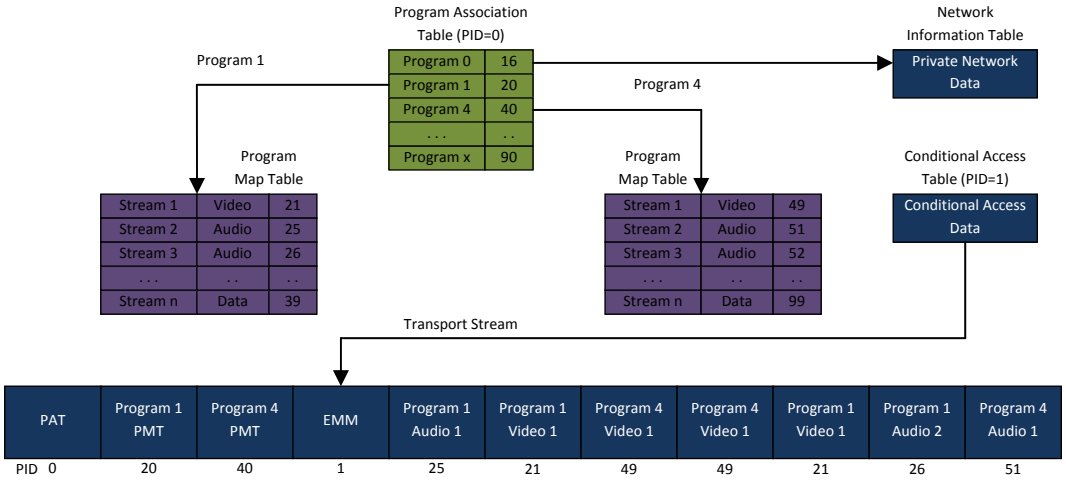
Packetized Elementary Stream Packet



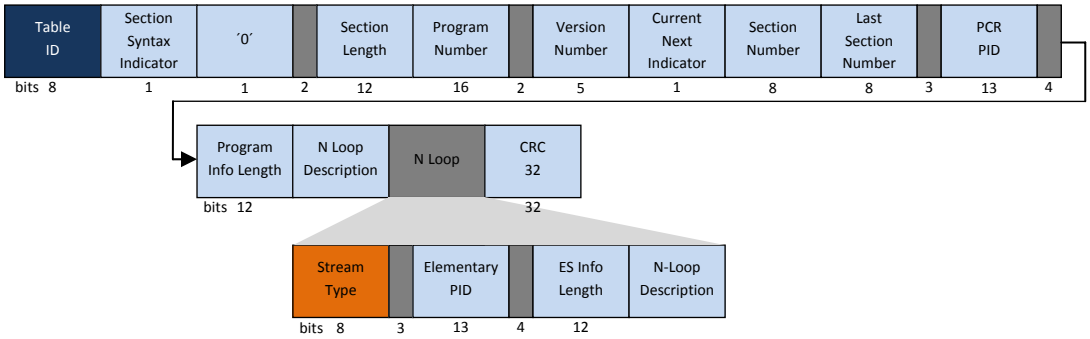
Transport Stream Description Section



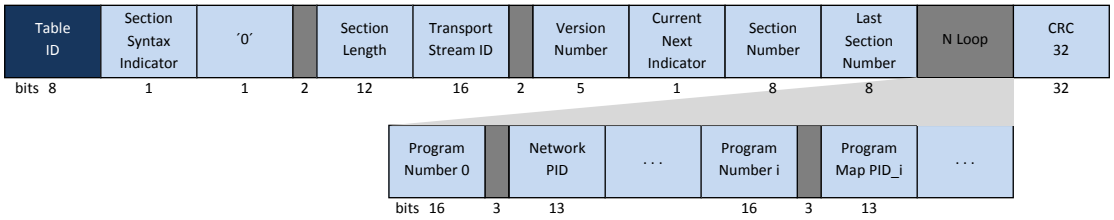
Program Tables Overview



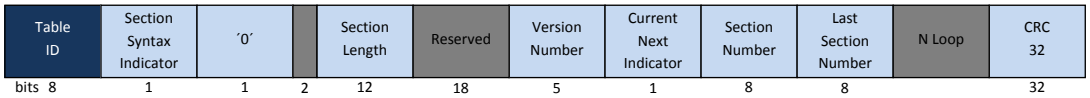
Program Map Table



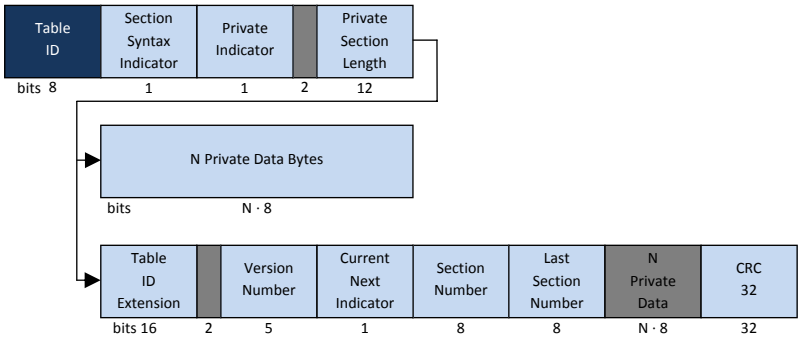
Program Association Table



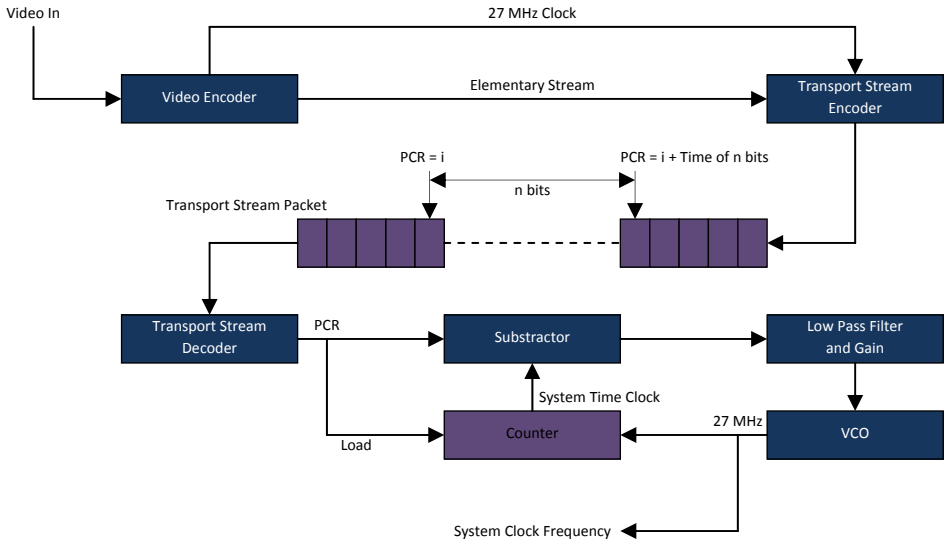
Conditional Access Section



Private Section



Clock Distribution (PCR)



Assignments

PID Assignments			
0x0000*	Program Association Table	**0x0010-**	Network_PID
0x0001*	Conditional Access Table	**0x1FFE***	Program_Map_PID
0x0002	Transport Stream		Elementary PID or other purposes
	Description Table	**0x1FFF**	Null Packet
0x0003-	Reserved		
0x000F			

Stream ID Assignments			
0xBC	Program Stream Map	**0xF3**	ISO/IEC_13522_stream
0xBD	Private Stream 1	**0xF4**	ITU-T Rec. H.222.1 Type A
0xBE	Padding Stream 1	**0xF5**	ITU-T Rec. H.222.1 Type B
