INTERNET A TCP/IP (6)

V této části seriálu se budeme zabývat protokoly a službami síťové vrstvy. Připomeňme si nejprve, že úlohou síťové vrstvy je poskytnout spojení systémům, které spolu hodlají komunikovat. Spojení musí být nezávislé na použitém přenosovém médiu a technologiích použitých v přenosových okruzích a podsítích, jejichž prostřednictvím se přenos uskutečňuje. Základní službou, kterou síťová vrstva poskytuje, je transparentní přenos dat mezi dvěma komunikujícími objekty.

K dalším službám, které síťová vrstva poskytuje, patří síťové adresování, zahajování, vytváření a ukončování síťových spojení, identifikace koncových bodů síťových spojení, oznamování vzniklých chyb či dohadování kvality služby. Náplň služeb, použité protokoly a konvence se samozřejmě liší v závislosti na použité síťové technologii. Vzhledem k rozsahu seriálu se však omezíme pouze na tu nejrozšířenější; TCP/IP použitou v celosvětové síti internet.

Přenos dat a směrování

Přenos dat od odesílatele k příjemci probíhá v každé síti po určité trase. Ta je, až na výjimky v případě velmi jednoduchých sítí, tvořena soustavou dílčích sítí vzájemně propojených prostřednictvím rozličných zařízení (viz obr. 1). Jednotlivé dílčí sítě se mohou lišit nejenom přenosovou rychlostí, ale také použitou infrastrukturou, technologiemi použitými k přenosu a dalšími vlastnostmi. Mezi odesílatelem a příjemcem může současně existovat několik různých cest, tras, po nichž lze data přenášet. Vlastnosti jednotlivých tras se mohou výrazně lišit jak z hlediska propustnosti, tak i z hlediska spolehlivosti či dalších charakteristik přenosu. Zařízení propojující jednotlivé dílčí sítě označujeme jako mezilehlé systémy (Intermediate System, IS). Úkolem mezilehlých systémů obecně je zabezpečit přenos dat mezi jednotlivými, vzájemně odlišnými dílčími sítěmi. Trasu paketu tedy tvoří soustava jednotlivých dílčích sítí, tzv. subsítí, a mezilehlých systémů. Výběr trasy na úrovni třetí vrstvy OSI modelu je označován jako směrování. Směrování může být buď statické, což znamená, že zvolená trasa je používána po celou dobu přenosu dat, nebo dynamické, kdy je trasa vybírána individuálně pro každý předávaný paket. Na použitém směrování jsou potom založeny dvě hlavní přenosové služby, o nichž jsme již hovořili: přenosová služba se spojením (Connection-Oriented Network Service, CONS) a přenosová služba bez spojení (Connection-Less Network Service, CNLS).

V případě přenosu se spojením, označovaném také jako spolehlivý nebo zabezpečený přenos, se používá statického směrování. Znamená to, že se nejdříve vytvoří trasa mezi oběma komunikujícími objekty, po níž se později přenášejí datové pakety. Spolehlivý přenos se proto skládá ze tří hlavních fází: navázání spojení, přenosu dat a ukončení spojení. Charakteristiky a průběh jednotlivých fází mnohdy závisejí na dalších parametrech či volbách, na nichž se mohou komunikující objekty předem dohodnout. Pro zvýšení pravděpodobnosti detekce ztráty paketu se používá metody potvrzování přijatých datových paketů. Potvrzování, jak sám název napovídá, spočívá v tom, že příjemce potvrdí odesílateli bezchybný přenos každého přijatého paketu či jejich skupiny.

Přenosová služba bez spojení, označovaná také jako datagramová, nespolehlivá či nezabezpečená přenosová služba, je pravým opakem služby spolehlivé. Používá dynamického směrování. Přenos paketu tak probíhá bez navazování spojení a potvrzování příjmu paketů. Trasa, po níž jsou jednotlivé pakety (zde označované jako datagramy) doručovány od odesílatele k příjemci, není předem definována a může se datagram od datagramu dynamicky měnit. Žádná obecná pravidla však ani nezakazují používat současně obou druhů přenosových služeb ani nestanovují jejich vzájemný poměr.

