# Architektura sítí a adresování

## Popište jednotlivé vrstvy modelu TCP/IP a jejich funkci. Vyjmenujte protokoly, které na nich komunikují

* TCP/IP se skládá z vrstvy síťového rozhraní, z IP vrstvy, z transportní a z aplikační vrstvy.
* Aplikační vrstva – DNS, FTP, SMTP... – zpracování dat na nejvyšší úrovni
  + Transportní vrstva – UDP, TCP – Přenos dat na cílové zařízení
  + Síťová vrstva – IP, ICMP – Adresování, směrování IP datagramů
  + Vrstva síťových rozhraní – Ethernet – Zajištění fyzického přenosu, přístup k fyzickému médiu (ovladače síťové karty)

1. Definujte zapouzdření a popište, jak probíhá. Uveďte, které síťové prvky, případně software, vytvářejí PDU na jednotlivých vrstvách modelu TCP/IP.
   * Zapouzdření spočívá ve vložení PDU (Protocol Data Unit) vyšší vrstvy do PDU nižší vrstvy. Vyšší vrstvy mají díky tomu přístup k protokolům nižších vrstev
   * Aplikační vrstva – daná aplikace – předá data na transportní vrstvu – kernel
   * Transportní vrstva – přidá tcp/udp hlavičku a vytvoří paket, který předá síťové vrstvě – kernel
   * Síťová vrstva – přidá IP hlavičku, zajišťuje tvorbu IP datagramů, které předává vrstvě síťovéh rozhraní
   * Vrstva síťového rozhraní – přidá Ethernet hlavičku, čímž vytvoří rámec – síťová karta
2. Vysvětlete pojem adresa. Jak je definována adresa na jednotlivých vrstvách modelu TCP/IP a kdo ji přiděluje? Uveďte příklady adres pro jednotlivé vrstvy TCP/IP.
   * Adresa je jednoznačný identifikátor zařízení v síti.
   * Aplikační vrstva – závisí na aplikaci (/home/noxx/data... ftp)
   * Transportní vrstva – Port – přiděluje OS nebo si vybere uživatel (př. 80 http)
   * Síťová vrstva – IP Adresa (v4 a v6), přiděluje ji DHCP a nebo uživatel sám (192.168.0.1)
   * Vrstva síťového rozhraní – MAC adresa (Síťová karta, přiděluje výrobce 05:49:4a:5b:3c)
3. Vysvětlete pojem směrování a ukažte, jak je implementováno na jednotlivých vrstvách modelu TCP/IP.
   * Směrování znamená určování cesty datagramu v síti
   * Aplikační vrstva – Závisí na aplikaci (email přiřadí mail do inboxu etc.)
   * Transportní vrstva – Paket je předán službě naslouchající na portu, pokud nikdo nenaslouchá, je zahozen a odeslána ICMP Dest. Unreachable
   * Síťová vrstva – Směrovací tabulka v routerech
   * Vrstva síťového rozhraní – Provádí switche za pomoci tabulky MAC adres
4. Popište průběh směrování na aplikační vrstvě u služeb DNS, elektronická pošta, IP telefonie, adresářové služby, správa sítě SNMP.
   * DNS
     + Rekurzivní a iterativní dotazy
     + **Rekurzivní** – Klient se zeptá cache, jestli zná adresu- když neví, zeptá se defaultního DNS serveru jestli ví
     + Jestli ne, tak se postupuje od root serveru (napevno umístěné jejich adresy v hint zóne)
     + Když neví root, pokračuje dál na doménu 1. řádu a ptá se DNS serverů, co je mají na starost
     + Ty se ptají případně DNS serverů u user domén
     + Uživatel nakonec dostane adresu, kterou si uloží do cache
     + **Nerekurzivní** – stejný bod 1
     + Jestli neví, tak vrátí nejlepší možnou odpověď
   * Email
     + Email je poslán klientem (MUA) za pomoci SMTP na MTA server.
     + Jestli server neví kam dál, zjistí MX záznam z DNS a pošle to získanému mail sserveru, který to doručí do cíle, kde si uživatel email stáhne za pomoci IMAP nebo POP3
   * IP telefonie
     + Skrz SIP server je získán cílový bod. Jestli SIP server neví, ptá se DNS.
   * Adresářové služby
     + LDAP – Uživatel je vyhledán v LDAP tabulce
   * SNMP
     + Data jsou zasílána agenty na SNMP server.
5. Vysvětlete, proč se mapují IP adresy na MAC adresy a jak toto mapování probíhá.
   * Aby bylo možné identifikovat rozhraní, kam se má paket poslat. Používá se u uniccastu (ARP) a multicastu (23 bitů IPv4 adresy se namapuje na 00:01:5e... a IPv6 se namapuje 33:33... dolních 32 bitů
6. Popište formát adresy IPv4 a třídy adres IPv4. Ukažte, jak se počítá maska a broadcastová adresa. K čemu slouží?
   * IPv4 se skládá z hostid a netid – netid určuje síť a hostid konkrétní zařízení. Toto dělení probíhá podle velikosti prefixu. Podle prvních 8 bitů adresy se počítají následující prefixy a třídy
   * Třída Adresa Prefix
   * A 0 0-127 8
   * B 10 128-191 16
   * C 110 192-223 24
   * D 1110 224-239
   * E 1111 240-255
   * Broadcast adresa: hostid jsou samé 1 – Posílání zprávy všem v síti
   * Maska – X bitů podle prefixu zleva je 1, zbytek 0
   * Slouží k určení adres v síti, rozdělení sítě do podsítí
7. Popište způsob přidělování adres IPv4. Jak lze zjistit, komu patří daná IP adresa?
   * Přidělování je buď skrz DHCP nebo manuálně. Zařízení pod IP adresou v místní síti lzde odhalit za pomoci protokolu RARP.
8. Popište formát adresy IPv6. Jaké typy adres IPv6 znáte a podle čeho se rozlišují? Jak probíhá přidělování adres IPv6?
   * 128 bitů, hexa čísla. Unicast, Multicast, Anycast. Rozlišují se prefixem. Probíhá skrz ICMPv6 RA
9. Vysvětlete význam služby ARP. Jak vzniká tabulka ARP na počítači a k čemu se využívá?
   * ARP slouží k zjištění MAC adresy pod IP adresou v síti. ARP Tabulka vzniká při dotazu na zařízení v síti, uloží se do ní výsledek dotazu, ať se příště nemusí zařízení ptát znovu. ARP dotazy jsou posílány přes broadcast, odpovědi získány jako unicast
10. Podle čeho síťový prvek pozná, na které rozhraní má předat odesílaný IP datagram? Jak lze zkontrolovat cestu, kterou putuje IP datagram v síti?
    * Pozná to díky ARP protokolu.
    * Cestu lze zkoontrolovat skrz nástrooj traceroute
11. Popište, jak probíhá překlad adresy IPv6 na MAC adresu. Jak lze na počítači vypsat mapování adres IPv6 na MAC adresy?
    * Za pomoci protokolu NDP (Neighbor solicitation) – ten přidává ICMPv6 zprávy, které nahrazují funkce z ipv4
    * Zpětně skrz ICMPv6 (obdoba RARP)
    * Mapování lze vypsat skrz *ip -6 neighbor*
12. K zadané adrese IPv4 spočítejte masku, adresu sítě a broadcastovou adresu.
    * Třeba 214.5.6.15
    * Začátek je 128+64+0+16 110 což je třída C a prefix tedy /24.
    * Maska je tedy 255.0.0.0
    * Adresa sítě je 214.0.0.0
    * Broadcast je 214.255.255.255
13. Jak byste vypsali na počítači seznam běžících síťových služeb? Co všechny výpis obsahuje?
    * *Netstat -natu*
    * Obsahuje protokol, počet odeslaných bitů, počet přijatých bitů, lokální a cílovou adresu a status.
14. Jak lze ověřit, že zadaný uzel v síti je aktivní a běží na něm konkrétní síťová služba?
    * Př. Skrz telnet – *telnet addr port*

# Pokročilé programování sítí TCP/IP

1. Definujte pojem protokol. Jakým způsobem lze protokol popsat? Uveďte příklad popisu vybraného protokolu.
   * Protokol je soupis sémantických a syntaktických pravidel, na základě nichž probíhá komunikace. Jednoduše řečeno určuje formát zasílaných zpráv.
   * Lze jej popsat stavovým automatem, gramatikou, diagramem posloupnosti zpráv...
   * Př. TCP:
   * KLIENT SERVER
   * SYN ->
   * <- ACK
   * ACK ->
   * Data ->
   * <- Data + ACK
   * ACK ->
   * FIN ->
   * <- ACK
   * <- FIN
   * ACK ->
2. Popište pojmy klient a server a vysvětlete jejich funkce. Uveďte příklad klienta a serveru pro základní síťové služby (e-mail, DNS, VoIP apod.)
   * Klient je koncové zařízení, jež má za úkol posílat požadavky na server a zpracovávat odpovědi.
   * Server má za úkol poslouchat (obsluhovat) příchozí komunikaci a reagovat na ni (while True)
   * Př web: Klient: Prohlížeč Server: Př. Apache server
3. Popište způsob přenosu dat na jednotlivých vrstvách modelu TCP/IP u komunikace typu i. Unicast ii. Multicast iii. Broadcast. Vysvětlete, jak se vytvářejí PDU na jednotlivých vrstvách.
   * PDU se vytváří na každé vrstvě přidáním PDU vyšší do PDU nižší, viz otázka hned na začátku.
   * Unicast
     + Síťové rozhraní – MAC adresa zjištěna za pomoci ARP/NDP (neighbor discovery protocol)
     + Síťová vrstva -- IP adresa zjištěna skrz routing table
     + Transportní vrstva – libovolný port
     + Aplikační vrstva – Podle aplikace
   * Multicast
     + Síťové rozhraní – vytvořena skupinová MAC adresa
     + Internetová vrstva – IGMP protokol pro připojení a opuštění skupiny, směrování za pomoci protokolu PIM
     + Transport – libovolný port
     + Apolikační vrstva – podle aplikace
   * Broadcast
     + Síťové rozhraní – ff:ff:ff:ff:ff:ff
     + Internetová vrstva – broadcast IP
     + Libovolný port
     + Podle aplikace
4. Co se stane, když je zahozen paket při přenosu? Popište chování unicastu, multicastu a broadcastu při zahození paketu. Čím se liší detekce chyb při přenosu IPv4 a IPv6?
   * Unicast – je poslána ICMP zpráva.
   * Multicast/Broadcast – není garantováno zaslání ICMP
   * Rozdíl v detekci:
   * IPv4 hlavička obsahuje checksum a proto ho u UDP nepožaduje
   * IPv6 hlavička neobsahuje a proto ho požaduje u UDP i u TCP
5. Vyjmenujte funkce knihovny BSD socket pro vytvoření klienta a serveru TCP.
   * Klient Server
   * Socket Socket
   * Bind
   * Connect Listen
   * Accept
   * Write Read
   * Read Write
   * Close Read
   * Close
6. Zapište kostru konkurentního serveru TCP pomocí funkce fork() a funkcí knihovny BSd sockets.
   * Totéž co nahoře, ale při acceptu se udělá fork, pid > 0 se zavře (close) a oblushuje další a ten druhý pokračuje v obsluze
7. Zapište kostru klienta a serveru UDP pomocí služeb knihovny BSd sockets.
   * Klient Server
   * Socket Socket
   * Bind
   * Sendto Recvfrom
   * Recvfrom Sendto
   * Close
8. Vysvětlete problém implementace konkurentního serveru UDP. Navrhněte způsob řešení.
   * Když klient pošle data ve 2 a více paketech, při každém z nich se vytvoří nový fork a jelikož je UDP bezstavové, nejsme schopni přiřadit nový paket k předchozímu.
   * Řešit lze tak, že server pro každého klienta zavolá bind a je tak schopný rozlišit klienty podle portu. Od klienta ale požaduje, aby další zprávy odesílal na tento port (Klient posílá na Port P, server odpovídá z P1 – další komunikaci klient směřuje už na P1)
9. Zapište kostru programu pro zasílání a čtení broadcastu pomocí schránek BSD.
   * Getsockopt, setsockopt, sock\_dgram pro UDP
10. Ukažte, jak lze implementovat vysílání a přijem multicast pomoci schránek BSD.
    * Setsockopt – ttl, sendto
    * Klient – setsockopt – přidání do skupiny, recvfrom, potom drop membership
11. Vysvětlete, co jsou spojované schránky UDP a k čemu se používají. Čím se liší od klasických schránek UDP?
    * Recvfrom je blokující, může čekat do nekonečna klient
    * Spojované schránky jsou UDP co využívá funkci connect pro test dostupnosti.
    * Při oodesílání nelze zadat celou IP a port, musí se použít write a read (získají port/ip z connecct funkce)
    * Komunikace pouze s 1 zařízením, pro více se musí znovu volat connect
    * Přijímá asynchronní chyby, v tom se liší
    * Vhodné pouze když komunikujeme po celou dobu jen s 1 partnerem.
12. Vysvětlete pojem síťovy formát dat a jeho použití. Jak lze převádět data do síťového formátu pomocí knihovny BSd sockets?
    * Formát, kdy je IP adresa převedena do binární podoby za pomoci funkce getaddrinfo.
13. Jaká funkce knihovny BSD sockets slouží pro komunikaci se systémem DNS?
    * Getaddrinfo zkonvertuje url na IP.

