

Základní pojmy z oblasti počítačových sítí, taxonomie sítí

Rozdělení počítačových sítí (taxonomie)

Počítačové sítě můžeme rozdělit do různých skupin podle kritérií, které nemusí být přesně definována a můžou se vzájemně prolínat. To znamená, že výsledné skupiny nemají pevně určeny hranice a jedna síť může patřit do více skupin současně.

Nejzákladnější dělení je podle:

- Velikosti
- Topologie
- Přenosové rychlosti
- Typu uzlu
- Vztahu mezi uzly
- Architektury
- Mobility

síť - je to skupina počítačů navzájem propojených (pomocí kabelů) za účelem jejich vzájemné spolupráce

k čemu síť slouží:

- intranet - je síť sloužící potřebám organizace (podniku, firmy, instituce, ...)
- firemní informační a komunikační systém
- propojení fyzicky oddělených a někdy velmi vzdálených segmentů firemní sítě (pobočky ve světě)
- ochrana firemních dat před přístupem cizích subjektů
- využití Internetových technologií (TCP/IP) „uvnitř“ podnikových sítí
- používat jednotný styl práce směrem „dovnitř“ i „navenek“
- pracovat s jednotným uživatelským rozhraním

Uzel

- PC nebo server, který je identifikován v rámci sítě svou jedinečnou adresou
- postavení uzlů sítí:
- chová se jako server
 - pouze nabízí své vlastní zdroje k využití ostatním uzlům formou sdílení
- chová se jako klient
 - pouze využívá zdroje ostatních uzlů prostřednictvím sdílení
- chová se současně jako klient i server
 - nabízí vlastní zdroje a současně využívá zdroje jiných uzlů
- pokud převažuje současně využívání i nabízení, jde o síť typu peer-to-peer
- pokud existuje jasná hranice mezi nabízením a využíváním, jde o síť typu klient-server
 - postavení uzlů je asymetrické, některé uzly se chovají jako klienti, jiné jako servery

Vývoj LAN a WAN

- hranice mezi LAN a WAN není ostrá
- rozdíl se stále více stírají - sítě LAN se zvětšují, sítě WAN se zrychlují
- trend: rozdíl mezi oběma druhy sítí se bude neustále zmenšovat
- uživatel si nebude muset uvědomovat rozdíl mezi LAN a WAN

Paket

- Neutrální označení paketu – datagram. Fragmentace a defragmentace.
- Přenášený blok dat na úrovni IP vrstvy. Skládá se z hlavičky, těla, tail (trailer). Hlavička paketu se skládá z IP zdroje, IP cíle. V těle paketu jsou pak uložena samotná data.
- Time to life – životnost paketu – při rozesílání z uzlu určuje dobu života – zabraňuje zhroutilí sítě

Spoj

Samotné kanály a okruhy ještě nejsou schopny poskytovat potřebné přenosové služby. Např. telefonní okruh je sice schopen přenášet telefonní signály, ale k jeho praktickému využití je potřeba nutně i telefonní přístroje, které převádí lidský hlas na telefonní signál a opačně. Teprve telefonní okruh, vybavený na obou koncích telefonními přístroji, vytváří tzv. spoj, v tomto případě telefonní spoj. V oblasti počítačových sítí jsou samozřejmě zajímavější takové spoje, které souží k přenosu dat. Pak jde o tzv. datové spoje.

Topologie sítí

=uspořádání prvků sítě a spojů mezi nimi: neorientovaný graf: hrany = spoje, uzly = prvky

topologie sítě ovlivňuje některé její vlastnosti:

- rozšiřitelnost (možnost a snadnost doplňování nových uzlů do sítě)
- rekonfigurovatelnost (možnost změnit strukturu sítě při závadě komponenty)
- spolehlivost (odolnost proti výpadkům komponent)
- složitost uzlů (HW, SW)
- výkonnost (využití média, zpoždění přenášených dat)

kruhová topologie (ring), hvězdicová topologie (star), stromová topologie (tree), sběrníková topologie (bus), polygon (WAN), extended star, mesh

Reálné vlastnosti přenosových cest, přenosová média, sdílená média, časový-frekvenční a kódový multiplex

reálné vlastnosti - přenosové cesty nejsou nikdy ideální

negativně ovlivňují přenášený signál:

útlum (zeslabuje přenášený signál – obdélníkový signál se zmenšuje)

zkreslení (deformuje přenášený signál – obdélníkový signál se zakulacuje)

šum (tepelný šum součástek, slunce, radioaktivita, ... – podprahové a nadprahové rušení)
přeslech (pronikání signálu z jiných vedení –)

důsledky:

každá přenosová cesta přenáší některé signály lépe a jiné hůře

- záleží zejména na frekvenci změn přenášeného signálu a na povaze těchto změn
- některé signály by přenosová cesta „pokazila“ tak, že nemá smysl je touto přenosovou cestou přenášet
- jestliže je kvalita přenosové cesty mnohem vyšší, než je nutné pro přenesení signálu, není přenosová cesta plně využita a přenos obvykle není ekonomický

při zpracování signálu záleží na okamžiku vyhodnocení a rozhodovací úrovni

- signál je nutné vyhodnotit ve vhodném okamžiku, kdy již došlo k ustálení po změně, ale ještě se neprojeví následující změna
- rozhodovací úroveň je nutné umístit tak, aby rušení mělo na vyhodnocení co nejmenší vliv

Počítačové sítě

při nadprahovém rušení nelze vyloučit chybné vyhodnocení signálu

časová synchronizace :

pro přenos a vyhodnocení signálu je potřebný určitý časový interval

signál se po modulační změně musí ustálit

přijímač musí být informován o tom, že došlo k modulační změně

současně s daty je nutné přenášet informaci o tom, ve kterých časových okamžicích se má signál vyhodnotit

Šířka pásma

praktický důsledek obvodových vlastností všech přenosových cest je pak následující

- pro každou konkrétní přenosovou cestu existuje určitý rozsah frekvencí (= šířka pásma) takových, že signály s frekvencí v tomto rozsahu jsou přenosovou cestou přenášeny s přijatelným zhoršením kvality signálu
- signály s frekvencí mimo tento frekvenční rozsah jsou již přenášeny s neúnosně velkými zkreslením a útlumem

Jak souvisí šířka pásma s objemem přenášených dat

je-li šířka pásma omezena, pak není schopna přenášet harmonické složky od určité frekvence výše

Modulační rychlost udává, s jakou frekvencí se mění signál

Přenosová rychlost vyjadřuje objem dat, přenesených za jednotku času

Zvyšování přenosové rychlosti

možné zdroje zvyšování:

- šířka přenosového pásma - obvykle vyžaduje změnu přenosového média a zvýšení ceny (nákladů)
- počet stavů přenášeného signálu (stupeň modulace)
 - stupeň modulace nelze zvyšovat donekonečna! - čím více stavů, tím jsou hůře rozlišitelné
 - intuitivně: při překročení určitého stupně modulace (počtu stavů signálu) již příjemce nebude schopen tyto stavy od sebe rozeznat

Přenosové cesty

- linkové (drátové)
 - koaxiální kabely – pro přenos v základním i přeloženém pásmu 105 – 109 Hz
 - optické vlákno – mnohovidové a jednovidové 1014 – 1015 Hz
 - kroucená dvoulinka – nestíněná (UTP) stíněná (STP) 104 – 109 Hz
- bezdrátové
 - radiové – mikrovlnné – radioreléové – satelitní – optické

Sdílená média

- vybudování přenosové trasy s větší přenosovou kapacitou je levnější než vybudování většího počtu tras se srovnatelnou celkovou propustností
- propustnost existující přenosové trasy je vyšší než požadovaná přenosová kapacita zbytek kapacity by zůstal nevyužit

- požadavky na přenos jsou jen krátkodobé a nepravidelné
- ve zbývajících dobách by trasa nebyla využita

Multiplex - pro sdílení přenosového média s používá:

- frekvenční multiplex
frekvenční pásmo, které je k dispozici, se rozdělí na kanály s požadovanou šířkou pásma
- časový multiplex
jednotlivým kanálům se přidělí pravidelně se opakující časové úseky, ve kterých disponují celou šířkou pásma
- kódový multiplex
jednotlivé kanály používají pseudonáhodné kódování, jeví se ostatním kanálům jako šum

Kolize

při časovém multiplexu obvykle nesmí vysílat více uzlů najednou

– dochází k nežádoucímu „smísení“ signálů

frekvenční a kódový multiplex obvykle připouští současné vysílání více uzlů

Základní komunikační funkce – synchronizace, adresace, detekce a oprava chyb, řízení přístupu, řízení toku

Synchronizace příjemce a vysílatele

v přijímači je nutné rozpoznat hranice jednotlivých symbolů bitů, znaků, bloků, zpráv,

přímá synchronizace - synchronizační informace je obsažena v přijímaném signálu

PŘEDPOKLAD:

časová základna přijímače se liší od časové základny vysílače jen málo a synchronizaci proto není nutné obnovovat v každém bitu

nepřímá synchronizace - synchronizační informace se odvozuje z přijímaného signálu

nepřímou - start-stopní (arytmický) přenos, fázový závěs (PLL) ...

Vznik a detekce chyb

mezi vysílačem a přijímačem dojde ke změně, např. vlivem rušení, přenášeného signálu, který se pak demoduluje a dekóduje na jiný znak, než byl původně vyslán – vysláno 1111, přijato 1101

Kódová (Hammingova) vzdálenost

– kolik bitů je nutno změnit v kódu symbolu, aby vznikl kód jiného symbolu

- např. kód $3n+2$ má kódovou vzdálenost 2, což umožňuje detekci všech jednoduchých chyb

vyslaný symbol	vyslaný kód	přijatý kód	přijatý symbol
0	00010	00010	0
0	00010	00011	neznámý - chyba
0	00010	01011	3 - nelze zjistit chybu

PARITA

– jednoduchá metoda zabezpečení proti chybám

– ke kódu se přidá další bit, jehož hodnota udává počet jedniček MODULO 2

– parita zvyšuje kódovou oblast o 1

číslícekód 8-4-2-1 s paritou kód $3n+2$ s paritou

0	0000 0	00010 0
1	0001 1	00101 1
2	0010 1	01000 0

Počítačové sítě

Samoopravný kód umožňuje následnou opravu chyby v jediném bitu, přidává ke každému 8-bitovému bytu navíc pět bitů (resp. 6 bitů ke každému 16-bitovému slovu).

Kódová krychle

– symboly A, B jsou zakódovány pomocí 3 bitů tak, že při změně A na B nebo opačně se musí změnit hodnota všech 3 bitů

symbol	kód
A	0 0 0
B	1 1 1

kódová vzdálenost = 3

– je-li kódová vzdálenost větší nebo rovna $2n+1$, umožňuje kód detekci $2n$ chyb a automatickou opravu n chyb

Zabezpečovací kódy

větší kódové vzdálenosti lze dosáhnout speciálními kódy

Hammingovy a cyklické kódy využívají vlastnosti polynomů

zákrytové (Orchard) kódy využívají geometrické principy

ve fyzikálním prostředí se chyby často vyskytují ve shlucích

rušivý impuls potlačí několik přenášených bitů za sebou

poškození povrchu optického či magnetického paměťového media zasáhne několik bitů za sebou

důležitou vlastností zabezpečovacích kódů je odolnost proti shlukům chyb

BSC

Binary synchronous communication (bisync). Znakově orientovaný protokol spojové vrstvy.

HDSL

High-data-rate digital subscriber line. Jedna ze čtyř DSL technologií s přenosovým pásmem 1,544 Mb/s v obou směrech, využívající dva kroucené dvoupáry. Bez použití opakovačů je vzdálenost omezena na 3658,5 m.

Řízení přístupu

v době, kdy uzel nevysílá, zůstává část přenosové cesty přidělená uzlu zcela nevyužitá výhodnější je dynamické přidělování (alokování) přenosového kanálu

přenosové médium je přidělováno (typicky celé) dynamicky, na základě skutečné potřeby (požadavku)

Možné varianty řízení přístupu

- řízené metody (deterministické)
 - např. Token Passing (ARCNet, Token Ring, FDDI, ...)
- neřízené metody (stochastické)
 - jejich pravidla obsahují „náhodný“ prvek - např. „počkej náhodně zvolenou dobu“
 - výsledek není predikovatelný - vedou k výsledku jen s určitou pravděpodobností
- centralizované metody
 - většinou jde o řízené (deterministické) metody - např. MIL 1553, 100 VG AnyLAN
- distribuované metody
 - metodu realizují jednotlivé uzly ve vzájemné součinnosti např. CSMA/CD (Ethernet)