Protokolová sada TCP/IP

Protokolová sada TCP/IP (Transport Control Protocol/Internet Protocol) vznikala v rámci výzkumných prací zahájených americkým ministerstvem obrany (USA Department of Defence) na pokusné akademické síti ARPANet, která byla předchůdcem dnešní sítě internet. Práce na vytváření protokolů TCP/IP byly ukončeny v roce 1979 a do roku 1982 probíhalo na síti ARPANet

jejich ověřování a testování. Vzhledem k tomu, že vývoj protokolové sady TCP/IP probíhal ještě před vznikem referenčního modelu OSI, není s ním vnitřně zcela kompatibilní.

Její začlenění do struktury referenčního modelu OSI je znázorněno na obr. 2. Na rozdíl od OSI je model TCP/IP čtyřvrstvý. Nejnižší vrstva, vrstva síťového rozhraní, zajišťuje fyzickou komunikaci uzlů sítě. Integruje v sobě současně služby fyzické a spojové vrstvy OSI modelu. Další vrstva, internet, zabezpečuje služby, které v OSI modelu vykonává právě vrstva třetí, síťová. Zajišťuje síťové adresování a nezabezpečenou datagramovou výměnu paketů prostřednictvím protokolu IP (Internet Protocol). Mezilehlými prvky IP sítě jsou označovány jako IP směrovače. Služby další, transportní vrstvy odpovídají službám transportní vrstvy referenčního modelu OSI. Transportní vrstva zajišťuje jak spolehlivý přenos dat protokolem TCP (Transport Control Protocol), tak i nespolehlivý datagramový přenos užitím protokolu UDP (User Datagram Protocol). Aplikační vrstva sady TCP/IP pak zahrnuje služby všech vyšších (relační, prezentační a aplikační) vrstev modelu OSI.

Protokol IP

Jak už bylo řečeno, pracuje protokol IP na úrovni síťové vrstvy OSI modelu. Jeho základní funkcí je směrování a přenos datových paketů předaných vyššími vrstvami (TCP/UDP) od zdrojového uzlu (odesílatele) k cílovému uzlu (příjemce) sítí tvořenou větším počtem vzájemně propojených dílčích sítí a označovanou jako IP Internet (IP intersíť). Z hlediska služeb definovaných na síťové vrstvě poskytuje IP protokol nezabezpečenou datagramovou službu bez vytváření spojení a potvrzování příjmu paketů. Tyto služby jsou následně v protokolové sadě TCP/IP implementovány ve vrstvách vyšších. Pakety používané IP protokolem jsou označovány jako IP pakety.

Protokol IP pracuje se dvěma různými typy uzlů sítě: koncové uzly (Host) a IP směrovače (IP Router). Zatímco koncové uzly vysílají a přijímají pakety, směrovače zajišťují přenos a směrování paketů mezi jednotlivými subsítěmi. Pro přenosovou službu pak IP protokol vykonává tyto funkce:

adresování koncových uzlů a dílčích sítí v IP intersíti;
vytváření IP paketů z paketů protokolů vyšších vrstev;
směrování IP paketů intersítí;
fragmentace IP paketů.

Zabývejme se nyní jednotlivými činnostmi vykonávanými protokolem IP podrobněji.

Adresování v sítích IP

Principy adresování v prostředí IP intersítě vycházelo z požadavků na efektivní směrování dat v rozsáhlých sítích. Proto bylo použito adresovací schéma, které umožňuje vytváření hierarchické adresové struktury uzlů, logicky rozdělené na jednotlivé dílčí subsítě. IP adresu, jak se hierarchická adresa protokolu IP nazývá, tvoří dvě části: adresa sítě a adresa uzlu (viz obr. 3). Délka IP adresy je 32 bitů, tj. 4 bajty. Symbolicky se adresa zapisuje ve tvaru posloupnosti čtyř dekadických čísel oddělených tečkami. Tvůrci protokolu IP vycházeli z předpokladu, že bude třeba adresovat sítě různého rozsahu o různém počtu uzlů, a definovali tři základní třídy IP adres. Třídy jsou označovány A, B a C a liší se počtem adresovatelných sítí (tj. počtem možných síťových adres) a počtem uzlů, které lze adresovat v rámci každé sítě. Je zřejmé, že při konstantní délce IP adresy jsou počty sítí a počty v nich adresovatelných uzlů nepřímo úměrné. Adresy sítí jsou přidělovány centrálně jednotlivými správci IP adres, a poté přerozdělovány poskytovateli služeb internetu. Adresy uzlů přiděluje správce sítě. K hlavním správcům IP adres patří American Registry for Internet Numbers (ARIN) ve Spojených státech, Résau IP Européene (RIPE) v Evropě či Asia Pacific Network Information Center (APNIC) v Asii.

