Architektura počítačových sítí

24. července 2009

Počítačová síť je souhrné označení HW a SW prostředků, které umožňují komunikaci a výměnu informací mezi počítači.

OSI model

Jedná se o síťový standard pro propojování systémů. Norma neuvádí způsob implementace, ale abstraktní model reálného komunikačního systému. Paralelou může být komunikace dvou manažerů ve firmě. Dopis musí projít až na nějnižší vrstvu - pošťáka, který jej doručí. Zároveň je nutné uprait obálku tak, aby ekvivalent ve druhé společnosti zprávě rozuměl.

1. Fyzická vrstva - jedná se v podstatě o vodič signálu. Definuje způsob přenosu jednotlivých bitů, Definuje elektrické a fyzikální vlastnosti média. Na této vrstvě pracují huby a opakovače.

2. Linková vrstva - zajišťuje propojení dvou bodů na lokální síti (médiu). Rozděluje data z vyšších vrstev na rámce, které jsou sítí odesílány. Umí opravoovat jednoduché chyby a hlásit neopravitelné. Je schopna logicky odělit dvě vedlejší sítě. Zajišťuje přístup k médiu, soupeření o něj. Protokoly jsou Ethernet, TDMA, CSMA, atd.

3. Síťová vrstva - zajišťuje spojení dvou bodů mimo lokální síť. Zajišťuje hierarchickou adresaci, směrování, informace o stavu sítě, atd. Protokol IP.

4. Transportní vrstva - Určuje způsob spojení a jeho kvalitu. Mezi protokoly patří třeba TCP a UDP. TCP zajišťuje spolehlivý přenost dat. Naproti tomu UDP je nespojovaná služba, která nechává spolehlivost na aplikaci.

5. Relační vrstva - Vytváří, ruší a udržuje spojení mezi dvěma uzly sítě a řídí spojení mezi nimi. Příkladem je například SSH, SSL, NFS.

6. Prezentační vrstva - Má za úkol přeložit data z lokálně používaného formátu do formátu používaného sítí a opačně. Příkladem je protokol SMB. HTML

7. Aplikační vrstva - Zpřístupňuje síť jednotlivým aplikacím. Řadíme sem například FTP, DNS, POP3, SSH.

Síťové (směrovací) protokoly (IP) a směrovače

Mezi síťové protokoly patří například ARP pro překlad ze síťových adres na hardwarové, IPSec, což je obohacení IP protokolu o bezpečnostní prvky a zejména protokol IP, který je základem dnešního Internetu.

IP se používá pro přenos informací dat v sítích ve formě paketů datagramů - paketů. Pakety putují sítí nezávisle na sobě. Pro jejich přenos není nutné apriori ustavovat spojení. Protokol nezajišťuje spolehlivost přenosu. Každý z prvků po cestě se snaží o best-effort, tedy dělá maximum proto, aby byly pakety doručeny. Paket nemusí být doručen vůbec nebo může být doručen několikrát. Nic se nepředpokládá o pořadí doručení.

Každému komunikujícímu rozhraní používajícímu IP protokol je přiřazena jednoznačná adresa - identifikátor (alespoň v rámci sítě). Datagramy obsahují adresu odesilatele i příjemce. Podle adresy je pak po cestě rozhodováno, jak mají být pakety směrovány (ve směrovačích).

Dnes se nejčastěji používá IP protokol verze 4. Jeho adresa je 32 bitů dlouhá a zpravidla se zapisuje bytech oddělených tečkou (například 192.168.1.3). Původním předpokladem bylo, že jednotlivé byty budou rozlišovat sítě a podsítě (192.168/16 je podsítí 192/8), ale pro nedostatečný počet IP adres se dnes používá pro označení posítí prefix (nebo maska podsítě). Dále rozlišujeme speciální adresy - například zpětnou adresu tzv. loopback (127.0.0.1), adresy pro všesměrové vysílání, atd.

Novou verzí protokolu by měla být verze 6. Jednak rozšiřuje počet adres (délka je nyní 128 bitů) a dále přidává nové vlastnosti jako je šifrování (zpětně implementováno do IPv4), podpora mobility, bezstavovou autokonfiguraci, atd.

