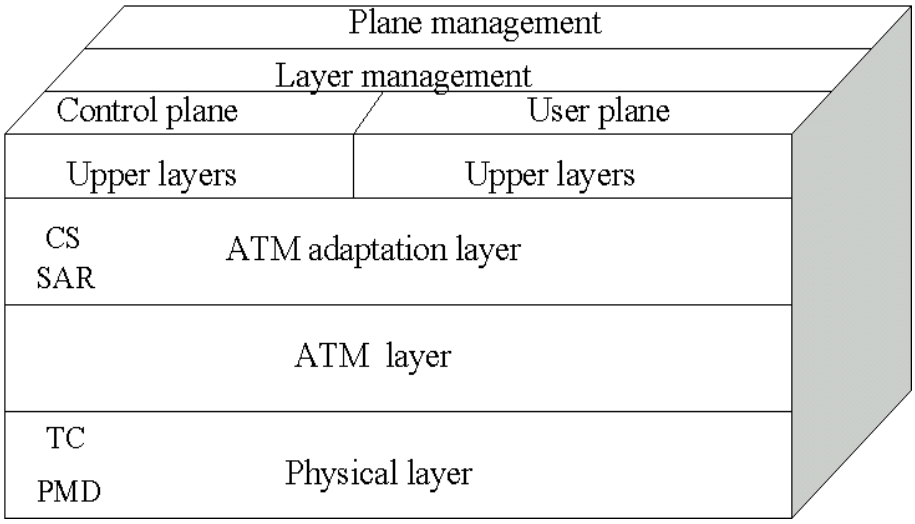
Projektování distribuovaných systémů

vypracované státnicové okruhy

1 Současné trendy vývoje komunikačních technologií: základy ATM (referenční model ATM, ATM buňka, AAL, signalizace, adresy, okruhy, QoS, kategorie služeb, CBR, VBR-rt, VBR-nrt, ABR, UBR, řízení provozu CAC, UPC, tvarování, směrování, IISP, PNNI)

Základní vlastnosti ATM:

- spojově orientovaná technologie
- ATM síť – soubor přepínačů propojených 2bodovými spoji
- data jsou rozděleny do ATM buněk o velikosti 53 bytů (z toho 5 bytů hlavička)
- přenosové rychlosti až 155 Mbit/s
- 2 typy rozhraní:
  - UNI (User Node Interface) – propojení směrovačů, hostitelských systémů s ATM přepínači
  - NNI (Network Node Interface) – vzájemné propojení přepínačů



ATM spojení:

- propojení virtuálními okruhy
- virtuální cesty (virtual path) VPI (identifikátor)
  - obsahují více virtuálních kanálů
- virtuální kanály (virtual channel) VCI (identifikátor)
- přepínání virtuálních cest / kanálů
- VPI a VCI mají pouze lokální význam (vztahuje se k lince)
- typy spojení:
  - PVC (Permanent Virtual Circuit): VPI/VCI nastavováno ručně
  - SVC (Switched Virtual Circuit): dynamické vytváření a rušení spojení (signalizační protokoly)
  - Soft PVC
    - PVC vytvářeno manuálně na úrovni UNI, dynamicky mezi NNI

- spojení typu Bod – Bod
  - jednosměrné nebo obousměrné
- spojení typu Bod – Multibod
  - jednosměrné
  - kořen a list (počátek, konec), připojování (join) a odpojování (leave) listů k doručovacímu stromu

ATM buňka

- přenášená data rozděleny do jednotlivých buněk
- velikost 53 bytů (48 bytů data, 5 bytů hlavička)
- použití buněk je z důvodu co nejmenšího zpoždění přenosu

AAL (ATM Adaptation Layers)

- adaptační vrstvy ATM, kvůli podpoře protokolů, které nejsou založeny na ATM
- definují, jak rozdělovat pakety vyšších vrtsev do ATM buněk
- příklady „služeb“, které potřebují AAL – Gb Ethernet, IP, Frame Relay, SONET, UMTS …
- **hlavní činnosti AAL**:
  - segmentace a skládání paketů vyšších vrstev
  - ošetření chyb přenosu
  - ošetření ztracených a špatně umístěných buněk
  - časování a řízení toku
- **typy AAL**:
  - *Type 1*:
    podpora CBR, synchronní, spojově orientovaný, podpora T1, E1 a x64kbit/s emulace
  - *Type 2*:
    VBR-RT, synchronní, spojově orientovaný, podpora Voice over ATM
  - *Type 3/4*:
    VBR, asynchronní, spojově/nespojově orientovaný, podpora Frame Relay, X.25
  - *Type 5*:
    podobné typu 3/4, podpora IP over ATM, Ethernet over ATM, SIMDS, LAN emulation (LANE), nejvíce rozšířený

Signalizace

- využívá virtuální kanál VPI/VCI = 0/5
- vytvářené spojení je potvrzované
- signalizační protokol zjednodušení Q.2931

Adresace

- identifikace zdrojových a cílových uzlů
- typy:
  - *Peer model*
    - využívání adresování i smerovacích protokolů „neseného“ protokolu (IP, OSPF)
    - složitější ATM přepínače
  - *Subnetwork (Overlay) model*

        - nové adresní schéma
        - existující protokoly operují nad ATM
        - obdoba IP nad X.25 nebo IP nad PPP
        - potřeba ARP (mapování IP adres na ATM adresy)
        - oddělení ATM od vyšších protokolů
- 3 formáty adres:
    - NSAP E.164 (ITU)
    - DCC (Data Country Code) – státy
    - ICD (BSI) – organizace

QoS (Quality of Services)

QoS - vlastnost sítě, pomocí které je možné rozlišovat mezi různými třídami přenosů a chápat je diferencovaně.

