Obecně o GPRS ve vztahu k IP

Autor: František Ryšánek <rysanek@fccps.cz>

FCC Průmyslové systémy s.r.o.

Úvod

Všeobecně známou specifickou vlastností GPRS je paketový provoz. Koncové IP zařízení registrované do sítě nezabírá v klidovém stavu žádnou kapacitu datového kanálu a může proto být neustále online na internetu, aniž by blokovalo kapacitu kanálu ostatním účastníkům. Většina GSM operátorů proto koncipuje své GPRS služby tak, že se neplatí za čas, po který je zařízení registrováno do GPRS sítě, ale za objem přenesených dat – k dispozici jsou odstupňované paušály s volnými kilobajty.

Rovněž všeobecně známá a zjevná je skutečnost, že koncové zařízení (mobilní telefon, GPRS modem) se připojuje k počítači přes sériový kabel (nebo infračervený přenos) a PPP. Z čehož na první pohled plyne, že v tomto typickém uspořádání má vlastní „IP osobnost“ připojený počítač, nikoli koncové GSM zařízení. Skutečnost je sice o něco složitější, ale v zásadě je tomu skutečně tak.

Jak jde vlastně dohromady paketová síť a PPP, tj. Point-to-Point Protokol? Kudy se data z mobilu dostanou až na veřejný internet? Dá se pomocí GPRS připojovat do privátní sítě (VPN) a pokud ano tak jak? Pokud Vás zajímají podobné záludnosti, čtěte dál.

Pokud Vás podrobnosti nezajímají, možná Vás bude zajímat kapitola „Zádrhele“ (str.10).

Hrubé schéma GPRS sítě

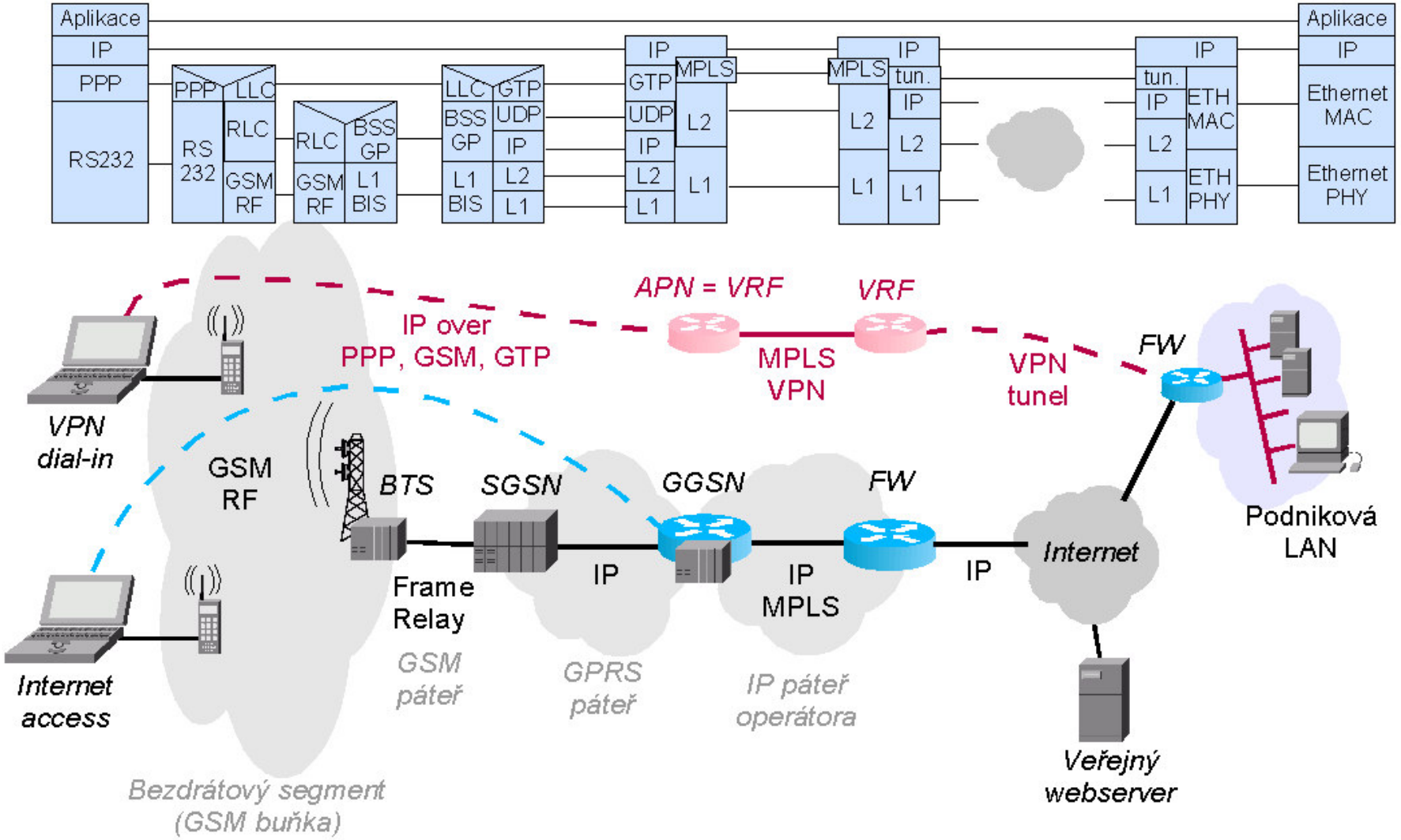
Infrastruktura pro připojení do internetu (případně VPN) přes GPRS má několik základních částí, které mají s vlastním GPRS více či méně společného – viz obrázek na další straně.

Zobrazené vrstevnaté schéma síťových stacků na jednotlivých zařízeních je zejména v GSM sekci zjednodušené v zájmu přehlednosti – o něco úplnější pitvu najdete v příloze (původní obrázky od firmy Cisco) a pochopitelně ve standardech GSM. Cílem ilustrace bylo především předvést několik relayů (transparentních konverzí enkapsulace) pod vrstvou IP mezi koncovým účastnickým IP zařízením a GGSN bránou – nižší vrstvy jsou v rámci tohoto článku vcelku nezajímavé.

Obrázek také neobsahuje pomocnou infrastrukturu, jako např. adresářové/autentikační servery.

V níže uvedeném přehledu budeme jednotlivé části probírat zhruba ve směru od koncového zařízení k operátorově páteřní síti a k internetu – komunikace je ovšem pochopitelně obousměrná, účastní se jí mnoho vrstev atd.

Obr. 1 – Hrubé schéma GPRS sítě



Především je tu rádiový segment GSM mezi mobilním telefonem a základnovou stanicí (BTS), se svými frekvenčními kanály, timesloty, přidělováním pásma a signalizací.

