1. **Uveďte formát adresy IPv4, co je to subnetting, co je to supernetting, co je to CIDR.**

V počátcích Internetu se IP adresa dělila na síťovou a lokální část fixně. Hranice byla dána podle tříd IP adresy (A,B,C, D-pro multicast, E – experimentální účely). V dnešní době se tak děje podle masky podsítě, což umožňuje větší granularitu.

Subneting – Metoda, jak rozmělnit jednu síťovou adresu např. třídy C pro několik subsítí tím, že posuneme pomocí masky podsítě pomyslnou dělící čáru mezi složkami IP adresy blíže k nižším bitům. Tímto dostaneme několik subsítí. Je důležité, aby tyto subsítě měly jediný společný vstupní bod, neboť tato skutečnost není viditelná z venku.

Superneting – Opak subnetingu. Posouvá pomyslnou dělící čáru k vyšším bitům a tak agreguje několik původně samostatných síťových IP do jedné – je důležité, aby to byly sousední adresy.

CIDR – Reakce na nárůst směrovacích tabulek. Používá techniku supernetingu. IP adresy se přidělují po tzv. CIDR blocích. Nahrazuje původní třídní charakter IP adres. IP adresy jsou ale závislé na konkrétním poskytovateli připojení.

2. **Co je to MIME? Popiš některou z kódovacích technik, které dovolují přenos ne-ASCII znaků prostřednictvím zpráv elektronické pošty.**

MIME je standardizovaný způsob označování obsahu zpráv, v praxi především elektronických dopisů a dokumentů WWW.

Pokud chceme přenášet i jiné než ASCII znaky, můžeme použít jinou znakovou sadu a tu správně uvést v parametru chrset hlavičky Content-Type. Můžeme také nastavit jiné přenosové kódování v hlavičce Content-Transfer-Encoding.

3. **Popište protokol DHCP, funkce, typy zpráv (protokol výměny zpráv), parametry (hlavní parametry, pomocné), jak souvisí DHCP s bootováním počítače.**

Protokol aplikační úrovně (na UDP). DHCP server přiděluje klientům IP adresy: Statické – k MAC je pevně definována IP; Dynamické – IP adresa je klientům přidělována z určitého rozsahu permanentně; Adaptivní – adresa je z určitého rozsahu přidělena na určitou dobu – klient může žádat o její prodloužení.

Při bootování získá klient IP adresu tak, že pošle zprávu DHCPDISCOVERY(broadcast), na tu mu odpoví DHCP zprávou DHCPOFFER – IP adresa a další nastavení (broadcast), to mu potvrdí klient DHCPREQ a DNS server DHCPACK/NAK. Povinné parametry: IP a maska. Nepovinné: Brána, DNS, WINS, jméno hostitele a domény, POP a SMTP.

4. **Jaký je vztah mezi: Doménovým jménem a IP adresou, jak se převádí. IP adresou a fyzickou adresou počítače, na které pracuje klient? Jak se tyto identifikátory získávají?**

IP adresa může mít více doménových jmen – zjišťuje se to pomocí tzv. resolverů. Fyzické adrese může být přiřazeno víc IP adres. IP adresa se používá na síťové úrovni, fyzická na linkové. Fyzická adresa je přímo spojená HW. Klient pracuje s IP adresou. Převod mezi IP a MAC adresou je pomocí ARP a zpět RARP.

5. **RMON, princip činnosti, skupiny RMON (vyjmenujte alespoň 4), tabulky RMON a princip přístupu k informacím.**

RMON sonda promiskuitně sleduje data na síti, ke které je připojena. Oznamuje výjimky, vede statistiky hostitelských systémů (MAC adresy), historie pro analýzu trendů, statistiky kdo s kým hovoří, zachytává packety pro statistiky. Skupiny:

- Historie – zachycuje časové statistiky segmentu LAN. Není vztaženo k ind. hostům. Nepracuje přes přepínače mosty ani směrovače.
- Hostitelské systémy – Kdo přenáší. Poskytuje statistiky založené na MAC adresách.
- Statistiky – ukazuje statistiky na LAN segmentu, není vztaženo k individuálním hostům, nepracuje přes mosty, přepínače a směrovače.
- Alarmy – sonda monitoruje jakékoliv statistiky podle MIB. Je-li překročena hodnota, vytvoří vnitřní událost. Pokud hodnota neklesne pod úroveň obnovy, není spuštěna žádná další akce.
- Horních N hostů – Kdo přenáší nejvíce. Statistiky založené na MAC adresách.
- Matice – Kdo s kým komunikuje. Poskytuje statistiky vztažené k párům komunikujících MAC adres.
- Události – Událost vznikne, je-li překročen práh alarmu. S každou událostí jsou spojeny akce jako je záznam do logu (interního), poslání SNMP trapu (do konzole síťového manageru) apod.

- Filtr – Podle parametrů v packetu (např. aplikace, protokol, adresa), dovoluje nastavit podmínky, které zajistí buď monitorování nebo záznam packetů.
- Zachycování – Podle parametrů definovaných ve skupině filtrů zachycuje v sondě packety.

Informace jsou uspořádány lexikograficky do stromové struktury. Přistupuje se na listy přes jejich OID.

6. RMON2

Prostředek pro centralizované sledování velkého množství podsítí. Offline operace – samostatná práce sondy bez nutnosti kontinuálního sledování. Proctive monitoring – nepřetržitý běh diagnostiky. Pracuje na síťové úrovni. Skupiny:

- Adresář protokolů – každá sonda umí pracovat s omezenou množinou protokolů, neumí se je naučit za běhu. Dekódování paketu provádí programové vybavení podle tabulky.
- Distribuce protokolů – shromažďování informace o packetech a oktetech různých protokolů detekovaných na segmentu sítě.
- Mapa adres – Mapování síťových adres na adresy linkové úrovně.
- Host systémy síťové úrovně – Zachycuje počty packetů a oktetů daného protokolu síťové úrovně přijatých nebo vyslaných z jednotlivých síťových adres na specifickém rozhraní.
- Matice hostů síťové úrovně – čítá počty marketů a oktetů mezi dvěma síťovými adresami. Rozlišuje spojení tam a zpět. Vybírá N nejaktivnějších spojení.
- Host systémy aplikační úrovně – zachycuje počty packetů a oktetů daného protokolu aplikační úrovně přijatých nebo vyslaných z jednotlivých síťových adres na daném rozhraní.
- Matice hostů aplikační úrovně – čítá počty packetů a oktetů mezi dvěma síťovými adresami předávanými mezi dvěma aplikacemi. Rozlišuje spojení tam a zpět. Vybírá N nejaktivnějších spojení.
- Historie – dovoluje zachycovat data podle přání uživatele. Nahrazuje typickou funkci řídící stanice – periodické dotazování.
- Konfigurace sondy – řídí konfiguraci různých parametrů sondy. Dovoluje určit, které skupiny sonda zpracovává. Dovoluje zavádět programové vybavení z TFTP serveru. Dovoluje provádět reset sondy. Dovoluje komunikovat se sondu pomocí sériového rozhraní.