Při vytváření spojení ATM sítí mohou aplikace specifikovat parametry, které se vztahují k charakteristice přenášeného provozu:

- *PCR (Peak Cell Rate)*
  maximální okamžitá rychlost vysílání buněk
- *SCR (Sustained Cell Rate)*
  rychlost vysílání měřená v dlouhodobém průměru
- *CLR (Cell Loss Ratio)*
  poměrné množství buněk ztracených sítí z důvodu chyb nebo zahlcení
- *CTD (Cell Transfer Delay)*
  zpoždení buňky mezi vstupním a výstupním bodem sítě
- *CDV (Cell Delay Variation)*
  míra kolísání CTD
- *BT (Burst Tolerance)*
  maximální velikost nárazového provozu, který může být zasílán maximální okamžitou rychlostí (PCR)
- *MCR (Minimum Cell Rate)*
  minimální požadovaná rychlost

Třídy služeb

Důvod: různé požadavky na různé charakter přenosu.

CBR (Constant Bit Rate)

- konstatní rychlost přenosu
- garance max. přenosového zpoždění
- buňka vyhrazena pro CBR nemůže být použita jinak
- použití: vše co by jinak potřeboval samostatný „drát“ nebo generuje konstantní datový tok (nekomprimované video, zvuk...)

VBR (Variable Bit Rate)

- každý přenos dohodne kapacitu mezi MIN a MAX (kapacita do MAX rezervována)
- nevyužité buňky se mohou využít jinak
- RT-VBR (Real Time) – minimální nebo garantované zpoždění (kompr. obraz, zvuk)

- NRT-VBR (Non Real Time) – dávkové přenosy (transakční systémy, rezervační systémy)

ABR (Available Bit Rate)

- každý přenos dohodne kapacitu mezi MIN a MAX (kapacita MIN rezervována)
- vyšší než MIN je poskytnuta pouze, pokud jsou volné zdroje
- použití: propojení LAN sítí

UBR (Unspecified Bit Rate)

- žádné garance
- požadavky jsou prováděny až po provedení CBR, VBR a ABR
- jako „BestEffort“ z paketových přenosů
- použití FIFO pro data, která čekají na zpracování
- použití: aplikace tolerující nepravidelnost doručování a možnosti ztráty dat (IP, UDP, TCP)

Směrování

Směrovací protokoly:

- *IISP (Interim Inter-Switch Signaling protocol)*
  jednoduchý protokol s manuálně konfigurovanými tabulkami v přepínačích, limitovaná rozlehlost sítě
- *P-NNI (Private NNI)*
  směrování v privátních sítích, podpora QoS
  hierarchie, link-state, stejný algoritmus jako používá OSPF
- *B-ICI (Broadband Inter-Carrier Interface)*
  směrování ve veřejných sítích

CAC (Connection Admision Control)

„Funkce“, která zhodnotí dostupné místní zdroje a rozhodne jestli jsou dostačují pro přenos dat, tak aby byli splněny požadavky na QoS.

2 Multiprotokolové sítě nad ATM (klasické IP, RFC1483, RFC1577, NHRP), emulace LAN (LANE) a MPOA, MPLS

Protokoly L3 nad ATM

- přenos nativního protokolu přes ATM síť
- dva problémy:
  - zapouzdření paketu
  - resoluce adresy (IP – ATM)

tři řešení zapozdření a resoluce adresy:

LANE (LAN Emulation)

- MAC protokol použitý pro realizaci transparentních LAN služeb nad ATM

Operace v původním režimu (native mode)

- **Classical IP and multiprotokol Encapsulation over ATM (Classical IP over ATM)**
  - založeno na protokolech definujících IP konektivitu nad ATM s použitím:
    - zapouzdření IP nad ATM (obecně protokol L3)
    - resoluce ATM adresy ze síťové adresy ATM

Tag Switching

- kombinuje výhody směrování s výkonností přepínání

Classical IP and multiprotokol Encapsulation over ATM

Classical IP and ARP over ATM (RFC1577)

- používá přepínané virtuální okruhy (SVCC) a permanentní virtuální kanály (PVCC)
- specifikuje mechanismus pro resoluci a a vyhledávání adres
- velké bloky dat jsou „rozsekány“ na 48bytové kusy
- ATM použito k přímé náhradě propojení LAN segmentů (**LIS – Logical IP Subnets**, identické s konvenčními LAN subsítěmi) obsahujících stanice s IP adresami a směrovači
- systémy v různých LIS mají různé síťové adresy a mohou komunikovat pouze prostřednictvím směrovačů, i když jsou v téže ATM síti
- resoluce adres: ATMARP, InATMARP
  - v ATM neexistují broadcasty: řešeno ATMARP serverem, který obsahuje tabulku IP a ATM adres pro jednu síť
  - libovolný klient může získat ATM adresu zařízení a navázat tak přímo spojení
  - v každé LIS musí být směrovač, konfigurovaný jako ATMARP klient nebo lépe ve směrovači může běžet ATMARP server