GPRS provoz je dále přenášen pevnou GSM páteří k zařízením SGSN. Zdá se, že na SGSN zařízení je ukončován „GSM hovor" GPRS, tj. typické číslo *99***1# je patrně telefonním číslem SGSN – až na to, že dost možná k vytáčení čísla (signalizaci hovoru) v pravém slova smyslu nedochází – autor v tomto bodě tápe.

SGSN tvoří bránu z původní GSM sítě (rádiové a pevné) do GPRS páteře. Zatímco GSM síť používá protokoly z lůna telco odvětví (GSM Association a ETSI), GPRS páteř používá jako jednotný transport protokol IP. Ještě se ovšem nejedná o IP síť, do které se přímo připojují účastnická koncová zařízení – jde o čistě privátní páteř, skrz kterou je účastnický provoz transportován pomocí tunelů, vytvářených protokolem GTP. GTP je tedy svého druhu IP over IP tunel, dokonce s účastí UDP jakožto mezivrstvy. GTP přenáší účastnická data mezi zařízeními SGSN a GGSN.

GGSN je opět svého druhu brána – tentokrát mezi GPRS IP páteří a čistokrevnou IP páteří operátora. Na zařízení GGSN jsou totiž zakončovány GTP tunely jednotlivých účastníků. Jedná se tedy v zásadě o IP směrovač (router). GGSN je z pohledu koncového GPRS účastníka prvním IP zařízením po cestě – prvním hopem v traceroutu. GGSN obsluhuje část autentikace a „přidělování služby" přihlášenému účastníkovi – podle jeho nakonfigurovaného profilu a na základě jeho identifikace.

Tím jsme se dostali na páteřní IP síťku operátora. Následuje typicky ještě firewall (opevněný externí směrovač) z páteřní IP sítě operátora do „divokého" internetu.

V případě, že operátor provozuje koncovému účastníkovi „GPRS VPN", není provoz směrován do internetu, ale z externího firewallu ještě šifrovaným tunelem nebo pevným spojem do firemní sítě – na straně firemní sítě je tento tunel či pevný spoj ukončen typicky opět na firewallu.

Rádiový segment

Původní datové služby v GSM síti používají komutovaný isochronní datový kanál, podobně jako hlasové služby. Tento datový kanál má v případě datových služeb užitečnou kapacitu 9,6 kbps (skutečná surová kapacita je vyšší) a zabírá jeden z osmi timeslotů v rádiovém kanálu. Na jednom rádiovém kanálu konkrétní základnové stanice (BTS) tedy může běžet současně osm hovorů. Technologie HSCSD umožnila spřažení několika isochronních kanálů pro vyšší kapacitu.

Základní alokační jednotkou GPRS je také timeslot. Také GPRS umí využít timeslotů několik. Rozdíl je v tom, že koncové zařízení si timeslot nezabere po dobu trvání spojení pro sebe, ale může ho sdílet s dalšími koncovými zařízeními a v tom případě se statisticky dělí o kapacitu (paketový multiplex). Timeslot nepředstavuje kolizní doménu – tak jako u dalších podobných systémů s jedním masterem (zde BSC) a mnoha koncovými zařízeními se i u GPRS používá metoda přidělování vysílacího času. Vysílací čas centrálně spravuje a na vyžádání per paket přiděluje BSC (řídící jednotka několika BTS) a proto nedochází ke kolizím. Přidělování vysílacího času funguje i napříč několika timesloty.

Postupem času vycházejí nové revize a doplňky GSM a GPRS standardů a postupně přibývá využitelná kapacita timeslotu:

Kódování	Rychlost
CS-1	9.05 Kb/s
CS-2	13.4 Kb/s
CS-3	15.6 Kb/s
CS-4	21.4 Kb/s

Je zřejmé, že u nejnovějších revizí je využitelná kapacita timeslotu rovna surové bitové rychlosti standardního GSM. Dosavadní GPRS je v rámci timeslotu omezeno na původní modulační schéma GSM (GMSK), ale existují návrhy na rozšíření standardu o schémata výkonnější, s větší bitovou hloubkou na symbol - např. Edge (QPSK8). Zavedení Edge do sítě se ovšem neobejde bez výměny či hardwarového upgradu BTS.

Různá koncová zařízení (a různá zařízení na straně operátora) zvládají různý maximální počet kanálů. Mezi typické kombinace patří 2+1, 4+1 nebo 3+2 (downlink+uplink). Například kombinace 4+1 CS-4 tedy v současnosti umožňuje maximální kapacitu downlinku cca 85 kbps.

IP a koncová zařízení

V nejobvyklejším případě má vlastní IP „osobnost“ (adresu v síti) až samotný připojený počítač. Použitý mobilní telefon nebo GSM modem provádí pouze emulaci PPP serveru, resp. relay na GSM transport, bez složitějšího směrování v třetí vrstvě. Tento mobilní telefon či GSM modem nemá vlastní IP adresu a nemá co mluvit do IP parametrů. Na dohadování IPCP se tedy částečně účastní GGSN – ovšem nikoli přímo v rámci PPP handshaku, ale zprostředkovaně skrz GTP.

Z výše uvedeného plyne, že koncové zařízení musí zvládat provoz PPP a TCP/IP stacku. Většina zařízení, se kterými koncové uživatele vůbec kdy napadne připojit se na internet, tyto požadavky přirozeně splňuje. Může se vyskytnout problém v tom, že emulace PPP v mobilním telefonu bývá hodně spartánská, nepružná a otestovaná pouze proti nejrozšířenějšímu operačnímu systému, takže si s ní jiné kvalitní implementace PPP nemusejí rozumět – ale takový je život.

V průmyslovém prostředí se ale může také vyskytnout potřeba připojit přes GPRS zařízení, které vůbec nemá systémové prostředky k tomu, aby provozovalo PPP a TCP/IP. Jedná se typicky o zařízení s mikrokontroléry, většinou bez operačního systému, které zvládnou nanejvýš primitivní komunikaci přes holou linku RS232. I v tomto případě ovšem existuje řešení – je třeba použít GPRS modem, který má vlastní TCP/IP stack, tj. mj. také vlastní IP adresu („osobnost“ v síti) a především jednoduchý „aplikační“ software, který umožní např. transparentní transport RS232 přes TCP spojení, ať už navazované směrem ven, či dovnitř.

Takovým GPRS modemem je např. Maestro 100 TCP/IP od firmy Fargo Telecom, který umí navíc jednoduchou obsluhu internetových aplikačních protokolů FTP, SMTP, POP aj. Zůstaneme-li v teoretické rovině, je zřejmé, že takovýto modem nepotřebuje vnitřně sám sobě emulovat PPP – vybaluje si IP nativně přímo z GSM transportu a rovněž autentikace a registrace do GPRS sítě může probíhat přímo GSM signalizaci, bez zprostředkování skrz PPP emulaci.