Pomocným protokolem souvisejícím s IP je ICMP. Pomocí něho se uzly vzájemně informují o svém stavu, stejně jako jednotlivé uzly o stavu sítě. Je generován jako reakce na chyby - příkladem je TTL expired, destination unreacheble, redirect

Úkolem směrování je nalezení cesty mezi dvěma uzly sítě. Buď se používá statická varianta, kde jsou cesty předdefinovány nebo adaptivní varianta schopná reagovat na změny v síti - dynamické směrování. Podle toho, zda sm2rova4e po cestě rozhodují samy za sebe či globálně rozlišujeme přeposílání a směrování. Směrování v Internetu je step-by-step, deterministické, distribuované, jednocestné, jednocestné.

Pro směrování je samozřejmě důležitý výběr nejkratší cesty jsou využívány algoritmy Dijkstra (neustálé přepočítávání vzdálenosti daného vrcholu od počátku) a Bellman-Ford (mohou být i záporné hrany). Využíváme zejména protokoly OSPF, RIP a BGP.

Algoritmus RIP používá princip distance vector, kdy si každý uzel pamatuje vzdálenost ke každému jinému uzlu, a algoritmu Bellman-Ford. Získanou informaci, kterou si uzly přeposílají mezi sebou nikdy nezasílá zpět, aby nedošlo k zacyklení. Používá se pro směrování uvnitř autonomních systémů (pod správou nějaké organizace).

Algoritmus OSPF využívá algoritmus link state. Udržuje informace o celé síti (periodickými informacemi o sousedech, změny jsou posíláy všem) a neustále přepočítává informace. Používán uvnitř AS. Využívá Dijkstrova algoritmu.

Algoritmus BGP je používán pro směrování mezi AS. Využívá pricip path-vector, což je obdoba distance vector, ale pamatuje si celou cestu. Nepočítá se pouze nejkraší cesta, ale i další možné informace jako load-balancing, atd.

Směrovací tabulky jsou velmi rozsáhlé. Směruje se na základě adres sítí - podle nejdelšího prefixu.

Transportní protokoly - TCP, UPD a další

Odpovídají transportní vrstvě ISO/OSI modelu. Tyto protokoly zajišťují spolehlivý přenos a případně určitou míru kvality.

Protokol TCP je jedním ze základních protokolů současného Internetu. Umožnuje vytvoření spojení mezi dvěma uzly a přenost informací mezi nimi. Je zajištěno spolehlivé doručování a doručení ve zprávném pořadí. Umí rozlišit data pro různá spojení na dané IP adrese přes tzv. porty - každému procesu, který komunikuje je přiřazen port. Příjemce posílá potvrzení, že dané pakety obdržel. Neobdržené nebo poškozené pakety je možné poslat opakovaně. Důležitou součástí protokolu TCP je řízení zahlcení. Po cestě od odesílající strany k příjemci je spousta aktivních prvků, jejichž výkon nemusí být dostatečný, aby zvládl obsloužit proud paketů takovou rychlostí jakou jsou odesílány. Vysílající strana začíná vysílat pomalým startem - zašle ve svém okně dva segmenty. Příjemce potvrzuje každé dva přijaté pakety. Za každé potvrzení, odesílající zvýší o jeden paket okno. Skončí jakmile dosáhne určité hranice sstresh a přechází do ochrany zahlcení. Zvýší okno o jeden segment za každý RTT (dobu pro vyslání a vrácení informace od odesilatele k cíly). Pokud se ztratí pakety - dublované potvrzení, pak se přepočítá sstresh jako maximum z dat na cestě/2 a dvojnásobku segmentu. Poté se v případě Tahoe varianty vrátí k pomalému startu, v případě Reno k ochraně zahlcení. Pro ustavení TCP spojení se využívá třífázový handshake. Odesílatel odešle *Návrh na spojení a návrh sekvenčního čísla.* Příjemce potvrdí a pošle inkrement sekvenčního čísla. První strana potvrdí a odešle další inkrement.

Protokol UDP je nespojovanou službou. Nezaručuje doručení paketů, jejich pořadí ani cestu. Je ovšem rychlejší. Využívá se například při multicastu, kdy by potvrzování příliš zatěžovalo síť.