7. Směrování RIP, princip, algoritmus opravy směrovacích tabulek, algoritmy urychlení konvergence.

RIP je směrovací protokol postavený na algoritmu směrování podle vektoru vzdáleností DVA – používá Bellman-Fordův Algoritmus (dynamické programování). Ohodnocení linek 1. Maximální ohodnocení 15, 16 je nekonečno. Vektor vzdáleností pro uzel X je minimální vzdálenost z uzlu X do všech ostatních. Každý uzel posílá vektor vzdáleností svým sousedům. Přijímá vektor vzdáleností od sousedů. Vypočítává nové vzdálenosti na základě přijatých vektorů. Vektory vzdáleností jsou posílány periodicky (30s); při změně položky ve směrovací tabulce. Uzel detekuje chyby uzlů periodickou výměnou "Hallo" packetů nebo výměnou směrovací informace.

Problém čítání do nekonečna: Split horizon – X nesmí poslat do uzlu Y svou vzdálenost k Z, je-li uzel Y ve směru z X do Z. Split horizon with poisoned reverse- X posílá do uzlu že je jeho vzdálenost k Z nekonečno, je-li Y ve směru z X do Z.

Nic však nezabrání cyklům. Urychlení konvergence: triggered update – okamžité spuštění opravy.

RIP2 – zabezpečení komunikace mezi routery pomocí šifrovaného hesla; přenos síťových masek ve zprávách mezi routery umožňuje implementovat subnetting

8. Protokoly pro přenos v reálném čase: RTP, RTCP, RTSP, RSVP.

RTP – real-time transport protokol. Formát pro doručování zvukových a obrazových dat po internetu. Používá UDP.

RTCP – RTP kontrol protokol slouží k řízení RTP relace a k sledování kvality toku. Port obvykle o jedno větší než RTP

RTSP – real-lime streaming protokol. Používá se k řízení streamového audia / videa. Postaven na http, ale je stavový. Formát protokolu: text, MIME záhlaví. Typu požadavek / odpověď. Stavové kódy. Bezpečnostní mechanizmy. Formát URL. Vyjednávání obsahu.

RSVP – je výhradně signalizační protokol, který pro své šíření využívá informací získaných běžnými směrovacími protokoly. Zajištění QoS je založeno na explicitních rezervacích zdrojů ve všech routerech podél datového toku. Každý router tedy musí v paměti uchovávat potřebné stavové informace. Jedná se však o tzv. "měkký stav" (soft-state), neboť všechny tyto informace mají omezenou životnost a musí být periodicky obnovovány

zprávami typu PATH a RESV. Informace a rezervace příslušející danému toku lze též zrušit explicitně pomocí zpráv typu PATHTEAR a RESVTEAR. Rezervace jsou iniciovány příjemcem a realizují se postupně proti směru datového toku. To je velmi výhodné zejména pro multicastové toky, protože se tím rozděluje zátěž spojená s instalací cest pro datový tok a umožňuje se též efektivní agregace rezervačních požadavků. Rezervace mohou též být heterogenní, tj. každý příjemce si stanoví vlastní parametry QoS.

9. Jaký je rozdíl mezi řízením toku dat a obranou proti zahlcení při přenosech pomocí protokolu TCP? Vysvětlete princip řízení toku dat v sítích TCP/IP. Vysvětlete jak se TCP brání zahlcení, jak se zahlcení projevuje. Uveďte alespoň 2 algoritmy obrany proti zahlcení včetně principu činnosti.

Řízení toku dat se provádí velikostí okna, pořadovými čísly oktetů dat a potvrzováním. Záhlaví TCP segmentu obsahuje pole okno, které specifikuje, kolik oktetů dat se může přenést od odesílatele k příjemci bez průběžného potvrzování doručení jednotlivých segmentů. Minimální velikost okna je 1 segment, a to vyžaduje potvrzovat příjem každého segmentu. Protože tento způsob přenosu je neefektivní, využívá se větší šíře okna, tj. většího množství segmentů, které se mohou odeslat ihned za sebou a teprve poté získat na jejich doručení potvrzení. Po obdržení potvrzení jejich příjmu může odesílatel opět vyslat skupinu segmentů podle velikosti okna. Tento mechanizmus TCP se nazývá klouzající okno (sliding window), protože vysílací okno se jakoby posunuje o příslušný počet segmentů dál v řadě segmentů čekajících na odeslání. Maximální počet dosud nepotvrzených vyslaných paketů je dán velikostí okna. Ve skutečnosti mechanizmus „klouzajícího okna“ pracuje na úrovni oktetů (nikoliv na úrovni segmentů nebo paketů) a pořadová čísla segmentů specifikují „pořadové číslo“ prvního oktetu jejich datové části vzhledem k původnímu pořadí dat určených k vyslání.

TCP podporuje proměnnou velikost „klouzajícího okna“, protože každé potvrzení, které specifikuje počet přijatých oktetů, zároveň obsahuje informaci kolik dalších oktetů je příjemce připraven akceptovat (např. podle aktuální velikosti paměti, stavu sítě…) a vysílač pak upraví velikost svého okna.

Velikost okna se dohaduje při navazování spojení na základě velikosti paměti příjemce a odesílatele. Vysílací stanice přizpůsobí své vysílací okno velikosti paměti příjemce, aby nedošlo k jeho zahlcení. Pokud má příjemce problémy, paměť nestačí na přijímaná data, inzeruje ve své odpovědi velikost okna nula, čímž signalizuje vysílací stanici, aby přestala vysílat. Pokud se v síti tato situace často vyskytuje, pak to může znamenat nedostatečnou kapacitu stanic. TCP odpovídá na zahlcení sítě dynamicky snížením velikosti okna, čímž se sníží její propustnost. Poté postupně zvyšuje velikost okna do původní hodnoty, pokud opět nedojde ke ztrátě dat.

Pomalý start znamená, že každé nové spojení se zahajuje vysláním jednoho segmentu (přidává ještě jedno okno, okno zahlcení, *congestion window*). Po přijetí potvrzení doručení tohoto segmentu se okno zahlcení dvojnásobně zvětší. S každým dalším potvrzením se velikost okna zahlcení zvětšuje exponenciálně do kapacity okna příjemce nebo pokud nedojde ke ztráté jednoho datagramu.
Předcházení zahlcení: Po dosáhnutí prahu (SSTHRESH) se rychlost navyšuje lineárně. Blížíme se tak k CWND poněkud pomaleji.
Fast retransmit: Při přijetí duplicitního ACK se nečeká na timeout a posílá se znovu nepotvrzený rámec.
Fast recovery: Při přijetí tří duplicitních ACK se snižuje práh na ½.

10. Jaký je rozdíl mezi TFTP a FTP? Který z nich je realizován pomocí TCP a který pomocí UDP? Který z nich má zabudované ověřování? Na jaké účely se používají?