Řízené centralizované metody

počítají s existencí centrálního arbitra

arbitr se musí dozvědět, kdo a kdy chce vysílat (získat přístup)

metodou výzev (polling) - centrální arbitr se pravidelně (cyklicky) dotazuje všech potenciálních zájemců o vysílání

z explicitních žádostí uzlů o právo na vysílání

ízené distribuované metody

nemají centrálního arbitra

algoritmus přidělování „běží“ na všech uzlech

počítají s důslednou disciplínou všech uzlů - že každý dodrží stanovená „pravidla hry“
varianty:

rezervační metody - distribuovaná obdoba přidělování na žádost

prioritní přístup - existuje způsob, jak žadatelé mohou ze svého středu vybrat (koordinovaným, deterministickým způsobem) jednoho, a ten může vysílat

metody s předáváním pověření (token)

 vysílá pouze držitel oprávnění

 kruh je pouze logický

 lze garantovat přístup do doby x

Neízené distribuované metody

Metoda Aloha (tzv. „čistá“)

odešli, když potřebuješ (na nikoho se neohlížej), pokud nedostaneš včas potvrzení, opakuj
dochází často ke kolizím, efektivnost do 18%

Metoda CSMA

poslouchej nosnou a pokud nikdo nevysílá, můžeš začít vysílat sám

kdy může dojít ke kolizi:

- více uzlů (zájemců o vysílání) současně zjistí, že nikdo nevysílá, a začne vysílat
- více uzlů čeká, až někdo jiný přestane vysílat, a pak začnou všichni najednou

nenaléhající CSMA

podívá se jestli někdo vysílá, pokud ano, odmlčí se na náhodnou dobu

naléhající CSMA

jakmile je volno, začne vysílat

Metody CD

– snaží se detekovat výskyt kolizí

– metody „bez CD“ pokračují ve vysílání, i když ke kolizi došlo

– metody s CD využívají schopnost detekce k (téměř) okamžitému ukončení vysílání

– uzel, který detekoval kolizi, vyšle zvláštní „rušení“ (jam), aby ostatní uzly určitě detekovaly kolizi také

Algoritmus CSMA/CD

pokud nikdo právě nevysílá (CS), můžeš začít vysílat sám

– pokud někdo vysílá, čekej až skončí

pokud začneš vysílat a dojde ke kolizi, přestaň, a odmlč se na náhodně zvolenou dobu
při vyšší zátěži vykazují nestabilitu

Spojovaný a nespojovaný přenos, síťové modely a architektury, referenční model ISO/OSI, architektura TCP/IP

P epojování okruh (spojovaný p enos)

pochází ze „světa spojů“

obdoba telefonní sítě

mezi příjemcem a odesilatelem vzniká přímá, souvislá cesta

kommunikace probíhá v reálném čase

představa: od odesilatele vede až k příjemci jednoduše „roura“, kterou protékají data
data nemusí být příjemci explicitně adresována

P epojování paket (nespojovaný p enos)

pochází ze „světa počítačů“

fungují tak prakticky všechny sítě LAN a WAN

obdoba listovní pošty

mezi příjemcem a odesilatelem nevzniká žádná souvislá vyhrazená cesta

data se přenášejí po blocích (paketech, datagramech, buňkách, ...)

přenos neprobíhá v reálném čase - přestupní uzel nejprve přijme celý přenášený blok dat
a teprve pak jej předá dál

přenášená data musí být explicitně adresována

čím jsou bloky větší

- tím je přenos dat efektivnější klesá režie
- tím více rychlost přenosu závisí na kvalitě přenosové cesty, při chybě se musí opakovat přenos celého bloku
- tím větší je rozdíl mezi přepojováním paketů a přepojováním okruhů
 - důležité např. pro přenos zvuku a obrazu

při extrémně malých blocích (buňkách) se rozdíl téměř ztrácí - toho využívá technologie ATM – přenos dat je založen na přepojování velmi krátkých bloků dat (buněk), vyhovuje potřebám „světa spojů“ i „světa počítačů“

Síťové modely a architektury

kommunikační proces můžeme rozdělit na tři fáze – otevření, přenos, ukončení

Vrstvy

implementovat síť je hodně složité a náročné

jde o rozsáhlý problém, který se vyplatí dekomponovat

dekompozice se provede po hierarchicky uspořádaných vrstvách

Způsob komunikace:

Vrstvy vždy komunikují vždy mezi sousedními. Nižší poskytuje služby vyšší vrstvě a vyšší využívá služby nižší vrstvy. Další komunikací je komunikace s partnerskou (rovnocennou – peer) vrstvou jiného uzlu.

Počítačové sítě

Protokol definuje pravidla komunikace stejnohlých vrstev.

Definováno protokolem – obálka (envelope) s údaji pro partnerskou vrstvu se vloží do obálky nižší vrstvy a obálka nejnižší vrstvy se přenesení s obsahem do cílového uzlu.

Protokol - vrstvy nejsou „jednotlivé“

- v každé vrstvě může existovat a fungovat několik relativně samostatných entit
 - entitou může být např. proces, démon, úloha
- entity ve stejné vrstvě mohou
 - plnit rozdílné funkce (nekonkurovat si)
 - plnit obdobné funkce, ale jiným způsobem (konkurovat si)
- protokol definuje pravidla komunikace mezi entitami stejnohlých vrstev
- protokol určuje způsob, jakým je realizována určitá služba
 - pro každou vrstvu může existovat několik alternativních protokolů
 - současné použití různých protokolů (v rámci téže vrstvy) se nemusí vylučovat

Síťový model a síťová architektura

síťový model je ucelená představa o tom, jak mají být sítě řešeny zahrnuje:

- představu o počtu vrstev
- představu o tom, co má mít která vrstva na starosti

nezahrnuje:

- konkrétní představu o tom, jak má která vrstva své úkoly plnit tedy konkrétní protokoly

síťová architektura obsahuje navíc také:

- konkrétní představu o způsobu fungování jednotlivých vrstev
- tj. obsahuje konkrétní protokoly

příklad síťového modelu: referenční model ISO/OSI

příklad síťové architektury: TCP/IP

switching = přepínání

- přepojování na nižší úrovni (linková vrstva)
- bere v úvahu jen nejbližší okolí uzlu
- lze řešit HW

routing = směrování

- přepojování na vyšší úrovni (síťová vrstva)
- bere v úvahu topologii celé sítě
- řeší se SW

ISO/OSI

pokus o vytvoření univerzální síťové architektury

pochází ze světa spojů

používá se pro srovnávací účely

fyzická vrstva – zabývá se přenosem bitů

- neinterpretuje co přenáší
- rozlišuje se paralelní a sériový přenos
- přenos v základní a přeloženém pásmu

– linková vrstva – přenáší celé bloky (frames)

- zajišťuje přenos pouze v dosahu přímého spojení
- funguje spolehlivě, nespolehlivě, spojovaně, nespojovaně
- synchronizace na úrovni rámců
- zajištění spolehlivosti – detekce chyb
- řízení toku
- přístup ke sdílenému médiu

– síťová vrstva – přenáší bloky dat jako datagramy či pakety

- zajišťuje doručení paketů až ke koncovému adresátovi
- v prostředí kde není přímé spojení hledá vhodnou cestu až k cíli
zajišťuje tzv. směrování (routing)
- musí si uvědomovat skutečnou topologii celé sítě (obecně)
- může používat různé algoritmy směrování:

neadaptivní, izolované, distribuované

adaptivní,

– data v přestupních uzlech se nedostanou výš než na úroveň síťové vrstvy

– transportní vrstva – s vlastnostmi a funkcemi nižších vrstev nelze „hýbat“

– vyšší vrstvy mohou chtít něco jiného, než co nabízí nižší vrstvy

– je úkolem transportní vrstvy zajistit potřebné přizpůsobení!

