7. Architektura počítačových sítí, OSI model, IP, transportní protokoly (TCP, UDP a další), základní služby počítačových sítí. Bezpečnost, základy kryptografie, soukromé a veřejné klíče, autentizační protokoly, digitální podpis. Správa sítí, směrování, směrovací protokoly. Firewalls, řízení přístupu. Kvalita služeb.

Architektura počítačových sítí

Parametry sítě dle nároků aplikací:

- **Propustnost** – objem přenesených dat za jednotku času
- **Zpoždění** (latence) – doba mezi požadavkem a odezvou
- **Rozptyl** (jitter) – kolísání zpoždění

Architektura počítačové sítě určuje strukturu sítě – z jakých stavebních a funkčních celků se skládá a jak tyto celky spolupracují. Většina sítí je organizována ve vrstvách (s tím pak souvisí ISO/OSI model) a počet vrstev a jejich vlastnosti se liší síť od sítě.

Pro dva síťové uzly platí, že pokud je komunikace mezi nimi pomocí sítě možná, pak vrstva *n* prvního uzlu komunikuje vždy s vrstvou *n* druhého uzlu. Pravidla takové komunikace se nazývají *protokol*. Např. 10baseT Ethernet se na fyzické vrstvě domlouvá protokolem Manchester.

Součástí protokolu je:

- syntax – formátování dat, tvar signálových prvků (Manchester)
- sémantika – řídící informace pro koordinaci, reakce na chyby (např. CSMA/CD - Carrier Sense Multiple Access/Collision Detection, CSMA/CA - WIFI)
- časování – rychlost přenosu signálů po médiu (např. 10baseT – 10Mhz)

MAC – Medium Access Control (řízení přístupu k médiu)

Protokoly pro MAC mohou být založeny na:

- soupeření (connection-based) - Aloha, CSMA, Ethernet (CSMA/CD)
- rezervaci prostředků (času, kanálu) – TDMA (GSM), SDH a SONET, ATM
- předávání oprávnění (token-based) - Token Bus, Token Ring
- kombinaci předchozích metod

Faktory, jež ovlivňují výběr MAC protokolu:

- konfigurace spoje (jednosměrný, half duplex, full duplex)
- (ne)možnost všesměrového vysílání
- topologie spoje (point-to-point, bus, ring)
- spolehlivost a chybovost
- přenosová rychlost (b/s)
- vzdálenost nebo délka vedení

- rychlost šíření signálu v médiu
- zpoždění signálu v aktivních prvcích

MAC protokoly se soupeřením
Negarantují, kdy bude moci stanice vysílat. (Garantují, že nemusí vysílat nikdy. ;))

Alohavznikl na Hawaii

- všesměrové rádiové vysílání
- každá stanice vysílá, kdykoliv má požadavek
- využití teoretické kapacity kanálu max. 18 %

CSMA
- Carrier Sense Multiple Access
- nesynchronizovaná kolizní metoda (jako Aloha)
- vysílající poslouchá signál
- tři druhy
    - **nenaléhající CSMA** – je-li kanál obsazen, čeká náhodný interval
    - **1-naléhající CSMA** – čeká, dokud není volno, potom okamžitě vysílá
    - ***p*-naléhající CSMA** – je-li volno, vysílá s pravděpodobností *p* (*p* by měla být menší než 1/(počet vysílajících))

CSMA/CD

- CSMA/Collision Detection
- dtto CSMA, navíc vysílající poslouchá při vlastním vysílání
- zjistí-li kolizi, přeruší vysílání a vyšle rušící signál, aby kolizi detekovala i druhá vysílající stanice
- **není použitelné u rádiových přenosů**, protože přijímací část by při současném vysílání i naslouchání byla zahlcena vlastním signálem (rušila by sama sebe)

CSMA/CA

- CSMA/Collision Avoidance
- nenaléhající CSMA, začátek čekacího intervalu je synchronizován na pravidelný čas
- **použití v bezdrátových sítích**
- potřeba opakování přenosu na základě potvrzení přijetí rámce

Ethernet

- 1-naléhající CSMA/CD s exponenciálním růstem čekacího intervalu
- průchodnost se zmenšuje a zpoždění zvětšuje s rostoucím počtem vysílajících stanic
- není spravedlivý:
    - pravděpodobnost vysílání při další příležitosti je menší u stanice, která je déle blokována
    - stanice vysílající delší pakety jsou zvýhodněné
    - spravedlivost roste s počtem stanic (ale…)
- řešení ⇒ propojení přepínačem (dojde ke zmenšení kolizních domén)