Multiprotocol Encapsulation over ATM AAL5 (RFC1483)

- definuje zapouzdření různých typů PDU pro transport nad ATM
- zajišťuje i přenos jiných rámců než jsou IP pakety

- 2 možnosti jak to zařídit:
  - **LLC/SNAP zapouzdření** – různé protokoly mohou být přenášeny jedním ATM spojením a identifikovány standardním LLC/SNAP záhlavím
  - **Multiplexování** virtuálního spojení – přes ATM je přenášen pouze jeden protokol, který je implicitně dán při vytváření spojení

NHRP (Next Hop Routing Protocol)

- cílem je dosáhnout switchovaného provozu místo směrovaného
- 2 typy cest:
  - *přes routery*
    potřeba IP adresy cíle na každém routeru -> složení celého paketu a „znovurozsekání“ -> složité
  - *přes ATM switche díky NHRP*
    klient se dotáže NHRP serveru na ATM adresu cíle, poté je vytvořeno spojení přímo přes ATM síť (ATM switche)

LANE (LAN Emulation)

- důvod vzniku: použít „LAN-based“ aplikace v ATM sítích
- v ATM neexistuje broadcast, multiacast, doručení datagramů podle MAC adresy
- konverzní vrstva LANE zajišťující převod nespojovaných služeb do spojovaného prostředí
  - emulace se týká pouze okrajů sítě, tzn. LANE se nachází jen u koncových uživatelů a aktivních prvků typu směrovač nebo ethernet switch
- **Komponenty sítě**:
  - *LEC (LANE Client)*
    koncové zařízení
  - *LES (LANE Server)*
    jen jeden pro každou emulovanou LAN, řídící funkce (převody adres ...)
  - *BUS (Broadcast and Unknown Server)*
    server, který se stará o rozesílání paketů typu broadcast a multicast
  - *LECS (LANE Configuration Server)*
    jeden pro každou doménu, přiděluje konfigurační informace

MPOA (Multiprotokol over ATM)

- řeší zapozdření a resoluci adres
- *MPOA server*
  výpočetní zpracování (správa adres, topologické informace)
- *MPOA client*
  provádí vlastní fyzické směrování paketů

MPLS (Multiprotocol Label Switching)

- značkování paketů a řízení jejich přenosu sítí
- switche se rozhodují podle značek, na konci jsou značky odebrány
- inteligence je soustředěna do hranových zařízení
- *Architektura:*
  směrování, přepínání, řídící komponenta, forwardovací tabulka, forwarding equivalence class, label

3 Principy VLAN

- rozdělení fyzicky propojených počítačů do logických segmentů, které fungují tak, jako by nebyli fyzicky propojené, vznik samostatné broadcastové domény
- mobilita uživatelů
- lepší bezpečnost a výkonnost (přenosy uvnitř VLAN jsou přepínané, mezi VLAN směrované)
- členství ve VLAN:
  - *podle portů (VLAN úroveň 1)*
    - neumožňuje mobilitu
    - nižší bezpečnost, izolovanost
    - nezkoumá se obsah rámce
  - *podle MAC adres (VLAN úroveň 2)*
    - předchozí registrace počítačů
    - počítače různých VLAN mohou být na jednom portu
    - mobilita uživatelů, vysoká bezpečnost
    - složitá administrace
  - *podle protokolu L3 a vyšší (VLAN úroveň 2)*
    - členství odvozeno od pole TYPE
    - pomalejší než předchozí typy -> musí se analyzovat paket
    - IP adresa je pouze použita na mapování do VLAN, není jinak zpracována
- **Trunk**
  - přenos více VLAN jednou linkou -> propojení lokálních sítí
  - rámce Ethernetu jsou označována VLAN ID (tag)
- zapouzdření **IEEE 802.1Q**
  - až 4095 VLAN
  - všechny typy VLAN
  - dovoluje míchat klasické i VLAN přepínače
  - IEEE 802.1p přidává priority
- **GVRP (Generic Attribute Registration Protocol VLAN Registration Protocol)**
  - vytváření a propagace dynamických VLAN položek
  - GARP členové vytváří / ruší členství ve VLAN
  - VLAN přepínače propagují změny členství ve VLAN na všechny aktivní porty
- **GMRP (Group Multicast Registration Protocol)**
  - položky registrace skupin

4 IP QoS, IntServ, DiffServ, RSVP

QoS (Quality of Services)

- schopnost sítě zajišťovat lepší služby vybraným přenosům
- principy:
  - **Princip 1 – značkování paketů**
  - **Princip 2 – vzájemná izolace tříd**
    - mechanismus pro zařazení zdrojů podle požadavků na šířku pásma
    - kontrola dodržování dohodnutých rychlostí
    - označení paketů probíhá na okrajích sítě
  - **Princip 3**
    - při izolaci tříd využít zdroje co nejefektněji
    - nepodporovat přenosy, které překračují kapacitu linky
  - **Princip 4**
    - Call Admission Proces – kontrola na vstupu
    - potřeby se deklarují předem
- **algoritmy rozvrhování:**
  - *FIFO*
  - *Prioritní rozvrhování* – třídám přiřazena různá priorita
  - *Round Robin (Cyklická obsluha)* – více tříd obsluhy, cyklické testování front
  - *Weighted Fair Queueing (WFC)* – zobecněný Round Robin, všechny stejnou prioritu
- **Token Bucket:**
  - mechanismus politiky
  - pověření spojeno s právem vysílat paket nebo množství dat
  - pokud neexistuje pověření vysílat, paket je zahozen
  - pověření jsou doplňovány stálou rychlostí