Existují také klasické mobilní telefony, u kterých lze zprovoznit autonomní „IP osobnost“ – takové telefony se vyznačují tím, že zvládají WAP přes GPRS, vybírání e-mailu přes POP3 z internetu, odesílání e-mailů přes SMTP ven do internetu (autonomní, tj. nikoli přes SMS), prohlížení HTTP webu a případné další služby, které si jen operátor dokáže vymyslet. Díky přítomnosti IP sítě je rozšiřitelnost prakticky neomezená, zejména v kombinaci s Javou (případně s konkurenčními technologiemi od Microsoftu, pokud se uchytí).

IP na páteřích

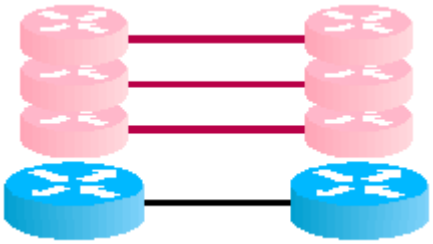
Varování: obsah této a následující kapitoly vychází z implementace GGSN a APN od firmy Cisco. Jedná se pouze o jednu z několika implementací, proto níže uváděné detaily nemusí být všeobecně platné.

Jak již výše uvedeno, zařízení GGSN je v podstatě IP směrovač – má v nejjednodušším případě dvě IP rozhraní zvaná Gn (do GPRS páteře) a Gi (do internetové páteře). V případě GGSN od firmy Cisco to platí doslova – Cisco GGSN se skládá z klasického hardwaru Cisco 7200 VXR a speciální verze operačního systému Cisco IOS, obohaceného o funkce GGSN. Nově lze použít také platformu Cisco Catalyst 6500/7600, povinně rozšířenou o modul MWAM. Z toho plynou následující rysy Cisco GGSN zařízení:
- nezávislost na médiích GPRS a IP páteře. Obě IP rozhraní mohou být realizována některou ze široké palety modulárních karet, které jsou k dizpozici – od synchronních sériových linek přes E1, E3, ATM a Fast Ethernet až po STM1 POS nebo Gigabit Ethernet.
- přiměřený výkon. Funkce GGSN jsou procesorově náročnější než běžný routing a jsou hůře hardwarově akcelerovatelné, takže je pochopitelný požadavek na vyšší modely procesorové karty (NPE300/400 na platformě Cisco 7200) a povinné rozšíření platformy 6500/7600 o modul MWAM (tato platforma je původem ethernetový switch – switche vykazují vysoký jmenovitý výkon při hardwarovém switchování L2/L3, ale procesorově bývají od přírody relativně slabé).
- modularita a jistá škálovatelnost
- kompatibilita s dalšími produkty Cisco – nejen s dalšími směrovači, ale také s podpůrnou infrastrukturou, jako jsou systémy pro centrální autentikaci a přidělování systémových zdrojů koncovým účastníků, správu konfigurací, dohled sítě atd. (Radius, DHCP, DDNS, CiscoWorks...)
- obchodní model firmy Cisco

Zařízení Cisco 7200 je „přístupový směrovač“ střední třídy, který se tradičně používá na páteřích internetových providerů pro agregaci zákaznických sériových pevných linek (synchronních okruhů) a popř. dial-up polí menšího rozsahu. Zařízení Cisco Catalyst 6500/7600 je ethernetový přepínač nejvyšší výkonnostní kategorie.

Přístupové směrovače firmy Cisco mají historicky kvalitní a otevřenou (nebo přinejmenším svéráznou avšak rozšířenou) softwarovou výbavu pro obsluhu dial-up klientů, spočívající na protokolech Radius, Bootp/DHCP a OSPF. Nověji přibyly speciality z rodiny MPLS, z nichž nejzajímavější je patrně MPLS VPN a s ní související schopnost vytvářet virtuální směrovače zvané VRF. A neměli bychom zapomínat na možnost práce s virtuálními sítěmi (VLAN) v rámci Ethernetu. Směrem ven se také uplatní tunelové technologie Cisco s protokoly GRE a IPSec. To vše jsou díly skládačky, ze které lze budovat pokročilejší vlastnosti GGSN směrem do venkovní IP sítě.

Pozorný čtenář si na obrázku jistě povšiml zkratky MPLS a podivného vrstvení protokolů v příslušném segmentu. Aniž bychom zabíhali do detailů, řekněme si pouze, že původní myšlenkou MPLS je akcelerace směrování na bázi sdružování toků. V našem náčrtku je ovšem využita jiná, „vedlejší“ vlastnost MPLS: podpora MPLS VPN. Dnešní MPLS umožňuje provozovat nad jedinou L2 linkou několik vzájemně oddělených IP sítí, aniž by o tom linková vrstva musela něco vědět či to nějak explicitně podporovat. A právě tuto vlastnost zařízení Cisco využívají k provozu několika virtuálních „venkovních“ IP sítí na jediné fyzické síti.



Na směrovači se konfigurují instance VRF, ovšem základní „globální“ směrovací tabulka zůstává. Tabulky „uzavřené“ ve VRF instancích jsou ovšem dokonale oddělené a na globální směrovací tabulce nezávislé. VRF instance na dvou a více směrovačích lze navzájem propojovat vyhrazenými fyzickými L2 médii, nebo pomocí MPLS nad jediným L2 médiem.

Venkovní IP síť nemusí být a typicky není jediná – pomocí VRF jich lze provozovat na jednom GGSN systému paralelně několik. Na jednom GGSN je typicky nakonfigurováno několik Access Pointů. Teoreticky lze zajisté nakonfigurovat několik access pointů do jediné IP sítě, ale tato možnost nemá valný praktický význam. Mnohem zajímavější je možnost mít jeden access point pro „divoký“ internet, jeden pro WAP, další pro přístup do interní sítě operátora, a N dalších pro zákaznické VPN. Pochopitelně je ovšem třeba mít každý access point přiřazen k jiné IP síti, které budou navzájem neprodyšně odděleny. Navíc tyto IP sítě mohou mít a typicky mají překrývající se adresní prostory, protože zákazníci (a vlastně i operátoři) typicky používají ve vnitřní síti privátní adresní prostor dle RFC1918.

Z výše uvedeného plyne, že prakticky je možno položit rovnítko mezi zkratky APN a VRF – jde o dvě různé věci, ale v reálných konfiguracích je velice obvyklé, že každému APN je přidělena samostatná instance VRF. Správci systému zbývá zvolit, zda ponechá veřejný internet v globálním směrovacím procesu, nebo zda jej opouzdří do VRF a globální směrovací proces použije na režijní účely (remote management, Radius, logování).

Podobně lze VRF instance vytvářet na „firewallu“ a zakončovat do nich např. stálé IPSec tunely či fyzické pronajaté okruhy, vedoucí ze zákaznických podnikových sítí. Tímto způsobem lze zařídit, aby jednoduchá mobilní GPRS zařízení (i bez možnosti provozovat IPSec) byla dostupná ze zákazníkovy podnikové privátní sítě, bez překladu adres a s poměrně vysokým stupněm zabezpečení. Toto uspořádání samozřejmě vyžaduje speciální dohodu s operátorem a vyplatí se spíše při větším počtu mobilních zařízení.