MAC s rezervací

- TDMA (Time Division Multi Access) – pevně stanovená časová okna pro každou stanici (např. GSM)

SDH a SONET

- Synchronous Digital Hierarchy (Evropa), Synchronous Optical NETwork (USA)
- protokoly pro vysoké rychlosti na optických médiích
- stejné principy, odlišné časování
- striktně point-to-point
- vychází z multiplexování digitalizovaných telefonních hovorů
- *synchronní* – data jednotlivých příspěvkových toků se vždy nachází na stejném místě v rámci; rámce jsou neustále generovány na základě jednotného hodinového signálu
- na vzdálenosti tisíců kilometrů
- 10 Gb na stovky kilometrů, experimentálně 40 Gb

ATM

- vznikl na popud několika velkých firem
- Cíle:
    - podpora pro všechny existující i budoucí služby
    - efektivní využití zdrojů
    - zjednodušené směrování → vysoké rychlosti
    - QoS (Quality of Service) pro existující i budoucí služby
- rodina protokolů od síťové po fyzickou vrstvu
- **malé rámce pevné délky 53 B** – buňky
- PCR – Peak Cell Rate – špičková přenosová rychlost
- SCR – Sustainable Cell Rate – agregovaná přenosová rychlost za nějakou dobu
- dohoda o parametrech spojení při jeho ustavení (connection-oriented služba)
- zvláštní protokolové vrstvy pro přizpůsobení běžným potřebám
- nakonec max. 622 Mb/s
- Typy provozu (BR = Bit Rate)
    - CBR (Constant BR) – specifikuje se datový tok, emulace pevné linky, snadná implementace, PCR=SCR
    - VBR (Variable BR) – složitá implementace, definuje zvlášť PCR a SCR
        - VBR-rt (real time) – streaming, pevně stanovené zpoždění
        - VBR-nrt (non-real time) – video on-demand, neexistují pevné limity pro zpoždění
    - ABR (Available BR) – pokus o adaptabilní službu typu TCP
        - Resource Management Cell – obsahuje informaci o požadavku na PCR, zajišťuje tak explicitně kontrolu zahlcení, přepínače po cestě RM sníží, nebo zachovají, cíl pošle RM s aktuální hodnotou vysílajícímu
    - UBR (Unspecified BR) – Best effort služba, je možné definovat PCR

MAC s předáváním oprávnění

- oprávnění vysílat (token) má vždy jedna stanice, je předáváno
- MAC protokol musí obsloužit chybové a neobvyklé stavy
    - vytvoření tokenu při inicializaci

    - obnovení tokenu po ztrátě v důsledku chyby média
    - obnovení tokenu po ztrátě či zdvojení v důsledku chyby nebo vypnutí některé stanice
- řešeno algoritmy distribuované dohody
- Token Bus – topologické uspořádání sběrnice
- Token Ring – topologické uspořádání kruh

OSI referenční model (Open Systems Interconnection)

OSI je abstraktní model počítačové sítě založený na 7 vrstvách:

- **fyzická** – specifikuje fyzickou komunikaci, signály na přenosovém médiu. Hlavní poskytované funkce: Navazování a ukončování spojení s komunikačním médiem; modulace a demodulace digitálních dat na signály používané přenosovým médiem.
- **spojová (linková)** – přenos rámců mezi dvěma systémy, uspořádává data z fyzické vrstvy do logických celků (rámce), formátuje rámce, opatřuje je fyzickou adresou. Na této vrstvě pracují veškeré mosty a přepínače.
- **síťová** – Tato vrstva se stará o směrování v síti a síťové adresování. Poskytuje spojení mezi systémy, které spolu přímo nesousedí. Obsahuje funkce, které umožňují překlenout rozdílné vlastnosti technologií v přenosových sítích. Síťová vrstva poskytuje směrovací funkce a také reportuje o problémech při doručování dat. Veškeré směrovače pracují na této vrstvě a posílají data do jiných sítí. Např. IP.
- **transportní** – zajišťuje přenos dat mezi koncovými uzly. Vrstva nabízí spojově (TCP) a nespojově orientované (UDP) protokoly.
- **relační (session) –** Smyslem vrstvy je organizovat a synchronizovat dialog mezi spolupracujícími relačními vrstvami obou systémů a řídit výměnu dat mezi nimi. Umožňuje vytvoření a ukončení relačního spojení, synchronizaci a obnovení spojení, oznamovaní výjimečných stavů.
- **prezentační –** Funkcí vrstvy je transformovat data do tvaru, který používají aplikace (šifrování, konvertování, komprimace).
- **aplikační –** poskytuje aplikacím služby pro uživatele např. FTP, SMTP