Best Effort (s maximálním úsilím)

- aplikace posílají data, kdy se jim zachce
- síť se snaží přenést data co nejlépe i když nemohou data doručit
- použití: doručování v IP sítích

Integrated Services (Integrované služby)

- aplikace předem oznámí síti své požadavky -> síť se rozhodne zda může požadavkům vyhovět (vstupní kontrola požadavků – **admission control**)
- v případě úspěchu jsou informovány všechny komponenty, aby pro přenos rezervovaly odpovídající prostředky -> rezervační protokoly (RSVP)
- IntServ rozlišují mezi kategoriemi aplikací:
  - *elastické aplikace*
    bez požadavků na doručení (např. http, e-mail)
  - *Real Time Tolerant (RTT)*
    požadováno omezení na max. zpoždění, občasná ztráta přijatelná (např. bufferované video)

- *Real Time Intolerant (RTI)*
  požadována minimální odezva a rozptyl zpoždění (jitter) (např. videokonference)

Differentiated Services (Rozlišované služby)

- aplikace neoznamuje předem své požadavky na QoS
- použití rezervačních protokolů není nutné
- pakety jsou značkovány třídou přenosu (značkování probíhá na vstupu sítě)
- směrovače během přenosu čtou značku a podle ní řídí způsob zpracování paketu
- **klasifikace paketů:**
  - TOS (type of services – IPv4), Traffic Class (IPv6)
  - DSCP (DiffServ Codepoint) – 6bit značka
- **zpracování paketů:**
  - PHB (peer hop behaviour): směrovače zpracovávají pakety nezávisle na ostatních
    - *expedicted forwarding (urychlené)*
      pakety jsou odesílané průměrnou rychlostí, která se rovná alespoň stanovené rychlosti
    - *assured forwarding (zajištěné)*
      4 třídy paketů, každé třídě přidělen určitý objem prostředků, každému paketu přiřazena jedna ze tří priorit zahození v případě zahlcení

RSVP (Resource reSerVation Protocol)

- rezervace zdrojů pro přenos
- hosti- požadavky na rezervaci
- směrovače – forward požadavků na rezervaci dalším směrovačům
- pracuje nad existujícím směrováním
- identifikace spojení:
  - IPv4 – cíl. adresa, protokolem, cíl. portem
  - IPv6 – IP adresa, flow label, cíl. IP adresa
- zpráva obsahuje **flowspec** (požadavky QoS) a **filterspec/session id**
- způsoby rezervace:
  - *fixed filter (FF)* - daný zdroj spojen s daným flowspec
  - *shared explicit filter* – více zdrojů s daným flowspec
  - wildcard filter – sdílí flowspec zdrojů mezi toky od různých zdrojů
- udržování rezervace zprávami PATH i RESV (15s-45s)
- nevýhody:
  - paměťově i procesorově náročné
  - spotřeba kapacity kanálu (pro zprávy PATH a RESV)

5 Protokol IPv6

přínos:

- rozšíření adresního prostoru (min. 65536 subsítí pro každého, třída A z IPv4 pro každou stranu)
- bezpečnost mezi koncovými uzly jako u IPSec
- bez překladu adres (NAT)
- rozšířitelnost, zlepšená funkčnost, zavedení streamů, plug'n'play

adresy:

- přiřazeny rozhraním, identifikátor uzlu může být jakékoliv rozhranní
- Broadcast není, Multicast – identifikátor více rozhraní
- posloupnost „0“ může být vypuštěna a nahrazena „::“
- za lomítkem je délka prefixu
- ::1 – localhost
- ::0 – nespecifikovaná adresa (používá se během inicializace)
- *link-local:*
  - unikátní na subsíti
  - vyšší část – fe80::/10
  - nižší část – identifikátor subsítě a rozhraní
  - nesmí forwardovat pakety
- *site-local:*
  - unikátní pro site
  - vyšší část – fec0::/10
  - nižší část – identifikátor subsítě a rozhraní
  - obdoba privátních adres v IPv4
  - bylo ZRUŠENO
- autokonfigurace:
  - interface ID – MAC adresa
  - link-local – horních 8 slabik ze směrovače

předpoklady fungování:

- IPv6 jako ostrovy v IPv4 síti, mezi nimi jsou tunely -> zapouzdření IPv6 do IPv4 (př. 6BONE)
- automatické tunelování:
  - *6to4:*
    - hraniční směrovače mají IPv4 adresu
    - speciální prefix 2002::/16, dalších 32 bitů je IPv4 adresa směrovače
  - 6over4:
    - tunelování vykonávají koncové uzly

Systém jmených domén:

- přidány dva typy záznamů:
  - *AAAA* – jméno -> adresa
  - *PTR* – adresa -> jméno