TFTP=Trivial File Transfer Protocol(port69) = aplikační protokol pro přenos souborů, implementační SW mohl být umístěný v paměti ROM bezdiskových počítačů → umožňoval 2fázovou zaváděcí proceduru=síťové informace přes BootP a přenos SW přes TFTP.Transportní služby bez spojení UDP, přenos po blocích 512b,server čeká na potvrzení každého bloku. Na rozdíl od FTP nezabezpečuje přenos = nepožaduje identifikaci/heslo.
FTP=File Transfer Protocol(port21/20) = aplikační protokol *71, princip klient-server, uživatelské rozhraní,typ/formát dat bin, ASCII,EBCDIC,identifikace nešifrovná uživatel+heslo/anonymous, spolehlivá transportní služba s řídícím 21/datovým 20 spojením TCP. Řídící existuje po celou dobu/Datové jen pro daný přenos dat. Přenos dat není chráněn.

11. Architektury obranných valů. Načrtněte architekturu následujících typů obranných valů. Screened Router, Bastion Host, Dual Homed Gateway, Screened Subnet.

Screening Router - Provádí filtraci paketů podle směru přenosu, IP adresy a čísla portu.

Screened host geateway – Vnitřní síť je chráněna filtrujícím směrovačem, který propouští pouze pakety určené pro vybraný počítač (Bastion Host). Pakty mohou být filtrovány nejen podle IP adresy, ale i podle portu (přístup k určitým službám).

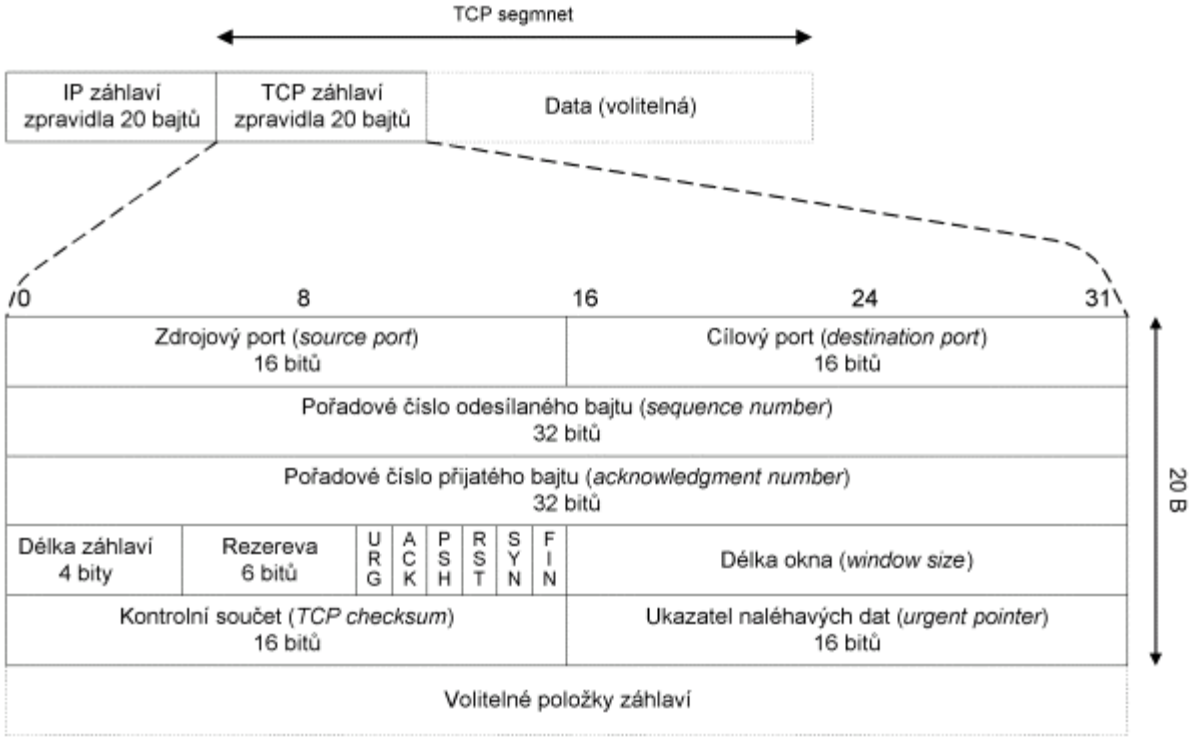
Bastion Host (Opevněný počítač) – Používá se při realizaci důležitých serverů, které mají být navíc velmi bezpečné. Např. SMTP, FTP, DNS, HTTP, atd.

Dual Homed Gateway – Úplně odděluje vnitřní a vnější síť. Služby musí být umístěny na této bráně a jsou přístupné jak z vnitřní sítě, tak i z vnější sítě.

Screened Subnet – Pomocí dvou filtrujících směrovačů se vytvoří oblast mezi vnitřní a vnější sítí, nazývaná demilitarizovaná zóna. Do této subsítě se připojí Bastion Hosts, nesoucí služby, které mají být přístupné jak z vnější, tak i z vnitřní sítě. Filtrujícími směrovači lze dosáhnout toho, že pakety s vnějšími adresami nejsou přenášeny do vnitřní sítě a naopak pakety s adresami vnitřní sítě nejsou přenášeny do sítě vnější.

Brána aplikační úrovně – Pomocí filtrujícího směrovače jsou propouštěny pouze pakety určené aplikační bráně. Zde jsou instalovány aplikační proxy, které umožní komunikaci a klienty ve vnitřní síti.

12. Protokol TCP, formát záhlaví, volitelné parametry.



Pořadové číslo odesílaného bajtu je pořadové číslo prvního bajtu TCP segmentu v toku dat od odesílatele k příjemci (TCP segment nese bajty od **pořadového čísla odesílaného bajtu** až do délky segmentu). Tok dat v opačném směru má samostatné (jiné) číslování svých dat. Jelikož pořadové číslo odesílaného bajtu je 32 bitů dlouhé, tak po dosažení hodnoty 2^{32}-1 nabude cyklicky opět hodnoty 0. Číslování obecně nezačíná od nuly (ani od nějaké určené konstanty), ale číslování by mělo začínat od náhodně zvoleného čísla. Vždy když je nastaven příznak SYN, tak operační systém odesilatele začíná znovu číslovat, tj. vygeneruje startovací pořadové číslo odesílaného bajtu, tzv. ISN (*Initial Sequence Number).*

Pořadové číslo přijatého bajtu vyjadřuje číslo následujícího bajtu, který je příjemce připraven přijmout, tj. příjemce potvrzuje, že správně přijal vše až do pořadového čísla přijatého bajtu mínus jedna.

Délka záhlaví vyjadřuje délku záhlaví TCP segmentu v násobcích 32 bitů (4 bajtů) – podobně jako u IP-záhlaví.

Délka okna vyjadřuje přírůstek pořadového čísla přijatého bajtu, který bude příjemcem ještě akceptován.