Slučování funkcí GGSN a firewallu není na zařízeních Cisco vyloučeno, dokumentace tuto možnost dokonce místy explicitně zmiňuje. Ušetřil by se tím jeden směrovač a jeden MPLS hop a s ním spojená režie dynamického směrování. Takovéto slučování funkcí ale z různých praktických důvodů není úplně běžné. Nejběžnější praktickou překážkou může být tendence k nahromadění softwarových chyb, která složitější kombinaci „features“ na jediném stroji učiní prakticky nepoužitelnou. Už jen kombinace GGSN, MPLS VPN (VRF) a IP-Secu může přinést mnoho zábavy. Nezapomínejme také na vysokou procesorovou náročnost jednotlivých funkcí.

V praktických konfiguracích se tedy využije schopnost MPLS „rozprostřít“ či vzájemně propojit/spárovat VRF instance mezi několika sousedními směrovači – v našem případě mezi GGSN a firewallem.

Pro vzájemné propojování VRF mezi směrovači lze namísto MPLS tagů alternativně použít VLANy nad Ethernetem, kanály v PDH trunku nebo ATM PVCčka (řazeno podle použitelnosti sestupně).

Centralizovaná autentikace a přidělování zdrojů

Důležitou součástí jakékoli sítě pro velké množství uživatelů je identifikace, autentikace a přidělování systémových prostředků. Základem těchto funkcí je centralizovaná správa uživatelských „účtů“ či profilů. Uživatelské účty se spravují v databázi někde na serveru. Když se nově příchozí uživatel pokusí o připojení ke GPRS síti, přístupové aktivní prvky sítě se dotazují autentikačních serverů, co mají s uživatelem dělat – zda ho mají vpustit dál a kam vlastně, jakou má dostat IP adresu a nameservery apod.

GPRS je hybridní systém, na půl cesty mezi GSM sítí a IP páteří. Podle toho vypadá skladba adresářových serverů všeho druhu, které se v síti vyskytují. Jedná se přinejmenším o tyto:

- HLR – jde o základní registr uživatelů v GSM síti, nově s GPRS rozšířeními. Uživatel je identifikován a typicky také autentikován IMSI kódem SIM karty, ke kterému HLR server drží 1:1 „číslo volajícího“ (též MSISDN). IMSI kód je považován za důvěrnou informaci, není nikde navenek prezentován - aby se ztížilo jeho kopírování a případné zneužití.
  Díky GPRS rozšířením umí HLR server resolvovat APN jména, základní oprávnění uživatele ohledně přístupu k APN a případně i statickou IP adresu uživatele (tím ovšem s IP končí). Obrací se na něj mj. SGSN brána s dotazem, na kterou GGSN bránu se má směrovat hovor.
  Jinak řečeno, když si necháváme u operátora povolit GPRS pro konkrétní SIM kartu, propadne tato informace skrz klikací zákaznickou databázi až do technologické konfigurační databáze HLR serveru.
- RADIUS – jde o protokol pro centrální ověřování uživatelských hesel, přidělování IP adres, směrování L2TP tunelů apod. v IP sítích. Umožňuje centralizovanou správu uživatelských účtů na jednom serveru, který řídí velký počet přístupových směrovačů. Výrazně snižuje časovou náročnost konfigurace a správy směrovačů (oproti hypotetickému scénáři, kdy je třeba konfigurovat uživatelské účty přímo na směrovačích).
  Jde o otevřený standard vyvinutý lidmi od firmy Livingston (svého času slavný výrobce směrovačů), výrazně podporovaný a používaný firmou Cisco, ale např. i Microsoftem. Je prakticky všudypřítomný na velkokapacitních dial-in polích připojených do JTS – na této pozici jsou masivně nasazovány přístupové směrovače Cisco.
  S Radiusem se tedy v GPRS síti budou bavit především směrovače Cisco, tj. prakticky výhradně GGSN (konfigurace Firewallu nebude mít mnoho dynamických prvků).
- DHCP, (D)DNS a případně další.

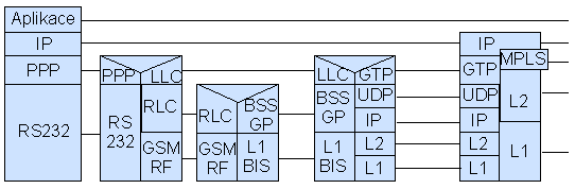
Kompetence HLR a Radiusu se na první pohled překrývají a například GGSN se baví s oběma. Celá věc by se teoreticky dala zařídit výhradně s použitím HLR (bez Radiusu). Některé zdroje ovšem uvádějí, že prakticky se Radius používá přinejmenším pro přidělování IP adresy. Další podrobnosti se ovšem budou u různých operátorů lišit a v případě problémů je z pozice outsidera těžké říci, proč to nechodí a kde se stala chyba - díky dvojitému relayi L2 pod prvním IP hopem a díky nemožnosti debugovat z pozice koncového uživatele rádiové rozhraní mobilního telefonu. Pak nezbývá než zkoušet kombinovat různé operátory / mobilní telefony / PPP stacky a zjišťovat, co s čím funguje.

V klasických dial-up systémech, jejichž klientskou částí je typicky PPP, se k identifikaci a autentikaci používá striktně uživatelské jméno a heslo, v extrémním případě ještě radiusový realm (část loginu před zavináčem - v systémech s distribuovaným Radiusem).

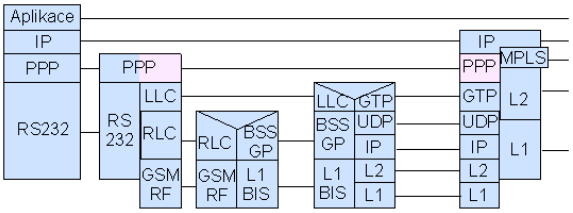
Tuzemští operátoři jméno a heslo nepoužívají. Autor má pouze nepřímé indicie, že jde možná o platné/použitelné autentikační atributy uživatelského profilu na HLR. Přinejmenším mobilní telefony a GSM modemy si typicky v rámci LCP dohodnou PAP nebo CHAP a následně ho vůči klientovi uplatní. Což je s prázdným jménem a heslem mimochodem možná lehce nekorektní. Dále na GSM modemech Maestro 100 TCP/IP existují „proměnné prostředí“ pro autonomní TCP/IP režim, které jsou nazvány „APN User Name“ a „APN Password“. Těžko říci, zda se např. jméno a heslo dostane přes dvojitý relay až na GGSN (a třeba do Radiusu).