RTP je protokol postavený, ale částečně realizující vlastnosti TCP jako například číslování paketů. Používá se pro multimediální přenosy po síti, kdy je nutné zajistit pořadí paketů, ale ztracené pakety je zbytečné přeposílat.

Služby počítačových sítí

V souvislosti se stítěmi mluvíme v součastnosti nejčastěji o přístupu k informacím, nejčastěji na webu. Rozlišujeme dva základní pricipy: jednak pull model, kdy si uživatel informace explicitně vyžádá například přes prohlížeč. Podle typu požadovaných dat je vyžadována i různá šířka pásma. Naproti tomu push model není explixitně vyžádán a je zasílán automaticky na základěznalosti uživatelova profilu - jde dejme tomu o zasílání informačních sms o dané oblasti.

Další důležitou službou počítačových sítí je telepřítomnost. Jde o jednal základní a jednoduché protokoly jako je například email nebo usenetové skupiny přes různé typy chatu typu IRC, Jabber, ICQ, které poskytují textovou komunikaci případně kombinovanou o výměnu souborů (dat) přes VOIP, tedy hlasové služby až po různé systémy umožňující silovou vazbu na dálku. Podle složitosti také roste náročnost na šířku pásma. Tyto služby umožňují rychlejší komunikaci, spolupráci (i na velkou vzdálenost) a ,,přiblížení“.

Dalšími službami jsou distribuované výpočty a gridy. Ty umožňují sdílení výkonu a prostoru. Neformálně řečeno se poskládá výkon několika slabších počítačů připojených k síti a vytvoří se dojem jednoho silného stroje.

Principy přenosu dat

Jedná se o problematiku fyzické a linkové vrstvy. Data se přenášejí signály. Problémem je jaké kódování do signálů použít. Využívá se elektromagnetických a optických signálů. Pro přenos dat využíváme vlastností signálů - fázový posun, frekvence, intenzita. Kontrolujeme změny těchto vlastností a tyto změny dekódujeme jako daný signál.

V principu rozlišujeme dva základní typy signálu - analogový se spojitou změnou funkční hodnoty v čase a hodnotě a digitální signál se skokovou změnou. Zároveň s tím samozřejmě můžeme rozlišit analogová a digitální data. Signály jsou komponentní jevy - skádají se z harmonických složek - různých sinusovek. Rozsah frekvencí složek signálu určuje šířku pásma. Problémem při přenosu signálu jsou přenosové defekty - ať už jde o zkreslení, útlum nebo šum. Ty snižují kvalitu signálu.

Přenosová média jsou vodičová a nevodičová. Digitální data digitálním přenosem lze přenášet přímo. Pro analogový přenos používáme fázový, frekvenční nebo aplitudový posun - modulace signálu. Analogová data pro přenos digitálním signálem je nutno vzorkovat (například PCM). Pro přenos analogově je nutné je přeložit do cílového signálu amplitudovou, fázovou nebo frekvenční modulací.

Problémem z hlediska IT je synchronizace - vzorkování musí probíhat všude ve stejné části signálu, detekce chyb, oprava chyb a podpora rozhraní. Dále je nutné zajistit řízení datového spoje - tedy správu soupeření o médium, přeposlání chybných přenosů, řízení objemu přenášených dat.

Rozdělení média pro víc spojů se provádí multiplexováním - časovým, frekvenčním. Častokrát se v rámci signálu řeší i samotná synchronizace - například Manchester u LAN.

Modem kóduje digitální data na analogový signál. Naproti tomu codec analogový signál na digitální.

Komunikační sítě, protokoly, protokolové sestavy

Jako příklady komunikačních sítí můžeme uvést telefonní a datovou síť. První z nich je spojovanou sítí, udržující spojení po celou dobu (nutnou). Přenáší se analogový signál. Je také zajištěna netriviální kvalita dat. Naproti tomu datové sítě jsou digitální s nezajištěnou kvalitou, ale jsou bezstavové a nevyžadují tak velký overhead. Kompromisem mezi nimi měla být ATM, která vybrané vlastnosti tel. sítí přenášela na datové - zajišťovala kvalitu dat, udržovala spojení po celou dobu, avšak vykazovala obrovskou režijní zátěž a dnes se považuje za mrtvou technologii.