Ukazatel naléhavých dat může být nastaven pouze v případě, že je nastaven příznak URG. Přičte-li se tento ukazatel k pořadovému číslu odesílaného bajtu, pak ukazuje na konec úseku naléhavý dat. Odesilatel si přeje, aby příjemce tato naléhavá data přednostně zpracoval. Tento mechanismus používá např. protokol Telnet.

V poli příznaků mohou být nastaveny následující příznaky:

URG – TCP segment nese naléhavá data.

ACK – TCP segment má platné pole "Pořadové číslo přijatého bajtu" (nastaven ve všech segmentech, kromě prvního segmentu, kterým klient navazuje spojení).

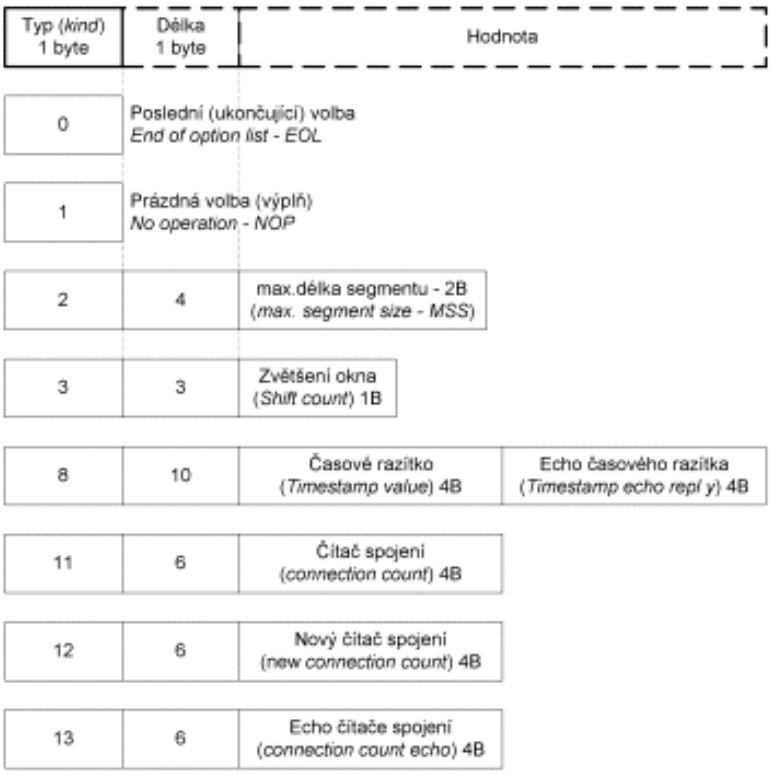
PSH – Zpravidla se používá k signalizaci, že TCP segment nese aplikační data, příjemce má tato data předávat aplikaci. Použití tohoto příznaku není ustáleno.

RST – Odmítnutí TCP spojení.

SYN – Odesílatel začíná s novou sekvencí číslování, tj. TCP segment nese pořadové číslo prvního odesílaného bajtu (ISN).

FIN – odesilatel ukončil odesílání dat. Pokud bychom použili přirovnání k práci se souborem, pak příznak FIN odpovídá konci souboru (EOF). Přijetí TCP segmentu s příznakem FIN neznamená, že v opačném směru není dále možný přenos dat. Jelikož protokol TCP vytváří plně duplexní spojení, tak příznak FIN způsobí jen uzavření přenosu dat v jednom směru. V tomto směru už dále nebudou odesílány TCP segmenty obsahující příznak PSH (nepočítaje v to případné opakovaní přenosu).

Kontrolní součet se počítá z TCP-segmentu, ale i z některých položek IP-záhlaví.



Povinné položky TCP záhlaví tvoří 20B,pak následují volitelné položky. Skládají se z typu, délky, a hodnoty. Délka TCP záhlaví musí být dělitelná čtyřmi, jinak se záhlaví doplňuje prázdnou volitelnou položkou – NOP. Jelikož pole délka záhlaví je pouze 4 bity dlouhé, tak toto pole může nabývat maximálně hodnoty $1111_{2=1510}$. Délka záhlaví se udává v násobcích čtyř, tudíž záhlaví může být dlouhé maximálně 15x4=60 bajtů, takže na volitelné zbývá nejvýše 40 bajtů.

13. Popište protokol ARP a RARP, funkce, typy zpráv.

Používá k získání ethernetové (MAC) adresy sousedního stroje z jeho IP adresy. Vysílající odešle *ARP dotaz (**ARP request**)* obsahující hledanou IP adresu a údaje o sobě (vlastní IP adresu a MAC adresu). Tento dotaz se posílá linkovým broadcastem – na MAC adresu identifikující všechny účastníky (`ff:ff:ff:ff:ff:ff`). ARP dotaz nepřekročí hranice dané podsítě, ale všechna k ní připojená zařízení dotaz obdrží a zapíší si údaje o jeho odesilateli do ARP cache. Vlastník hledané IP adresy odešle tazateli *ARP odpověď (**ARP reply**)* obsahující vlastní IP adresu a MAC adresu. Tu si tazatel zapíše do ARP cache a může odeslat datagram.

RARP se používá k získání IP adresy počítače při znalosti MAC adresy (tu každý počítač zná, má ji v trvalé paměti síťové karty). Vysílající vyšle *RARP dotaz (**RARP request**)* obsahující vlastní MAC adresu. Dotaz se posílá na MAC broadcast. V ní by se měl nacházet RARP server opatřený tabulkou obsahující IP adresy příslušející jednotlivým MAC adresám. Server prohlédne tabulku, a pokud v ní najde MAC adresu tazatele, pošle mu zpět *RARP odpověď (**RARP reply**)* s IP adresou, kterou si má nastavit.

ARP Proxy – z několika fyzických sítí se vytvoří jedna IP síť. Směrovač mezi nimi podvádí a vydává se za počítače z druhé podsítě (na výzvy pro ně odpoví sám a pošle svou linkovou adresu, když pak dostane data, předává je do druhé fyzické sítě). Musí vědět, kdo je kdo.

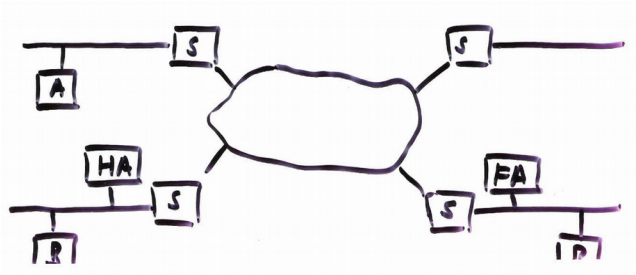
14. Směrování OSPF, architektura.

Open Shortest Path Firs) je určen k výměně informací o směrování v rozsáhlých a velmi rozsáhlých strukturách propojených sítí. Efektivní – nezatěžuje příliš přenosové cesty, ale je složitější.