6 IP multicast (IGMP, směrování, PIM sparse/dense mode)

- směrovací technologie – 1 zdroj, více cílů (1 data odeslány celé skupině)
- výhody: menší objem přenášených dat -> menší zatížení sítě
- Určení rozsahu doručování:
  - *Implicitní*
    - Použiti link-local adresy
    - Neopustí podsíť
  - *Omezení rozsahu založené na TTL*
    - Multicast směrovače maji nastaven práh (TTL prah)
    - Jestliže je TTL ≤ TTL práh, je datagram zahozen
  - *Administrativní omezení*
    - Použití skupiny adres 239.0.0.0 až 239.255.255.255
    - Omezení na administrativní doménu
    - V IPv6 je rozsah součastí atributu uvedeného v adrese

IGMP

- protokol pro přihlašování do skupin

IGMPv1

- pouze registrace / uvolnění
- výzva poslána na 224.0.0.1, TTL=1
- odpověď: posílána jen jedním hostem ze skupiny na skupinovou adresu, pokud se nikdo neozve skupina neexistuje

IGMPv2

- připojení / odpojení ze skupiny zprávou
- host posílá zprávu o opuštění na 224.0.0.2 (all routers) -> zkrácení doby pro detekci prázdné skupiny
- směrovač reaguje specifickou výzvou aby zjistil jestli je skupina prázdná

IGMPv3

- podpora SSM (Source Specific Mcast)

Směrovací protokoly

DVMRP (Distance Vector Mcast Routing Protocol)

- hustý režim (dense mode)
- záplavové doručování
- explicitní připojení do subsítě
- source-based distribuční stromy

MOSPF (Mcast OSPF)

- hustý režim
- připojování pomocí Join
- není třeba šířit data záplavou od každého zdroje do každé subsítě

PIM-DM (Protocol Independent Mcast – Dense Mode)

- **hustý režim** = implicitně doručuje do všech subsítí
- libovolný směrovací protokol pro zajištění Reverse Path Forward (zjištění nejkratší cesty ke zdroji)
- routery používají záplavu s odřezáváním (flood and prune)

PIM-SM (Protocol Independent Mcast – Sparse Mode)

- **řídký režim** = použití explicitní Join zprávy pro připojení toku do subsítě
- RPF nezávislé na protokolu
- doručovací stromy se zavádí mezi příjemcem a RP (Randezvous Point)

CBT (Core Based Tree)

- charakteristiky jako PIM-SM, ale efektivnější při hledání zdrojů
- vytváří infrastrukturu pro doručování Mcast zpráv
- komerčně se nepoužívá

7 Přenosy v reálném čase, základy IP telefonie, H.323, SIP, VoIP

RTP (Real Time Protocol)

- představuje pouze mechanismy
- protokolově neutrální
- oddělené řízení a data
- bezpečnost (šifrování, ověřování)
- **funkce:**
  - fragmentace / defragmentace, znovuuspořádání (pokud je potřeba)
  - detekce ztrát, obnova
  - synchronizace uvnitř média (odstranění chvění zpoždění, vyrovnávání vzorkovacích hodin, synchronizace audia a videa, QoS zpětná vazba a adaptace rychlosti)
  - identifikace zdroje
- použití UDP, lib. port, RTCP = RTP+1
- nativní podpora ATM (AAL5)
- **řízení: RTCP (Real Time Control Protocol)**
  - QoS zpětná vazba
  - odhad členství
  - detekce smyček
- **Mixer:**
  - několik mediálních proudů na jeden nový (nové kódování)
  - redukuje požadovanou šířku pásma
  - jeví se jako nový zdroj s vlastním identifikátorem
- **Převodník:**
  - jeden mediální proud
  - může konvertovat kódování
  - transformace protokolu (nativní ATM – IP)
  - pro všechny pakety: zdroj. adresa = adresa translátoru

RTSP (Real Time Streaming Protocol)

vlastnosti:

- hrubá synchronizace (doladění – RTP sender report)
- virtuální prezentace = synchronizování přehrávání od několika serverů
- vyrovnávání zdrojů
- podpora ovládání zařízení
- vyrovnávací paměti (obdoba http)
- 1 TCP spojení na relaci

podobnosti s http:

- formát protokolu: text, MIME záhlaví, typ požadavek – odpověď
- stavové kódy, formát URL, bezpečnostní mechanismy

odlišnosti od http:

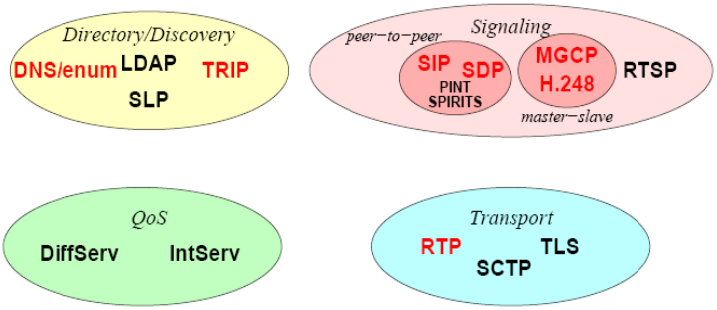
- stavový server, odlišné metody
- data přenášená mimo pásmo
- odstranění http chyb (požadavky s relativními cestami, kódování 8859-1)

VoIP, H.323, SIP

VoIP

- přenos hlasu přes IP síť
- postaveno na H.323 a SIP protokolech

architektura:



H.323

- určený pro přenos multimediální informace paketovými sítěmi
- zastřešující standard (H.225, H.245, H.255, RTP a další)
- kódování PER (Packet Encoding Rules)
- **entity:**
  - *terminál* – IP telefon
  - *brána* – komunikace se zařízeními v jiné komunikační síti
    - MGC (Media Gateway Controller) – signalizace
    - MG (Media Gateway) – směrování audio/video streamů
  - *konferenční jednotka* – MCU (Multipoint Controller Unit)
  - *gatekeeper* – centrální jednotka, překlad adres a řízení provozu

SIP (Session Initiation Protocol)

- protokol aplikační úrovně
- řídící pro vytváření, modifikaci a ukončování spojení
- **komponenty:**
  - *User Agents* – SIP telefony
  - *SIP servery* (typicky realizováno vše v jednom):
    - registrar
      příjem požadavků na registraci od uživatelů
    - proxy
      přepíná signalizaci navazování spojení, transparentní vzhledem ke koncovým stanicím, přepínání hovorů, větvení
    - redirect
      redirekce volání na ostatní servery
  - *SIP PSTN brány* (napojení na telefonní sítě), *Aplikační servery* (média servery)

8 Sítě typu P2P

Rozdělení

základní rozdělení:

- sdílející obsah
- vyhledávající obsah

jiné dělení:

- pro paralelní výpočty
- přístup k souborům a informacím
  - sdílení obsahu, vyhledávání …
- kooperující
  - instant messaging, sdílené aplikace, hry

rozdělení podle decentralizace:

- *čisté P2P systémy*
  - člen = server i klient
  - bez centrálního serveru a směrovače
- *hybridní P2P*
  - centrální server pro udržování informací o členech
  - směrování pomocí převodu reference
- *kombinované*

Typy P2P

- **nestrukturované**
  - *Napster* (centralizované)
  - *Gnutella* (distribuované)
  - *Kazaa/FastTrack* (hierarchické)
- **strukturované**
  - *Chord* (uzly v kruhu)
  - *Pastry* (overlay síť – sousední členové propojeni virtuálními hranami)

Charakteristiky P2P sítí

- uzly jsou autonomní (bez administrace), velice odlišné
- dynamická síť (časté připojování / odpojování uživatelů)
- efektivní využívání zdrojů
- škálovatelnost (možnost replikace, geografická distribuovanost)
- jednoduchá administrace
- **aplikace:**
  - sdílení souborů (DC++, Gnutella, Kazaa, Napster, ...)
  - síťové hry
  - sdílené aplikace (ICQ, ...)
  - distribuované výpočty (seti@home, …)

Anonymita

- ve většině sítí uživatelé vědí kde co je a kdo co požaduje

Freenet

- data jsou přenášena v opačném směru než dotaz
- nění možné zjistit, je-li uživatel iniciátorem nebo pouze data přenáší dál nebo je spotřebovává

Strukturované P2P sítě

- druhá generace
- samoorganizující se struktura
- založeno na distribuované hashovací tabulce
  - ukládá páry (klíč, hodnota) - klíč je podobný jménu souboru, hodnota může být obsah souboru
  - cíl: efektivní vkládání, prohledávání, rušení párů (klíč, hodnota)
  - každý uzel ukládá do systému podmnožinu párů (klíč, hodnota)
  - základní operace: nalezení uzlu, který obsahuje klíč, mapování klíčů na uzly
- př. Chord, Pastry

Ostatní

BitTorrent

- Dělení souboru na kousky (16kB)
- stahování přes Web server

9 Spolehlivé skupinové doručování

- řeší problém mnohonásobného doručení téhož obsahu
- **použití:**
  - přenos dat v reálném čase
  - přenos objemných dat
  - opakovaný přenos dat
- **vlastnosti:**
  - *skalabilita* – tisíce až miliony příjemců
  - *heterogenita uzlů, kanálů i obsahu*
  - *spolehlivost* – odolnost proti ztrátě paketů
  - *ochrana proti zahlcení*
- **modely:**
  - *push:*
    - synchronní, všichni příjemci musí být před příjmem připraveni
  - *on demand:*
    - přenos se provádí cyklicky (karusel)
  - *streaming:*
    - přenos dat v reálném čase (audio, video)
    - přednost synchronizace před spolehlivostí

Scalable Reliable Multicast (SRM)

- data mají přiřazeno stálé jméno (id) – id zdroje a sekvenční číslo
- přenos pomocí IP multicastu, všichni účastníci ve stejné skupině, žádný rozdíl mezi vysílači a přijímači
- oprava dat:
  - požadavek na ztracená data je vysílán na skupinovou adresu s určitým zpožděním

Asynchronous Layered Coding (ALC)

- nevyžaduje zpětnou vazbu mezi vysílačem a příjemci
- netřeba explicitně vytvářet skupiny
- jednosměrné přenosy
- push model, on demand, streaming
- zabezpečení pomocí FEC kódů
- víceúrovňové přenosy (různé kvality v různých časech, příjemce se připojí k tomu, který mu vyhovuje)
- základy:
  - *Layered Coding Transport* – informace o probíhajícím přenosu
  - *FEC* – spolehlivost a škálovatelnost
  - *Congestion Control*
  - *Authentication* – kontrola integrity paketu, ověření pravosti zdroje