Jednotlivé třídy se liší hodnotou prvních dvou bitů IP adresy a následnou délkou té její části, která tvoří adresu sítě (viz obr. 4). Kromě tříd A, B a C se v praxi používají ještě některé další speciální adresové třídy a adresy s předem určeným významem. Jde např. o třídu D, která slouží pro tzv. skupinovou adresaci, a třídu E, používanou pro experimentální účely. Vlastnosti jednotlivých adresových tříd a speciálních adres shrnuje tabulka 1.

Vzhledem k neefektivnímu rozdělení adresového prostoru IP adres spočívajícím jak v omezeném počtu uzlů adresovatelných ve třídě C, tak naopak v jejich nevyčerpatelné zásobě ve třídě A se později začal používat adresovací mechanismus označovaný jako podsíťování (Subnetting). Podsíťování spočívá v tom, že část adresového prostoru, která je určena pro adresování uzlů, se rozdělí na dvě části: adresu podsítě a vlastní adresu uzlu. Pro adresu podsítě se využívá souvislého pole bitů začínajícího zleva od adresy sítě, přičemž je velmi důležité mít na zřeteli, že vlastní adresa sítě je nedotknutelná a nesmí být nijak měněna či modifikována. Pole adres uzlů začíná od nejvyššího (nejpravějšího) bitu IP adresy. Formát IP adresy používající podsíťování je naznačen na obr. 5.

Použití podsíťování s sebou samozřejmě přináší další problémy. Zatímco v případě adresování bez použití podsíťování je z hodnoty prvého bajtu IP adresy zřejmé, jaká je její struktura, tj. které třídy adresa je, jakou délku a hodnotu mají její síťová adresa a adresa uzlu, nelze v případě podsíťování tyto údaje zjistit bez použití dalších doplňujících informací. K určení jednotlivých polí IP adresy s podsíťováním se proto používá tzv. maska podsítě (Subnet Mask). Jde o číselný údaj stejné délky, jako je délka IP adresy, který obsahuje hodnoty 1 v bitech určujících adresu sítě a podsítě a hodnoty 0 v bitech určujících adresu uzlu. Implicitní masky podsítí pro jednotlivé třídy bez podsíťování jsou:

pro třídu A – 255.0.0.0
pro třídu B – 255.255.0.0
pro třídu C – 255.255.255.0

Při podsíťování se však nedá použít pro adresu podsítě libovolný počet bitů. Jednak musí být zajištěna možnost adresovat alespoň několik uzlů sítě a naopak musí být naprosto jednoznačně možné určit, zda jde o adresu sítě, či podsítě. Pro adresování uzlů se tedy jako adresa podsítě nepoužívají poslední dva bity IP adresy, pro zajištění jednoznačnosti se jako adresa podsítě nevyužívá první bit pole podsítě, tj. bit bezprostředně následující za adresou sítě. Adresa podsítě mívá tedy délku alespoň dva bity, avšak nejvýše o dva méně, než je délka celého původního zbývajícího pole pro adresování uzlů tak, aby dva poslední bity tohoto pole zůstaly k dispozici pro adresování alespoň čtyř uzlů. Kromě toho by neměly adresu podsítě tvořit samé nuly, protože ne všechna síťová zařízení, především směrovače, nemusejí být nakonfigurována tak, aby takovouto adresu interpretovala správně. Z důvodu nebezpečí kolize s univerzální adresou by rovněž neměla adresa podsítě obsahovat samé jedničky.