– může měnit -

nespolehlivý charakter přenosu na spolehlivý

méně spolehlivý přenos na více spolehlivý

nespojovaný přenos na spojovaný

– relační vrstva – zajišťuje vedení relací

- může zajišťovat: synchronizaci, šifrování, podporu transakcí

– prezentační vrstva – nižší vrstvy se snaží doručit každý bit přesně tak, jak byl odeslán

– stejná posloupnost bitů může však mít pro příjemce jiný význam než pro odesílatele,

např. pro rozdíly:

v kódování znaků (ASCII, EBCDIC,...)

– prezentační vrstva má na starosti potřebné konverze

– aplikační vrstva – původně měl obsahovat aplikace

- problém: aplikací je moc, musely by být všechny standardizovány

– později:

- aplikační vrstva měla obsahovat pouze „jádro“ aplikací, které má smysl standardizovat

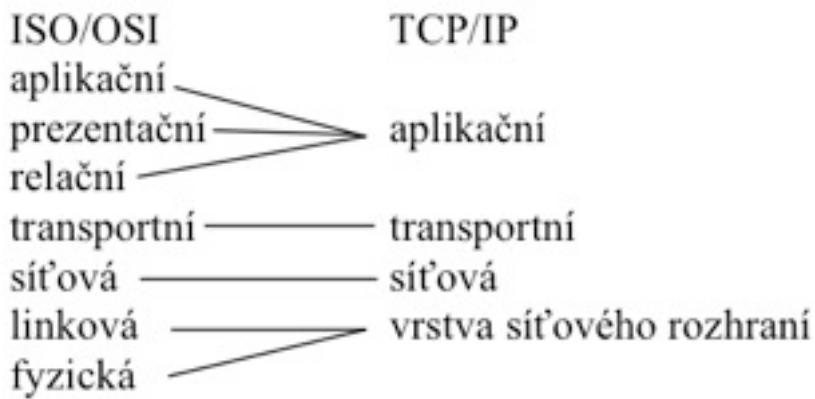
- například přenosové mechanismy elektronické pošty

TCP/IP

– obsahuje ucelenou představu o počtu a úloze vrstev

– síťová architektura – obsahuje konkrétní protokoly

– nejdříve vznikají protokoly a později vrstvy



vrstva síťového rozhraní

zahrnuje vše, co se nachází „pod síťovou vrstvou“
předpokládá se, že bude používat to, co vznikne někde jinde

síťová vrstva

zajišťuje pouze nespojovaný a nespolehlivý přenos
protokol IP snaží se zakrývat specifika přenosových technologií nižších vrstev a fungovat nad nimi optimálně

transportní vrstva

sama využívá nespojovaný a nespolehlivý přenos na úrovni síťové vrstvy
sama nabízí spojovaný a spolehlivý přenos
protokol TCP /transmission control protocol/
zajišťuje spolehlivý přenos a spojovaný
tváří se jako proud /stream/
protokol UDP /User Datagram Protocol/
zajišťuje nespojovaný a nespolehlivý přenos

aplikační vrstva

koncepte obdobná modelu ISO/OSI
původní - elektronická pošta, přenos souborů – později vznikají další, sdílení souborů, správa sítě...

Technologie Ethernet, CSMA/CD, exponential back-off, typy a vlastnosti aktivních síťových prvků

První komerčně dostupná verze Ethernetu byla společným projektem firem DEC, Intel a XEROX (Ethernet II, DIX Ethernet), dnešní podoba je standardizována organizací IEEE - existuje celá řada verzí (včetně Wireless)

Ethernet přenosové cesty optické, drátové rychlosti 10,100,1000 Mb/s

paket: hlavička a datová část (adresa odesílatele, příjemce, opravný crc kod)

adresace: pevně alokovaná adresa 48 bitů (světově unikátní)

zabezpečení: 32-bitový cyklický kód (CRC)

řízení přístupu: adaptivní CSMA/CD

Počítačové sítě

CSMA/CD + exponential backoff

adaptivní metoda (přizpůsobující se zátěži)

střední doba odložení vysílání závisí na násobnosti kolizí

formát paketu: preamble + SFD (Start of Frame Delimiter) 7+1byte

adresa cíle 2/6byte

adresa zdroje 2/6byte

typ/délka 2byte

data 48-1500byte

CRC (Cyclic Redundancy Check) 4byte

Ethernet 10Mb/s

10BASE-T - hvězdicová topologie (společné medium tvoří opakovač nebo port přepínače),

MAU (Samostatné jednotky, ke kterým lze připojit až 8 uzlových počítačů.) na desce, připojení

k rozbočovači nebo přepínači konektorem RJ45 a dvojicí kroucených dvoulinky

10BASE-F - verze používající optické kabely (FL, FB, FP)

Ethernet 100Mb/s je 10x rychlejší

všechny časy jsou 10x kratší, ve stejném poměru se však zmenšily maximální vzdálenosti

100BASE-TX - hvězdicová topologie, populární díky kompatibilitě s *10BASE-T*, připojení

konektorem RJ45 a dvojicí kroucených dvojvodičů; některé síťové prvky se dokáží

automaticky přizpůsobit provozu rychlostí - 10 i 100 Mb/s

100BASE-FX - varianta pro připojení optickým kabelem

10BROAD36 - verze 10Mb/s používající technologii kabelové televize

Wireless Ethernet - bezdrátová verze Ethernetu, používá kódový multiplex

Ethernet 1Gb/s - nová verze Ethernetu, opět 10x rychlejší než Ethernet 100Mb/s (max. délka přípojky 25m)

Aktivní prvky:

- fyzická vrstva: opakovač (repeater)
rozbočovač (hub)
- linková vrstva: most(bridge)
přepínač (switch)
- síťová vrstva: směrovač (router)
- aplikační vrstva: brána (gateway)