Další dimenzí jsou potom spojované a nespojované služby. V případě prvních z nich je spojení udržováno po celou dobu spojení, což jednak může znamenat neefektivní využití pásma a pak taky zátěž na celou síť. Takové spojení se také těžko vyrovná s výpadkem a spojení je ztraceno. Na druhou stranu máme zajištěnou určitou kvalitu služeb.

Protokol je předpis určující jakým způsobem a jakými zprávami spolu budou dva uzly komunikovat. Určují kódování zpráv, jejich zpracování a způsob spojení

a výměny dat. Řídí syntaxi, sémantiku a synchronizaci komunikace. Mohou být realizovány přes HW i SW. Zpravidla jsou schopné dojednat i některé parametry spojení.

Přesný popis protokolů usnadňuje implementaci aplikací a zároveň, pokud jsou protokoly otevřené může vést k rychlešímu vývoji. Příkladem protokolů je například IP, TCP, UDP, HTTP a další.

Návrh protokolů může být velmi náročnou a zdlouhavou činností, kdy je potřeba model navrhnout, otestovat, opravit chyby, implementovat, verifikovat proti modelu a otestovat. Samozřejmě každá s fází může ovlivnit předchozí fáze a vyžádat si na nich změnu.

Pro popis se často používá abstraktní formální notace vycházející z notace Pascalu.

Protokolovými sestavami potom rozumíme kombinaci více protokolů (a jejich použití), takže z určitého hlediska mohou vytvářet dojem jednoho komunikačního protokolu.

Přenosové systémy pro WAN

WAN neboli Wide area network je počítačová síť, která pokrývá rozsáhlé území (překračuje území města/státu). Největší WAN sítí je Internet. Obecně jsou používány pro propojení lokálních sítí LAN (nebo podobných), takže uživatelé jedné sítě mohou komunikovat s uživateli sítě jiné. Spousta WAN je budováno pro nějaké společnosti a jsou soukromé. Ostatní jsou provozovány a budovány nějakými ISP. Propojení LAN sítí může být provedeno na pronajatých linkách (End-to-end). Je drahé, ale bezpečné používají se protokoly PPP, HDLC.

Další možností je přepojování okruhů (analogie s telefonními spojeními) a přepojování paketů. První je velmi levné, ale vyžaduje sestavení spojení. Používají se protokoly PPP a ISDN. U druhého je problémem sdílení média a tudíž nezajištěná kvalita. Používají se protokoly X.25 a Frame Relay. Poslední možností je přeposílání buněk - paketů stejné délky. To je vhodné pro kombinaci hlasu a dat, ale zase vyžaduje extrémní režijní nároky. Protokolem je ATM.

V případě použití optických vláken se používají protokoly SDH a SONET.

Architektury LAN/MAN

LAN jsou lokální sítě pokrývající malé území - například domácnost, dům, společnost. Vyznačuje se vysokými rychlostmi - až GiB/s. Nejčastěji používané technologie jsou Ethernet a Wifi, dříve token-ring. Zpravidla jsou budovány na vlastní náklady jednotlivci a firmami. Umožňují sdílení připojených prostředků - diskového prostoru a tiskáren.

MAN jsou propojené LAN na území města, které společně využívají společnosti. Využívá se Wi-fi a optické vlákno.

Používají se následující architektury:

- Sběrnice - průběžné spojoací vedení z něhož jsou odbočky ke každému připojenému přístroji. Má malou spotřebu materiálu a rychlý přístup, ale médium je logicky neodděleno a je citlivé na poruchy. Konce kablů je nutné zajistit terminátorem, aby se signál neodrážel zpět.

- Hvězda - Jednotlivé stanice jsou připojeny na centrální prvek - switch. Ten přijme a přepošle požadavek. V praxi vytváří stromovou strukturu

(vnitřními uzly jsou huby). Selhání počítače neovlivní síť, síť snadno rozšíříme. Centrální prvek je slabé místo. Více kabelů víc stojí.

- Kruh - stanice jsou propojeny tak, že vytváří kruh. Zprávy jsou předávány od stanice ke stanici. Protože se jedná o jednosměrné dvoubodové propojení, je možné kombinovat média. Je velmi průchodný, jednodušše zapojitelný, ale citlivý na výpadek i jen jednoho uzlu. Je u něj nutné řešit problém ztráty a zdvojení oprávnění.