Veterána telefonického připojení proto první setkání s tuzemským GPRS lehce šokuje či zhnusí – jméno a heslo jsou ponechána prázdná, jako jediný identifikační a autentikační token je přijata SIM karta a well-known jméno APN, které je nota bene do telefonu zadáno po startu, případně se natrvalo zadává do „custom settings“ v připojeném počítači. Takhle přece nevypadá zabezpečený přístup do sítě...

Dokumentace Cisco mluví o tom, že kromě výše popsaného klasického IP režimu s dvěma relayi (v rámci PLMN) je novějšími GPRS standardy zakotven také režim s transportem PPP až na GGSN. Odpovídá tomu mimochodem první argument standardního modemového příkazu AT+CGDCONT, kterým je klasicky „IP“ a alternativně „PPP“ (následuje APN jméno). Cisco tento PPP režim podporuje a používá ho ke svým oblíbeným Radiusovým kejklím – klasickým artistickým kouskem je distribuovaný Radius s realmy a podle něj navazovaný L2TP tunel na firewall zákazníka.
S příchodem VPN-over-APN to na první pohled mírně postrádá smysl, ale nedotažená autentikace do APN může být pro někoho dost dobrým důvodem.



Klasický IP režim se dvěma „retranslacemi“



Alternativní režim PPP over GTP

V případě, že čistý PPP režim není k dispozici, umí si Cisco GGSN také „regenerovat“ PPP z IP/GTP tunelu a výsledek forwardovat přes L2TP. Také je možné per-VRF nastavení Radiusových serverů (takže nejsou potřeba realmy a Radius běží po vnitřní síti). V obojím případě je výsledek ten, že se zaměstnanec firmy dostane pomocí APN Name do konkrétní VPNky a další speciality na straně IP nadiktuje Radius server přímo spravovaný zákazníkem.

Po pravdě řečeno, distribuovaný Radius mezi firmami je prakticky dost utopie, nebo přinejmenším hračka extrémně náročná na koordinaci mezi partnery (zde mezi GSM operátorem a velkým zákazníkem) – ale když se ho povede politicky prosadit a společnými technickými silami nakonfigurovat, funguje moc hezky.

Ostatně end-to-end PPP režim v GPRS se prakticky také nepoužívá – operátoři ho obvykle nemají nakonfigurovaný.

Cisco dále samozřejmě podporuje DHCP a DDNS – prakticky se ovšem DHCP na internetových a GSM páteřích příliš nepoužívá, protože všechno potřebné je předáno pomocí PPP.

Lze shrnout, že GPRS nezklamalo jakožto bod střetu mezi GSM a IP. Některé autentikační funkce jsou zdánlivě nebo i fakticky duplicitní. Cisco jakožto výrobce GGSN má na svou část koláče vlastní názor (jako obvykle) a rádo by do této oblasti propašovalo co nejvíce svých osvědčených „access“ triků. Hlavní překážkou je mu zřejmě neochota správců GGSN provětrávat za každou cenu všechny pentličky, které Cisco umí. Někdy možná i na úkor bezpečnosti.

Roaming

Základem roamingu jak v GSM tak v GPRS je celosvětově unikátní identifikace koncového uživatele (SIM karty) a distribuované zpracování autentikačních transakcí, které pochopitelně funguje jedině za předpokladu vzájemného propojení GSM sítí.

IMSI kód (identifikátor SIM karty) má přesně danou strukturu, která obsahuje údaj o zemi a operátorovi, kde byla SIM karta vydána. Na základě těchto údajů dotazovaný místní VLR server získá autoritativní autentikační informace z domovského (HLR) serveru daného roamujícího účastníka.

V rámci GPRS existuje možnost směrovat / relayovat GTP tunely na GGSN v cizí GPRS páteři. Z toho plyne, že GPRS páteře musí být vzájemně propojeny. A o tom je GPRS roaming.

V této souvislosti je na místě poznámka o atributu „APN Name“. Zdá se, že se nejedná tak docela o „tupý jednoslovný řetězcový identifikátor“. Některé zdroje uvádějí, že APN jména jsou resolvována interním/privátním DNS systémem v GPRS páteři. Tím dostává nový smysl zdánlivě přihlouplá konvence operátorů dávat APNkám jména „jakoby“ z DNS, která ovšem ve veřejném DNS neexistují. Zmíněný smysl je v tom, že APN jména tak mohou být bez problémů celosvětově unikátní a lze je také distribuovaně resolvovat, což je užitečné při GPRS roamingu. Používání domén již registrovaných ve veřejném DNS odstraňuje velkou část potenciálně duplicitní byrokracie a právních zádrhelů spojených s registrací doménových jmen – zůstává pouze správa kořenových serverů privátního jmenného prostoru a administrativa kolem případné delegace TLD a 2nd-level domén. Kromě toho jsou veřejně známé domény operátorů pro zákazníky mnemotechnicky velmi dobře pochopitelné a odstraní se tak spousta překlepů při konfiguraci koncových zařízení (=> helpdesku ubyde spousta práce). Autor bohužel v tuto chvíli netuší, zda skutečně existuje celosvětový systém GPRS DNS, nebo zda si ho pouze interně zavedli někteří mezinárodní operátoři či aliance roamujících operátorů, nebo zda je to od základu blábol.

Pokud by skutečně existovala souvislost mezi pseudo-doménovými APN jmény a GPRS roamingem, něco by to naznačovalo např. o schopnostech GPRS roamingu u různých operátorů – viz. Oskarovo APN „ointernet“ versus T-mobilí „internet.t-mobile.cz“.

Praktické zádrhele GPRS

Blues o dlouhém pingu

Nevýhodou per-packet přidělování pásma je vyšší a nepravidelná doba odezvy => horší interaktivní odezva a nižší reálná průchodnost. Nejlepší dosažitelnou dobou odezvy (ping round trip) je asi 500 ms, ale poměrně běžné jsou hodnoty až do 1 s (bez zátěže). Nízká kapacita, přirozeně vysoká a kolísavá doba odezvy – oba tyto faktory mají neblahý vliv na chování TCP flow control. Jinak řečeno, reálná rychlost downloadu nemusí zcela odpovídat jmenovité maximální bitové rychlosti použitých zařízení.

Registrace do GPRS sítě: jen na popud koncového zařízení

Ať už IP stack běží na koncovém počítači nebo přímo na mobilním telefonu, platí obvykle zásada, že registraci do GPRS sítě (tzv. „sestavení PDP kontextu“) musí vyvolat koncové účastnické zařízení. Nové verze GGSN softwaru Cisco podporují i obrácený směr, tj. registraci konkrétního koncového zařízení na žádost GGSN (ekvivalent dial-outu z přístupového směrovače) – taková věc se ale musí konfigurovat pro konkrétní SIM kartu a statickou IP adresu natvrdo na GGSN (tj. nejde to přes Radius či HLR) a kromě toho patrně neexistuje mnoho koncových zařízení, která by tuto variantu podporovala. Na rozdíl od tradičních telefonních modemů, které byly v zásadě peer-to-peer, komunikace přes GPRS je od základu jaksi asymetrická. Sečteno a podtrženo, připojit koncové zařízení do GPRS sítě lze jedině na popud tohoto koncového zařízení.