# Multicast. Zpracování dat na linkové vrstvě.

1. Definujte multicastové vysílání. Jaké adresy používají multicast na L2 a L3 a pro IPv4 a IPv6?
   * Multicastové vysílání funguje tak, že jsou data posílána pouze na ty koncové stanice, které jsou přítomny v multicast skupině.
   * L2 – 00:01:5e:...... IPv4
   * L2 – 33:33:..... – IPv6
   * L3 – adresy ze skupiny D (224-239) – IPv4
   * L3 – ff00 – IPv6
2. Vysvětlete princip mapování multicastových adres L3 na adresy L2. Proč vzniká překryv adres a jaký vliv má na komunikaci?
   * U ipv4 se mapuje 23 bitů na zbytek mac (dolních)
   * U ipv6 se mapuje 32 bitů (dolnícch)
   * Překryv vzniká kvůli tomu, že se ignorují první bity a může pro různé adresy vzniknout stejný multicast
   * Řeší se to tak, že po přijmutí multicastu skrz rozhraní se zkontroluje, jestli odpovídá IP adresa, jinak je paket zahozen
3. Pro zadanou multicastovou adresu IPv4 a IPv6 vypočítejte odpovídající multicastovou adresu ethernetu.
   * 224.0.1.5 (xxxx.0.0000 0001.0000 0101 – 01:00:5e:00:01:05
   * Ipv6 obdobně, ale beru 32
4. Na čem závisí dosah (viditelnost) multicastového přenosu? Jak lze omezit zasílání multicastových IP datagramů?
   * Omezit zasílání lze za pomoci TTL, na kterých i dosah závisí.
5. Vysvětlete funkci protokolů IGMP a MLD. Jaké příkazy obsahují?
   * Slouží k připojení do multicastových skupin pro IPv4, respektive IPv6.
   * Obsahují příkazy join, leave
6. Popište, jak probíhá komunikace pomocí multicastu včetně připojení stanice k multicastovému přenosu, odebírání dat a ukončení příjmu dat.
   * Komunikace probíhá připojením do multicast skupiny za pomoci IGMP/MLD (join), kdy se nastaví speciální adresa pro přijimání
   * Ze serveru jsou odeslána data, která jsou přijímána na výše zmíněné rozhraní
   * Jakmile má uživatel všechna data co potřebuje, odpojí se od multicast skupiny za pomoci IGMP zprávy typu leave
7. Uveďte příklad síťových služeb, které používají multicast. Co by se stalo, kdyby multicast na LAN nefungoval?
   * Videostreaming, kdyby na LAN nefungoval, nefungovaly by směrovací protokoly (RIPv2)
8. Uveďte příklady standardních multicastových skupin a jejich využití.
   * 224.0.0.1 – všechna zařízení v podsíti
   * 224.0.0.2 – všechny routery
9. Popište vlastnosti multicastového přenosu dat. Čím se liší od unicastu či broadcastu?
   * Je vysílán pouze pro konkrétní stanice (kterých může být narozdíl od unicastu ale více)
   * Oproti broadcastu nevysílá pro všechny, ale pouze pro stanice v multicast skupině
   * Implicitní TTL 1
   * Pouze UDP (nespolehlivý přenos dat)
   * Dynamické členství ve skupinách¨
10. Zapište kostru programu pro čtení a vysílání multicastových dat pomocí BSD sockets.
11. Vysvětlete jaké síťové aplikace využívají přímý přístup k paketům L2 a proč. Jaké prostředky či knihovny můžeme využít pro vytváření těchto aplikací?
    * Aplikace, které sledují pohyb dat v síti (wireshark, tcpdump..)
    * Lze využít libpcap, scapy, BPF filtr
12. Zapište kostru programu pro čtení a zpracování paketů pomocí knihovny libpcap
13. Vysvětlete pojem filtr BPF. Jaký má formát a kde se používá? Zapište filtr BPF pro filtrování síťového provozu typu multicast IPv6, webový provoz, komunikace DHCPv4, veškerý L2 provoz mimo multicastu apod.
    * BPF filtr slouží k filtrování paketů. Je zavolán před každým přijmutím/odesláním paketu a aplikacce, která jej využívá, zachytí pouze konkrétní pakety. Ip6 multicast, ip4 multicast, port 80...
14. Popište možnosti knihovny Scapy pro vytváření a analýzu paketů. Jak lze pomocí scapy odesílat a číst data na L2?
15. Uveďte, v čem se liší použití knihovny BSD socket a libpcap při implementaci síťové služby.
    * BSD socket slouží primárně pro vytváření a odesílání paketů, navazování spojení...
    * Libpcap nemá funkce pro tvorbu paketů, ale slouží k analýze zachycené komunikace

# Zabezpečení počítačové komunikace

1. Popište bezpečnostní rizika při provozování počítačové komunikace. Uveďte příklady útoků a jejich důsledky.
   * Odposlech přenášených dat
     + Data jsou odposlouchávána někým, kdo by k tomu neměl mít přístup
     + Př. Sledování posílaných hesel – útočník může ukrást účet
   * Neautorizovaný přístup k zařízením
     + Př. Někdo může ovládat IoT zařízení, aniž by to byl majitel
   * Podvržení dat
     + Př. Podvržení DNS výsledku, takže uživatel bude přesměrován na nesprávnou stránku
     + Př. Stránka, co se bude tvářit jako stránka banky, ale zadané údaje budou útočníky zneužity
   * Falšování identity
     + Př. Falešné jméno odesílatele emailu
   * Zahlcení zdrojů
     + Zařízení budou nedostupné
   * Viry
     + Nainstalujeme si nějaký vir, který bude posílat data útočníkovi
2. Vyjmenujte základní požadavky na bezpečnost počítačové komunikace. Ukažte, jak je lze řešit za pomoci konkrétních technologií.
   * Šifrování dat – Data budou zašifrovaná, že i když je útočník zachytí, nic z nich nepřečte. šifrovací funkce.
   * Autentizace – Elektronický podpis (př u emailu)
   * Integrita dat – data nebyla po cestě změněna – hash funkce, které zaručují, že data nebyla změněna
   * Neodmítnutelnost – Elektronický podpis lze získat z jiné zprávy – musí být další vrstva obrany – asymetrická kryptografie
   * Dostupnost – Zdroje jsou natolik výkonné, že je DoS útok nezahlti
   * Kontrola přístupu – autentizace uživatelů, přístup pouze skrz konkrétní IP...
3. Popište princip symetrického a asymetrického šifrování.
   * Při symetrickém šifrování se komunikující zařízení domluví na společném klíči, kterým bude komunikace šifrována.
   * Při asymetrickém má každý svůj soukromý a veřejný klíč. Vymění si veřejné a a tím rozklíčují zprávy, co si navzájem poslali. Veřejný klíč lze odvodit z soukromého, ale ne naopak.
4. Vysvětlete pojem soukromý a veřejný klíč. Popište, jak probíhá šifrování, zajištění integrity dat a ověření odesílatele zprávy pomocí těchto klíčů.
   * Soukromý klíč má uloženo koncové zařízení a nesmí ho nikde zveřejňovat. Veřejný klíč zařízení naopak zveřejňuje a lze pomoci něj rozšifrovat komunikaci zašifrovanou soukromým klíčem. Šifrování probíhá soukromým klíčem. Zajištění integrity lze docílit tím, že se vygeneruje kryptografický hash zprávy, předtím se k původní zprávě ještě přidá domluvený tajný klíč, ať útočník není schopný hash sám dopočitat. Cílové zařízení poté zprávu rozšifruje, přidá k ní tajný klíč a jestli se hashe rovnají, integrita byla zachována.
5. Co je kryptografický hash, jak vzniká a k čemu slouží? Uveďte algoritmy pro generování kryptografického hashe.
   * Je to hash, který vznikne z hashovací funkce, která je puštěna na zprávu.
   * Slouží k zajištění integrity dat.
   * Algoritmy: SHA1, SHA2, SHA3, MD5
6. Čím se liší klasická hashovací funkce od kryptografického hashe? Uveďte příklad použití klasického hashe a kryptografického hashe v síťové komunikaci.
   * Hashovacích funkcí je mnoho, kryptografický hash využívá nějakou z nich.
   * Každá kryptograficá hashovací funkce je hashovací funkce, ale ne naopak.
   * Zaručuje bezpečnost aplikace a neprolomitelnost hashe.
   * Kryptografický hash: hashování zpráv včetně tajného klíče
   * Hash: funkce, která se používá na hashování výše
7. Vysvětlete pojem elektronický podpis. Popište proces vytvoření a verifikace podpisu.
   * Podpis sloužící k ověření odesílatele dat
   * Vytvoření: Osoba vygeneruje 2 klíče – soukromý a veřejný
   * Za pomoci hashovacích algoritmů se ze zprávy vytvoří hash
   * Hash je zašifrován za pomocci soukromého klíče a tento hash je přiložen ke zprávě.
   * Verifikace:
   * Příjemce obdrží zprávu, oddělí od ní podpis a dešifruje jej za pomoci veřejného klíče, číjmž získá původní hash zprávy.
   * Sám si ze zprávy stejným algoritmem spočítá hash a ověří, že se rovnají, čímž dojde k ověření podpisu
8. Definujte pojem digitální (elektronický) certifikát. Uveďte, co obsahuje, k čemu se využívá a jak probíhá ověření platnosti.
   * Certifikát je dokument ověřující pravost veřejného klíče. Obsahuje ID majitele, informaci kdo ho vydal, jeho platnost a klíč samotný a účel klíče.
   * Oověření platnosti probíhá tak, že klient získá od serveru certifikát, podívá se do seznamu certifikačních autorit kterým důvěřuje a dešifruje podpis certifikátu pomocí veřejného klíče dané autority. Jestliže je ověřen, je klíč v něm dále používán pro komunikaci se stránkou.
9. Vysvětlete princip algoritmu Diffie-Hellman. Uveďte příklad aplikací, které tento algoritmus využívají.
   * Algoritmus sloužící k vytvoření tajného klíče skrz nezabezpečený kanál. Slouží k symetrickému šifrování. z^x % m = k
   * Oba dva jsou dohodnutí na číslech m a z. X si zvolí každý svoje a přepošlou si výsledek k
   * Vypočítají oba k znovu, ale základ bude získané k. Výpočtem dostanou konečný výsledek. Používá se u SSL, SSH.
10. Popište zabezpčení TLS. Ukažte, jak dochází k ustanovení spojení a které informace si strany vyměňují. Jaká omezení má zabezpečení TLS?
    * U TLS si obě komunikující strany vymění za pomoci asymetrického šifrování klíče k navázání komunikace, zbytek je pak skrz symetrické šifrování.
    * Ustanovení probíhá skrz TLS handshake, strany si vymění dostupné šifrovací algoritmy a dohodnou se na tom, který zvolí. Server pošle svůj certifikát.
    * Klient Server
    * Hello (verze, šifry..)
    * Hello (certifikát, veřejný klíč..)
    * Certifikát, veřejný klíč, CipherSpec (přepína na šifrování)
    * CipherSpec
    * Data
    * Omezení: Vyžaduje ověřený certifikát serveru, nezajišťuje autentizaci klienta
    * Výpočetně náročné, problém u IoT, senzorů..
    * Problém při monitorování sítě (vše zašifrované)
11. Vysvětlete princip zabezpečení IPSec. Uveďte význam protokolů AH a ESP pro zabezpečení komunikace na L3.
    * IPSec je architektura, která slouží k zajištění šifrovaní, autentizace a integrity dat na sítové vrstvě
    * Využívá 2 protokoly – AH a ESP.
    * AH – integrita a autentizace
    * ESP – šifrování podle zvoleného modu (tunel – enkryptuje celý paket/Transport – pouze data, hlavička zůstává)
    * Musí obě strany znát své veřejné klíče
12. Vysvětlete rozdíly při použití transportního a tunelovacího režimu IPSec.
    * Viz výše,, tunel – celý paket je enkryptován, transport – pouze transportní vrstva + aplikační vrstva, IP hlavička zůstává (tunel je default)
13. Popište, jak funguje systém PGP a jaký typ zabezpečení poskytuje. Uveďte postup pro zabezpečení a ověření zprávy.
    * Zajišťuje šifrování, autentizaci, integritu a neodmítnutelnost. Používá se u emailu.
    * Využívá symetrický šifrovací algoritmus IDEA. RSA pro autentizaci, MD5 pro integritu.
    * Zabezpečení: PGP vygeneruje charakteristiku zprávy (hash) soukromým klíčem odesílatele.
    * Charakteristika se připojí k nezašifrované zprávě.
    * Zpráva je zkomprimována
    * PGP vygeneruje klíč pro symetrické šifrování
    * Zpráva + charakteristika jsou tímto klíčem zašifrovány.
    * Klíč pro symetrické šifrování je zašifrován veřejným klíčem příjemce a připojen ke zprávě. Výsledek je transformován do Base64 kvůli 7-bitovému formátu SMTP.
    * Ověření:
    * Je dešifrován klíč za pomoci soukromého klíče.
    * Klíč je využit k dešifrování zprávy a charakteristiky.
    * Zkontroluje se, jestli charakteristika odpovídá přijaté zprávě.
14. Ukažte, jak lze zabezpečit směrovací protokoly. Demonstrujte postup na příkladu protokolu OSPF.
    * Heslem a nebo kryptografickým hashem (MD5).
    * Hash je připojen k OSPF paketu (tvořen z paketu + předem domluveného sdíleného tajného klíče). Router si pak hash spočítá znovu a ověří, jestli sedí.
    * Předem domluvený klíč se musí předat bezpečnou cestou, př. Administrátor ručně nastaví na routeru.
15. Jaký vliv má autentizace a šifrování na soukromí uživatele síťových služeb?
    * Znemožňují utočníkům sledovat cizí komunikaci a brání jím vydávat se za někoho jiného.