Protokol OSPF počítá směrování podle algoritmu LSA (link state algorithm) který se počítá pomocí Dijkstrova algoritmu. Vyměňují se doručovací stromy. Každý uzel zná celou topologii. Minimální výměna dat. Rychlá konvergence.
Se zvětšováním databáze stavu linky rostou nároky na paměť a na dobu přepočtu tras. Protokol OSPF tento problém řeší rozdělením struktury propojených sítí na oblasti (skupiny sousedících sítí), které jsou navzájem propojeny páteřní oblastí. Databáze stavu linky jednotlivých směrovačů obsahují pouze údaje o oblastech, ke kterým je daný směrovač připojen. Spojení páteřní oblasti s ostatními oblastmi zajišťují směrovače ABR (Area Border Router).
Z důvodu dalšího omezení množství informací šířených do jednotlivých oblastí umožňuje protokol OSPF použití oblastí se zakázaným inzerováním. Oblast se zakázaným inzerováním může obsahovat jediný vstupní a výstupní bod (jediný směrovač ABR) či více směrovačů ABR, kdy každý ze směrovačů ABR je možné použít k dosažení externích tras k cílům.

15. Mobilní IP, princip činnosti.

Stanice na cizím segmentu – Pokud je stanice B doma, tak s ní ostatní komunikují normálně. Pokud přijde na jiný segment, musí si pomocí ICMP zprávy najít cizího agent FA. Tento agent kontaktuje domácího agenta HA. Pokud pak chce někdo komunikovat s B, tak HA to přebírá a odesílá to FA. Ten to předává FA a ten B.



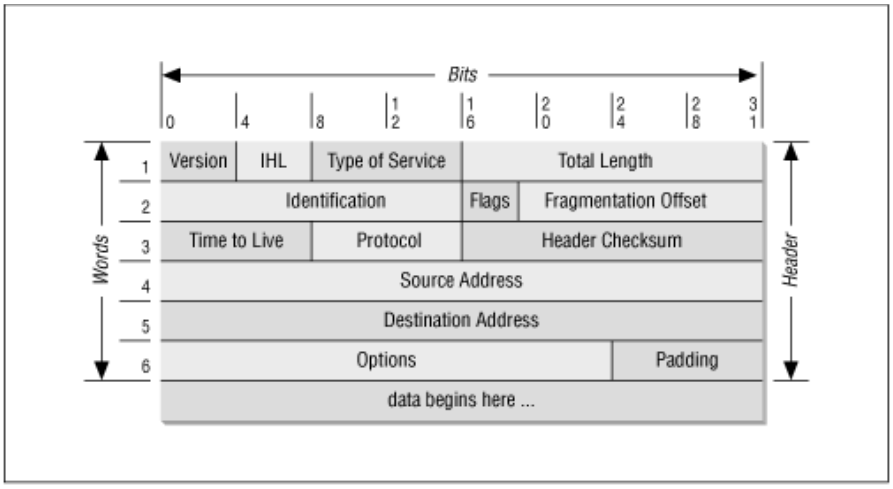
Care-of-address – Tento princip může fungovat i bez FA, ale stanice musí na daném segmentu získat care-of-adrese. S touto adresou sama kontaktuje HA, který jí pak může na tuto adresu data posílat. B může A odpovídat přímo.

16. Funkce relační úrovně.

Podporuje prezentační i aplikační úroveň. Podporuje spojované i nespojované služby. Služby:

a) Řízení dialogu a řízení toku dat – dovoluje realizovat duplexní nebo poloduplexní přenos dat
b) Rušení relačních spojení – na transportní úrovni okamžité rušení spojení
    a. Rušení uživatelem (aplikační) / poskytovatelem (relační úrovni) – hrozí stráta dat
    b. Uspořádané rušení spojení – spojení ruší jedna ze stran a to tak, která si je jista, že přenesla všechna data
    c. Rušení na základě vlastnictví pověření – dohadované rušení spojení, ruší ten, kdo má pověření
c) Synchronizace přenosu dat – dvě formy (hlavní a vedlejší synch. body), dovolují vytvořit značky se sériovými čísly
    a. Hlavní synch. bod – je-li zadán, nemohou se posílat další data; je-li potvrzen, jsou data spolehlivě uložena
    b. Vedlejší synch. bod – nevyžaduje potvrzení; velikost okna potvrzení dohaduje aplikační úroveň; není-li potvrzeno, vrací se k předchozímu (hlavnímu, vedlejšímu) bodu
d) Aktivní jednotky a aktivity – váží se k synch. bodům

17. Protokol IP, formát záhlaví, fragmentace, TTL, TOS, volitelné parametry.



Protokol na síťové úrovni – nespolehlivý, nespojovaný. Jednotka přenášených dat – IP datagram.

IP datagram a jeho formát - dvě základní části: řídící část, tvořenou hlavičkou datagramu, a datovou část.

TOS – type of services (priorita-3 | typ služeb-4 | nevyužito-1)

Fragmentace datagramů: Skutečnost, že IP protokol musí být schopen přenášet své datagramy prostřednictvím různých druhů přenosových cest, má některé významné

důsledky. Například velikost datových rámců, přenášených na úrovni vrstvy síťového rozhraní TCP/IP modelu, je závislá na konkrétní přenosové technologii, pomocí které je daná dílčí síť realizována.
V případě lokálních sítí typu Ethernet je to 1500 oktetů, zatímco například sítě Token Bus připouští rámce až do velikosti 8191 oktetů, a veřejné datové sítě na bázi doporučení X.25 pracují s rámci až do velikosti 4096 oktetů. Některé moderní přenosové technologie však pracují s mnohem menšími rámci - například jen 128 oktetů či ještě méně. Protokol IP se ale dost dobře nemůže přizpůsobit nejmenšímu možnému formátu rámce, aby do něj mohl vždy vložit svůj IP datagram celý. Proto musí počítat s možností fragmentace, při které pro potřeby přenosu dochází k rozdělení původního datagramu na několik dílčích fragmentů - tak velkých, aby se již vešly celé do těch rámců, které je příslušná síť schopna skutečně přenést Jde přitom o tzv. netransparentní fragmentaci, při které jednotlivé fragmenty skládá do původního celku až jejich koncový příjemce. Ten pak k tomu využívá položky IDENTIFICATION, FLAGS a FRAGMENT OFFSET jednotlivých fragmentů.
(Aby byl cílový uzel schopen složit originální datagram, musí mít dostatečný buffer do něhož jsou jednotlivé fragmenty ukládány na příslušnou pozici danou offsetem. Složení je dokončeno v okamžiku, kdy je vyplněn celý datagram začínající fragmentem s nulovým offsetem a končící segmentem s příznakem "More Data Flag" nastaveným na False.)