IP

IP protokol orientovaný na přenos dat (používaný v Internetu) a je založený na přepojování paketů (datagramů). Funguje ve třetí vrstvě OSI modelu. Data z vyšších vrstev rozděluje do jednotlivých paketů přiměřené délky, vzhledem k nižším vrstvám, kterým je pak předává. Každý datagram je samostatná datová jednotka, která obsahuje všechny potřebné údaje o adresátovi i odesilateli a pořadovém čísle datagramu ve zprávě. Datagramy putují sítí nezávisle na sobě a pořadí jejich doručení nemusí odpovídat pořadí ve zprávě. Doručení datagramu není zaručeno, spolehlivost musí zajistit vyšší vrstvy (TCP, aplikace).

IP protokol zabezpečuje spojení většinou mezi dvěma koncovými uzly. Spojení se nijak v síti neustavuje.

IP pakety se v sítí doručují podle IP adres. IP protokol verze 4 v současné době používá adresy o délce 32bitů, což dává celkem 2^{32} možných adres (cca 4 miliardy, dnes už téměř nedostačující.)

IPv6

- 128 bitové adresy
- podpora bezpečnosti
- podpora pro mobilní zařízení
- funkce pro zajištění úrovně služeb (QoS - Quality of Service)
- fragmentace paketů - rozdělování
- jednoduchý přechod z IPv4 (musí podporovat systém, provider)
- snadnější automatická konfigurace (NDP - Neighbor discovery protocol)

TCP,UDP a další

TCP je protokol nad IP vrstvou. Zabezpečuje spolehlivé spojení s garantovaným pořadím doručení paketů bez duplicit mezi dvěma síťovými uzly. Této funkce je dosaženo pomocí zasílání ACK (potvrzení) přijatých paketů a číslováním jednotlivých paketů.

TCP

3 way handshake je způsob ustavení TCP spojení. Odehrává se třemi pakety. Klient pošle SYN paket požadující spojení na cílovém hostiteli na určitém portu, cílový hostitel odpoví buď SYN-ACK pokud spojení povolí nebo RST pokud ne. Klient pak pošle ACK zpět serveru.

TCP používá řadu mechanismů pro dosažení co nejlepšího využití pásma a zároveň zamezení zahlcení pásma. Aby nebylo nutné potvrzovat v TCP každý paket, používá TCP tzv. **sliding window** tj. okno, kdy je potvrzení odesíláno až po přijetí vždy několika paketů = velikosti okna paketů.

Pro rychlé zaplnění dostupného pásma používá TCP tzv. **slow start,** kdy exponenciálně zvyšuje množství odesílaných paketů u kterých nečeká na potvrzení. Teprve, když se mu potvrzení přestanou vracet, zpomalí a přejde na lineární zvyšování množství odesílaných paketů.

Různé implementace TCP reagují různě na výpadky paketů. Např. **TCP Reno** má vlastnost **Fast recovery**, kdy po výpadku paketu nezmenšuje velikost vysílacího okna na 1, ale znovu vyšle pakety nepotvrzeného okna a čeká na potvrzení, na 1 se vrátí jen pokud nedostane odpověď.

Obecně s TCP je drobný problém v tom, že bylo navrženo pro spíše pomalejší a chybující sítě. V prostředí vysokorychlostních sítí představují případné ztráty paketů a s tím související zpomalovaní TCP nežádoucí jev. Proto se objevily návrhy High Speed TCP.