# Systém DNS

1. Popište jmenný prostor DNS, jeho strukturu, způsob uložení dat a vyhledávání informací.
   * Je strukturován jako kořenový strom.
   * Uzly ve vzdálenosti 1 od kořenu jsou TLD (Top level domains – cz, com, org)
   * Doména je podstrom
   * Data jsou distribuována skrz mnoho DNS serverů. Jednotlivé domény se delegují na další organizace.
   * Domény se dělí na zóny. Stub – subdomény, které server obsahuje. Hint – kořenové servery.
   * Vyhledávání probíhá od kořenového serveru, který se případně dotazuje nižších serverů, které spravujíé jednotlivé domény.
2. Vysvětlete proces delegace správy domén v DNS. Jak najdeme správce konkrétní domény?
   * Jednotlivé organizace mají na starost konkrétní domény – je mnoho DNS serverů, každý spravuje svoji doménu (Doména může být spravována více servery). Je to distribuovaný systém. Správce lze najít skrz databází organizce IANA a nebo příkaz whois.
3. Co je doména prvního řádu (TLD), druhého řádu apod? Kdo je spravuje?
   * Uzly ve vzdálenosti 1 od kořene DNS stromu. Jsou to národní domény (cz, sk) a obecné domény (com, org). Spravují je národní organizace a nebo ICANN.
4. Vyjmenujte a popište základní typy serverů DNS.
   * Primární, sekundární, záložní (cache)
   * Primární – Obsahuje úplné záznamy o doménácch, které spravuje. Pro každou doménu pouze jeden
   * Sekundární – obsahují autoritativní kopie obsahu primárního serveru. (přenos zón)
   * Cache – Pouze přijímá dotazy, které předává dalším DNS serverům. Ukládá odpovědi do vyrovnávací paměti. Poskytuje neautoritativní odpovědi.
5. Uved’te, jak probíhá přidělování IP adres. Jak lze zjistit, kdo vlastní danou IP adresu?
   * Adresy přidělují regionální registrátoři (RIPE NCC). Na lokální úrovni pak adresu přidělí ISP. Který ji koupil od vyššího ISP (Lokálního registrátora)... Majitel lze zjistit skrz whois
6. Co jsou reverzní záznamy DNS a k čemu slouží? Uved’te příklad reverzního záznamu.
   * Jsou to záznamy typu PTR, které mapují domény na IP adresy (in-addr.arpa). Tyto IP jsou zapsány odzadu. Slouží k autorizaci, kdy se kontroluje, zda má IP záznam – jeslti nemá, může jít o podvrženou IP. Taktéž zajišťují vlastníci subdomén.
   * Mám ip 224.1.0.5. Reverzní záznam –
   * 5.0.1.224.in-addr.arpa.
7. Definujte pojem rezoluce DNS. Popište princip rezoluce. Kde začíná a jak probíhá?
   * Rezoluce znamená určení IP adresy, na kterou patří doména aneb proces vyhledání v DNS. Princip je buď rekurzivní a nebo iterativní.
   * Vyhledávání začne dotazem na cache server, případně pak na sekundární server (získány skrz DHCP a nebo nastaveny manuálně) pro autoritativní odpověď. Pokud ani ten neví, tak se jde od kořene stromu podle subdomén.
8. Porovnejte chování rekurzivního a iterativního DNS serveru při rezoluci.
   * Rekurzivní –
     + Zeptám se cache. Když neví, dotážu se na autoritativní odpověď.
     + Když sekundární server neví a nezná ani adresu nejbližšího serveru pro danou doménu, jde se od kořene stromu.
     + Dotaz směřuje k TLD doménám. Jestli neví, přeposílají dotaz k subdoménám podle toho, jaký TLD byla. (jestli cz, tak hledá adresy co mají .cz...)
     + Takhle se zanořuje, jakmile najde odpověď, vrátí ji.
   * Iterativní –
     + Zeptám se cache. Když neví, dotážu se na autoritativní odpověď
     + Když neví, vrátí nejlepší odpověď
9. Vysvětlete pojem kořenový server DNS. Uved’te, k čemu slouží a jak je lze vyhledat?
   * Kořenový server je ten, který vrací adresy autoritativních serverů pro TLD. Je jich více, jsou uloženy v zónovém souboru hint.
10. Popište proces směrování a adresování dotazů v DNS. Co udělá klient DNS, když chce najít konkrétní záznam v globálním jmenném prostoru DNS?
    * Směrování je většinou rekurzivního charakteru, kdy se resolver zeptá svého lokálního DNS serveru, jestli zná odpověď a pokud záznam nenajde, pokusí se začít od nejbližšího serveru pro tu doménu, když se mu to nepovede, začne od kořene. V takovém případě se ptá serverů ze zóony hint. Výsledek je uložen do cache paměti, stejně tak v případě, že server nevěděl, je uloženo, že ten daný server neví. Tyto výsledky jsou průběžně mazány/aktualizovány, aby nedošlo k tomu, že server se už adresu dozvěděl, ale lokální server stále myslí, že neví. Délka života záznamu je nastavena při konfiguraci DNS.
11. Vysvětlete pojem autoritativní odpověd’ DNS. Jak ji lze určit?
    * Autoritativní odpověď znamená, že je aktuální (poskytnutá sekundárním/primárním serverem, nikoliv z cache) a server, co ji poskytl, je za ni zodpovědný. Autoritativnost lze určit na základě bitu v DNS hlavičce. NS záznamy jsou autoritativní, SOA je primární.
12. Popište obecný formát záznamů DNS. Vyjmenujte základní typy záznamů a jejich použití. Zapište příklady záznamů.
    * Jméno TTL Třída Typ Adresa
    * Stud.fit.vutbr.cz 11400 IN CNAME eva.fit.vutbr.cz
    * Eva.fit.vutbr.cz 11400 IN A 147.229.176.14
    * Základní typy:
    * SOA – Primární DNS server (Refresh – jak často se aktualizují sekundární, Serial – číslo identifikující změnu, Retry – jak často při neúspěchu zkoušet aktualizovat zónu, Expire – platnost dat na sekundárním, Minimum – implicitní TTL)
    * NS – Autoritativní DNS servery
    * PTR – Reverzní záznam (mapování IP adres na doménu) (nslookup)
    * SRV – různé služby
    * A – IP adresa patřící doméně
    * AAAA – totéž al pro IPv6
    * CNAME – alias
    * NAPTR – převod čísla telefonu na SIP URI.
    * MX – mailové servery (různá priorita – čím nižší tím přednější)
13. Vysvětlete použití záznamů A, AAAA, SOA, MX, PTR, CNAME, SRV, NAPTR a NS.
    * Viz výše
14. Pro danou doménu vytvořte zónový soubor obsahující záznamy SOA, NS, A, MX, NS a CNAME.
    * @ IN SOA ns1.xlogin00.cz. admin.xlogin00.cz. ( #admin je email spravce
    * 20211102 # !!! yyyymmdd
    * 10h
    * 10m
    * 1w
    * 1h
    * )
    * @ IN NS ns1.xlogin00.cz.
    * @ IN MX 10 mailhost.example.com 45000
    * ns1 IN A 10.10.10.108 # !!! IP enp2s0
    * pcuc IN A 10.10.10.1
    * pc01 IN A 10.10.0.101 # !!! IP PC1
    * pc02 IN A 10.10.0.102 # !!! IP PC2
    * pc03 IN A 10.10.0.103 # !!! IP PC3
    * server IN CNAME ns1.xlogin00.cz.
15. Pro danou doménu vytvořte reverzní zónový soubor obsahují záznamy SOA, NS a PTR.
    * @ IN SOA ns1.xlogin00.cz. admin.xlogin00.cz. (
    * 20211102 # !!! yyyymmdd
    * 10h
    * 10m
    * 1w
    * 1h
    * )
    * @ IN NS ns1.xlogin00.cz.
    * 108 IN PTR ns1.xlogin00.cz.
    * 1 IN PTR pcuc.xlogin00.cz.
    * 101 IN PTR pc01.xlogin00.cz.
    * 102 IN PTR pc02.xlogin00.cz.
    * 103 IN PTR pc03.xlogin00.cz.
16. Jak lze ověřit věrohodnost informací v DNS?
    * Za pomoci rozšíření DNSSEC, které funguje na principu asymetrické kryptografie
    * RRSIG – záznam, který obsahuje podpis jiného záznamu. Ten vzniká zašifrováním hashe podepisovaného záznamu privátním klíčem ZSK.
    * DNSKEY – Záznam, který obsahuje veřejný klíč ZSK.
    * Za pomoci něj lze ověřit podpis záznamu. To se dělá tak, že se spočítá hash záznamu a porovná se s tím, co dostaneme po dešifrování podpisu veřejným klíčem.
    * Zóna běžně obsahuje 2 DNSKEY – ZSK a KSK.
    * DS – záznam obsahuje hash veřejného KSK. Tím se ověřuje podpis záznamu DNSKEy
    * KSK se kontroluje tak, že se udělá hash public KSK a porovná se s hashem v DS u nadřazené domény.
    * Privátní klíč KSK i ZSK se nachází v jedné zóně. Do vyšší zóny se dává hash public KSK.
    * Privátním KSK se podepíše hash DNSKEY a uloží se do RRSIG DNSKEY (ten se ověří za pomoci public KSK ve stejné źóně)
    * DS, ZSK a KSK – vznká chain of trust
17. Popište formát protokolu DNS. Uved’te příklad přenášených dat.
    * Header, question, answer, authority, additional
18. Analyzujte paket DNS. Určete identifikátor dotazu či odpovědi, typ a jednotlivé části.
19. Vysvětlete, co je přenos zón, jak a proč probíhá.
    * Proces aktualizace dat na sekundárních serverech z dat na primárním.
    * Dochází k němu po vypršení refresh intervalu, nebo po přidání záznamu do primárního serveru (cchová se, jako by vypršel refresh). Stahují se pouze aktualizace. IXFR AXFR
20. Popište základní typy útoků na službu DNS. Jak je možné se proti nim bránit?
    * Odposlech paketů – útočník sleduje komunikaci a v případě DNS dotazu poskytne nesprávnou odpověď, čímž může př. Přesměrovat komunikaci na jinou adresu.
    * Hádání paketu, predikce odpovědi – identifikační číslo má jen 16 bitů, existuje predikovatelný počet odpovědí, čímž může útočník poslat jinou odpověď dříév, než DNS server.
    * Znemožnění služby - DoS útok, kdy DNS nebude fungovat, protože zpracovává milion jiných.
    * Zřetězení jmen – útok na cache, kdy je změněna odpověď serveru. Lze se bránit pomocí DNSSEC a ověřování záznamů.
21. Vysvětlete, jak pracuje DNSSEC a proti čemu chrání.
    * Pracuje se ZSK, KSK a DS. Podepisuje záznamy. Chrání proti podvrhu záznamů. Více viz otázka 16.
22. Vyjmenujte záznamy DNS, které využívá DNSSEC. Uved’te jejich význam.
    * DNSKEY – KSK, ZSK
    * RRSIG – záznam obsahující podpis jiného záznamu
    * NSEC – odkaz na další záznam při dotazu na neexistující doménu.
    * DS – záznam pro ověření KSK, uložen v nadřazené doméně.
23. Vysvětlete pojmy zónový klíč (ZSK) a klíč pro podpis klíčů (KSK). Uved’te, jak se vytvářejí a kde jsou uloženy.
    * ZSK – slouží pro podpis záznamů
    * KSK – slouží pro ověření ZSK
    * Vytvářejí se jako klasický pár veřejný/soukromý klíč. Veřejný KSK je uložen v DNSKEY, stejně tak ZSK. Pravost ZSK se ověřuje pomocí KSK.
24. Definujte pojem řetězec důvěry (chain of trust). Jak vzniká a k čemu slouží?
    * Posloupnost navzájem se potvrzujících klíčů. Vzniká tím, že DS ověří KSK, KSK ověří ZSK.
25. Diskutujte problém soukromí uživatele u DNS. Jak mohou data DNS narušit soukromí uživatele?
    * Původně zamýšlené jako veřejná služba přenášející otevřené data – lze však zjistit, kdo navštěvuje jaké stránky. Lze zabepzečit pomocí TLS a nebo tunelováním nad HTTPS.
26. Popište fungování DNS over HTTPS (DoH). Jak se implementuje, jaké má výhody a rizika?
    * DNS server je předkonfigurován ve webovém prohlížeči. Výhoda je, že komunikace bude šifrovaná. Riziko je, že poskytovatel prohlížeče (google) stále vidí vše. ISP navíc stále má možnosti, jak stránku odhalit.
27. Porovnejte DoT (DNS over TLS) a DoH (DNS over HTTPS). Uved’te, proti čemu chrání DoT a jak probíhá rezoluce DNS při použití DoT.
    * DoT – TLS handshake, pak jako obvykle (?), DoH skrz někoho jiného.
    * Chrání proti sledování DNS dotazů.