Z toho plyne, že na koncové zařízení se dá zvenčí z internetu dostat jedině v případě, že se napřed samo aktivně přihlásí do GPRS sítě. Poučení pro průmyslové aplikace zní: pokud mají být koncová zařízení kdykoli dostupná zvenčí, musí se ihned po zapnutí automaticky přihlásit do GPRS sítě.

Přístup do internetu: ano, ale pouze přes NAT

Aneb statická veřejná IP adresa pouze za další peníze.

GSM operátoři přidělují GPRS adresy pro přístup na veřejný internet dynamicky a především z privátních poolů (dle RFC1918), takže na rozhraní mezi operátorovou IP páteří a veřejným internetem je NAT. Z toho plyne, že na IP zařízení připojené přes GPRS se nedá dostat z veřejného internetu – navenek je vidět pouze venkovní adresa firewallu, která se používá pro NAT. Což je v průmyslových aplikacích (typicky dálkové ovládání či sledování) obvykle překážka.

Pokud potřebujeme ovládat koncová zařízení ze serveru někde v internetu, existuje několik řešení:

a) buď se musí koncová zařízení pravidelně dotazovat serveru na instrukce, případně ihned po zapnutí spustit GPRS a navázat na server trvalé TCP spojení (pak už zařízení může fungovat jako slave).

b) nebo je třeba u operátora objednat statickou veřejnou IP adresu (jedná se typicky o placenou doplňkovou službu)

c) nebo lze koncová zařízení osahávat také přes GPRS modem, připojený k témuž operátorovi. V rámci privátně číslované IP páteře operátora by měl fungovat přímý přístup. Nevýhodou je, že už tak dost dlouhá odezva rádiového segmentu GPRS se rázem zdvojnásobí.

Paketový provoz, ale stále point-to-point.

Kontrolní otázka: Když mám vedle sebe na stole dva notebooky a dva telefony připojené ke GPRS a pingám z jednoho na druhý, kam až pakety generované pingem cestují? Mezi mobily, na BTSku, na MSC, na SGSN, nebo na GGSN? Odpověď: pakety se obracejí na cestu zpět na GGSN. Důvod: teprve GGSN je první IP hop. Což ovšem netřeba považovat v jakémkoli smyslu za problém.

Literatura - odkazy

Cisco GGSN introduction
http://www.cisco.com/en/US/products/sw/wirelssw/ps873/index.html

GPRS White paper (obchodnické, povrchní - složité obrázky bez vysvětlení)
http://www.cisco.com/en/US/products/sw/wirelssw/ps873/products_white_paper09186a00800ad645.shtml

Configuration Information for GGSN 4.0
http://www.cisco.com/en/US/products/sw/iosswrel/ps5413/products_feature_guide_book09186a00801c5df2.html

Configuring PPP support on the Cisco GGSN
http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide_chapter09186a008012997d.html#93211

GSM & GPRS prezentace

http://www.atis.org/atis/Pictures/Supercomm01/Presentationfolder/T1P1zelmer3Gtemplate2.PDF

Slovníček zkratek

Zkratka	Význam
APN	Access Point Name (nikoli Access Point Network). Jde o termín ze žargonu GPRS. Access Point je přístupový bod do sítě operátora – v případě IP tedy přístupový bod do IP sítě. Parametr APN je jménem přístupového bodu, jeho unikátním identifikátorem v síti konkrétního operátora. Jinak řečeno, jde o jméno sítě, do které chceme připojit náš mobilní telefon.

BSC Base Station Controller – řídící jednotka několika základnových stanic (BTS)

BTS Base Transceiver Station – základnová stanice rádiového segmentu

BSS Base Station System = BSC + nx BTS (řídící jednotka + několik základnových stanic)

GTP GPRS Tunneling Protocol – svého druhu IP over IP tunel (popř. PPP over IP)

HLR Home Location Register – adresářový server pro remote autentikaci v síti GSM (a GPRS – komunikuje s ním hlavně SGSN, ale také GGSN). Nabízí se srovnání s autoritativním DNS serverem.

IMSI International Mobile Subscriber Identifier – identifikační číslo SIM karty. Používá se jako interní primární identifikátor uživatele v GSM síti. Není totožné se sériovým číslem SIM karty. HLR server vydávajícího operátora drží jeho vazbu 1:1 na konkrétní účastnické telefonní číslo (MSISDN).

IMEI International Mobile Equipment Identifier – identifikační číslo mobilního telefonu (aparátu) – nezávislé na SIM kartě.

MPLS MultiProtocol Label Switching – švýcarský armádní nůž moderních IP páteří. MPLS mechanismus umožňuje původně v zásadě automatizovanou agregaci toků v páteřní síti, jejich značení tzv. MPLS tagem nebo labelem a zjednodušené akcelerované switchování podle tohoto tagu, namísto náročnějšího routingu podle cílové IP adresy. Na tuto základní myšlenku se ovšem postupem času nabalila spousta „sousedních“ technologií, jako je QoS, symbióza s ATM signalizací, transport všeho možného over MPLS, a také MPLS VPN.

MS Mobile Station - koncové GSM zařízení, tj. mobilní telefon nebo GSM modem.

MSC Mobile Switching Center – ústředna obsluhující vyšší územní segment GSM sítě. Směruje/přepojuje hovory uvnitř sítě a funguje též jako gateway mezi GSM sítí a JTS. Síť konkrétního operátora se skládá typicky z několika MSC.

MSISDN Mobile Station ISDN number - mezinárodní telefonní číslo účastníka v jednotném formátu E.164. HLR server vydávajícího operátora ho váže 1:1 na IMSI konkrétní SIM karty.

PLMN Public Land Mobile Network – GSM a GPRS páteře

RADIUS Remote Authentication Dial-in User Service – protokol pro centrální autentikaci, autorizaci a accounting.