18. Jmenné služby, architektura, typy serverů, princip převodu, typy převáděných informací.

DNS – celosvětově distribuovaná databáze uchovávající záznamy, která IP adresa patří ke kterému doménovému jménu, přitom IP adresa jich může mít více. O databázi se starají programy jmenné servery, které data z databáze poskytují klientům, tzv. resolverům. Jmenný prostor všech domén je uspořádán do hierarchické struktury podobné souborového systému.
Doména - skupina jmen, které spolu logicky souvisejí (geografická poloha, organizace).Lze je členit na menší celky (subdomény).
Reverzní doména – zpětný překlad IP adresy na reverzní doménu (doménové jméno). Pro tyto účely byla definována doména in-addr.arpa (v případě protokolu IPv6 ip6.arpa), která má subdomény 0 až 255. Domény jsou tvořeny IP adresami psanými v opačném pořadí.
Doménové jméno – vznikne spojením příslušných řetězců (domén) vzájemně oddělených tečkou, kde první řetězec je jméno počítače, druhý jméno domény, do níž počítač náleží atd. Celé maximálně 255 znaků dlouhé.
Zóna – je část prostoru jmen domény, kterou obhospodařuje konkrétní správce. Je tedy tvořena doménou nebo její částí.
Resolver – část systému, která dokáže nalézt IP adresu k příslušnému jménu a naopak.Většinou implementován jako soubor knihovních funkcí.
Jmenný server – správce, který dohlíží na data definující příslušnou zónu a zajišťuje překlad jmen počítačů na IP adresy a naopak na žádost resolveru nebo jiného jmenného serveru. Podle uložení dat rozlišujeme následující typy jmenných serverů:
Root server – existuje 7 root serverů. Znají všechny domény nejvyšší úrovně. Umí získat informaci o hostech podsítí. Určuje je NIC (Network Information Centre)
Master server – každá zóna je pod správou alespoň dvou master serverů (primární, sekundární), který obsahuje kompletní data o zóně, tzv. autoritativní data. Tento server se označuje jako autoritativní. Je doporučováno, aby každá zóna měla nejméně dva servery tohoto typu.
Primární server – je autoritativním jmenným serverem pro zónu a data o zóně získává z databází uložených na lokálním disku. Každá zóna má právě jeden primární jmenný server.
Sekundární server – je autoritativním jmenným serverem pro zónu a data o zóně pravidelně kopíruje z databází primárního jmenného serveru (případně z jinych sekundárních jmenných serverů).
Caching server – uchovává informace ve vyrovnávací paměti. Doba života informace je omezena. Nemají žádné pravomoce, neudržují databáze. Informace čtou z ostatních serverů.
Forwarder (předávající) jmenný server – funkce libovolného server (master, cache). Zpracovávají rekurzivní dotazy, které nemohou podřízené servery řešit lokálně. Mají přístup k Internetu – info od root serverů. Slave servery + forwarding servery se používají tehdy, pokud nechceme, aby servery spolupracovaly se zbytekm sítě.
Dotazy – Resolver zformuluje dotaz, pošle jej místnímu jmennému serveru a očekává jeho odpověď. Zná-li náš server na příslušný dotaz odpověď, zašle ji nazpět. Pokud ji nezná, kontaktuje další servery, přitom vždy začíná kořenovým jmenným serverem.

Protokol DNS – aplikační protokol využívající k transportu dat protokol UDP a TCP. K jednodušším dotazům, jako je překlad adres, se používá UDP. Pro odpovědi se používá UDP, ale pouze pokud je odpověď kratší než 512B. V opačném případě se použije pro přenos TCP. Protokol TCP se také používá pro přenos zón mezi primárním a sekundárním jmenným serverem. Jmenný server naslouchá dotazům na portu 53 (UDP i TCP).
Zdrojové záznamy – Autoritativní data zóny jsou uloženy v databázi ve formě tzv. zdrojových záznamů (RR, Resource Records). Každý záznam má přidělen typ, který popisuje druh dat v záznamu, a dále třídu, která vyjadřuje adresovací schéma sítě (např. IP adresám odpovídá třída IN),. Záznamy RR se přenáší sítí protokolem DNS a používají se v konfiguračních souborech systému DNS.

19. Co jsou to cookie? K čemu slouží?
Jako cookie se v protokolu HTTP označuje malé množství dat, která WWW server pošle prohlížeči, který je uloží na počítači uživatele. Při každé další návštěvě téhož serveru pak prohlížeč tato data posílá zpět serveru. Cookies běžně slouží k rozlišování jednotlivých uživatelů, ukládá se do nich obsah „nákupního košíku“ v elektronických obchodech, uživatelské předvolby apod.

20. Co je to OID, jaký je rozdíl mezi identifikátorem objektu a jeho instancí, uveďte příklad.
OID je jednoznační identifikátor každého objektu v MIB databázi. Dva typy MIB objektu: skalární (např. integer) a tabulární (např. routovací tabulka). Př.: iso.org.dod.internet.mgmt.mib-2 (1.3.6.1.2.1)

21. Co je to Network Virtual Terminal, jak se provádí dohadování parametrů (Telnet), které příkazy se používají.
Protokol pro vzdálený přístup (emulace terminálu). NVT je obousměrné, znakově orientované zařízení, které lze nejlépe přirovnat ke dvojici klávesnice-tiskárna. Klávesnice generuje jednotlivé znaky v kódu ASCII, zatímco tiskárna je průběžně tiskne. Celek pak odpovídá představě tzv. **znakového**, resp. **řádkového terminálu** (**scroll mode terminal**).
Protokol TELNET nabízí čtyři příkazy pro "licitaci" o použití rozšíření:

WILL – odesílatel chce danou volbu zapnout
DO – odesílatel chce, aby příjemce danou volbu zapnoul
WONT – odesílatel chce danou volbu vypnout
DONT – odesílatel chce, aby příjemce danou volbu vypnul

22. Jak se provádí DoS útok pomocí protokolu TCP a jako pomocí ICMP.
TCP – Na cílový systém jsou odesílány stovky falešných požadavků SYN (Synchronization), které normálně slouží pro synchronizaci při zahajování spojení. Reakcí systému je vyhrazení části systémových prostředků pro jednotlivé spojení a odeslání odpovědi ACK-SYN. Normálně by měl systém odpovědět (ACK) o úspěšném navázání spojení, to však není tento případ a žádná odpověď nepřijde vzhledem k neexistující (neaktivní) podvržené IP adrese. Cílový systém po nějaké době vyšle znovu odpověď ACK-SYN a teprve po nějaké době jednotlivá spojení uzavírá (desítky vteřin). Při velkém počtu požadavků dochází k otevření velkého množství polo-otevřených spojení (half-open), zahlcení paměti a nemožnosti obsloužit normální uživatele.
ICMP – ICMP Echo funguje tak, že my pošleme ICMP Echo request a cílový počítač posílá zpátky ICMP Echo reply. Přitom zachovává velikost paketu (až 64kB). Toho lze využít tak, že zfalšujeme adresu odesílatele a tím docílíme, že datová linka oběti bude ucpávána dvakrát. Jednou daty směrem tam a podruhé daty zpátky (která budou určena oné zfalšované adrese).