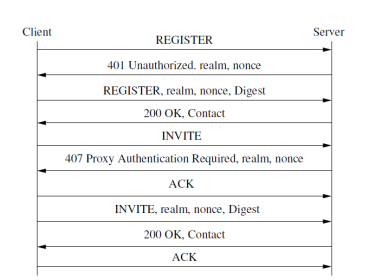
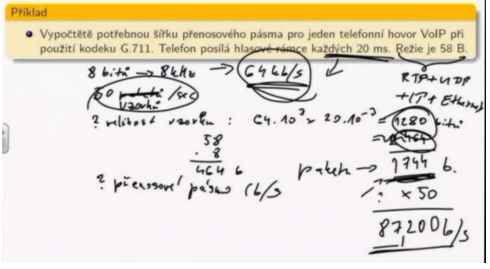
# Poštovní služby

1. Popište architekturu elektronické pošty. Vyjmenujte související služby a protokoly, které jsou nezbytné pro správné fungování elektronické pošty.
   * SMTP – Protokol pro přenos mailů. MUA – klient. MTA – server. Tyto 2 entity tvoří architekturu. Pro čtení se používá POP3/IMAP.
   * Pro vyhledávání uživatelů se využívá LDAP.
2. Popište formát zpráv elektronické pošty. Jak se tvoří obálka a tělo zprávy? Vyjmenujte základní hlavičky SMTP.
   * Před odesláním tvoří MTA „obálku“, která obsahuje adresáta a odesílatele.
   * Tělo zprávy je pak dle SMTP 7bitové a vícebitové znaky se tedy musí do 7bitů zakódovast (př. Skrz Base64) – rozšíření MIME. Strukturuje data tak, že obsahují i netextové přílohy. Tělo tvoří MUA. V hlavičce mailu je Datum, odesílatel, ID.
3. Popište funkci protokolů SMTP, POP3 a IMAP. Uved’te základní příkazy těchto služeb.
   * SMTP je přenosový protokol, který slouží k odesílání emailů. Funguje nad transportní vrstvou TCP. Jednoduchý textový protokol. Nepodporuje defaultně autentizaci uživatele – možno použít skrz rozšíření. Příkazy – MAIL FROM, RCPT TO
   * IMAP a POP3 slouží k jejich čtení na straně klienta.
   * POP3 – Aplikační protokol, funguje skrz TCP. Kopíruje data ze vzdáleného serveru a kopíruje je na lokální PC. Pouze 1 stránka na straně serveru – inbox. U klienta lze zprávy číst i offline díky tomu, že se přenesou a pak už jsou lokálně. Manipulace probíhá taky offline, k synchronizaci dojde až před ukončením komunikace. Pokud si poštu stáhne uživatel na jednom PC, z jiného už se k ní nedostane – hlavní nevýhoda. Po přenesení ze serveru se totiž zprávy mažou. Nezabezpečený (id, heslo) – nutno zabezpečovat dodatečně skrz tls.
   * IMAP – Aplikační protokol, funguje skrz TCP. Umí pracovat s více schránkami na vzdálených poštovních serverech. Umí pracovat i s jednotlivými částmi hlavičky, což redukuje náročnost přenosu – pouze když si chce uživatel přečíst tělo emailu, stáhne se i ono. Umožňují klienti práci i offline s pozdější synchronizací jako POP3. Ke zprávám umožňuje přidávat atributy (seen, answered, draft..), což usnadňuje práci.
4. Porovnejte protokoly pro čtení pošty POP3 a IMAP, uved’te jejich výhody a nevýhody.
   * IMAP obecně lepší, POP3 vhodný pro nestálé připojení, umožňuje práci offline, je víc lightweight, ale velmi omezený. Více viz předchozí otázka
5. Popište formát elektronické adresy. Ukažte, jak probíhá směrování elektronické pošty. Co udělá systém elektronické pošty, pokud adresát neexistuje?
   * Adresa se skládá ze 2 částí – uživatel@mailserver.
   * Směrování probíhá skrz SMTP servery, když lokální server neví, hledá skrz DNS MX záznam dané domény. Pokud server neexistuje, mail se neodešle a je oznámeno, že se nepoveldo najít server. Pokud je neznámý příjemce, mail se pošle na server a je na správci serveru, jestli informuje o neexistujícím uživateli.
6. Uved’te, jaké informace loguje poštovní server a co lze pomocí nich zjistit.
   * Datum odeslání, adresáta, odesílatele, informace o odeslání a přijetí, použitý protokol...
7. Vysvětlete pojem MIME. K čemu se využívá? Uved’te příklad konkrétního použití.
   * Jedná se o rozšíření SMTP, které se používá pro zasílání netextových částí či diakritiky etc k emailu. Každou část nějak zakóduje – netextová data často skrz base64 a osmibitová textová data skrz quoted-printable
8. Analyzujte hlavičku MIME. Vysvětlete základní položky v hlavičce a jejich význam.
   * Verze, Content-Type (typ obsahu – text..), Content-Disposition(inline/attachment), content-transfer-encoding (typ kódování – base64,quoted-printable..)
9. Vysvětlete princip kódování Quoted Printable a Base64 u elektronické pošty. Cím se liší? ˇ
   * Quoted printable – sedmibitové nepřevádí, pouze osmibitové – převede na 3 sedmibitové. Prvním znakem je =, následuje reprezentace osmibitového znaku v hexa podobě. Čau převede na =E8au. Jednodušší než base64.
   * Base64 – algoritmus, který zakóduje znaky do ASCII formátu. Převede 3 osmibitové znaky na 4 šestibitové.
10. Ukažte, jak lze zabezpečit přenos elektronické pošty.
    * SSL na SMTP a IMAP. HTTPS, PGP.
11. Popište způsob zabezpečení a ověření e-mailové zprávy pomocí PGP.
    * Popsáno už u popisu PGP.
    * Ze zprávy je spočítán hash, ten je zahashován soukromým klíčem odesílatele, hash a zpráva jsou zkomprimovány a zahashovány domluveným tajným kódem (symetrická kryptografie).
    * Kód je zahashován veřejným klíčem příjemce a společně se zprávou odeslán.
    * Ověření probíhá rozšífrováním pomocí soukromého klíče, za pomocci odhaleného klíče se pak rozšifruje zpráva a spočítá z ní hash. Jestli odpovídá tomu, který byl doručen (a odhashován veřejným klíčem odesílatele), integrita nebyla porušena.
12. Popište systém Sender Policy Framework (SPF), způsob jeho implementace a využití.
    * Umožňuje vlastníkovi domény deklarovat, odkud můžou chodit emaily, tzn. Omezit přístup pouze pro konkrétní IP adresy. Implementace v DNS TXT záznamu pro danou doménu. Slouží k zamezení spamu.
13. Jakým způsobem a proti čemu zabezpečuje elektronickou poštu systém DKIM (DomainKeys Identified Mail)? Uved’te příklad použití.
    * Podepisování zpráv klíčem. Chrání zprávy před podvržením. Může provádět kterýkoliv článek email infrastruktury, ne nutně uživatel. Specifikace v DNS TXT záznamu.
14. Vysvětlete pojem adresářová služba (directory service). K čemu se využívá?
    * Elektronická databáze pro vyhledávání uživatelů, původně navrženo jako podpora emailu. Globální distribuovaný systém s jednotným adresováním (Dnes lokálně). Používá se pro vyhledávání uživatelů, autentizaci a autorizaci (web, unix), ukládání údajů (active direčctory)