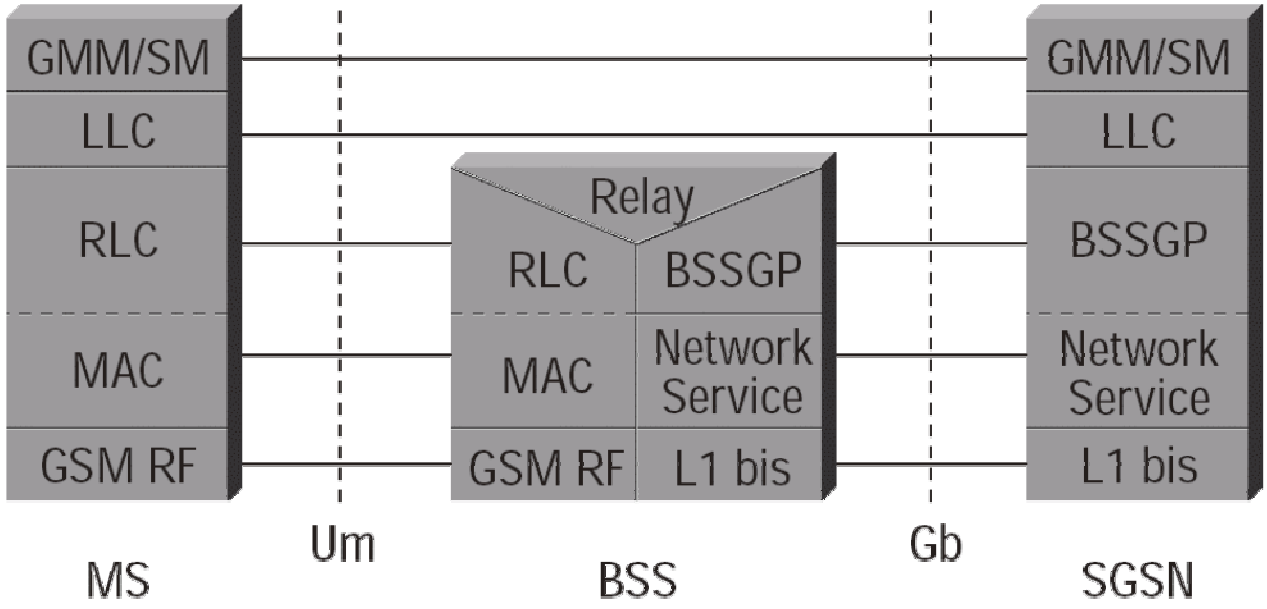
RAN Radio Area Network – rádiový segment (popř. i pevná GSM infrastruktura)

VLR Visitor Location Register – pomocný/podřízený registr autentikačních údajů. Vyřizuje autentikační transakce (tj. dotazuje se HLR serverů), zvládá distribuovanou autentikaci mezi operátory (při roamingu), funguje také jako cache – udržuje po omezenou dobu autentikační údaje „návštěvníků“. Nabízí se srovnání s neautoritativním DNS serverem.

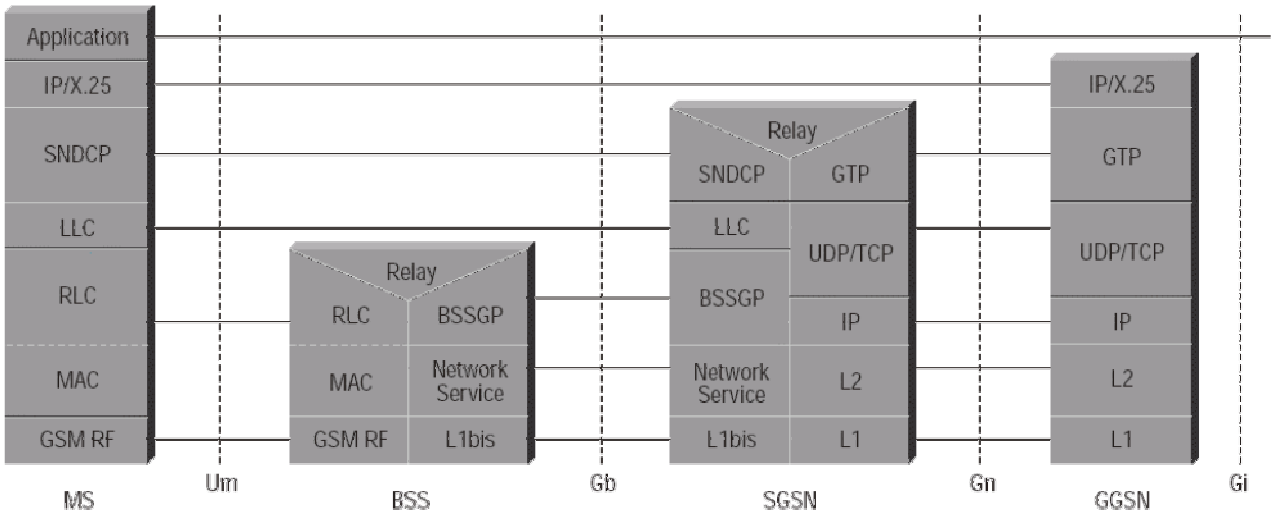
VRF Virtual Routing and Forwarding. VRF instance je virtuální směrovač, nakonfigurovaný v operačním systému fyzického směrovače (jde patrně o specialitu firmy Cisco a jejího softwaru IOS)

Příloha – původní obrázky

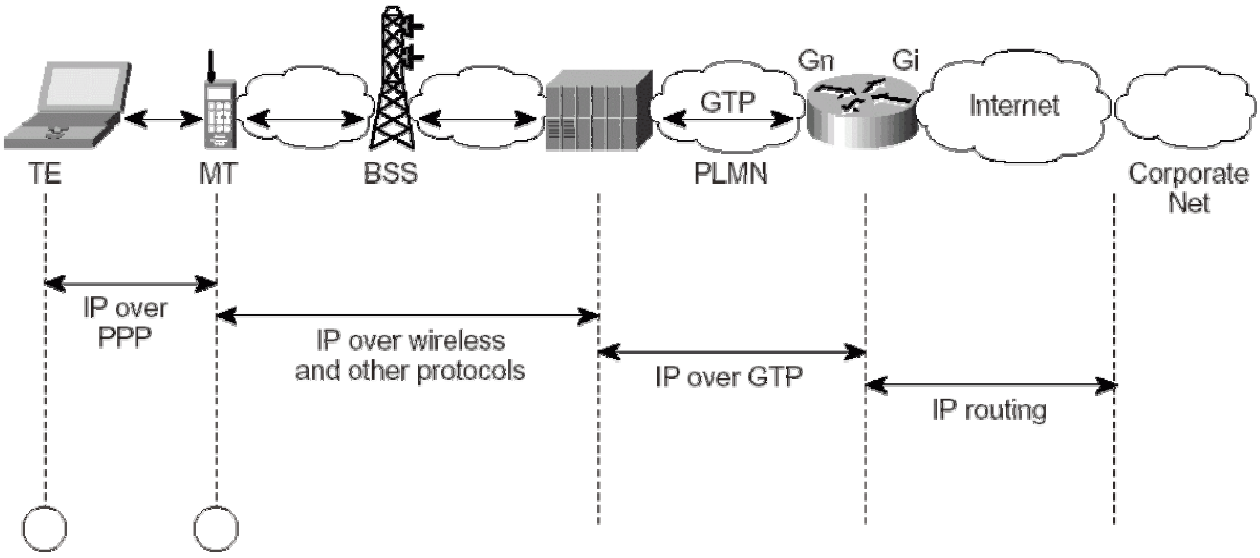
Pro pořádek následují původní, nezjednodušené obrázky GPRS stacků od firmy Cisco. Tytéž diagramy lze najít i v jiných zdrojích, zajisté především ve standardizačních dokumentech GSM. Cisco ostatně uvádí u obrázků jako zdroj ETSI.