ZHRNUTIE:

- potvrzuje zaslané zprávy
- používá piggybacking (potvrzení posílá spolu s dalšími daty)
- pro zachování pořadí čísluje pakety
- pokud nedorazí paket, příjemce vyšle potvrzení o nedoručení a všechny následující pakety zahazuje
- existuje několik různých implementací protokolu (Tahoe, Reno, Vegas – názvy dle měst v Nevadě :))

4 základní algoritmy

- Pomalý start
  - congestion window (`cwnd`), vysílající definuje objem dat, který smí být vyslán
  - receiver advertised window (`rwnd`), příjemce definuje objem dat, který akceptuje
  - po každém potvrzení se zvyšuje `cwnd` o jeden segment (512 B)
  - dochází k exponenciálnímu navyšování objemu posílaných dat až do `ssthresh`, pak končí
- Zábrana zahlcení
  - nárůst pouze lineární
  - `cwnd` se zvyšuje o segment pouze za RTT
  - Round Trip Time – čas, jenž data potřebují na cestu mezi vysílajícím a přijímajícím a zpět)
- Rychlá retransmise
  - reakce na duplikované potvrzení (příjem 3 duplikovaných potvrzení detekuje ztrátu segmentu)
  - následuje jeho opětovné zaslání
- Rychlé vzpamatování
  - jedná se o způsob, jak předejít návratu do fáze pomalý start po ztrátě paketů
  - posíláme více dat a čekáme na potvrzení, podle toho pak upravíme `cwnd`

UDP (User Datagram Protocol)

Nespojovaná, nezajištěná služba (odpovědnost za pakety nese aplikace) 4. vrstvy ISO/OSI. Určená pro prostý přenos paketů. De facto je to rozšíření IP protokolu o informaci o portech.

UDP funguje obdobně jako TCP ve čtvrté vrstvě OSI. Podporuje např. stejně jako TCP porty a umožňuje vytvořit mezi dvěma body spojení. Na rozdíl od TCP však negarantuje doručení ani pořadí paketů. Typicky se používá pro služby, kde výpadek několik paketů nevadí např. voip, a je rozhodující rychlost přenosu před správností.

RTP (Real-time Transport Protocol) – vhodny pro soft real time prevoz, postavený nad UDP protokolem, nezaručuje kvalitu přenosu, pouze poskytuje prostředky pro zaručení kvality aplikacím-číslovanie paketov. Určita nahrada TCP tam, kde striktne poziadavky TCP nie su treba – čiže sú povolene určité vypadky ale nemoze tolerovat prilis velke opozdenie. Musí být doplněn konkrétní aplikační vrstvou. Určen pro multicast, lze jej využít i v unicastovém prostředí.

ICMP (Internet Control Message Protocol)

ICMP plní v Internetu zejména diagnostickou a routovací funkci (Používají ho operační systémy počítačů v síti pro odesílání chybových zpráv atd.). Např. lze vysílat pakety ICMP echo request a pokud cílový uzel má povolenou odpověď na ICMP echo request, pošle zpět ICMP echo reply. Lze posílat pakety s nastaveným TTL – Time To Live a router, který sníží TTL na 0 pošle zpět ICMP time exceeded in transmit. Takto funguje např. traceroute nebo ping. Typů ICMP zpráv je v současné době okolo 40.

IGMP (Internet Group Management Protocol)

Rozšiřuje požadavky na implementaci protokolu IP (IPv4) o podporu IP multicastu. Využívá se pro dynamické přihlašování a odhlašování ze skupiny u multicastového routeru ve své lokální síti.

ARP (Address Resolution Protocol)

Používá se k nalezení fyzické adresy MAC podle známé IP adresy. Protokol v případě potřeby vyšle datagram s informací o hledané IP adrese a adresuje ho všem stanicím v síti. Uzel s hledanou adresou reaguje odpovědí s vyplněnou svou MAC adresou. Pokud hledaný uzel není ve stejném segmentu, odpoví svou adresou příslušný směrovač.

Příbuzný protokol RARP (Reverse Address resolution Protocol) má za úkol najít IP adresu na základě fyzické adresy.

Základní služby počítačových sítí

Pull model – uzivatel si informacie explicetne vyziada napr WWW
Push model – informacie su zasielane automaticky na zaklade uzivatelovho profilu napr. Info SMS
Telepritomost – email, IRC, ICQ, VOIP
Distribuovane vypocty a gridy
Synchronizácia času - NTP
Vzdialena pracovna plocha – VNC, RDP
Adresárové a autentizačné služby – LDAP, Kerberos, PAM
Zdielanie súborov – NFS, CIFS, FTP, SCP resp. SFTP(prenos suborov cez SSH)
Synchronizacia suborov a adresarov - Rsync

Příklady:

- **FTP** – client/server přenos souborů
- **HTTP** – přenos WWW stránek, autentizace
- **HTTPS** – důvěrný (zabezpečený) přenos WWW stránek
- **SIP (Session Initiation Protocol)** – voip
- **SSH (Secure Shell)** – důvěrné vzdálené přihlášení
- **Mail** – přenos elektronické pošty

Bezpečnost

Bezpečností v IT se rozumí souhrn pravidel a praktik pro manipulaci s citlivými informacemi. Informace se zpravidla objevují v nějakém informačním systému. V IS jsou *objekty*, což jsou pasivní entity, které obsahují informace, které přidávají/modifikují subjekty.