# 7 Adresářové služby

1. Popište způsob uložení dat služby LDAP. Jak probíhá adresování a vyhledávání dat?
   * Aplikační protokol nad TCP. Zjednodušení X.500
   * DIB a DIT – báze dat a definice umístění ve stromu.
   * Modeluje objekty, které mají atributy a vycchází ze tříd.
   * Základní jednotka uložení je záznam, který je tvořen atributy. Záznamy jsou uspořádány v DIT.
   * DN – jednoznačný identifikátor v DIT.
   * Informační model – typy dat, atributy
   * Naming model – Organizace dat
   * Funkccionální model – přístup k datům a vyhledávání
   * Security model – autorizace, nastavení přístupu.
2. Definujte pojem adresářové schéma. Ukažte, k čemu slouží a co obsahuje. Zapište příklad adresářového schématu.
   * Množina pravidel určující, co bude uloženo v adresářové službě a jak se s těmito poloožkami má zacházet. Před vložením nového záznamu je zkontrolováno, zda odpovídá schématu.
3. Popište formát záznamu LDAP. Vyjmenujte základní atributy LDAP. Napište příklad záznamu pro třídu objektů student FIT.
   * Je popsán třídou objektů. Obsahuje seznam atributů. Má jendoznačný identifikátor DN.
   * Základní atributy: o, ou, uid, cn, sn, dc
   * Dn: uid=xfiala61, ou=FIT BIT, dc=FIT, dc=vutbr, dc=cz
   * objectClass=Person
   * cn=Vojtech Fiala
   * sn=Fiala
4. Popište komunikaci protokolem LDAP. Jaké příkazy se používají pro vyhledávání dat v adresáři LDAP?
   * Komunikace klient-server. Klient tvoří dotaz, server odpovídá jednou či více zprávami. Používá se příkaz search.
   * Komunikace probíhá napojením na server, posláním hledané položky a vrácením výsledků.
5. Jaké operace používá protokol LDAP pro modifikaci dat?
   * Příkaz modify pro změnu konkrétního záznamu a modifyDN pro změnu nejlevější kompoennty v DN.
6. Ukažte, jak lze lokalizovat (najít) LDAP server pro danou doménu (organizaci).
   * Přes SRV záznam v DNS. Zjistím skutečné jméno aliasu a pomoci DNS získám adresu.
7. Jakým způsobem se kódují data přenášená protokolem LDAP?
   * Skrz standard BER – Typ/Délka/Hodnota.
8. Ukažte, jak lze omezit přístup k informacím v systému LDAP.
   * Nastavit data jako pouze pro čtení. Nastavit autentizaci heslem či klíčem.
9. Popište způsob propojení lokálních adresářů LDAP do globálního adresáře.
   * Záznam v LDAP typu alias – odkazuje na jiný záznam.
   * Odkazy typu referal – specciální LDAP url.
10. Ukažte, jak se využívá služba LDAP pro vyhledávání adresáta elektronické pošty.
    * Vyhledává se hodnota atributu mail u hledané osoby.
11. Popište využití služby LDAP pro přístup na webový server.
    * Webový server ověří obdrržené údaje za pomoci LDAP serveru, kdy do příkazu bind s autentizací zadá jméno a heslo. Pokud se povede přihlásit, web server se odpojí a považuje uživatele za autorizovaného, jinak chyba.
12. Vysvětlete mechanismu IEEE 802.1x, jeho význam a použití protokolů Radius a LDAP.
    * Klientovi je zaslána výzva k přihlášení. Přijatá data jsou přeposlána na Radius, který ale neobsahuje jména a hesla, pouze autorizační informace. Tento server zašle data na LDAP a ověří je tam stejným principem jako u otázky výše.

# 8 Hlasové služby

1. Popište architekturu klasické telefonní sítě. Vysvětlete funkci jednotlivých prvků. Jaké typy signalizace PSTN používá?
   * Architektura se skládá z koncových zařízení (digitální/analogové telefony), lokální smyčky (tvoří rozhraní do sítě), ústředny (basically switch – centrální a nebo privátní) a páteřních spojů (propojují ústředny)
   * Signalizace:
     + Kontrolní (zavěšeno, vyzvánění, sluchátko zvednuto)
     + Adresová (tónová volba, pulzní volba)
     + Informační (Oznamovací tón, obsazovací tón,neznámé číslo, tón neprůcchodnosti)
2. Porovnejte architekturu a vlastnosti PSTN a IP telefonie.
   * PSTN
     + Dedikované kabely
     + Circuit switching
     + Garantovaná šířka pásma
     + Spolehlivost, bezchybnost (dedikované spoje)
     + Adresování pomocí tel. Čísel
   * IP Telefonie
     + Přenos po internetu
     + Packet swwitching
     + Nemá dedikované kabely
     + Kvalita přenosu může být nižší, podle zátěže linky
     + Adresování pomocí SIP URI
3. Popište architekturu sítě VoIP. Vysvětlete funkci základních stavebních prvků VoIP.
   * IP Telefon – koncové zařízení
   * Ústředna (gatekeeper)
     + Síťové zařízení, které zabezpečuje přístup do telefonní sítě
     + Registruje a vyhledává uživatele
     + Zajišťuje směrování
   * Brána (gateway)
     + Síťový prvek, který zajišťuje spojení více telefonních sítí
     + Př. Spojení s PTSM
   * MCU
     + Umožňuje vytváření vícebodové komunikace
     + Řídí komunikaci vícero zařízení a bran
   * Aplikační servery
     + Další služby
     + Přidělování adres, hlasová pošta...
4. Jaké parametry musí splňovat IP telefonie z pohledu uživatele?
   * Dostatečné přenosové pásmo
   * Dostatečná kvalita hlasu
   * Spolehlivost a dostupnost srovnatelná s klasickou telefonní sítí
   * Bezpečnost
   * Integrace s veřejnou tel. Sítí a mobilními sítěmi.
5. Uved’te základní sít’ové služby, kterou jsou nezbytné pro správné fungování IP telefonie.
   * SIP, RTP, DNS, IM, LDAP, WWW, DHCP
6. Popište, jak vypadá adresování a směrování u IP telefonie pomocí protokolu SIP.
   * SIP je signalizační protokol pro VoIP, nad UDP.
   * Adresovaní
     + SIP URI
     + <Sip:user@domain>
   * Směrování
     + V SIP hlavičce uloženy: Via, Route, Record-Route
     + Směrování provádí SIP servery po cestě paketu (využívají DNS)
7. Vysvětlete, k čemu slouží registrace telefonu u VoIP. U kterého serveru se daný VoIP telefon registruje?
   * Přidání uživatele do seznamu dostupných uživatelů, ať se na něj skrz SIP server mohou napojit ostatní.
8. Popište jednotlivé kroky při navazování a ustavení spojení VoIP pomocí SIP.
   * Registrace
     + Metoda REGISTER na SIP server
     + SIP server si k user uri uloží device uri, které obsahuje IP zařízení uživatele
     + Pomocí lokální databáze potom umí hovory směrovat
   * Vytvoření spojení
     + Volající pošle volanému zprávu INVITE
     + Volaný odpoví OK (pokud chce)
     + Volající potvrdí přijetí a začne komunikaci
     + INVITE může vyžadovat autorizaci
9. K čemu slouží identifikátory User URI a Device URI? Zapište příklad těchto identifikátorů.
   * Device URI slouží k uložení IP adresy, ze které se uživatel registroval, pro směrování hoovorů.
   * User URI obsahuje uživatelské jméno uživatele, je spojené s device URI toho uživatele.
10. Ukažte, jak probíhá lokalizace (nalezení místa) volaného účastníka u VoIP.
    * V rámci fáze ustanovéní hovoru skrz SIP protokol dotazem na lokalizační server. Pokud v lok. Tabulce uživatele nenajde, skrz DNS zjišťuje, kterému serveru uživatel patří.
11. Popište protokol SIP a jeho základní metody. Zakreslete výměnu dat protokolem SIP (a) při registraci a (b) při volání.
    * Session Initiation Protocol – základní signalizační protokol pro VoIP.
    * Aplikační protokol nad UDP
    * Zabezpečuje registraci uživatelů, navazování spojení a směrování hovorů
    * Tvořen z SIP klientů a SIP serverů
    * Metody
      + REGISTER – registrace na server
      + INVITE, ACK, CANCEL – tvoření spojení
      + BYE – ukončení spojení
      + OPTIONS – možnosti přenosu
    * Výměna při registraci:
      + REGISTER na server, server potvrdí
    * Volání:
      + INVITE na klienta, klient potvrdí OK, ukončí BYE
    * 
12. Analyzujte hlavičku paketu SIP. Určete metodu, User a Device URI volajícího a volaného, použitý software a další důležité parametry.
13. Vysvětlete, k čemu slouží protokoly RTP a SDP, na jaké vrstvě modelu TCP/IP pracují a jaká data přenáší. Uved’te příklad informací obsažených v paketech RTP a SDP.
    * RTP slouží k přenosu dat během hovoru. Pracuje nad UDP.
      + Obsahuje typ obsahu, sekvenční číslo, timestamp
      + Nezaručuje kvalitu přenosu
      + RTCP – řídící protokol pro RTP, posílaný každýcch pár sekund, informuje o stavu
    * SDP slouží k výběru možností spojení – použitého protokolu etc.
      + Slouží pro vyjednávání parametrů, sám nic nepřenáší
      + Používá se v SIP Invite a OK
    * Oba pracují na aplikační vrstvě
14. Popište způsob, jak se komunikující strany u VoIP domlouvají na parametrech spojení (porty, kodek).
    * Za pomoci SDP při navazování spojení.
15. Popište vytváření spojení VoIP u telefonování bez registrace? Jaké má omezení?
    * Lze volat přímo na konkrétní IP adresy. Omezení je to, že když neznám IP, nezavolám si.
16. Jaké jsou požadavky VoIP na velikost a kvalitu přenosového pásma? Jak je lze zajistit?
    * 4kHz -> 8kHz – vzorek každých 125 us.
    * Nároky na pásmo závisí na použitém standardu, které určují velikost každého vzorku. To je ještě zvýšené o režii. Může to být př. 12 RTP, 8 UDP, 20IP (B).
17. Srovnejte klasickou IP telefonii pomocí SIP s komerčními systémy VoIP typu Skype, WhatsApp apod.
    * SIP je otevřený, známý protokol, funguje decentralizovaně.
    * Skype/Whatsapp..
      + Proprietární protokoly, častá změna koncepce
      + Služba není garantovaná
      + Proprietární správa účtů
18. Vyjmenujte a popište jednotlivé fáze převodu hlasu na pakety. Kde se implementují?
    * Mikrofon – zaznamenání zvuku
    * Vzorkování analogového signálu na digitální (Pulzní amplitudová modulace)
    * Kvantifikace vzorků – Rozděluje vzorky do segmentu tříd diskrétních hodnot
    * Kódování na binární čísla za pomoci kodeku (PCM, ADPCM..)
    * Komprese (není nutná)
    * Převod analogu na digitál je za pomooci A/D převodníku s DSP procesorem.
19. Definujte pojem kodek. Uved’te, jak souvisí typ kodeku s požadavkem na přenosové pásmo. Vyjmenujte nejběžnější audio a video kodeky pro IP telefonii.
    * Způsob kódování informací do binárního formátu. Podle kodeku se určuje šířka pásma – každý kóduje jinak. Nejběžnější: G.711 (PCM)
20. Pro daný kodek a zapouzdření vypočítejte potřebnou šířku přenosového pásma VoIP.
    * 
21. Vyjmenujte bezpečnostní rizika VoIP. Ukažte, jak je lze eliminovat.
    * Odposlech, DoS útoky, výpadky napájení, neautorizované použití služby
    * Způsoby zabezpečení:
    * Řízení přžístupu skrz 802.1X
    * IPSEC, secure RTP
    * Záložní zdroje