Prvky pro tvorbu propojených sítí a propojování sítí

Jedná se o propojení dvou fyzických spojů za účelem zvýšení počtu připojených uzlů, logického oddělení provozu. Pro jejich spojení používáme princip přepínání.

Základním aktivním prvkem je most - bridge - vytváří transparentní přemostění dvou sítí. Všechen provoz prochází přes něj, ale oddělí fyzická média, takže kolize se nepřenáší. Můstek naslouchá na médiu a sleduje adresy. Podle toho rozhoduje, zda má nějaká data přeposlat z jedné sítě do druhé. Zasílá podle cílové adresy. Informace časem expirují a jsou zapomenuty.

Pomocí můstků lze vytvořit cykly. Pak je nutné vypočítat kostru grafu. Používá se distribuovaný algortimus. Uzel s nejnižší adresou se vezme jako kořen. Postupně se vybírají uzly s nejkratší vzdáleností a nejmenší adresou. Nepoužité porty se vypínají. Každý můstek posílá periodicky svoji adresu a vzdálenost od kořene. Podle zprávy od sousedů upraví svoji znalost. Informace stárne, není propagována hned - zabrání se cyklům.

Switche jsou v podstatě víceportové můstky. Dá se říct, že se jedná o směrování na druhé vrstvě. Vhodné pro malé sítě,

Směrovače

Aktivní prvky propojující sítě na síťové vrstvě. viz IP

Technologie bezdrátových komuničních systémů a bezdrátových místních smyček

Bezdrátovým spojením rozumíme spojení dvou komunikujících stran jiným než mechanickým způsobem (kabelem). Podle nosného média pak rozlišujeme komunikaci optickou, radiovou a sonickou. Vzdálenost může být od několika málo metrů (infračervené spojení) do milionů kilometrů (ve vesmíru).

Pro optickou komunikaci můžeme použít laserová pojítka, infračervené spoje, signální komunikaci (vlajky, kouř). Pod rádiovým spojením si můžeme představit spojení pro rozhlas a televizi, mobilní sítě atd. Sonickou komunikaci používají lidé při verbální komunikaci, ale je také využívána například ponorkami v sonaru.

V počítačové komunikaci se používá zejména nelicencované pásmo 2.4GHz. Je možné s ním připojit notebook, jehož uživatel cestuje (nemá možnost být připojen napevno). Dalším způsobem připojení je satelitní komunikace.

Důvody pro použití bezdrátové komunikace jsou zejména vzdálenost znemožňující použití kabelu, překonávání fyzických překážek, použití bezdrátu jako záložního připojení, ustavení dočasného spojení a vzdálené připojení.

V praxi se setkáváme s point-to-point spojeními, point-to-multipoint komunikací, plošným vysíláním (broadcast) a celuárními sítěmi.

Bezdrátovou místní smyčkou rozumíme širokopásmové připojení typu point-to-multipoint. Představuje řešení tzv. poslední míle (poslední část připojení vedoucí od ISP k uživateli. De facto drát do uživatelova počítače), kdy má ISP přístup k uživateli. Přípojka uživatele je fixní (stálá) - rozdíl oproti GSM, kde se uživatel pohybuje.

Dalším rozdílem oproti GSM je, že bezd. místní smyčky jsou spíše typem sítě. Nemají jasně definované protokoly a pravidla a záleží na konkrétním případě, co bude použito.

První variantou jsou úzkopásmová spojení (zejména pro hlas). Využívají například 2.4 GHz, 3,5 GHz, atd. širokopásmová spojení mají pak podstatně vyšší rychlost, ale požadují přímou viditelnost a jsou náchylná na atmosferické vlivy. (10.5, 26, 28, 40 GHz).

Do této kategorie připojení je možné ještě zařadit celuární princip - síť je tvořena základnovými stanicemi, z nichž každá spravuje okolo sebe buňku. Terminály uživatele pak komunikují s tou nejbližší. Oproti GSM (kde je přístup také použit) není vysílání všesměrové a je vždy po nějakým úhlem směrováno na vysílač (pod ostrým úhlem). Princip však vyžaduje, aby sousední stanice používali jiné frekvenční pásmo, což znamená problém pro návrh sítě. Kapacita se dělí mezi uživatele dané oblasti.