Subjekty jsou aktivní entity (osoby, procesy nebo zařízení), které s informacemi pracují.

Bezpečný systém je takový, který se chová jen dle předem daných pravidel.

V bezpečnosti zpravidla pracujeme se třemi základními operacemi:

Autentizace je proces ustavení určité míry jistoty o identitě subjektu, např. já jsem já, zde je můj certifikát.

Autorizace je proces zpravidla následující po autentizaci, který přiděluje subjektu práva např. k manipulaci s objekty.

Accounting je proces vytváření záznamů o tom, co subjekty prováděly s jakými objekty.

Základy kryptografie

Klasickou kryptografickou úlohou je bezpečná komunikace po nezabezpečených kanálech.

Podrobnější pohled požaduje od kryptografických funkcí zabezpečení:

- **Utajení (Confidentality)** – kdy přenášeným informací rozumí jen přijímající a odesílající subjekt.
- **Integrita (Integrity)** – kdy přenášená informace nemůže být nepozorovaně změněna.
- **Nepopiratelnost (Non-repudability)** – kdy odesílající subjekt nemůže popřít odeslání informace.
- **Autentizace** – zjištění a prokázání identity buď příjemce nebo odesílatele informace.

V common criterias (mezinárodní standard pro počítačovou bezpečnost) pro hodnocení bezpečnosti informačních systémů se objevily některé nové požadavky, např.

- **Anonymita** – nemožnost spojit si činnost se subjektem, který ji provádí.
- **Nesledovatelnost** – nemožnost spojit si dvě různé akce jednoho subjektu.

Obecně kryptografické funkce jsou matematické funkce, které lze rozdělit na skupiny:

Symetrická kryptografie

- Stejný klíč pro šifrování i dešifrování.
- Problém: distribuce klíčů.
- Výhody: vysoká rychlost, malá délka klíčů, výpočetní náročnost
- Nevýhody: distribucia klučov, počet kľúčov – čím viac kom. strán tým viac kľúčov

Symetrické šifry se často používají společně s asymetrickými. Obvyklé použití je takové, že otevřený text se zašifruje symetrickou šifrou s náhodně vygenerovaným klíčem. Tento symetrický klíč se zašifruje veřejným klíčem asymetrické šifry, takže dešifrovat data může pouze majitel tajného klíče dané asymetrické šifry.

Symetrické šifry se dělí na dva druhy. Proudové šifry (FISH, RC4)zpracovávají otevřený text po jednotlivých bitech. Blokové šifry (AES, DES, IDEA)rozdělí otevřený text na bloky stejné velikosti a doplní vhodným způsobem poslední blok na stejnou velikost. U většiny šifer se používá blok o 64 bitech, AES používá 128 bitů.

Asymetrická kryptografie

- Dvojice klíčů veřejný klíč- šifrovanie/soukromý klíč- dešifrovanie.
- Problémy:
    - Jak se přesvědčit, že veřejný klíč skutečně patří danému subjektu?
    - Pomalost asymetrické kryptografie.
    - Délka klíčů
- Výhody:
    - Množství klíčů
    - Posiela sa len verejný kľúč

Asymetrická kryptografie je založena na tzv. jednocestných funkcích, což jsou operace, které lze snadno provést pouze v jednom směru: ze vstupu lze snadno spočítat výstup, z výstupu však je velmi obtížné nalézt vstup. Nejběžnějším příkladem je například násobení: je velmi snadné vynásobit dvě i velmi velká čísla, avšak rozklad součinu na činitele (tzv. faktorizace) je velmi obtížný. (Na tomto problému je založen např. algoritmus RSA.) Dalšími podobnými problémy jsou výpočet diskrétního logaritmu či problém batohu.
Používaná je tiež při elektronickom podpise.

Typickým zástupcem je šifra RSA, dále podpisové schéma DSA, ECDSA nebo El-Gamal.