# 9 Streamování a videokonference

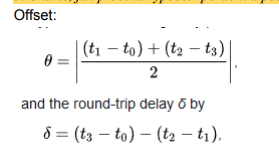
1. Vysvětlete pojem streamování multimediálních dat. Jaká média se využívají při streamování?
   * Jednosměrný přenos multimedálního obsahu, ze zdroje ke koncovým stanicím. Po síti v reálném čase. RTP, HLS (HTTP Live Streaming)...
2. Popište průběh živého přenosu (live streaming), jeho vlastnosti a způsob implementace.
   * Všem klientům jsou ve stejný okamžíik zasílána stejná multimediální data, která si klienti přehrávají. Přehrávání nelze řídit. Implementuje se skrz RTP, RTSP.
3. Vysvětlete pojem streaming na vyžádání (video on demand). Popište, jak vypadá komunikace, kdo ji řídí a jaké protokoly se používají.
   * Jedná se o zasílání klientovi předem vytvořeného multimediálního obsahu. Přehrávání lze řídit (zastavit, spustit..)
4. Porovnejte živý přenos multimédií (live streaming), přenos na vyžádání (video on demand) a přehrávání souboru (download). Cím se tyto přenosy liší a jaké protokoly využívají? ˇ
   * Přenos na vyžádání
     + Lze řídit
     + Je zasílán předem vytvořený obsah
     + HLS
   * Live streaming
     + Přehrávání nelze řídit
     + Všem klientům je zasílán ve stejný okamžik tentýž obsah
     + RTP
   * Přehrávání souboru
     + Probíhá lokálně.
     + Soubor je nejprve celý stažen, u ostatních se přehrává postupně
     + HTTP
5. Jaké příčiny snižují kvalitu přenosu multimediálního přenosu? Ukažte, jak je lze eliminovat.
   * Pomalé připojení, zahlcení linky, nekomprimovaný obsah
   * Je nutno mít výkonný server, cco dokáže v dostatečné kvalitě odesílat všem data. Tato data je nutno skrz kodek kombinovat, jinak by velikost videa byla nepoužitelná
   * Řešení je použití Cache – kus videa se stáhne do cache, začne se přehrávat, postupně se do cache stahují další části
6. Kde a proč dochází ke kompresi multimediálních dat?
   * Před odesláním dat (videa a audia) po síti. Bez komprimace by byly soubory velmi velké, na což síť není připravena.
7. Vysvětlete pojem MPEG Transport Stream (MPEG TS). Popište jeho formát a využití pro přenos TV programů.
   * Standard popisující, jak jsou data kombinována do datového toku – multiplexing. Umožňuje v jendom datovém toku i více streamů.
   * Skládá se z paketů pevné velikosti.
8. Popište postup vytváření datového toku MPEG TS z jednotlivých vstupů. Jak se identifikují jednotlivé kanály a podle čeho je přijímající stanice určí?
   * Identifikují se podle PID.
9. Vysvětlete význam tabulek PAT (Program Association Table) a PMT (Program Map Table) u přenosu MPEG TS.
   * PAT obsahuje všechny programy dostupné v přenosu.
   * PMT obsahuje data o jednotlivých programech.
10. Popište protokol RTP, jeho formát a použití. Jak probíhá synchronizace streamů u RTP?
    * Určen pro unicast i multicast. Standard pro přenos dat v reálném čase.
    * Podporuje detekci ztráty dat a pořadí doručených paketů.
    * Nezaručuje kvalitu.
    * Synchronizace: Podle timestampu.
11. Které služby využívají RTP? Jaký obsah může protokol RTP přenášet a podle čeho se identifikujte?
    * Live=streaming, VoIP. Může přenášet obraz a zvuk.
    * Identifikuje se podle payload type flagu v hlavičce.
12. Jak lze zajistit kvalitu multimediálních přenosů u protokolu RTP?
    * Použitím cache.
13. Popište protokol RTSP a jeho využití. Uved’te základní operace RTSP. Zakreslete průběh komunikace. Jaké služby využívají RTSP?
    * Signalizační protokol, který slouží k navázání a ukončení spojení k řízení streamů. Textový protokol, syntax podobná HTTP.
    * Operace:
    * DESCRIBE, SETUP, PLAY, PAUSE, TEARDOWN, OPTION
    * Využívá ho RTP.
14. Analyzujte RTSP stream uložený v IS FIT mezi příklady ISA. Ukažte, jak si komunikující strany vymění potřebné informace ohledně portů a kodeků pro přenos multimediálních streamů.
15. Vysvětlete, čím se liší videokonference od streamování. Porovnejte oba systému z pohledu funkce, použitých přenosových protokolů i požadavků na přenos.
    * Videokonference není jednosměrná, ale všichni si v reálném čase navzájem posílají data.
    * Protokoly: Standard MPEG, RTP + RTCP.
16. Popište architekturu systému pro přenos multimédií H.323. Vyjmenujte základní prvky systému, popište jejich funkci.
    * Terminal – koncové zařízení zajišťující realtime komunikaci s jiným terminale,
    * Gateway – koncové zařízení umoňující komunikaci mezi terminály
    * MCU – přijímá a dekóduje výstupní streamy, přeposílá streamy.
17. Uved’te, z čeho se skládá videokonferenční terminál dle standardu H.323. Popište funkci jednotlivých prvků.
    * Videokamera, zobrazovací ploccha, mikrofon, reproduktory, kodek, UI.
18. Vysvětlete, k čemu slouží MCU (multipoint control unit). U kterých přenosů je jednotka MCU nezbytná?
    * Umožňuje pořádat vícebodové videokonference, přijímá a přeposílá streamy. Přijímá a dekóduje výstupní streamy, vytváří příslušný výstupní stream pro koncové uzly.
    * Nezbytná u CP (zobrazení 2+ učástníku konference současně)
    * VAS – obraz zasílán v závislosti na hlasitosti příchozího audia na MCU

# 10 Prostředky pro správu sítí

1. Vysvětlete, co je cílem správy sítě a jaké úkoly musí zajistit. Jaké prostředky k tomu využívá?
   * Cílem je zajistit správné fungování sítě
   * Úkoly:
     + Monitorování zařízení v síti, uživatelů, správa nastavení a systému
     + Autorizace přístupu k zařízením
     + Sledování zátěže, řešení výpadků a chyb
     + Bezpečnostní monitorování, detekce útoků
     + Zálohování a obnova zdrojů na síti
   * Prostředky:
     + Pasivní sběr monitorovacích dat (SNMP, netflow, syslog)
     + Aktivní sběr (ICMP, SNMP)
2. Vyjmenujte a popište oblasti správy sítě definovaného podle standardu FCAPS. Pro každou oblast uved’te možný způsob implementace.
   * FCAPS – fault, configuration, accounting, performance, security
   * Fault
     + Detekování poruch
     + Izolování porucch – ať neovlivní celou síť
     + Rekonfigurace sítě – bez narušení běhu funkční části sítě
     + Oprava nefunkčních zařízení
   * Configuration
     + Sledování síťových zařízení, přidělování identifikátorů síťovým rozhraním
     + Změny sw konfigurace síťových zařízení
   * Accounting
     + Správa uživatelských účtů a poplatků za služby
     + Řízení přístupu uživatelů k síti
     + Definování kvót, alokace prostředků...
   * Performance
     + Monitorování sítě – sběr dat
     + Řízení sítě – zlepšování výkoonnosti na základě nasbíraných dat
       - Dostupnost, Odezva, Propustnost, využití –
       - Př, skrz SNMP
   * Security
     + Řízení přístupu k síťovým zdrojům na základě policy
     + Distribuce klíčů, certifikátů, firewall..
     + Reagování na podezřelé události
3. Vyjmenujte zdroje monitorovacích dat pro správu sítě a uved’te způsob jejich získávání.
   * SNMP – Statistiky o počtu paketů co prošli určitým rozhraním, informace o uptime, vytížení CPU...
   * Netflow – detailní statistiky o tocích
   * Syslog – logy o událostech – př. Chybné přihlášení skrz ssh
4. Jaké znáte typy zpráv ICMPv4. Ukažte jejich použití. Diskutujte bezpečnostní rizika ICMP.
   * ECHO, ECHO REPLY, Destination unreacchable, time exceeded
   * ECHO – ping, test dostupnosti zařízení
   * ECHO REPLY – odpověď na ping,, která může být př. Dest. Unreachable, time exceeded.
   * Bezpečnostní rizika – Prohledávání sítě pomocí icmp echo
5. Vysvětlete význam zprávy ICMPv6 pro správné fungování sítě. Vyjmenujte základní typy a jejich použití.
   * Slouží k přihlašování do multicast skupin
   * Slouží k přidělení IP adresy (namísto dhcp)
   * Nahrazuje RARP a ARP (IND a NDP respektive)
   * Router soliccitation (zjištění adresy směrovačů)
   * Typy: ECHO, ECHO REPLY, Packet too big, destination unreachable, time exceeded, MLD, ND, IND.
6. Popište architekturu systému SNMP. Vysvětlete činnost jednotlivých prvků a způsob implementace.
   * Agent na monitorovaném zařízení
     + Aktivní proces, který běží na monitorovaném zařízení a sbírá provozní informace (statistiky o přenosech, konfiguraci..)
     + Oodpovídá na požadavky řídíccí stanice, zasílá vyžádané objekty obsahující monitorované informace
     + Může posílat asynchronní zprávu trap
     + Objekty které spravuje lze nastavit read-only, write-only...
   * Databáze objektů MIB (Management information base)
     + Soubor všech objektů na monitorovaném zařízení
     + Objekt je datová struktura reprezentující sledované informace
   * Řídící stanice NMS (network management system)
     + Serverová aplikace, kterou tvoří nástroje pro sběr a analýzu dat
     + Může nastavit stav objektů podle požadavků správce sítě
   * Přenosový protokol SNMP
     + Slouží k předávání zpráv o sledovaných objektech mezi agentem a řídíccí stanící
       - Get (získej objekt), set (nastav objekt), trap (informuj o události)
7. Definujte pojem objekt MIB. Popište jeho formát, způsob adresace a uložení. Uved’te příklad alespoň tří typů objektů MIB včetně konkrétní hodnoty, kterou může objekt obsahovat.
   * Objekt je datová struktura, která reprezentuje sledované informace na cílovém zařízení.
   * Má jméno (OID), syntax (integer, object identifier..), kódování (reprezentace při přenosu po síti)
   * Ukládají se do MIB.
   * Příklad:
   * ipInDelivers OBJECT-TYPE
   * SYNTAX Counter32
   * MAX-ACCESS READ-ONLY
   * STATUS CURRENT
   * DESCRIPTION „a number“
8. Vysvětlete pojem databáze MIB. Vyjmenujte základní skupiny objektů podle standardu MIB-2. Pro každou skupinu uved’te příklady objektů.
   * MIB je stromová struktura obsahující monitorované objekty na zařízení. Listy = objekty, uzly = skupiny objektů
   * Základní skupiny –
     + Data popisující směrovací tabulky (at (ARP))
     + Data popisující přenos základních protokolů (TCP, IP, UDP, ICMP)
     + Informace o OS (System)
9. Vyjmenujte základní datové typy objektů MIB, které definuje jazyk ASN.1 a SMI. Uved’te příklady objektů, které využívají dané datové typy.
   * INTEGER, OCTET STRING, OBJECT IDENTIFIER, Ipaddress, Counter64, Counter32..
   * Counter – počítadlo paketů
   * Objec identifier – identifikátor objektů
10. Vysvětlete význam zápisu monitorovacích dat pomocí jazyka ASN.1.
    * Zapsána data jsou nezávislá na OS či programovacím jazyku
11. Popište princip kódování BER. Jaké sít’ové služby využívají kódování BER?
    * Hodnoty SNMP objektů se pro přenos v síti zapisují do binárního formátu za pomocí kódování BER.
    * Přenášená data reprezentuje v oktetech
    * Formát TLV – Type Length Value, což umoˇžnuje i identifikaci typu a možnost pro cílovou stanici si vyhradit potřebné množství místa
12. Popište komunikaci SNMP. Vyjmenujte základní příkazy SNMP, popište jejich funkci.
    * Komunikace slouží k předáváaní informaci o stavu objektů mezi řídící stanicí a zařízením. Využívá se příkazů get, set, trap
13. Popište formát protokolu SNMP. Jak se zabezpečuje přenos u SNMP verze 2 a 3?
    * Aplikační protokol nad UDP. Typ dotaz-odpověď
    * Zabezpečuje se heslem (2) a zajíštěním autentizace a integrity skrz MD5 a SHA (3)
14. Diskutujte výhody i omezení praktického nasazení monitorování SNMP.
    * Je nutné vzít v potaz, kolik zařízení chceme sledovat, jak často o nich chceme data sbírat a jak velká tato data budou. Může výrazně zatěžovat síť.
15. Uved’te příklady pasivního a aktivního monitorování sítě.
    * Pasivní – sběr statistik skrz asynchronní SNMP, Netflow, syslog
    * Aktivní – dotazování na stav zařízení skrz ICMP, telnet, SNMP
16. Porovnejte systémy SNMP a NetFlow z pohledu monitorovacích informací, které získávají. Jaké informace o síti je možné získat pomocí SNMP a nelze je získat pomocí NetFlow?
    * SNMP:
      + Získává statistiky rozhraní – počet přenesených bytů, konkrétní počet paketů na rozhraní..
      + Dokáže zjistit stav HW, vytížení systému etc
      + Oproti SNMP umožňuje získat informace o stavu zařízení, vytížení zařízení...
    * NetFlow
      + Sleduje toky
      + Poskytuje mnohem detailnější statistiky
      + Počet přenesených bytů pro jednotlivé IP, porty...
17. Jaké informace o síti lze získat pomocí NetFlow a nelze získat pomocí SNMP?
    * Konkrétní informace o typu dat, která protékají sítí
18. Porovnejte architekturu systémů SNMP a NetFlow.
    * SNMP – agent, MIB, NMS, přenosový SNMP.
    * NetFlow –
      + Exportér (Sonda, Router) – buď to může být router nebo dedikované zařízení (export je náročný) pro sběr dat
      + Komunikační protokol NetFlow – slouží k přenosu dat z exportéru na kolektor
      + Kolektor – ukládání záznamů o tocích pro dlouhodobější zpracování
      + Nástroje pro zobrazování grafů, statistik...
19. Porovnejte systémy SNMP a syslog z hlediska monitorování. Jaké informace lze získat pomocí syslogu a nelze získat pomocí SNMP?
    * Syslog slouží k monitorování událostí systému, obsahuje závažnost události, monitoruje události i na aplikační vrstvě (snmp ne)
    * SNMP slouží k monitorování více zařízení v síti – syslog je pouze lokální
20. Porovnejte architekturu systémů SNMP a Syslog.
    * SNMP - Agent, MIB, NMS, přenos SNMP
    * Syslog – Klient, Server
21. Jaké znáte konkrétní nástroje pro monitorování sítě pomocí SNMP? Uved’te příklad.
    * Snmpget, snmpset .. príkazy balíku net-snmp
22. Pomocí služby snmpwalk získejte ze serveru isa.fit.vutbr.cz hodnoty objektů MIB ze skupiny interface a system. U získaných objektů zjistěte název, OID, typ a hodnotu.
23. Pomocí analýzy paketů ve Wiresharku zjistěte standardní velikost SNMP paketu + velikost režie (hlaviček L2-L4). Kolik bytů je potřeba na přenos jednoho dotazu a odpovědi na objekty skupiny interface? Uvažujte, že každý dotaz je poslán samostatným příkazem Get. Kolik přenosového pásma vyžaduje pravidelné dotazování na 20 zařízení v síti na danou skupinu objektů, pokud frekvence posílání příkazů je 5 minut?