23. IGMP (Internet Group Membership Protocol) – popsat, včetně jednotlivých verzí. Algoritmus.
Tento protokol především používají multicastoví klienti, aby signalizovali routerům své členství v multicastových skupinách. Nicméně není to jen jediné jeho využití, používá ho například i protokol DVMRP pro přenos svých zpráv apod.
IGMPv1
Pokud se nějaký klient chce připojit k multicastové skupině a pošle zprávu typu **Membership Report** s vyplněným číslem skupiny na adresu té skupiny, příslušný router by ji měl zachytit a postarat se o zprostředkování. Router si průběžně kontroluje členství klientů ve skupinách a občas (jednou za 60 sekund) pošle zprávy typu Membership Query na adresu 224.0.0.1 a čeká na Reporty klientů. Každý z klientů, který uslyší Query, si zvolí náhodné číslo v rozsahu 0-10. Toto číslo vyjadřuje čas v sekundách, za který chce poslat Report. Zároveň ale poslouchá, zda nějaký jeho kolega Report pro danou skupinu pošle. Pokud se tak stane, klient už nic neposílá. V případě, že klient danou skupinu opustí, přestane jednoduše odpovídat na Query. Pokud router nedostane pro skupinu třikrát po sobě žádný

Report, přestane ji posílat. Query se posílají obvykle jednou za minutu – v nejhorším případě tedy router posílá data ještě tři minuty po té, co už o ně nikdo nestojí. Tento jednoduchý mechanismus je velmi nevýhodný, pokud klient často mění členství ve skupinách. V takovém případě může sít snadno přetížit.

IGMPv2

Signalizace přihlášení do skupiny je obdobná jako u IGMPv1. Novinkou je proces opuštění skupiny. Klient může poslat zprávu Leave Group. Router na takovou zprávu zareaguje posláním Group-specific Query do dané skupiny. Max Resp time je obvykle nastaven na 1 sekundu. Pokud je ještě někdo členem skupiny, odpoví, a router pokračuje v posílání dat. Další novinkou je volba routeru, ktery posílá Query. Je-li na síti více routerů, je pro posílání Query vybrán ten s nejvyšším IP. Ostatní pouze poslouchají a jsou připraveni převzít jeho roli. Mechanismus pracuje tak, že pokud router uslyší Query zprávu od routeru s vyšším IP, přestane ty své sám posílat a čeká 400 sekund, zda nepřijde další. Pokud nepřijde, vyhodnotí, že vybraný server už asi nefunguje, a začne posílat Query sám, čímž proběhnou nové volby. V IGMPv2 se Query posílá jednou za 125 sekund. IGMPv2 je zpětně kompatibilní s IGMPv1.

IGMPv3

V IGMPv3 nepřihlašujete pouze do skupiny (*, G), ale přihlašujete se k odběru dat z konkrétního zdroje v dané skupině (S, G). Přirozeně se výrazně změnil i formát zpráv. Zprávy již nemají konstantní délku. Význam zpráv je stejný jako u předchozích verzí, pouze se přidávájí políčka pro členství ve skupinách.

24. Silly Window Syndrome – kdy k němu dochází a jak se řeší na straně vysílajícího a přijímajícího uzlu.

K syndromu hloupého okna dochází, pokud přijímač opakovaně nabízí krátké přijímací okno, namísto aby počkal, až bude moci nabídnout větší. Syndrom vede k neefektivnímu vysílání po krátkých segmentech. Vyvarování se syndromu SWS na straně příjemce je implementováno neotevíráním přijímacího okna v přírůstku menším než je jeden segment protokolu TCP. Vyvarování se syndromu SWS na straně odesílatele je implementováno neodesíláním více dat, dokud není dostatečná velikost okna inzerovaná přijímajícím koncem, aby mol být poslán celý segment. Pro odesílatele existují z tohoto pravidla výjimky, které jsou popsány v dokumentu RFC 11.22.

25. Elektronická pošta, princip, protokoly pro příjem elektronické pošty.

SMTP=Simple Mail Transfer Protocol pro přenos elektronické pošty přímým TCP spojením mezi odesílatelem a adresátem. V případě přenosových problémů (nelze navázat spojení) se periodicky provádí opakované pokusy a teprve po určité době (např 3dny) je pošta vrácena odesílateli jako nedoručitelná. Každý email zůstává na odesílatelově počítači, dokud není úspěšně doručen adresátovi. Formát adresy: lokální_část@doménové_jméno, resp osoba@počítač, kde osoba je uživatelské jméno adresáta a počítač je doménové jméno počítače, na němž má adresát konto. Služba email funguje mezi různými počítačovými sítěmi=je nutno adresovat příslušnou poštovní bránu=mail gateway, která poštu převede. Standardní domény a pseudodomény=jsou na straně odesílatele automaticky, dle mnemonického jména cílové sítě, konvertovány do správného formátu, např s poštovní branou.
MIME=Multiprpose Internet Mail Extensions=rozšíření-lze posílat multimediální přílohy audio, video, aplikace
SMIME=Secure MIME=bezpečnost, ochrana šifrováním
POP=Post Office Protocol=přístup/získání emailů z poštovního serveru při ponechání pošty na serveru a vytvoření lokální kopie/stažení pošty
IMAP=Internet Message Access Protocol=číst/kopírovat/mazat emaily uložené na poštovním serveru

26. Jak zabezpečíte mail pomocí asymetrické šifry.

Pomocí programu PGP (Prejty Good Privaci). Používá asymetrické šifrování RSA pro šifrování symetrického klíče relace, se kterým pak šifruje zprávu. Pro symetrické šifování používá algoritmus IDEA. Pro kompresi dat před šifrováním PKZIP. Výpočet kontrolního součtu algoritmem MD5. Pro převod binárních dat na ASCII algoritmus Radix-64.

27. BOOTP

Používá se pro nastavení bezdiskových stanic. Tato stanice pošle broadcast se svojí FA adresou. Bootp server jí odpoví a pošle jí IP, masku, router, bootserver a bootsoubor. Nepodporuje dynamické přidělování adresy. Adresa je přidělena na neomezenou dobu. Postaveno na UDP. Mimo pevně definovaných parametrů můžou být stanici poslány i vlastní parametry. Každý parametr má typ a hodnotu.

28. Popsat a nakreslit mechanismus zašifrování poštovní zprávy asymetrickou šifrou a opatření otiskem. U odesilatele a u příjemce.

Pomocí S/MIME. Pro asymetrické šifrování: RSA s délkou klíče min 512 bitů. Pro symetrické: FOO, FOO/40, DES-CBC, triple DES. S/MIME vycází z toho, že má normu PKCS-7, která umí zprávu elektronicky podepsat, šifrovat i podepsat a zároveň šifrovat. Definují proto jen příslušnou hlavičku Content-Type.