NACK Oriented Reliable Multicast (NORM)

- opakování požadavků při chybě
- příjemci relativně homogenní a musí mít srovnatelnou dobu zpracování
- rychlost přenosu přizpůsobena nejpomalejšímu příjemci
- složitější než ALC

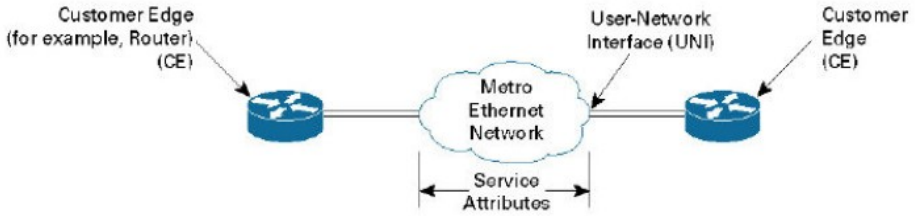
File Delivery over Unidirectional Transport (FLUTE)

- spolehlivý přenos hromadných (bulk) dat
- nad ALC
- přenos vlastních dat i meta informací o souboru (jméno, URI, velikost atd.) i typ přenášené informace (použitý kodek atd.)
- meta informace ve File Delivery Table (FDT) – XML reprezentace
- modely:
  - *pouze jednou*
    - jako push model, FDT doručena před souborem
  - *on demand*
    - soubory vysílány cyklicky, umístěné v karuselu, vysílány v náhodném pořadí
    - možnost opravy dat (v dalším cyklu)
    - statický karusel
    - dynamický karusel – musí se měnit instance FDT pro soubor

10 Vysokorychlostní sítě, Metro Ethernet, DQDB, DWDM, FibreChannel

Metro Ethernet Services

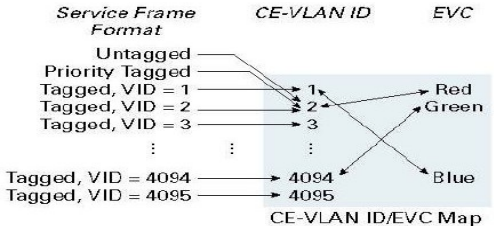
- integrace Ethernet služeb do všech sítí
- zaváděno poskytovatelem, nedotkne se uživatele
- umožňuje propojení více poskytovatelů



- typ a architektura uvnitř Metro sítě je „neviditelná“ (zákaznická síť je tak nezávislá na vývoji Metro sítě)
- **UNI (User Network Interface)**
  - fyzické rozhraní mezi zákazníkem a poskytovatelem (většinou ve vlastnictví poskytovatele)

Ethernet Virtual Circuit

- spojení 2 nebo více UNI (VPN na 2 vrstvě)
- servisní rámce přenášeny mezi UNI v EVC, nemohou do jiné EVC
- jedno UNI může být ve více UNI
- 2 typy:
  - Point-to-Point EVC
  - Multipoint-to-Multipoint EVC
    - propojení 2 nebo více UNI
    - Bcast a Mcas posílány do všech UNI v EVC
    - Unicast – 2 možnosti:
      - replikace do všech UNI (sdílený ethernet)
      - učení se MAC adresy (učící se mosty)
- **Custom Edge VLAN ID (CE-VLAN ID)**
  - identifikace UNI v EVC
  - odvozen od obsahu servisního rámce
    - CE-VLAN ID je totožný s 802.1Q (12bitů, VLAN ID není 0)
    - CE-VLAN ID je libovolný – bez 802.1Q, rámce s prioritou, implicitní VLAN
- **Mapování CE-VLAN ID na EVC**



- **CE-VLAN ID preservation**
  - Ponechání VLAN ID (propojení UNI ve více privátních VLAN sítích)
- **All-to-One Bunding Map**
  - V UNI pouze jedna EVC
  - Zavedení minimální konfigurace
  - Všechna CE-VLAN ID se napojí na jedno EVC v UNI
  - Dedikovaný privátní Ethernet

Distributed Queuing Dual Bus (DQDB)

- dvojitá sběrnice s rozprostřenou frontou (distribuovaná fronta)
- dvě jednosměrné sběrnice
- hlavní stanice řídí provoz sítě a generuje slova rámcové synchronizace každých 125ms, v tomto rytmu se „posouvají“ v síti volné časové intervaly o velikosti 53 bytů
- ve všech uzlech se průběžně vede evidence stavu sítě (délka front paketů)
- každá stanice tak má přehled o stavu sítě a ví kdy může vysílat
- tím je dosaženo vysokého využití přenosové kapacity blízké 100%
- až 500 uzlů, rozlehlost až 100km

Dense Wavelength Division Multiplexing (DWDM)

- přenášení optických signálů (každý jiné vlnové délky) po jednom optickém vlákně
- paralelní přenos jednotlivých signálů
- transparentní vůči přenášeným protokolům (SONET, Ethernet, ATM atd.)
- systém se skládá z:
  - vlnový multiplexer
  - vlnový zesilovač
  - vlnový přepínač (schopny podporovat až 256 vlnových kanálu o rychlosti 10Gb/s)
  - vlnové opakovače (EDFA (Erbium-Doped Fiber Amplifier), vzdáleny 10ky kilometrů a zvyšují intenzitu více světelných kanálů)