Mobilita v propojených sítích

Mobilita nám umožňuje připojit se i bez kabelu k síti a potažmo k Internetu. Klasickým příkladem technologie podporující mobilitu je zejména GSM. Ta má však značně omoezenou kapacitu prodatové přenosy. Pro ně jsou určeny zejména dva protokoly - Wifi používaná uvniře budov a WIMAX používaná zejména na dlouhé vzdálenosti.

Výhodou mobilních sítí je zejména vysoká pružnost, možnost sestavení ad-hoc sítí bez předešlého plánování, žádné problémy s kabeláží. Na druhou stranu zpravidla mají značně menší šířku pásma než kabelová připojení, problémem bývají rozdílná pravidla v jednotlivých státech a prosazování standardů.

GSM je nejpoužívanějším standardem pro mobilní telef. sítě na světě. Díky vzájemným roamingovým smlouvám se z GSM stává dostupná síť témeř kdekoliv. Blíží se tedy nejblíže ideálu mobility - tedy připojení odkudkoliv. Síť GSM je buňková síť, tedy síť vyslílačů, z nichž každý kolem sebe vytváří a spravuje buňku - ucelenou oblast. Ačkoliv byla podpora datových přenosů záhy dodána (GSM je digitální sítí), není pro přenos dat idální (malá šířka pásma).

Wifi je standardem pro lokální bezdrátové sítě WLAN. Umožňuje vytváření lokálních sítí (i ad hoc sítí). Sítě se navzájem od sebe odlišují identifikátorem SSID, což je řetězec ASCII znaků. Ten je v pravidelných intervalech vysílán jako broadcast. Toto vysílání není nutné (z hlediska bezpečnosti je i výhodnější jej vypnout). Uživatel pak musí apriori SSID znát.

Rozlišujeme dva typy spojení. Ad-hoc sítě - spojení dvou počítačů na krátkou vzdálenost. Obě strany jsou si rovné. Dalším typem jsou infrastrukturní sítě - síť obsahuje jeden nebo více access points, které vysílají SSID. Problematické je v souvislosti s Wifi zajištění bezpečnosti. Signál je totiž šířen všesměrově a není možné zabránit odposlechu. Jednou z možností je kontrola MAC adresy.

Další možností je zabezpečení 802.1X, WEP (symetrický klíč), WPA (WEP klíče dynamicky měněny za chodu).

WiMax je rozvíjejícím se standardem pro venkovní bezdrátové sítě. Je základem pro metropolitní sítě. V nejnovějších verzích standardu není už nutná přímá viditelnost, ale klesla také rychlost přenosu. WiMax je navrženo tak, aby jednotlivým zařízením bylo možné přidávat další funkce bez porušení vzájemné kompatibility. Využívá licencovaná i nelicencovaná pásma.

Bezdrátová LAN

Bezdrátová LAN neboli WLAN jsou místní bezdrátové sítě, které je možné chápat jako obdobu klasických LAN sítí. Má tedy omezený rozsah a provozovatelem je její vlastník.

Výhodou mobilních sítí je zejména vysoká pružnost, možnost sestavení ad-hoc sítí bez předešlého plánování, žádné problémy s kabeláží. Na druhou stranu zpravidla mají značně menší šířku pásma než kabelová připojení, problémem bývají rozdílná pravidla v jednotlivých státech a prosazování standardů.

Cílem je předávání účastníků mezi sítěmi - Roaming (bez toho, aby to pocítili), postačí nízký výkon (baterie), odolná síť, snadná použitelnost, bezpečnost, transparentnost.

Pro výstavbu WLAN se používají rádiové vlny.

Rozlišujeme dva typy spojení. Ad-hoc sítě - spojení dvou počítačů na krátkou vzdálenost. Obě strany jsou si rovné. Dalším typem jsou infrastrukturní sítě - síť obsahuje jeden nebo více access points, které vysílají SSID. Problematické je v souvislosti s Wifi zajištění bezpečnosti. Signál je totiž šířen všesměrově a není možné zabránit odposlechu. Jednou z možností je kontrola MAC adresy. Další možností je zabezpečení 802.1X, WEP (symetrický klíč), WPA (WEP klíče dynamicky měněny za chodu).