0xBF	Private Stream 2	**0xF6**	ITU-T Rec. H.222.1 Type C
110xxxxx	ISO/IEC: 13818-3 or 11172-3	**0xF7**	ITU-T Rec. H.222.1 Type D
	or 13818-7 or 14496-3 Audio	**0xF8**	ITU-T Rec. H.222.1 Type E
	Stream Number x xxxx	**0xF9**	Ancillary_stream
0xExxxx	ITU-T Rec. H.262, ISO:13818-2	**0xFA**	ISO/IEC
	or 11172-2 or 14496-2 Video		14496-1_SL-packetized_stream
	Stream Number xxxx	**0xFB**	ISO/IEC 14496-1_FlexMux_stream
0xF0	ECM_stream	**0xFC-**	Reserved Data Stream
0xF1	EMM_stream	**0xFE**	
0xF2	ITU-T Rec. H.222.0, ISO:13818-1	**0xFF**	Program_stream_directory
	AnnexA or 13818-6_DSMCC_stre		

Table ID Assignments			
0x00	Program Association Section	**0x06-0x37**	ITU-T Rec. H222.0,
0x01	Conditional Access Section		ISO/IEC 13818-1 Reserved
0x02	TS Program Map Section	**0x38-0x3F**	Defined in ISO/TEC 13818-6
0x03	TS Description Section	**0x40-0xFE**	User Private
0x04	ISO/IEC 14496 Scene Desc. Section	**0xFF**	Forbidden
0x05	ISO/IEC 14496 Object Desc. Section		