FibreChannel

- blokově orientované sériové rozhraní typu point-to-point
- chybějící podpora pro UTP
- slouží k přenosu dat mezi výkonnými úložnými zařízeními a servery na omezenou vzdálenost
- **rychlost:** 100, 200, 400 Mb/s, škálovatelnost až do 4 Gb/s
- **vzdálenost:** jednovidové vlákno - do 10 km, twinax - do 100 m

11 PAN sítě

- PAN – Personal Area Network
- dosah řádově metry, propojení zařízení jako laptop, PDA nebo mobilní telefon
- bezdrátové (IrDA, Bluetooth) i drátové (USB, FireWire)

Bluetooth

- standard IEEE 802.15.1, nejvíce rozšířená verze 1.2
- verze 2.0 EDR (Enhanced Data Rate) – až 2.1 Mb/s, větší výdrž baterií zařízení
- výkonné třídy:
  - *class 1* – 100mW, 100 m (max. teoretický dosah)
  - *class 2* – 10mW, 10 m
  - *class 3* – 2.5mW, 1 m
- rádiové vlny:
  - pásmo 2.4GHz
  - metoda FHSS, během 1 sekundy 1600 skoků mezi 79 frekvencemi s rozestupem 1MHz
  - rychlost okolo 720kb/s (i asymetrické rozdělení downloadu a uploadu)
- zařízení identifikována adresou BT_ADDR
- doubodová i mnohabodová síť (jedna stanice jako master, až 7 slave stanic, tzv. pikosítě)
- bezpečnost:
  - klíč spojení se odvozuje od PIN (buď vestavěný nebo zadávaný uživatelem)

IrDA

- přenos signálu infračerveným světlem
- infračervené LED diody – 780-950nm, přijímače jsou PIN fotodiody
- šíření podobné jako u viditelného světla (schopnost odrazu)
- výhody:
  - velká šířka pásma
  - žádný limit dostupným spektrem
- nevýhody:
  - dosah sítě (vysílací výkon je určen především citlivostí přijímače)
  - nízká rychlost

12 Ověřovací servery a ověřování, Kerberos, certifikáty

Ověřovací servery a ověřování

Ověřovací servery

- slouží k ověření pravosti uživatele
- lepší utajení klíčů
- KDC (Key Distribution Center) – databáze klíčů (indexovaná podle jmen uživatelů)

Ověřování

- schémata:
  - alespoň jedno tajemství a schopnost rozpoznat jeho správné použití
- ověřovací metody:
  - jednoduché (hesla)
  - přísné (založeny na šifrovacích metodách)

Přísné metody

- použití symetrických a nesymetrických kódů
- založené na ověřovacích serverech
- založené na protokolech s minimální znalostí
  - uživatel dokazuje svoji identitu odpovídáním na šifr. otázky serveru
    M1: {R, ID}
    M2: {C}K
    M3: {f(C)}K
    R … požadavek, K … tajný klíč, C … náh. číslo, f(C) … domluvená funkce

Kerberos

- zajišťuje ověřování uživatelů a požadovaných služeb
- architektura klient-server
- k ověřování využívá důvěryhodnou třetí stranu – ověřovací server AS
- prokazování identity pro každý požadavek
- prokazování heslem pouze jednou při přihlašování
- heslo se nepřenáší sítí a není uloženo ani v paměti
- každý klient a každá služba mají heslo
- všechna heslo jsou pouze v AS
- úrovně ochrany:
  - ověření při přihlášení
  - ověření každé zprávy
  - ověřování a šifrování každé zprávy

Funkce

- ověřovací server ověří pravost klienta
- na základě ověření, Ticket Granting Server poskytuje tickety pro přístup k požadovaným

serverům

- **tři fáze ověřování:**
  - získání pověření (credentials)
  - požadavek pověření na specifickou službu (ticket)
  - prezentace pověření koncovému serveru
- **ticket:**
  - obsahuje: jméno serveru, jméno klienta, IP adresu klienta, časové razítko, dobu života ticketu, náhodný relační klíč
  - omezen dobou života
  - šifrován klíčem serveru, kterému je určen

Kerberos databáze

- jméno uživatele a jeho privátní klíč
- pro uživatele generuje dočasné klíče (relační)
- citlivé informace v Kerberu, necitlivé v serveru HELIOS

Servery

- **Administrativní server:**
  - KDBM (Kerberos Database Management)
  - zajišťuje přístup do databáze Kerbera
  - klient může být kdekoliv, server u databáze
- **Ověřovací server:**
  - pouze operace čtení nad databází
  - ověřování uživatelů
  - generování relačních klíčů
  - uživatelské programy – přihlašování, změna hesla, zobrazení ticketů, ničení ticketů

Certifikáty

- datová struktura identifikující jejího držitele
- uložena v souboru nebo přímo v zařízení
- **struktura:**
  - hlavička
  - údaje o subjektu:
    - jméno
    - e-mail
    - další údaje (rč, url, atd...)
  - veřejný klíč subjektu
  - veřejný klíč CA (certifikační autorita, důvěryhodná třetí strana)
  - podpis CA
- používané algoritmy:
  - *podpisové*
    - RSA, DSA, DH
  - *hashovací*
    - MD5, SHA-1, SHA-2