Pro potřeby multiplexingu přenosu signálu se používá FHSS (frequency hopping, vysílač i přijímač se dohodnout na vzorku přeskakování frekvencí) a DSSS (rozprostření spektra, bit je překódaván tak, aby z něho samotného šlo poznat, kdo je odesilatelem).

Charakteristiky WLAN sítě: Asociace (každá stanice v dané chvíli s jedním přístupovým bodem), přeasociování (řízená změna AP stanicí), zrušení asociace, distribuce (cesta ze stanice přes síť k cíli), integrace (distribuce s výstuním AP), autentizace.

Pro přístup k médiu se používají pricipy CSMA (pokud je klid, stanice vysílá), konkrétně CSMA/CD (vysílání je ukončeno, pokud je detekována kolize) a CSMA/CA (je-li médium volné dostatečně dlouho, pak vysílá, jinak čeká. Přijímač musí nejprve přenos potvrdit - ACK), kterou používá třeba Wifi.

Pro zajištění synchronizace se do sítě posílají rámce, které obsahují údaje o čase a další správní data (roaming, atd.).

Používají se standardy 802.11a a 802.11g.

Správa sítí

Pod správou sítí rozumíme sledování jednotlivých prvků sítě (a jejich kombinací), analýzu získaných dat, proaktivní a reaktivní správu.

Monitorujeme jak aktivní prvky, které často nějakou úroveň správy samy implementují, tak i pasivní prvky. Kontrolujeme celkové zatížení (a přetížení).

Kontrolujeme zda správně pracuje směrování. Je vhodné monitorovat, zda jsou uplatňovány podmínky a smlouvy související s provozem a používáním sítě a na základě toho sledovat podezřelé chování účastníků.

Další dimenzí jsou správa výkonu (sledujeme nejen výkon jednotlivých prvků, ale i výkon celku - například end-to-end. Podpora SNMP protokolem), správa chyb (zaměřena na okamžité problémy - záznam, detekce a náprava chybových stavů), správa konfigurací (kontrolujeme, co je na síti, co se má sledovat; důležitá správa konfigurací - konfigurace z minulého pátku), správa účetnictví (hlídáme, kdo byl na síti, kdy a co dělal; možná návaznost na ekonomickou stránku) a správa bezpečnosti (povolení nebo odmítnutí přístupu podle definovaných vlastností; autorizace; dále s ní souvisí správa klíčů a firewallů atd.).

Rozlišujeme správce, který správu provádí, spravovanou entitu a protokoly, které jsou př správě použity. Spravovaným objektem je třeba router, switch, modem, tiskárna, atd. Může být tvořen i více objekty. Protokol správy zajišťuje komunikaci mezi spravovaným objektem a správcem (oboustraně - umožňuje zadávat příkazy a přijímat informace) - příkladem je třeba SNMP nebo OSI CMISE/CMIP.

SNMP vrací například čítač počtu datagrmů verzi směrovacího protokolu a stavovou informaci. Pro popis objektu se používá SMI jazyk. Definuje syntaxi a sémantiku informačních zpráv.

Zajištění bezpečnosti v sítích

Stejně jako v kryptografii se snažíme minimalizovat škodu, kterou může způsobit útočník.

Rozlišujeme dva základní rozměry - jedna AAA - autentizace, autorizace, accounting a pak zabezpečenou komunikace po síti.

Autentizací rozumíme identifikaci ve smyslu - *Já jsem.* Pro zajištění buď používáme sdílené heslo (symetrický klíč), asymtrické klíče (certifikáty X.509) nebo důvěryhodnou třetí stranu, která naši identitu potvrdí (Kerberos).

Autorizací rozumíme povolení používat danou službu nebo zdroj. Určuje úroveň oprávnění.

Accountingem rozumíme účtování co, kdo a v jakém rozsahu použil. O použití se uchovává záznam pro pozdější využití. Je nutná spolupráce s autentizací.

Zabezpečená komunikace - požadujeme aby jen odesilatel a příjemce rozuměli zprávě, autentizaci, integritu (potvrzení, že zpráva nebyla změněna) a nepopiratelnost.

V současnosti se objevují dva nové faktory - nevysledovatelnost a anonymita.