Opakova :

je to pouze digitální zesilovač, zesilující a znovu tvarující přenášený signál

kompensuje zkreslení, útlum a další vady reálných přenosových cest

vše, co přijímá, rozesílá („opakuje“) do všech připojených segmentů

šíří i kolize a poškozené pakety

uzly v jiných segmentech musí poznat, že k ní došlo

propojené segmenty tvoří jednu kolizní doménu

tj. oblast, ve které současné zahájení vysílání kterýchkoliv dvou uzlů způsobí kolizi

kolizní doména končí až na nejbližším mostu, přepínači nebo směrovači

Mosty, p epína e a sm rova e se nezajímají o datový obsah rámců resp. paketů mohou propojovat jen takové systémy, které do rámců/paketů „balí“ stejná data tj. stejné systémy, ev. systémy lišící se v přenosových technologiích nižších vrstev

Switche:

přepínání přepojování na úrovni linkové vrstvy
bere v úvahu jen nejbližší okolí uzlu
rozhodování o dalším směru přenosu je jednoduché
obecně jednodušší a rychlejší
lze „zadrátovat“ (tj. řešit přímo v HW)

Routry:

směrování přepojování na úrovni síťové vrstvy
bere v úvahu topologii celé sítě
vyžaduje náročnější rozhodování o dalším směru přenosu dat
obecně složitější a pomalejší
řeší se v SW, nelze snadno řešit pomocí HW

Brány:

pro spolupráci odlišných systémů je nutné rozumět přenášeným datům a provádět jejich konverzi
brány jsou vždy aplikačně orientované, rozumí jen datům určité aplikace (aplikací)

Adresování ve 2. a 3. vrstvě, mac adresa, ip adresa, třídy IP adres, podsítě a supersítě, princip všesměrového vysílání, šíření kolizí a všesměrového vysílání, kolizní doména, broadcast doména

úkolem síťové vrstvy TCP/IP je překrýt konkrétní přenosové technologie jednotnou pokličkou, která:

- zakrývá specifické vlastnosti přenosových technologií
- implementuje jednotný způsob adresování

Jaké zvolit adresy na úrovni síťové vrstvy?

takové, aby byl možný jednoznačný převod na fyzické adresy přenosových technologií, použitých ve vrstvě síťového rozhraní

takové, které odpovídají pohledu na soustavu vzájemně propojených sítí (internet)

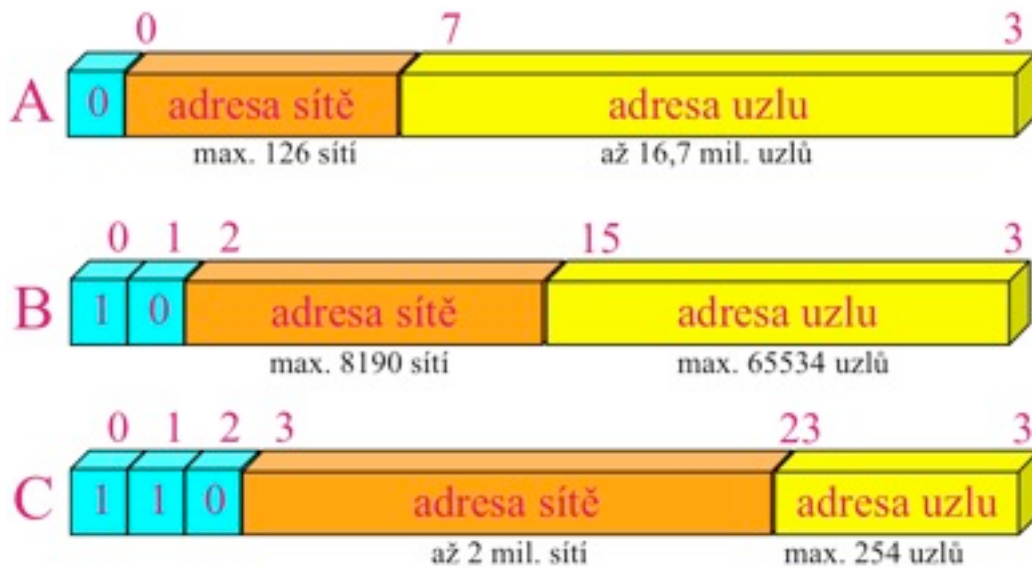
takové, které vyhovují potřebám směrování

- celosvětově jednoznačné
- dostatečně malé

Počítačové sítě

Třídy adres:

proměnný formát adresy spočívá v různém nastavení "předělu" mezi adresou sítě a adresou uzlu v rámci sítě



Podsítě:

- Řešení úbytku IP adres
- Posun Masky
- Dělení sítí - subnetting
 - Posun bytové masky doprava - možnost více adres sítí
 - Rozdělení v rámci jedné soustavy sítí, nešíří se do světa
 - Možnost využití jedné třídy IP adresy pro více sítí
- Neveřejné IP adresy
 - Na privátní sítí bez přímé komunikace ven.
 - Přístup přes Firewall.
 - Doporučené adresy 10.0.0.0; 172.16.0.0; 192.168.0.0 zahazované routery.
- CIDR Supersítě Classless InterDomain Routing alias Supernetting
 - Přidělování koncovým sítím přesně velké skupiny IP adres
 - Inverzní k subnettingu
 - Posun bitové pozice IP adresy mezi síťovou částí a uzlovou
 - Prefix = adresa sítě
 - Problém směrovacích tabulek - přeplněné
 - CIDR bloky agregují směrovací informace

Supersí : spojení podsítí jednou maskou 255.255.0.0

linková vrstva používá *mac adresování* pro rozhodování o přepínání, okolí prvku síťová rozhodování o směrování podle *ip adres* bere v úvahu topologii celé sítě *kolizní doména* oblast, kde dochází ke kolizím na úrovni linkové vrstvy (vysílá moc lidí) stěpeny switchi a bridge.

Broadcast domény - všesměrové vysílání obsazuje velmi kapacitu sítě, proto jsou omezeny na síťové úrovni. routry štěpí

Převod adres mezi 2. a 3. vrstvou, protokoly ARP a RARP. Princip doménového adresování, protokol DNS

síťová vrstva nezná IP adresy a neumí je používat, IP protokol sám provádí převod IP adresy na fyzickou adresu Mac.