# 11 Logování systému a služeb

1. Vysvětlete, k čemu je důležitá synchronizace času v síti. Ukažte, jaké důsledky mohou mít chyby v nastavení času na sít’ových zařízeních.
   * Důležitá pro dohledávání informací v síti (logy)
   * Provoz sítě (čas událostí)
   * Chyby: Nelze jendoduše dohledat chybu či událost – report neobsahuje správný čas.
2. Popište princip synchronizace času pomocí protokolu NTP. Jak probíhá komunikace klienta a serveru? Které typy časových razítek se používají? Zakreslete komunikaci NTP klienta a serveru pomocí časového diagramu.
   * Zařízení si od NTP serveru vyžádá čas, ten je mu zaslán, sleduje se i doba cesty paketu.
   * NTP využívá hierarchii serverů – Stratum 0 (atomové hodiny)
   * Stratum 1 – Synchronizace podle S0
   * S N-1 - synchronizace podle předchozího serveru
   * Komunikace – Klient získá čas od více serverů, když má nějaký moc velkou odchylku od ostatních, nepočítá s ním. Následně je zvolen server, který je použit k synchronizaci.
   * Časové razítka:
   * Originate timestamp, receive timestamp – časy poslání požadavku klienta a přijetí odpovědi serveru
   * Transmit – Destination – čas, kdy server dostal dotaz a klient odpověď
3. Ukažte, jak probíhá výpočtu zpoždění a posunu času při synchronizaci času NTP.



1. Jak lze zabezpečit službu NTP? Co se stane, když útočník podvrhne pakety NTP?
   * Útočník může poskytnout špatný čas, což lze zneužít k expiraci certifikátů etc.
   * Lze zabezpečit používnáím novějších verzí NTP – podporuje autentizaci (podpis)
2. Popište architekturu služby syslog. Jaké funkce vykonává klient (console) a server?
   * Syslog má klient, server a daemony.
   * Klient – zobrazuje logy
   * Server – přijímá a ukládá události
   * Daemon – posílá na server události v plain textu (UDP)
3. Popište komunikační protokol syslog. Jaké úrovně důležitosti zpráv znáte?
   * Facility – kód ze 2+ písmen, identifikuje, odkud zpráva přišla
   * Severity – závažnost
   * Mnemonic – unikátní identifikátor zprávy (nemusí být vždy)
   * Message text – zpráva samotná
   * Důležitosti:
     + 0 – emergency, most serious
     + 1 – alert
     + 2 – critical
     + 3 – error
     + 4 - warning
     + 5 – notice
     + 6 – informational
     + 7 – debugging, least serious
4. Co může být zdrojem logovacích zpráv? Jaké události se logují na sít’ových zařízeních?
   * SSH – neúspěšné přihlášení
   * Web Server – požadované stránky, přístup..
   * DHCP – přidělená adresa
5. Pro následující sít’ové služby uved’te příklady logovaných událostí: poštovní server, webový server, server DHCP, Radius, DNS. Diskutujte využití těchto dat pro správu sítě.
   * Mail SMTP logy, přístup do schránky..
   * Web: Odeslané stránky, přístup..
   * DHCP – Přidělené IP adresy
   * Radius – čas přihlášení...
   * DNS – požadavky na DNS
   * Lze tvořit statistiky, určit co se jak moc používá a tomu přizpůsobit síť...
6. Vysvětlete funkci služby TFTP a příklad použití.
   * Slouží k přenosu logů, používá se př. Pro zobrazení obsahu logu, nahrání konfigurace, zálohy.. na místní síti
   * Jednoduchý protokol k přenosu souborů, umí doslova jen to.
7. Které informace o síti lze získat pomocí logování a nelze získat pomocí SNMP či NetFlow?
   * Události z aplikační vrstvy
   * (SSH failed, výpadek služby..)
8. Jakým způsobem je možné zabezpečit službu syslog?
   * Šifrováním přenosu skrz TLS

# 12 Monitorování toků NetFlow

1. Definujte pojmy tok (IP flow) a záznam o toku (flow record). Vyjmenujte klíčové a statistické položky záznamu. Uved’te příklad konkrétního toku.
   * Posloupnost paketů mající nějakou společnou vlastnost a procházející bodem pozorování za určitý časový interval
   * Záznam o toku obsahuje informace o toku
     + Zdrojovou, cílovou IP
     + Protokol
     + Datum a čas zaznaménaní
     + Počet přenesených dat
2. Popište základní architekturu systému NetFlow. Vysvětlete funkci jednotlivých prvků systému.
   * Exportér (Sonda – samostatné zařízení, Router) – slouží ke sběru dat, ta jsou přeposílána na kolektor.
   * Kolektor – slouží k dlouhodobějšímu uložení a zpracování dat.
   * Protokol NetFlow – slouží k přenosu dat z exportéru na kolektor
   * Nástroje pro tvorbu grafů, statistik
3. Popište funkci sondy NetFlow. Vysvětlete, jak sonda vytváří záznamy o tocích.
   * Sonda je samostatné zařízení, které slouží ke sběru dat, jelikož je to náročný proces a router samotný v některých případech nestačí. Záznamy o tocích vytváří tak, že jednotlivé pakety analyzuje a na základě nějaké jejich společné vlastnosti je přiřadí jako součást toku.
   * U TCP ke konci toku slouží signalizace FIN
   * Tok se také může ukončit na základě podnětů –
     + Inactive timer expired – tok již není aktivní
     + Netflow cache full – cache je plná a je potřeba dát nějaké info pryč
     + Active timer expired – Tok je sice aktivní, ale běží již dlouhou dobu
4. Co je vzorkování a jak se využívá v systému NetFlow? Diskutujte výhody a nevýhody vzorkování u NetFlow.
   * Exportér nezaznamenává každý paket, ale pouze každý n-tý z toku. Výrazně snižuje nároky na HW za cenu toho, že o některá data přijdeme (pro obecné statistiky však dostačující)
5. Vysvětlete význam a princip agregace u systému NetFlow. Na příkladu záznamů NetFlow vypočtěte agregované záznamy. Uved’te výhody a nevýhody agregace.
   * Vytváření statistik podle klíčovýcch položek. Výhody: Menší nároky na HW, možnost se zaměřit pouze na konkrétní informace
   * Nevýhoda: Jiná data se ztráci
6. Na jaké vrstvě TCP/IP probíhá komunikace NetFlow a jak vypadá zapouzdření paketů?
   * Probíhá na aplikační vrstvě, využívá UDP. Vytvoří se hlavička s počtem záznamů, timestampem a identifikací sondy. Dále se přidá obsah paketu
7. Ukažte, jaká data jednotlivých vrstev TCP/IP lze monitorovat pomocí NetFlow? Uved’te příklad monitorovaných dat.
   * Z transportní – konkrétní porty
   * Z síťové – jednotlivé IP adresy
8. Popište, jak sonda NetFlow identifikuje jednotlivé toky a detekuje jejich ukončení. Vysvětlete funkci aktivního a neaktivního časovače.
   * Typicky generuje hash podle čtveřice (source:port, dest:port) a jestli se hashe shodují, jsou součástí toku, ke kterému se připočte +1 paket a přenesené byty. Jinak se vytvoří nový tok. Ukončení se detekuje u TCP př. Skrz příznak FIN.
   * Aktivní – Příliš dlouhý tok – když tok běží moc dlouho, po nastaveném čase se sám ukončí, aby nepřibývali př záznamy, cco přenesli 1tb dat etc
   * Neaktivní – Z toku nepřišel po nastavenou dobu žádný paket, ukončí se
9. Jaký vliv má nastavení aktivního a neaktivního časovače na monitorování toků NetFlow? Co se stane, když daný časovač snížíme či zvýšíme?
   * Slouží k omezení velikosti záznamu o toku. Zvýšením se zvýší velikost jednotlivých záznamů.
10. Popište formát protokolu NetFlow. Jaké informace o tocích paket obsahuje?
    * Hlavička – počet záznamů, timestamp, identifikace sondy
    * Obsah paketu
11. Vyjmenujte hlavní rozdíly mezi protokolem NetFlow verze 5, 9 a IPFIX.
    * 5 má pevnou hlavičku, 9 využívá šablony (pouze část hlavičky je fixní), IPFIX – postavený na netflow 9 – už není od cisca
12. Vysvětlete, k čemu slouží šablony u NetFlow.
    * Slouží k definici jednotlivých položek hlavičky
    * Podle ní se pak určují položky hlavičky
    * Kolektor musí nejprve zpracovat šablonu, jinak by paket neuměl zpracovat
13. Popište činnost kolektoru. Ukažte, jak lze pomocí nástroje nfdump vyhledat pět nejvíce komunikujících uzlů v síti, pět nejvíce využívaných služeb v zadaném časovém intervalu apod.
    * Kolektor slouží k ukládání a zpracovávání informací, které obdrží od exportéru. Nad těmito daty poté může provádět dootazy.
    * nfdump -R /home/user/isa5/netflow -c 5 -o extended -s dstport (podle počtu toků k danému protokolu)..
14. Diskutujte, jak lze pomocí záznamů NetFlow detekovat bezpečnostní incidenty typu skenování sítě, šíření malware, útok DoS, zasílání spamů apod.
    * Lze detekovat data přicházející z konkrétní IP – př. U icmp jsme schopni určit adresáta a když někdo skenuje všechny různé porty, tak to poznáme. Malware – poznáme, že se nějaký konkrétní program sám šíří, DoS – paketů přicchází mnoho a cílí na konkrétní službu...
15. Jaká omezení má monitorování toků NetFlow na síti s protokolem IPv6? Navrhněte způsob, jak rozšířit záznamy NetFlow tak, aby jednoznačně identifikovaly zařízení v síti IPv6.
16. Navrhněte způsob, jak využít záznamy NetFlow pro účtování zákazníků ISP na základě přenesených dat.
    * Lze měřit počet přenesených bytů na všech portech
17. Uved’te, které informace o síti lze získat pouze pomocí NetFlow a nelze získat pomocí SNMP.
    * Souhrnné statistiky, záznamy o tocích, kdo odkud kam kolik a čeho (ip adresa, port, použitá služba..)
18. Porovnejte architekturu NetFlow a SNMP.
    * SNMP – Agent, MIB, NMS, SNMP
    * netFlow – Exportér, kolektor, NetFlow, grafové nástroje, nástroje na zobrazení dat (nfdump)