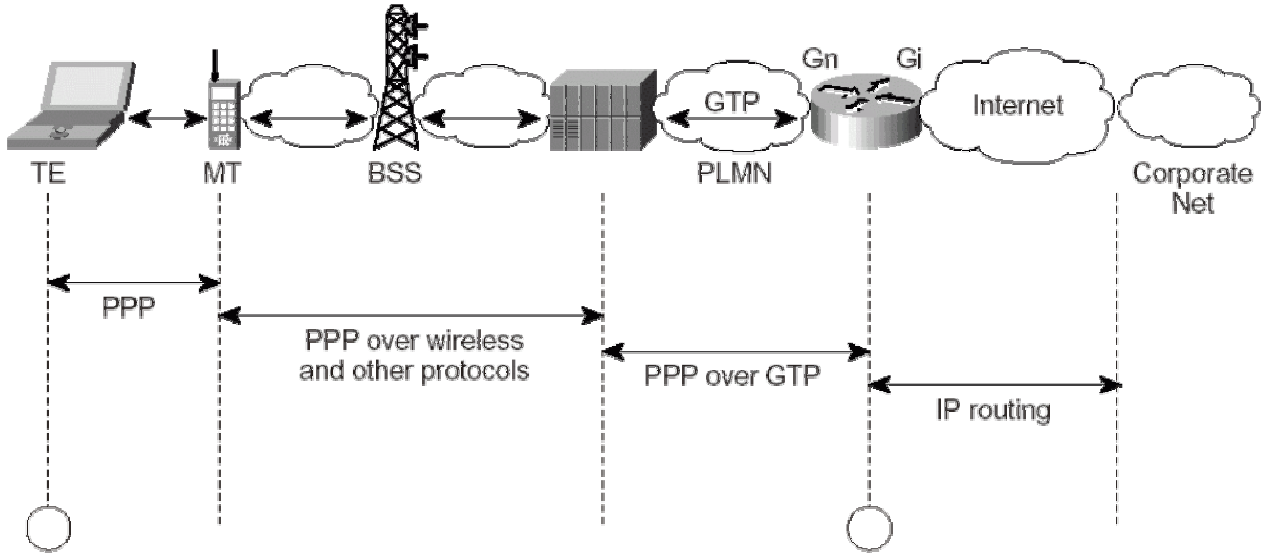
GSM vrstvy pod GPRS – rádiový a pevný segment GSM sítě



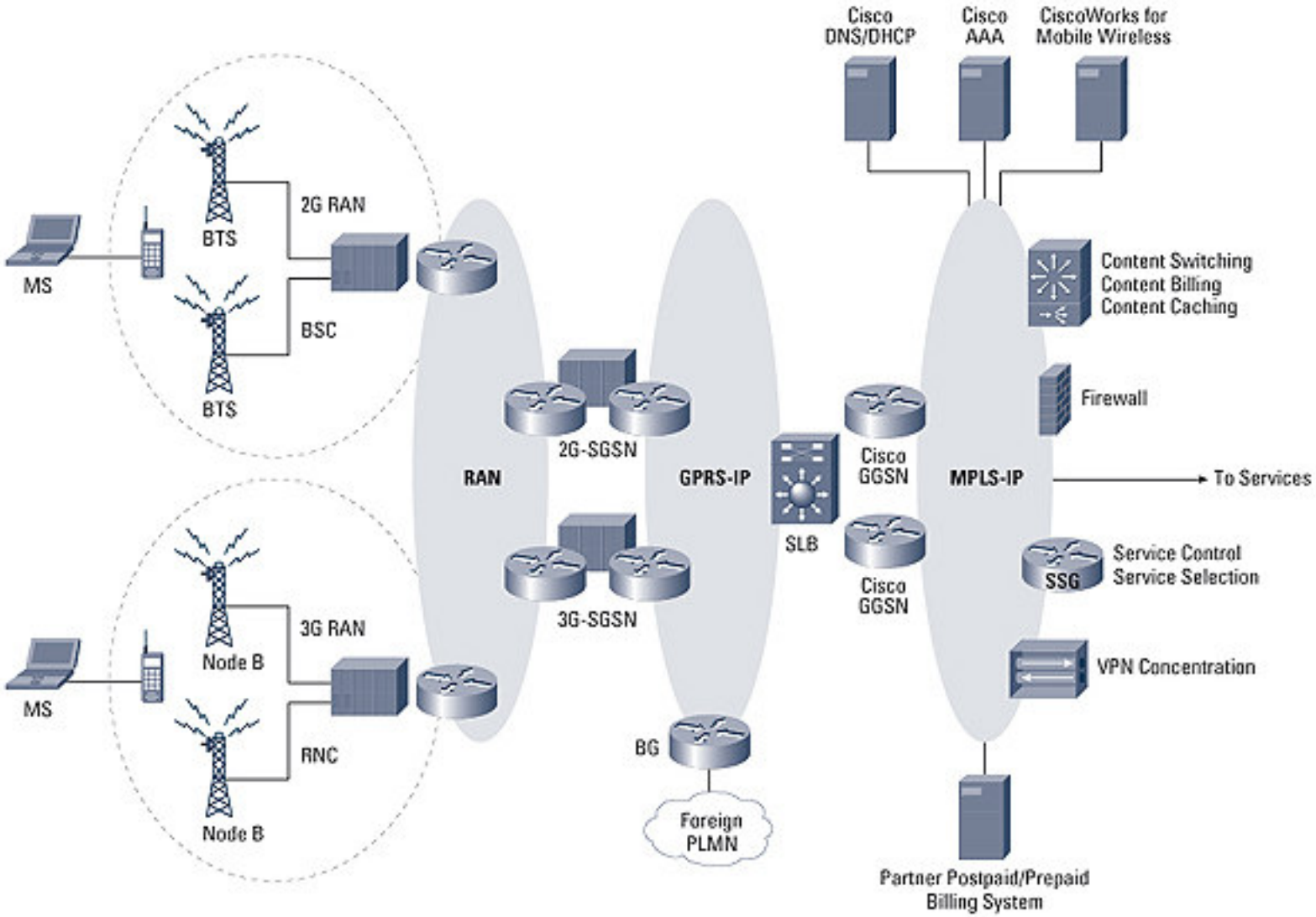
Vrstvy GPRS spojení – od „mobilního telefonu“ po GGSN bránu



Tradiční IP režim se dvěma „retranslacemi“ – PPP je pouze mezi PC a mobilem



Režim PPP-over-GTP – PPP je transportováno z PC až na GGSN



Další schematický obrázek GPRS sítě od fy. Cisco