Hašovací funkce

Jsou funkce, které pro určitý libovolný vstup vygenerují vždy stejný otisk – krátkou posloupnost. V ideálním případě mají tyto vlastnosti:

- Jednosměrnost – z otisku nelze dopočítat vstup.
- Bezkoliznost – nelze najít dvě zprávy se stejným otiskem.

Funkce se používají v elektronickém podpisu jednak pro zajištění integrity a také pro obcházení problému pomalosti asymetrické kryptografie (podepisuje se jen krátký otisk zprávy).

Mezi nejpoužívanější funkce v současné době patří SHA-1 u které se očekává nahrazení funkcemi SHA-2. Z dřívějších jde zejména o MD5.

Digitální podpis

Nebo také elektronický podpis dle direktivy evropské komise o elektronickém podpisu je informace připojená k nějaké zprávě, která zajišťuje právě zmíněné funkce:

- **Integrita** – kdy přenášená informace nemůže být nepozorovaně změněna.
- **Nepopiratelnost** – kdy odesílající subjekt nemůže popřít odeslání informace.
- **Autentizace** – zjištění a prokázání identity buď příjemce nebo odesílatele informace. (a také identifikace, pokud není použit např. pseudonym)

V současné době realizován převážně pomocí prostředků asymetrické kryptografie ve spojení s hašovacími funkcemi.

Autentizační protokoly

Příkladem autentizačních protokolů je např.

PAP (Password AP)

- autentizační protokol, kde hesla cestují v otevřené formě po sítí (plain-text), mohou být odposlouchávána.

CHAP (Challenge-handshake AP)

- challenge/response protokol, heslo se neposílá přes síť
- obě strany znají heslo, posiela sa hash MD5

RADIUS a TACACS

- Služby pro autentizaci a následnou autorizaci přístupu.
- Autentizaci neprovádí uživatel, ale zařízení kam se uživatel hlásí.
- Autentizace zahrnuje i autorizaci.
- RADIUS je složitější, používá challenge response, může být hierarchický a umí i záložní server.Protokol je rozšiřitelný.

Správa sítí

Správa sítí

Principem správy sítí je monitoring jednotlivých prvků a analýza výsledků.

- Reaktivní řízení - reakce na problémy
- Proaktivní - detekce možnosti vzniku problémů a předcházení jim

Dle ISO je rozdělení správy sítě na:

- Správa výkonu (SNMP)
- Správa chyb (SNMP traps)
- Správa konfigurací (často proprietární)
- Správa účtování (detekce uživatelů)
- Správa bezpečnosti (autorizace, ochrana před zneužitím)

SNMP (Simple Network Management Protocol)

Základem SNMP je definice objektů. Např. COUNTER – čítač paketů rozhraní, INTEGER – index rozhraní atd. Tyto informace jsou pak sdruženy do modulů.

Jazyk pro definici dat se nazývá SMI.

SNMP funguje na principu request – response, kdy řídící subjekt vydá požadavek, ten je přenesen řídícímu agentu spravované entity a následně je zpět přenesena odpověď.

Má tři verze: druhá obsahuje navíc autentizaci a třetí šifrování. Nejvíce zařízení podporuje druhou verzi.

Směrování, směrovací protokoly

Směrování

Směrovací schémata mohou být:

Distribuované vs. centralizované
„**Krok za krokem**“ vs. zdrojové
Deterministické (predurčený) vs. stochastické (náhodný)
Jednocestné vs. vícecestné
Dynamický vs. statický výběr cest

Pakety prochází řadou směrovačů. Směrování může být statické i dynamické.

Statické směrování

- známe topologii
- existuje centrální směrovací tabulka, bývá zpracovávána „ručně“ off-line. Díky tomu může být optimální pro danou topologii vzhledem k zadaným kritériím
- výhodou je jednoduchost, nevýhoda je vyšší citlivost na výpadky v síti a zátěž

Dynamické směrování

- adaptabilní na výpadky
- realizováno složitými algoritmy
- dynamické periodické výměny tabulek (dochází k dočasné nekonzistenci)
- hierarchie směrování

Směrovací algoritmy

Statické algoritmy

- jednorázové tabulky (často ručně vytvořené)
- neflexibilní, hodí se pro statickou topologii
- lze je dobře optimalizovat

Dynamické algoritmy

- flexibilní a robustní
- nutnost zajistit aktualizaci směrovacích tabulek, potřebují protokol
- Dále se dělí na:
    - centralizované – stav se posílá do centra, centrum posílá tabulky uzlům
    - izolované – řešeno metodou náhodné procházky, vyžaduje zpětnou vazbu, šíření tabulek broadcastem = vysoká zátěž sítě
    - distribuované – uzly spolu vzájemně spolupracují
- dochází k periodické výměně směrovacích informací

Síť je reprezentována jako graf. Uzly jsou jednotlivé prvky sítě, hrany jsou komunikační linky mezi jednotlivými uzly. Hrany mohou být ohodnoceny – lze určit cenu komunikace.