# 13 Zajištění kvality služeb

1. Definujte pojem SLA (Service Level Agreement) a uved’te, k čemu slouží a co obsahuje.
   * Je to smlouva, kterou podepíše zákazník a ISP při zřizování služeb. Slouží k vymezení, co ISP poskytuje zákazníkovi a jaké jsou limitace.
   * Obsahuje požadavky na fyzické připojení
   * Požadavky na síťový přenos
2. Jaké znáte prostředky pro zajištění kvality přenosu v počítačových sítích?
   * Označení paketů - každý paket je označen podle hlavičky
   * Konkrétní typy můžou mít prioritu (videokonference..) (prioritní fronty..)
3. Vysvětlete způsob řízení přenosu dat metodou ořezání a omezení provozu. Uved’te výhody a nevýhody obou přístupů. Jak je možné tyto metody implementovat?
   * Ořezání – Je omezena maximální rychlost – výhodou je, že data jsou omezena a přicházejí konstantní rychlostí, nevýhodou je, se některá data zahodí a musí se odesílat znovu, aby se vešly do rozložení
   * Omezení (rozložení) – Regulace rychlosti a objemu – Efektivnější než ořezání, náročnější na paměť. Nadbytečné pakety se uloží do bufferu a zpracují později – zpracování trvá déle, ale o nic nepřijdu.
   * Implementace – pakety se u shapingu uloží, u policingu zahodí
4. Vyjmenujte typy front, které se používají pro řízení kvality přenosu v počítačových sítích. Popište, jejich základní vlastnosti a způsob obsluhy vstupních dat.
   * FIFO, Round Robin, Prioritní fronta, WFQ – chytřejší prioritní fronta
   * FIFO –
     + First In First Out – nijak nereguluje, neřeší prioritu, výchozí nastavení
     + Pro zajištění kvality nepoužitelné
     + Garantované maximální zpoždění
   * PQ (priority queue)
     + Pakety jsou klasifikátorem rozděleny do N front podle priority
     + Obsluha nejdříve vyšších priorit
     + Riziko vyhladovění (nikdy se na ně nedostane)
   * RR
     + Fronty s cyklickou obsluhou
     + Řeší vyhladovění
     + Každý tok paketů tvoří nezávislou frontu na zpracování
     + Stejný počet paketů cyklicky odebrán z každé fronty a zpracován
     + Pokud je prázdná, pokračuje se obsluhou nejbližší neprázdné
     + Rychlost závisí na celkovém počtu front a rychlosti výstupu
   * WFQ
     + Pro každý tok se vytvoří nová fronta – dynamický vznik a zánik
     + Váha určuje, koolik se má v každém cyklu odebrat
     + Prioritní round robin
5. Vysvětlete, jak lze řídit rychlost provozu pomocí modelu tekoucího vědra (leaky bucket). Jak bude omezen provoz, pokud bude velikost vstupní fronty nulová?
   * Princip, kdy se napouští voda, ale vědro je děravé
   * Data se zpracovávají konstantní rychlostí, data navíc co přetečou se neřeší
   * FIFO s počítadlem bytů X
   * X se inkrementuje každou sekundu o X += X + r (rychlost, jakou chci)
     + Pakety o délce P se odešlou, když P < X, pak X = X – P
     + Pokud P > X, čeká se, dokud se X nezvětší
     + Pokud P\_New + P > SIZE\_OF\_BUCKET, P\_NEW je zahozen
     + Po odeslání paketů se čítač X resetuje (nemá paměť)
6. Jak lze implementovat model tekoucího vědra v síti?
   * jako FIFO s počítadlem bytů
7. Popište model zásobníku žetonů (token bucket). Vyjmenujte parametry, které slouží pro nastavení modelu a jejich význam. Ukažte, jak lze model implementovat.
   * Model zpracování dat (obvykle u integrovaných služeb)
   * Generování žetonů, když je dost žetonů, pošle se paket
   * Krátkodobě může rychlost překonat požadovanou průměrnou, velikost shluku je však omezena velikostí vědra
   * Na výstupu se mohou objevit shluky dat
   * Obsahuje paměť pro uložení nevyužitých paketů (odešlou se, až se objeví žeton)
   * Model definuje:
   * Průměrnou rychlost CIR – generování tokenů za čas T
   * Rychlost ve špičce PIR – CBS/T + CIR
   * Maximální velikost shluku CBS – velikost bucketu
8. Vypočtěte maximální rychlost výstupu u zásobníku žetonů při parametrech CBS, CIR a T.
   * CBS/T + CIR
9. Vysvětlete princip integrovaných služeb (IntServ). Popište jejich výhody a omezení. Ukažte, jak lze metodu IntServ implementovat.
   * Poskytují společnou službu množiě provozních požadavků
   * Úkolem je zajistit QoS v IP síti formou rezervace síťových zdrojů
   * Výhody: garance kvality přenosu
   * Nevýhody: výpočetně náročné, cesta je dynamická – musí se měnit
   * Implementace ve směrovači
     + HW část:
       - Prochází zde všechny pakety
       - Probíhá klasifikace toků do tříd podle hlavičky
       - Třída může odpovídat 1 a více toků
     + Plánovač paketů:
       - Obsluhuje fronty pro každý výstupní port
       - Určuje pořadí vybírání či zda se zahodí
     + SW část
       - Zajišťuje rezervaci zdrojů, správu zdrojů
10. Popište průběh rezervace přenosového pásma u integrovaných služeb. Co se stane, pokud nelze danému požadavku vyhovět?
    * RSVP
    * Před přenosem dat se za jeho pomoci rezervují prostředky na jednotlivých zařízeních po cestě
    * Žádost o rezervaci provádí koncová stanice
    * Když nelze vyhovět, je poslána zpět chybová zpráva
11. Popište architekturu diferenciovaných služeb (DiffServ). Ukažte, jak se implementují a jaké mají třídy kvality přenosu.
    * Klasifikují pakety (ne toky) do tříd podle hlavičky
    * Podle hodnoty IP precedence lze prioritizovat
    * Třídy provozu
    * EF (expedity forwarding – nejvyšší priorita), AF (assured forwarding – nastavení priority), BE (Best erffort – základní chování)
12. Porovnejte model diferenciovaných a integrovaných služeb. Ukažte jejich výhody a použití.
    * Integrované rezervují přenosové pásmo a garantují kvalitu pro daný tok
    * Diferencované přiřazují pakety do tříd a značí prioritu
13. Popište mechanismus RED a způsob implementace. K čemu RED slouží? Jak se určí pravděpodobnost zahození paketu?
    * Slouží k zahazování paketů ve frontách, prevence zahlcení
    * Čím víc je linka zaplněná, tím větší šance, že paket zahodí
    * Zahazuje bez ohledu na prioritu
    * Tři stavy zahazování:
    * Qavg < Qmin – nezahazuj
    * Qmin <= Qavg <= Qmax - nahodne vyber a zahod
    * Qavg = Qmax – zahazuj vše
    * Qavg – aktuální vytížení, Qmin – minimální pro zahazování, Qmax – kdy už zahazuju vše (velikost fronty)
14. Vysvětlete, jak se změní chování sítě při použití mechanismu RED, pokud upravíme hodnoty Qmin a Qmax u vstupní fronty?
    * Qmin – pakety se začnou zahazovat dřív, když je fronta naplněná méně
    * Qmax – Když je větší než Qmin, zmenší se pravděpodobnsot zahození
15. Vysvětlete problém globální synchronizace TCP a vyhladovění TCP. Jak lze tyto problémy eliminovat?
    * Globální synchronizace:
      + Každá fronta je konečná a je ji možné někdy zahltit. Když dojde k zaplnění, tak se začnou zahazovat všechny nově příchozí pakety. Pokud tyto pakety patří k toku TCP, tak mechanismus řízení toku TCP zmenší přenosové okno a sníží rychlost toku. To způsobí výrazný pokles nároků na přenosové pásmo i na uvolnění front. Až se průchodnost linky zlepší, TCP zase zvyšuje rychlost, dokud se zase nezahltí fronta. A pak přijde zase snížení rychlosti - cyklus. Je to tzv. problém globální synchronizace TCP.
      + Zhazováním paketů lze vyřešit částečně tak, že se rychlost toku bude preventivně držet nižší díky zahazování paketů i když linka je stále z části volná
    * Vyhladovění:
      + Při zahlcení může dojít k problému, pokud o přenosové pásmo soupeří TCP a UDP. Pokud sníží svou rychlost kvůli zahlcení TCP, tak UDP nemá žádný mechanismus řízení rychlosti a pokud přes zařízení prochází agresivní tok UDP, tak snížení TCP využije a obsadí další přenosovou kapacitu linky. To donutí ostatní toky TCP ještě k většímu snížení rychlosti až je vytěsní, tomu se říká vyhladovění TCP.
      + Řešení: Zahlcení je možné předcházet metodou náhodného zahazování paketů, což implementují metody RED a WRED (Použití algoritmu RED a WRED řeší problém globální synchronizace TCP a vyhladovění TCP, protože zahazování je přímo úměrné dravosti toku. Agresivní toky budou zahazovány s větší pravděpodobností. V konečném důsledku přináší tyto algoritmy efektivnější využití přenosového pásma)
16. Popište mechanismus WRED. Cím se liší od RED a jak ho lze implementovat? ˇ
    * Zahazuje s prioritami. Pravděpodobnosti zahození jednotlivých paketů jsou ovlivňovány precedencí. Weighted RED.
17. Pro dané parametry CIR a CBS vytvořte model zásobníku žetonů. Pokud přijdou pakety o dané velikost v určitý čas, jak se zpracují? Které budou zahozeny a které projdou na výstup?
18. Demonstrujte zpracování přicházejícího provozu při použití modelu tekoucího vědra.
19. Mějme rychlost výstupní linky R. S jakou rychlostí budou obsluhovány pakety ve frontě typu FIFO, při použití prioritních, cyklických a váhových front? Cím bude dáno maximální ˇ zpoždění paketu při zpracování?

- FIFO

 - cyklické