Používají se symetrické (DES, 3DES - trojnásobný průchod DES a AES. Všechny jsou blokové) i asymetrické protokoly a digitální podpis (neměl by se dát podvrhnout).

Pro zajištění integrity dat lze použít hashovací funkce - například SHA. Digitální podpis zajišťují asymetrické protokoly RSA a DSA.

Příkladem autentizačních protokolů jsou potom PAP a CHAP. První posílá heslo otevřeně. U druhého obě strany heslo znají a posílá se jen hash.

Certifikační autorita podepisuje veřejné klíče, címž se za ně zaručuje.

Typickým příkladem je zabezpečení emailu - protokol PGP zajišťuje autentizaci, integritu i šifrování. Klíče šíří sám uživatel.

SSL je základem pro TLS, což je protokol pro autentizaci klienta, serveru a šifrované spojení mezi nimi. Spojení se vyjedná na základě asymetrické kryptografie, vyjedná se šifrovací mechanismus, symetrický klíč a dále se používá symetrická kryptografie.

Na síťové vrstvě se šifruje pomocí IPSec - do hlavičky IP paketů se přidávají další položky. Jednak Authetication header pro autentizaci obou stran, zajištění integrity a pak encapsulation header pro šifrování paketů.

Hrozby pro síť jsou DoS (znepřístupnění služby), modifikace dat a získání soukromých dat. Ochranaa má několik úrovní fyzická (zabránit přístupu), softwarová (autentizace, šifrování, včasný zásah) a právní.

Firewally tvoří logické odpojení od Internetu - povolují jen určité služby.

Ochranou proti všem hrozbám je nepodcenění, monitoring, výchova uživatelů a postupy pro případ útoku.

Zajištění kvality síťových služeb

Základní parametry linky jsou kapacita, zpoždění, rozptyl. Pro zajištění vlastností je třeba udělat úpravy tak, aby se data nepředbíhala (nekradla si výkon), na vysílajícím a přijímajícím a aktivních prvcích po cestě.

Z tohoto pohledu jsou pro kvalitu služeb důležité fronty na jednotlivých prvcích sítě. Ovlivňují zpoždění a rozptyl a řazení paketů na výstupu.

Rozlišujeme tyto fronty:

- FIFO - obyčejná fronta, žádná priorita. Agresivní proudy jsou zvýhodněny.
- Fair queueing - různé fronty pro různé proudy. Fronty jsou obsluhovány po jednom paketu z každé. Penalizuje však krátké pakety.
- Processor sharing - každá fronta sdílí přesně 1/N kapacity. Posílá jen bity. Je pouze teoretickým návrhem.
- Bit-round fair queueing - je PS na úrovni paketů. Je férový, protože nikdo nepředbíhá a délka nehraje roli. Na druhou stranu neumožňují prioritu.

Práce s frontami značně ovlivňuje zpoždění, tedy je ho pak možné shora omezit.

Ochrana zahlcení nastupuje příliš pozdě. Používán tzv. RED - random early detection - zahazuje pakety dříve, než se fronta zaplní.

Popsaná řešení však nestačí je nutné řídit zdroje a koordinovat požadavky na ně. Je nutné rezervovat prostředky dopředu. K tomu slouží dva protokoly RSVP a DiffServ.

RSVP zajišťuje rezervaci zdrojů po cestě ze zdroje k cíli. Podporuje Multicast i Unicast. Je nutné rezervovat pro každý směr zvlášť. Kvůli multicastu rezervuje příjemce. Je tzv. soft statem - nutno po čase obnovit.

DiffServ naproti tomu umožňuje prioritu toků. Definuje pouze prioritní třídy, které zajišťují požadované vlastnosti. Hraniční směrovače takové sítě mohou pakety zahodit nebo pozdržet. Problémem protokolu jsou pouze statistické garance.

Další možností řešní QoS je ATM, která rozděluje proud do stejně velkých segmentů. Je spojovanou službou. Je schopný zajistit constant bit-rate(emulace vlastní linky), real-time b.r. (tok se v čase mění), available a unspecified b.r

(best-effort). Protokol je chopný dynamicky měnit rychlost přenostu podle stavu sítě. Neuchytil se, protože má příliš velký over-head.