Hierarchie směrování

- Směrování k sítím (autonomní systémy)
- Směrování uvnitř sítí

Směrování Distance Vector

- Předpoklad: každý směrovač zná pouze cestu (adresa) a cenu (hrana) k sousedům
- Cíl: směrovací tabulka pro každý cíl v každém směrovači
- Idea: oznam sousedům svou představu tabulky

DV algoritmus

- Distance Vector = dvojice <Cíl, Cena>
- inicializace – sousedé se známou cenou, zbývající uzly mají cenu nastavenu na nekonečno
- Periodické zasílání kopií DV sousedům
- Problém zacyklení (při výpadku hrany) řešen dělením horizontu, směrovač nikdy nesděluje cestu zpět k uzlu, od nějž se ji dozvěděl
- Typický zástupce: RIP (Routing Information Protocol)

Směrování Link State

- Stejný předpoklad a cíl jako u DV
- Idea: šíří se topologie, cesty si směrovače počítají samy
- Pracuje ve dvou krocích
    - šíření topologie (broadcast)
    - výpočet nejkratší cesty (Dijkstra)

Typický zástupce: OSPF (Open Shortest Path First)

Směrování ještě jednou trošku jinak:

Základní úrovně směrování v Internetu jsou:

- V lokálních sítích a podsítích
- V autonomních systémech
- Mezi autonomními systémy
- Páteřní směrování

Směrování v lokální sítí se realizuje na základě cílové IP adresy, IP adresy odesílatele a masky sítě odesílatele. Na základě těchto údajů se prohledá routovací tabulka a najde se nejdelší prefix a packet se pošle na adresu příslušné brány. Brána může být i default gateway.

Směrování uvnitř AS zpravidla funguje tak, že směrovač zná IP adresu a masku podsítě každé sítě v AS a zná ke každé takovéto síti optimální cestu. Směrování zpravidla funguje pomocí směrovacích algoritmů buď

- Distance vector – RIP
- Link based – OSPF

Distance vector protokoly fungují na základě periodického rozesílání své routovací tabulky ostatním hostům + přeposílání ostatních přijatých tabulek. Metrikou je pak počet hopů. Typickým zástupcem je protokol RIP (Routing Information Protocol) – směrovací protokol umožňující směrovačům (routerům) komunikovat mezi sebou a reagovat na změny topologie počítačové sítě. Ačkoliv tento protokol patří mezi nejstarší doposud používané směrovací protokoly v sítích IP, má stále své uplatnění v menších sítích a to především pro svoji nenáročnou konfiguraci a jednoduchost.

OSPF (Open Shortest Path First) funguje na základě zasílání Link State informací a Dijsktrova algoritmu, kdy každý směrovač dostane orientovaný graf sítě s ohodnocenými hranami. Ohodnocení představuje cenu cest. Cena cest se přenáší jako kumulativní součet.

Každý router v OSPF si udržuje ponětí o svých sousedech pomocí periodického OSPF Hello a o něco méně periodické zasílání LS zpráv. LS zprávy také dostává pokud se změní topologie sítě.

Zasílání LS zpráv je omezeno na jednu area (oblast). Jedna oblast může být označena jako páteřní a hraniční směrovače pak musí náležet do páteře a nejméně do jedné další oblasti.

Na hranicích OSPF area jsou zpravidla routery náležející jak do vnitřní sítě, kde používají OSPF (nebo I-BGP) tak ven, kde používají zpravidla BGP-4.

Směrování mezi AS
AS mohou být tři typy:

- *Multihomed* – AS, který si udržuje spojení k více ISP, většinou pro případ výpadku. Přes tento AS zpravidla netečou žádná tranzitní data.
- *Stub* – AS, který je připojen pouze k jednomu ISP.
- *Transit* – Tranzitní AS pro připojování dalších ISP.

BGP-4

Path-vector protocol - směrovače si mezi sebou vyměňují celé cesty zahrnující všechny skoky.