ARP je jedním možným mechanismem dynamického překladu IP adres na fyzické adresy využívá možnosti všesměrového vysílání (broadcastingu)

např. v Ethernetu

ARP dotaz (ARP request) obsahuje IP adresu, ke které se hledá fyzická adresa. Tento paket se rozešle všem uzlům dané sítě

ARP odpověď (ARP reply) posílá uzel, který rozpoznal svoji IP adresu. K odpovědi připojí i svou fyzickou adresu

Každý uzel musí znát svou IP adresu ještě dříve, než vyšle či přijme svůj první IP paket!

RARP předpokládá se existence RARP serverů, které znají IP adresy ostatních uzlů spolu s jejich fyzickými adresami

- RARP pakety se vkládají přímo do linkových rámců
- RARP se používá především v Ethernetu (využívá broadcasting)
- RARP neprojde přes směrovače,

tj. jeho působnost je omezena na lokální síť

DNS

IP adresy jsou srozumitelné pro počítač ... ale nejsou srozumitelné pro člověka

- dát jednotlivým uzlům symbolická jména (dostatečně mnemonická)
- zajistit možnost (rychlého a automatického) převodu
 - symbolické jméno > IP adresa
 - IP adresa > symbolické jméno

Name server:

- je uzel, odpovídající na dotazy typu "jakou IP adresu má uzel X.Y.Z?"
- ostatní uzly jsou jeho klienty
 - klient musí znát adresu (číselnou IP adresu) svého name serveru
 - klient musí umět komunikovat s name serverem
- name server používá "převodní tabulku" mezi symbolickými jmény a IP adresami
- name servery si po určitou dobu odpovědi pamatují v cache paměti a mohou pozdější shodné dotazy zodpovědět přímo ze své cache paměti

Protokol IP, formát paketu a záhlaví, TTL, MTU. Průchod IP paketu sítě, fragmentace a defragmentace, úloha protokolu ICMP

přenos dat zajišťuje protokol IP = Internet Protokol
nezajišťuje vlastní fyzický přenos, pouze si předává pakety s vrstvou síťového rozhraní
používá se nespojovaný a nespolehlivý přenos - tzv. datagramová služba

Hlavička IP paketu:

velikost hlavičky 4 byty
velikost paketu 16 bitů
IP adresu příjemce a odesilatele
identifikaci obsahu 8 bitů
dobu života 8 bitů (TTL)
údaj o verzi protokolu IP (IPv4)
volitelné položky (IP OPTIONS)
první část hlavičky (po verzi) má pevný formát a délku

MTU:

přenos paketů je nejefektivnější, když je lze vždy celé vložit do linkového rámce, protokol IP se o to snaží, ale ne vždy je to možné, proto je definován parametr MTU (Maximum Transfer Unit)

IP protokol má mechanismy pro dělení paketů do více rámců (fragmentaci) a opětné slučování fragmentů do paketu původní velikosti

Fragmentace - defragmentace:

- k potřebě rozdělit jeden IP paket do více rámců (fragmentace) pak dochází jen při přechodu přes jinou síť pokud je v této síti menší hodnota parametru MTU
- povinnost defragmentace (složení původního paketu z jednotlivých fragmentů) má až jejich koncový příjemce
- když už jsou pakety rozloženy, putují dál v tomto tvaru

Detekce zacyklení TTL:

- ve směrovacích tabulkách mohou být chyby důsledek: pakety se mohou dostat do smyčky a obíhat stále dokola ...
- protokol IP má proto zabudován mechanismus stárnutí paketů (Packet Aging)
- hlavička IP paketu obsahuje položku TIME TO LIVE ("doba života")
- hodnota této položky je v čase průběžně dekrementována, při průchodu každým mezilehlým uzlem se hodnota sníží o 1 – proto se někdy této položce říká HOP COUNT
- když hodnota dojde na nulu, je možné IP paket zahodit (zacyklil se)

ICMP:

- Protokol ICMP (Internet Control Management Protocol) je povinnou součástí každé implementace protokolu IP
- je mechanismem pro hlášení chyb a nestandardních situací
- pakety protokolu ICMP jsou přenášeny v datové části IP paketů
- ICMP není považován za protokol vyšší vrstvy ale spíše za součást protokolu IP

Transportní protokoly TCP a UDP, rozdílné a společné vlastnosti, porty, mechanismus výběru služby, potvrzující mechanismus v TCP, sliding window

služby transportní vrstvy používají entity aplikační vrstvy

rodina protokolů TCP/IP nabízí v transportní vrstvě dva alternativní protokoly:

- TCP = Transmission Control Protocol
- UDP = User Datagram Protocol

protokol UDP nezajišťuje spolehlivost, je pouze maximálně jednoduchou “obálkou” nad protokolem IP nabízí prakticky tytéž přenosové služby jako IP, funguje na nespojovaném principu přenáší tzv. UDP datagramy

protokol UDP přenáší data po blocích (UDP datagramech) a bezprostředně vyšší vrstvě to dává plně najevo

UDP vždy očekává, že dostane “kus” dat, ten vloží do svého datagramu a přeneše

UDP se nestará o ztrátu, nesprávné pořadí nebo zdvojení doručovaných “kusů” dat, to si musí zajistit aplikace

protokol TCP přidává spolehlivost kontroluje integritu paketů, zajišťuje opakování přenosu poškozených a ztracených paketů, kontroluje a opravuje pořadí došlých paketů, vyřazuje zdvojené pakety, funguje na spojovaném principu mezi odesilatelem a příjemcem vytváří virtuální spoj

protokol TCP také přenáší data po blocích (TCP segmentech), ale své bezprostředně vyšší vrstvě vytváří iluzi, že přenáší souvislý proud dat (stream), tvořený 8bitovými slabikami Slučování do bloků si TCP zajišťuje interně a sám tak, aby fungoval rozumně efektivně když od aplikace dostává data, nejprve si vždy naplní vyrovnávací paměť (buffer) a teprve pak její obsah odešle

Sliding window:

TCP používá metodu posuvného okénka (sliding window), odesílatel vysílá data “dopředu”, ještě než dostane potvrzení dříve odeslaných dat

- kladné potvrzení vyjadřuje “kolikátý byte příjemce očekává jako další”
- díky tomu je možné selektivní opakování vysílání (znovu se přenáší jen data, která se skutečně ztratila)
- při opakování odesílatel přechází na jednotlivé potvrzování (před odesláním dalšího bloku čeká na potvrzení předchozího)

Př. do vypršení timeoutu nepřijde potvrzení bytu n , mezitím byly přeneseny byty $n+1$, $n+2$, $n+3$...

byte n je přenesen znovu, odesílatel čeká na jeho potvrzení, dostane potvrzení ve smyslu: čekám byte $n+5$

Porty:

čísla portů mohou být přidělena staticky, tj. být předem dohodnutá (a všem známá) klient se potřebuje vědět, jaké číslo portu má server, na který se chce obrátit

servery by měly být dostupné na portech s předem dohodnutými (známými) čísly

porty však také mohou vznikat dynamicky (až na základě konkrétní potřeby) a čísla jim mohou být přidělována až v okamžiku jejich vzniku, server číslo portu klienta předem nemusí znát (dozví se ho z žádosti klienta o službu)

čísla portů, přidělená "staticky" (pevně, podle předem dohodnutých pravidel) - všichni znají, jsou tzv. dobře známá - well-known numbers není nutné je nijak explicitně inzerovat

7 = echo 21 = FTP 23 = telnet 42 = name server 67 = bootp server 68 = bootp klient
70 = gopher server 79 = finger server 80 = www server 110 = POP3 server 119 = NNTP server

jiným portům (než "dobře známým") jsou čísla přidělována dynamicky při vytváření

pokud lze očekávat, že relace bude trvat déle - (např. ftp, telnet), server spustí pro obsluhu klienta samostatný proces, který si nechá dynamicky přidělit nové číslo portu a klientovi toto číslo oznámí; tím se well-known port uvolní pro další klienty

Přepínání, proces samoučení přepínače, aging, problém redundance cest, algoritmus STA. Směrování, směrovací tabulky, rozhodovací kritéria, směrovací protokoly

propojovací uzel funguje v tzv. promiskuitním režimu zachycuje všechny datové rámce - i takové, které mu nejsou adresovány za normálních okolností by mu neměly být přímo adresovány žádné rámce, nemá vlastní adresu na úrovni síťové vrstvy (např. IP adresu)

Na úrovni síťové vrstvy: propojovací uzel je viditelný pro ostatní uzly

Propojovací uzel musí mít dostatečné informace o skutečné topologii sítě: na úrovni linkové vrstvy (most, přepínač) o svém nejbližším okolí v dosahu přímého spojení, k nejbližším směrovačům

na úrovni síťové vrstvy (směrovač) o skutečné topologii sítě

na úrovni aplikační vrstvy (brána) musí rozumět přenášeným datům

Most musí znát své nejbližší okolí jak se o něm dozví ????

Možnosti:

statická konfigurace informace se dodá na počátku, jednorázově
dynamické zjišťování ve spolupráci s ostatními mosty
zbytečně složité, není zapotřebí „samoučení“

Počítačové sítě

Sm rova musí znát skutečnou topologii celé sítě objem informací je výrazně větší než u linkové vrstvy

Možnosti:

- statická konfigurace
- statická konfigurace s dynamickou aktualizací

Pozorování:

rozsah informací, které most potřebuje, je relativně malý (týká se jen nejbližšího okolí) most je schopen fungovat, i když tyto informace nebude mít k dispozici, bude fungovat jako opakovač a rozešle všechno na všechny strany

Idea: lze připustit, aby si most sám získával potřebné informace ze svého okolí (učil se) a do doby než se „naučí“ fungoval neefektivně

důsledek: samoučící se most je zařízení, které se vůbec nemusí konfigurovat

nejprve most (přepínač) funguje jako opakovač protože nemá žádné informace o topologii svého okolí přitom sleduje adresy odesilatele ve všech přijatých rámcích když dostane rámec od uzlu A pro uzel B ze směru X, dozví se že „A leží ve směru X“ proto si zapamatuje umístění uzlu A neví-li dosud, kde leží uzel B, rozešle rámec do všech směrů (kromě X), jinak cíleně správným směrem od tohoto okamžiku již každý rámec určený uzlu A pošle cíleně jen do směru X

Proces samoučení nebude fungovat, když v síti budou cykly (smyčky) pak most (přepínač) přijme jeden rámec z více různých směrů inteligentní mosty se dokáží vzájemně domluvit a smyčku přerušit aplikují algoritmus *STA (Spanning Tree Algorithm)* a vytvoří kostru grafu automaticky shromážděné údaje o umístění uzlu ztrácejí platnost při změnách konfigurace sítě

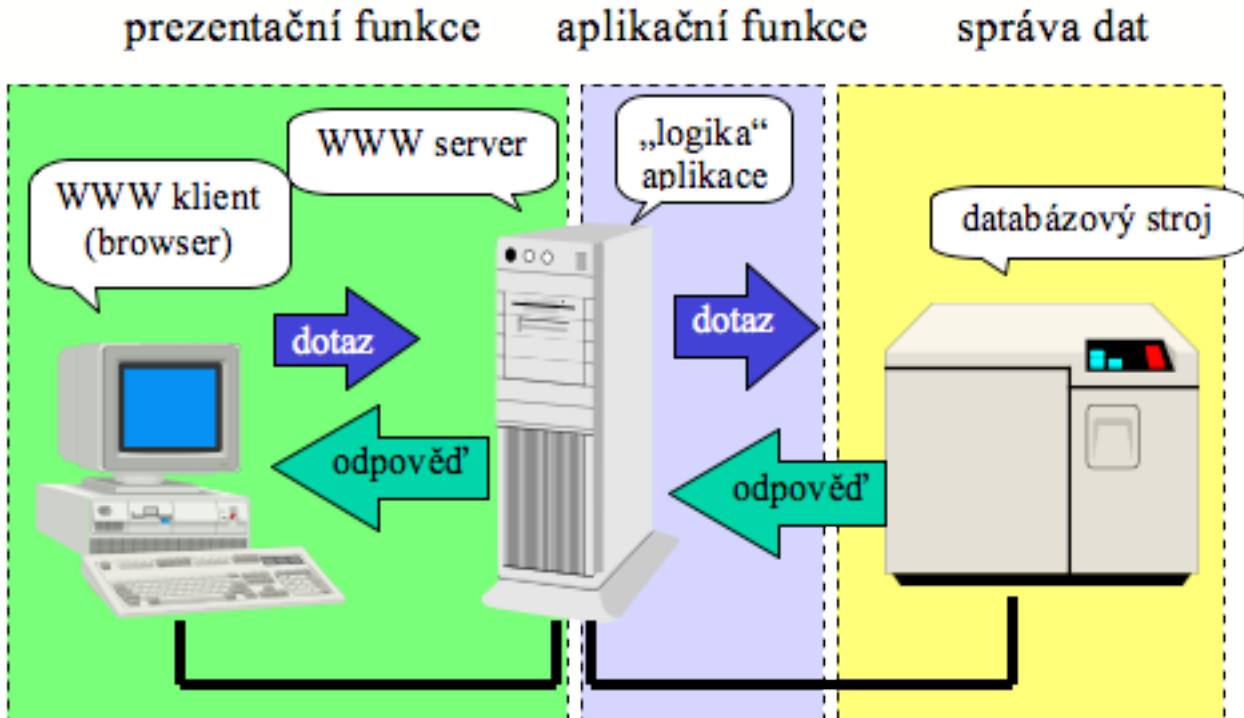
např. při přemístění počítače nejjednodušší způsob řešení: vymazání paměti
dokonalejší způsob řešení: každý údaj o umístění uzlu opatřit *asovým íta em*

Pojmem směrování (routing, routování) je označováno hledání cest v počítačových sítích. Jeho úkolem je dopravit datový paket určenému adresátovi, pokud možno co nejefektivnější cestou.