29. IPV6. Proč pro něj není definován protokol ARP a RARP.

Rozšíření adresního prostoru na 16 slabik. Některé technologie povinné. Plug and Play. Bezpečnost mezi koncovými uzly (jako IPsec). Od počátku agregovatelné globální adresy. Redukce externí směrovací informace na 8192 položek. IP adresy jsou přiřazeny rozhraním (ne uzlům). Adresy:

- Unicast – identifikace jednoho rozhraní
  - Loopback adresa - ::1 – obdoba 127.0.0.1
  - Link-local adresa – unikátní na subsíti
  - Site-local – unikátní pro site (zrušeno, nedohodli se co je to site)
- Multicast – identifikace více rozhraní
  - 1 – interface local
  - 2 – link local
  - 3 – subnet local
  - 4 – admin local
  - 8 – organisation local
  - E – global
- Anicast – identifikátor množiny rozhraní, packet je doručen na nejbližší rozhraní
- Broadcast – nezná. Adresa samé 0 i samé 1 je legální.

Předpokládá se, že počítač bude v síti fungovat po instalaci bez konfigurace -> adresa se získá z link local adresy a MAC adresy.

Místo ARP se používá podobný mechanismus: Neighbor Discovery Protocol.

30. Jaký je rozdíl mezi metodami symetrického a asymetrického šifrování, uveďte vlastnosti, známé šifrovací algoritmy, porovnání složitosti a bezpečnosti. Co je to hashovací funkce, kde se používá.

Symetrické šifrování – šifrování i dešifrování se provádí jedním tajným klíčem.

- DES – 56b klíč, silný ale prolomitelný
- Triple DEC – 112b klíč
- IDEA – 128b klíč, velmi silné, zatím nejsou algoritmy na prolomení
- Skijack – 80b klíč v šifrovacím čipu Clipper

Asymetrické šifrování – šifrování se provádí veřejným klíčem a dešifrování soukromým klíčem.

- RSA – podporuje proměnnou délku klíče, velmi silná šifra, algoritmus založen na práci s velkýma číslama

31. Přenos hlasu IP sítěmi, protokol VoIP.

Pro přenos hlasu IP sítěmi se můžou používat protokoly pro přenos v reálném čase – RTSP, RTCP, RTP, RSVP. Nebo můžeme používat protokol H323 (Voice over IP). Podporuje spojení 1:1 i 1:N. Bez podpory QOS na LAN. Řeší popis komponent, procedury signalizace, řízení a management, audio/video kodeky, datové protokoly. Komponenty:

- Terminály – koncová zařízení uživatelů, dvoubodová komunikace.
- Geateways – připojení na jiné sítě, převod kódování, převod přenosových formátů, napojení na terminály
- Geatekeepers – řízení, centrální bod pro volání v zóně, zajišťuje služby registrovaným uzlům
- MCU – participace více terminálů na konferenci

32. Protokol SNMP. Popište funkci operace get-next na příkladu s přístupem k tabulkám.

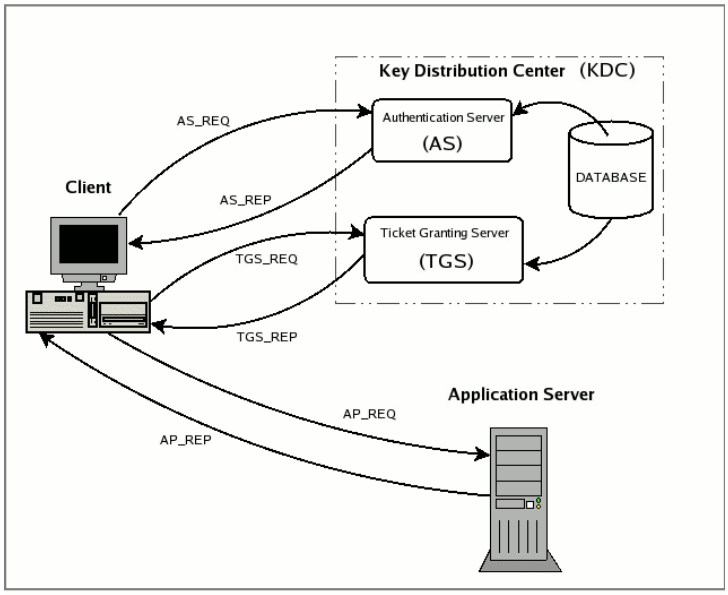
Model SNMP zahrnuje řízené uzly, řídící stanice, komunikační protokol a proxy agenty. Řídící stanice může pomocí protokolu SNMP komunikovat se stanicemi, na kterých je spuštěn SNMP agent. Tento agent jim pak zpřístupňuje informace uložené v MIB tabulce. MIB je popsána pomocí ASN1. Obsahuje databázi řízených objektů. Každý objekt je jednoznačně identifikován identifikátorem (skupina čísel oddělená tečkami). Pomocí operace get-next získává řídicí stanice následující data uložená v MIB tabulce včetně jejich identifikátoru.

SNMP1 – jednoduché ověřování pomocí community name

SNMP2 – šifrování zpráv, ověřování uživatele, víceúrovňový přístup, hierarchické řízení, podpora ukládání dat jako tabulky

33. Jakou strukturu mají tabulky ve skupině historie. Dovoluje RMON zachycovat pakety? Pokud ano, jak se určí které.
34. PC se stejnou hardwarovou adresou a různým DNS jménem. Jak se budou chovat na síti. (3 možnosti)
35. Co je to agregovaný index v RMON II, k čemu slouží, jaký má formát, uveďte příklad.
36. Zapiš pseudokód pro konkurenční server.
37. Popsat Truncated Reverse Path Broadcast (TRPB) a Reverse Path Broadcast (RPB) a RPM. Jaký je mezi nimi rozdíl. Nakreslit oba případy na síti se 4 uzly.
38. Schémata pro ověřování uživatele využívající symetrické i asymetrické šifrování.

Kerberos



- Klient pošle autoritě žádost o spojení se serverem, ve které uvede své jméno, jméno serveru a unikátní číslo U1.
- Autorita ověří právo klienta spojit se se serverem.
- Autorita pošle klientovi zprávu zašifrovanou jeho tajným klíčem KC, ve které uvede unikátní číslo U1 předtím zaslané klientem, náhodný klíč KR pro komunikaci se serverem a tiket T, což je ještě jednou klíč KR a jméno klienta, vše zašifrované tajným klíčem serveru KS.
- Klient ověří pravost autority tím, že byla schopna vrátit zaslané unikátní číslo U1 zašifrované jeho tajným klíčem KC.
- Klient pošle serveru zprávu, ve které uvede tiket T.
- Server pošle klientovi zprávu zašifrovanou klíčem KR, ve které uvede unikátní číslo U2.
- Klient pošle serveru zprávu zašifrovanou klíčem KR, ve které uvede domluvenou transformaci unikátního čísla U2.
- Server ověří pravost klienta tím, že byl schopen provést transformaci unikátního čísla U2 se znalostí klíče KR.

39. TCP/IP – synchronizační body
40. Popsat algoritmus pro odhad zpoždění u realtimových přenosů (RTT) Jak se bude chovat v případě, že odhadne nesprávně zpoždění a to bude příliš malé / příliš velké.

$RTT_i = \alpha.RTT_i+(1-\alpha).RTT_{i-1}$ kde $\alpha = 0.125$