Základem protokolu je zasílání oznámení – advertisements, která obsahují adresu cílové sítě, atributy cesty a identifikaci next-hop routeru

Základními operacemi BGP routeru jsou:

- Vysílání oznámení
- Přijímání a filtrování oznámení
- Výběr cesty

Předpokládá se, že BGP peerové nelžou o tom co posílají – případně lze filtrovat, pokud by posílali nesmysly. Filtrují se také vlastní cesty pro případ vzniku cyklů.

Zasílání oznámení definuje administrátor systému a umožňuje mu řídit kam potečou data.

Peerování se vesměs realizuje nepsanými dohodami či smlouvami. Příkladem je NIX.CZ.

BGP peering se realizuje ustaveným TCP spojením na portu 179, může být i autentizované.

Routovací tabulka vnějšího BGP směrovače v současné době roste k 200 tis. záznamů.

Firewalls, řízení přístupu

Firewall představuje logické odpojení od Internetu, které v podstatě rozliší mezi vnitřní a vnější sítí. Provoz, který jím pak prochází filtruje na základě nějakých pravidel. Firewall může fungovat buď na úrovni paketů nebo na úrovni aplikací – aplikační brána.
Příkladem takového zařízení je router s překladem adres **(NAT**), i když nejde přímo o firewall.
Paketový firewall (packet filter) funguje na základě analýzy zdrojové a cílové adresy a portů a řídících dat. Umí např. zabránit podvržení adresy zvenčí, umí blokovat iniciaci spojení zvenčí, ale povolit iniciaci spojení zevnitř sítě atd. Analyzuje hlavičky každého datagramu
Aplikační brána komunikuje přímo s uživatelovou aplikací – komunikace může být i transparentní. Příkladem je HTTP proxy nebo antivirový server pro kontrolu pošty.
Kontroluje obsah datagramů

Kvalita služeb

Základní úlohu v zajištění kvality služeb hrají linky a aktivní prvky na jejich koncích. Linky mají:

- zpoždění
- rozptyl
- kapacitu

Aktivní prvky mají na vysílací straně frontu paketů, kterou mohou ovlivňovat. Fronta může být:

- FIFO – nejjednodušší. Nemá žádnou podporu priority a nerozlišuje mezi krátkými a dlouhými pakety. Většinou vyšší latence.
- Fair Queue – každý paket je umístěn do příslušné fronty a ty se postupně obsluhují.
- Weighted Fair Queue – funguje stejně jako FQ, ale umožňuje jednotlivé fronty prioritizovat.
- Weighted Round Robin – obsluhuje z každé fronty určitý počet paketů daný jejich průměrnou velikostí.

Kvůli vlastnostem TCP může na zatížených sítích dojít ke stavu, kdy vlivem přetížení začnou všechny TCP proudy zpomalovat a zas pak zrychlovat. Aby se tomuto zabránilo používají se různé postupy, např.:

- RED – zahazuje pakety dříve než dojde k zahlcení
- IP ECN – v tomto případě si dva komunikující hosti musí domluvit, že ji budou používat.

Sestavení prioritizované relace na Internetu lze řešit buď vytvořením nějaké stavové informace po cestě – protokol RSVP nebo označováním paketů ToS nyní DiffServe.

RSVP (Resource reSerVation Protocol)

- Protokol, definující, jak jsou rezervovány zdroje na aktivních prvcích mezi odesílatelem a příjemcem
- Podpora unicastu i multicastu (navržen primárně pro multicast)
- Jednosměrnost: rezervace pro každý směr zvlášť
- Rezervaci iniciuje přijímající strana
- Obě vlastnosti vyplývají z charakteru multicastu
- Soft stav – brání nekonečnému blokování rezervovaných prostředků

DiffServ:

- Flexibilní, škálovatelný.
- Nedefinuje třídy služeb, pouze předdefinované prioritní třídy s různou rezervací zdrojů.
- Poskytuje rámec (funkční komponenty) z nichž je možné flexibilní službu sestavit – hraniční funkce a funkce jádra.
- Stará se primárně o datový tok.
- Vnitřní směrovače znají jen několik tříd a jejich prioritu. Hraniční směrovače řadí příchozí pakety do konkrétních tříd. Jádro prioritizuje pakety podle návěstí toku.
- Jediná stavová informace je držena na vstupním hraničním směrovači (nemusí být držena celou cestu).