Základní datovou strukturou pro směrování je směrovací tabulka (routing table). Představuje vlastně onu sadu ukazatelů, podle kterých se rozhoduje, co udělat s kterým paketem. Směrovací tabulka je složena ze záznamů obsahujících. Statické, dynamické směrování. zdroj: wiki

Princip programování síťových aplikací, rozdělení aplikace, souvislost mezi vrstvami síťové architektury a softwarem, sockets. Grafický terminál, princip ASP

Princip programování síťových aplikací



Výhody 3-úrovňové architektury

- programátor aplikace se nemusí zabývat klientem
 - aplikace komunikuje s WWW serverem
- pro generování výstupu a přístup k databázi programátor aplikace disponuje standardními funkcemi - např. PHP
- uživatel používá pro přístup k různým aplikacím stejného klienta (www prohlížeč)
 - je možný přístup přes Internet
 - snadnější zaškolování uživatelů

Socket je něco jako zobecnění souboru pro síťové služby. Nejčastěji se používá na internetu v protokolu TCP/IP k připojení klienta k serveru. Programátor používá socket velice podobně jako soubor, může číst ze socketu připojeného třeba na <http://www.zive.cz> stejně jako kdyby četl soubor. Sockety můžou být lokální nebo síťové. Celé Xwindows visí na jednom socketu, programy pro Xwindows, (třeba mozilla) posílají do tohoto socketu data pro grafické zobrazení. Stačí tento socket zaměnit za síťový, (nastavení proměnné DISPLAY) a mozilla spuštěná na počítači v USA se zobrazí a je plně funkční na počítači v Japonsku.

Žádost o vytvoření nového socketu, kterou aplikační proces předává operačnímu systému formou systémového volání (s příznačným názvem socket), však ve svých parametrech obsahuje údaj o tom, s jakou soustavou protokolů bude socket pracovat, dále druh spojení (spolehlivé spojované či nespolehlivé nespojované, případně spojení na nižší úrovni, než je transportní), a také konkrétní protokol z příslušné rodiny protokolů, který bude přenos zajišťovat (což pamatuje na případ, kdy požadovaný druh spojení může být v rámci zvolené soustavy protokolů realizován více alternativními protokoly).

Grafický terminál

X terminál je speciální grafický terminál, který slouží provozování X11 aplikací. K počítači se obvykle připojuje přes síť ethernet. Často je X terminál řešen jako PC bez disku, s velkou pamětí, dobrou grafickou kartou, systémem UNIX a programem nazývaným X server. Operační systém se tahá ze sítě.

X11

Je to okenní nadstavba Unixu, řešená velmi obecně a pružně. Grafické zařízení (obrazovka, X terminál, X server) může být k počítači připojené třeba i po síti - nemusí být součástí počítače, na kterém běží vlastní programy. Počet připojených "obrazovek" je omezen pouze výkonností počítače.

ASP - Application Service Provider

on-line služba – v podstatě jakákoliv služba poskytována pomocí dálkového přístupu
technika poskytování on-line služeb

- prostřednictvím WWW - jako webové služby resp. aplikace
- prostřednictvím terminálového přístupu – znakový telnet
- prostřednictvím Javy – funkčnost klienta zajišťuje applet jazyka Java

princip ASP představuje nový přístup k používání aplikací

- aplikace provozuje specializovaný subjekt (poskytovatel)
- uživatel tyto služby používá na dálku, prostřednictvím dálkového přístupu
uživatel platí pouze za použití
- za poskytnuté aplikace, nikoliv za pořízení aplikace

výhody:

- možnost využít takřka okamžitě a bez rizika
- i malí uživatelé mohou využívat drahé aplikace
- na poskytnutí aplikace se užíví více subjektů

Bezpečnostní rizika sítě, autentizace, certifikace, šifrování, proxy server, filtrace paketů, přístupové seznamy (ACL, iptables), firewall

Bezpečnostní rizika napadení viry(koně,červi, spyware...) Dos útoky (odepření služby), bezpečnostní díry v operačních systémech ==>>>> poškození systému, získání vašich privátních dat (zneužití dat, zneužití loginů pro páčání dalších zločinů)

Autentizace proces při kterém se ověřuje zda uživatel nebo entita je opravdu tím za koho se vydává (uživatelská webová rozhraní – hesla šifrovací klíče, identifikační karta, obraz sítnice,otisk prstu)

Certifikace pomocí certifikátů lze prokázat totožnost, prokazuje se základní znalost vlastnictví soukromého klíče, při komunikaci dojde nejdříve k výměně certifikátů pomocí, kterých se pak autentifikuje pro server se autentizace povinná

Šifrování

- symetrické jeden klíč
- asymetrické dva klíče

dva párové klíče soukromým šifrujete a veřejný pošlete známým, aby si zprávu dekódovali

Proxy server Aplikační brána (typ firewalu) umožňuje autentizaci z pohledu klientské aplikace server a z pohledu cílového serveru klient. Mezi klientem a cílovým serverem

Počítačové sítě

virtuální spoj, které řídí a kontroluje proxy server (tazatel nekomunikuje se serverem
zvýšení ochrany)

Paketový filtr pracuje na síťové vrstvě ISO/OSI zkoumá hlavičku IP paketu a podle ACL rozhoduje o puštění nebo zahození, dnes pracují i na linkové vrstvě s Ethernetovými adresami –nepodporuje autentizaci

ACL umožňují jemější nastavení práv pro uživatele, pro každý objekt je uložen seznam obsahující dvojici uživatel a práva aplikuje na Ip adresy a porty omezení přístupu Ip nebo služby.

Firewall zařízení zpravidla počítač nebo routr sídlící mezi dvěma a více sítěmi, který omezuje, monitoruje či upravuje veškeré informace proudící mezi nimi. Používá se jako ochrana lokální sítě proti útokům z internetu (intranet)