Stream Type Assignments			
0x00	ITU-T, ISO/IEC Reserved	**0x0E**	ITU-T Rec. H.222.0, ISO/IEC 13818-1
0x01	ISO/IEC 11172 Video		Auxiliary
0x02	ITU-T Rec. H.262, ISO/IEC:	**0x0F**	ISO/IEC 13818-7 Audio with ADTS
	13818-2 Video or 1172-2		Transport Syntax
	Constrained Parameter Video	**0x10**	ISO/IEC 14496-2 Visual
0x03	ISO/IEC 11172-2 Audio	**0x11**	ISO/IEC 14496-3 Audio with the
0x04	ISO/IEC 13818-3 Audio		LATM Transport Syntax as defined
0x05	ITU-T Rec. H.222.0, ISO/IEC 13818-1		In ISO/IEC 14496-3 / AMD 1
	private_sections	**0x12**	ISO/IEC 14496-1 SL-packetized
0x06	ITU-T Rec. H.222.0, ISO/IEC 13818-1		Stream or FlexMux Stream carried
	PES Packets Containing Private Data		in PES Packets
0x07	ISO/IEC 13522 MHEG	**0x13**	ISO/IEC 14496-1 SL-packetized
0x08	ITU-T Rec. H.222.0, ISO/IEC 13818-1		Stream or FlexMux Stream carried
	Annex A DSM-CC		In ISO/IEC 14496_section
0x09	ITU-T Rec. H.222.1	**0x14**	ISO/IEC 13818-6 Sychronized
0x0A	ISO/IEC 13818-6 Type A		Download Protocol
0x0B	ISO/IEC 13818-6 Type B	**0x15-**	ITU-T Rec. H.222.0, ISO/IEC 13818-1
0x0C	ISO/IEC 13818-6 Type C	**0x7F**	Reserved
0x0D	ISO/IEC 13818-6 Type D	**0x80-**	User Private
		0xFF	

Závěr

Problematika multimediálních přenosů je velmi široké téma a dosud žádná publikace se plně nevěnovala jak VoIP tak i streamování videa a videokonferenčním službám. Ačkoliv jsem se při zpracování tématu zprvu snažil o komplexní popis výše zmíněných okruhů, nakonec jsem se soustředil spíše na popis protokolového prostředí, fungování multicastového vysílání a řízení kvality služeb. Problematika kompresních algoritmů, formátů multimediálních souborů a aplikací podporující multimediální služby by vyžadovala mnohem rozsáhlejší rozbor a je proto již nad rámec této práce.

Při tvorbě této práce mě především zarazilo téměř nulové využívání multicastového vysílání na internetu. Ačkoliv problematika multicastu prošla dlouhým vývojem, nelze tvrdit, že jej podporují všechny sítě, natož sítě lokální. Pokud jej někdo používá v lokální síti, využívá multicast většinou jen k šíření do hraničních bodů své sítě. A tak je v České republice největší rozvoj multicastu v akademických sítích, kde se využívá zejména k testovacím účelům.

Při tom, kdyby se místo unicastového vysílání televizních (např. ČT24) a rozhlasových stanic používalo multicastové vysílání, snížil by se několikanásobně celkový datový tok a mohlo by tak dojít k zlepšení kvality především u vysílaných televizních programů. Proč by ale poskytovatelé internetu stáli o to, aby se snížil celkový provoz nebo proč by Telefónica O2 nabízela zdarma služby, za které jí zákazníci v podobě IPTV platí? Další překážkou v rozšíření služeb jsou licenční poplatky za distribuci signálu. Např. u televizního kanálu Nova Cinema je cena za zásuvku 3,90 Kč, ale nikdo nepočítá se šířením vysílání po internetu. Obdobná otázka je u šíření běžně dostupných TV programů (ČT1, ČT2, Nova, Prima a další). Žádný z provozovatelů vysílání nedal oficiální souhlas k celoplošnému šíření vysílání ani v rámci akademických sítí Cesnet a Sanet.

Seznam použitých zdrojů

Multimediální přenosy

Základy IP telefonie – Cisco
http://www.cisco.cz/index.sub.php?pid=iptel&typ=iptelefonie

Multicast

Články o IP multicastu – Ondřej Filip
http://www.lupa.cz/clanky/uvod-do-ip-multicastu

Multicasting na Internetu – Petr Mojžíšek
http://www.isdn.cz/clanek.php?cid=3605

Protokoly podporující multimediální služby

Multimedia over IP
http://dpnm.postech.ac.kr/mcs/papers/ch28_RT.pdf

Popis jednotlivých protokolů
http://www.protocols.com
http://www.ietf.org/rfc.html
http://www.iana.org

Multimedia Over IP: RSVP, RTP, RTCP, RTSP – Chunlei Liu
http://www2.ing.puc.cl/~jnavon/IIC3582/Present/3/mmip.htm

H.323
http://www.packetizer.com/voip/h323

Transportní protokol SCTP – Pavel Satrapa
http://www.lupa.cz/clanky/transportni-protokol-sctp

Protokol SCTP
http://dsn.felk.cvut.cz/education.cz/X36PKO/lectures/7b_sctp.pdf

Testing IPTV
http://www.ixiacom.com/solutions/testing_iptv

Quality of Service

QoS a diffserv – Sven Ubik
http://www.cesnet.cz/doc/techzpravy/2000-6

QoS v počítačových sítích – Jan Kacálek
http://amarok.cesketelekomunikace.cz/xkacal00/

MPEG-2 over IP protokol

Reklamní leták IXIA
http://www.ixiacom.com