IP verze 6

Bez ohledu na skutečně obrovský rozsah IP adres začíná být v souvislosti se stále se rozšiřujícím využíváním sítě internet v adresovém prostoru poněkud těsno. Proto byla vytvořena nová verze IP protokolu, označovaná jako IP verze 6. Hlavní rozdíl oproti IP verze 4, o němž jsme až dosud hovořili, spočívá ve zvětšení adresového rozsahu IP adresy z původních 32 na 128 bitů. Adresy se na rozdíl od předchozí verze zapisují ve tvaru osmice šestnáctkových (hexadecimálních) čísel oddělených dvojtečkami, namísto desítkových čísel oddělených tečkami, jak tomu bylo u verze 4 (viz obr. 6). IP adresy verze 4 tvoří nyní podmnožinu adres IP verze 6 a zapisují se do poslední osmice šestnáctkových čísel. Příklad IP adresy verze 4 v zápisu adresy verze 6 je uveden na obr. 7.

K dalším změnám, které IP verze 6 přináší patří zejména:
změna a zjednodušení záhlaví protokolu;
automatická konfigurace uzlů umožňující automatické přiřazování adres uzlům a směrovačům;
nové bezpečností procedury a kódování;
podpora multimediálních aplikací.

Vytváření IP paketů z paketů vyšších vrstev

Vytváření IP paketů probíhá na základě informací předaných IP protokolu vyšší vrstvou. K nim patří zejména adresa zdrojového uzlu, adresa cílového uzlu, vlastní paket transportní vrstvy s přenášenými daty a doplňující informace, které slouží k upřesnění parametrů přenosu paketu intersítí. K nim patří např. doba existence (života) paketu v síti, tj. doba, po jejímž uplynutí bude paket zrušen, aby se v intersíti nepohybovaly pakety, které z nějakého důvodu nedosáhly cíle, údaje o možnosti fragmentace paketu pro případné rozdělení paketu do většího počtu datagramů či identifikace protokolu vyšší vrstvy cílového uzlu. Protokol IP na základě těchto informací vytvoří IP datagram, doplní jej záhlavím a vypočte zabezpečovací informace. Paket předaný od vyšší vrstvy pak v jednom či více vytvořených datagramech odešle cílovému uzlu.

Protokol ARP

Protokol IP pracuje s IP adresami. Vlastní komunikace v síti však probíhá, jak bylo řečeno v předchozích částech, prostřednictvím fyzických (MAC) adres. K tomu, aby bylo možné vlastní komunikaci v síti uskutečňovat, potřebuje IP protokol další doplňkové mechanismy, které zabezpečí přiřazení IP adres MAC adresám. K tomuto účelu slouží protokol ARP (Address Resolution Protocol). ARP poskytuje dvě základní služby:

získává MAC adresy odpovídající cílovým IP adresám, s nimiž pracuje protokol IP,
udržuje tabulku přiřazení IP a MAC adres.

Princip činnosti protokolu ARP je jednoduchý. V okamžiku, kdy IP protokol získá od vyšší vrstvy IP adresu cílového uzlu, prohledá ARP lokální tabulku přiřazení IP a MAC adres (ARP Table),

kterou si udržuje. Nenalezne-li požadovanou dvojici adres v lokální tabulce, vyšle do sítě univerzální zprávu (zprávu, která je určena všem uzlům intersítě) s žádostí o předání MAC adresy odpovídající dané IP adrese (ARP Request). Uzel, jemuž je daná IP adresa přiřazena, pak na tuto zprávu odpoví (ARP Reply) příslušnou MAC adresou, kterou si žádající ARP protokol zařadí do své lokální tabulky.

Protokol ICMP

Protokol ICMP (Internet Control Message Protocol) je dalším doplňujícím protokolem IP vrstvy protokolové sady TCP/IP. Jeho úkolem je zajišťovat přenos chybových a řídicích zpráv mezi jednotlivými uzly a směrovači IP intersítě. Řídicí a služební informace jsou předávány v přesně definovaném formátu prostřednictvím speciálních zpráv, tzv. ICMP paketů.

K základním funkcím protokolu ICMP patří:
testování stavu a dostupnosti cílového uzlu;
řízení toku paketů a zahlcení sítě;
aktualizace směrovacích tabulek od jednotlivých směrovačů;
správa a předávání masek podsítí.

Protokol ICMP používá například známá služba PING používaná pro zjišťování dostupnosti uzlů sítě.

V příští části se budeme zabývat směrováním, směrovacími protokoly, směrovači a principy jejich činnosti.

Dag Jeger