1. Otázka
   * Jednoznačně identifikuje síťové rozhraní v počítačové síti, lépe pochopitelné pro uživatele, využívá IP (internet protokol) verze 4, funguje na 4. vrstvě OSI modelu, je 32bitova dělí se na čtyři oktety oddělené tečkou, (0-255)
   * Historicky se dělil na skupiny A (0-127), B (128-191), C(192-223), D (multicast 224-239), a E (wasted 240-254), adresa se zkládá z network part, host part, subnetmask, globálně je spravuje IANA, své rozsahy rozděluje jednotlivým organizacím na světadílech, došly
   * Krom identifikace nám poskytuje polohu a možnost se k němu dostat, existují i jiné protokoly ale krom 4 a 6 se žádný jiný tak moc neuchytil, dnes rozdělujeme ip adresy podle jednotlivých bytů
   * Privátní: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, Loopback: 172.0.0.0/8, Multicast 224-239(255), link-local: 169.254.0.0/16 (no ip adres assigned not routable), první adresa v síti je adresa sítě a poslední je broadcast sítě
   * Packet header 20-60 bajtů celkový packet může být velký až 2^16 bajtů. Unicast, Multicast, Broadcast
     1. Obsah obrázku text, snímek obrazovky, číslo, Písmo

        Popis byl vytvořen automaticky
     2. Version (4,4-bit), IHL(size of ip header) Total length(16-bit, header and data), Identificaation(16-bit)Flag(3-bit)Fragment Offset(13-bit) … pro fragmentaci paketů, time to live(8-bit, decreased on router), Header checksum(16-bi, router check the checksum), source destination(32-bit), options(0-40)
   * Ipv6, větší adres space, vylepšená security(poskytnuto šifrování a autentifikace), jednodužší header, používa : místo ., header je přesně 40bajtů, hůř zapomatovatelné, můžou se sami nastavovat bez dhcp, frgmentace probíhe jen u odesílatele
2. Otázka
   * Jednoznačně identifikuje síťové rozhraní v počítačové síti, využívá IP (internet protokol) verze 6, funguje na 4. vrstvě OSI modelu, byla vyvynuta Internet Engineering Task Force (IETF), kvůli nedostatkům ipv4, kterýma se v té době plýtvalo a které už došli, 128-bitová dělí se na osm skupin (hexadecimální soustava) rozdělena dvojtečkou
   * Dvě hlavní adresy linklocal (fe80::), global unicast address (routerprefix:eui-64), GUA je routovatelná ven ze sítě a LLA se používá jen na dané LAN, jednodužší nastavení (SLAC musí posílat DAD[Duplicate Address Detection] packet) adresa se dělí na routing prefix(64,10),subnet(LLA 54) interface id(64)
   * LLA: fe80::/64, loopback: ::1/128 (1), Multicast: ff00::/8 (2120)
   * Unicast, anycast (on of many), multicast, packet má přesně 40bajtů, velikost packet je znovu 2^16bajtů pokud má packet Jumbo option(in Hop-By-Hop Options extension head) header tak až 4GB
   * Obsah obrázku text, snímek obrazovky, číslo, Písmo

     Popis byl vytvořen automaticky
   * Version (4-bits,6), Flow label (20bits, patří do nějakého streamu), Payload length (16bits, length of payload and extension headers), Next header(8bits, dodatečné headery), Hop Limit (8bits, TTL in ipv4), source destination (128-bits)
   * Payload obsahuje kromě dat I extension headers
   * Ipv6, větší adres space, vylepšená security(poskytnuto šifrování a autentifikace), jednodužší header, používa : místo ., header je přesně 40bajtů, hůř zapomatovatelné, můžou se sami nastavovat bez dhcp, frgmentace probíhe jen u odesílatele
3. Otazka
   * LAN, MAN, WAN, komunikační protokoly které používáme na komunikaci zařízení v síti, a 4. Vrstvě TCP a UDP, na 7. Vrstvě HTTP, SMTP, FTP, protokoly umožňují přenos dat mezi počítači (některé zajišťují spolehlivost, bezpečnost apod.)
   * Switch … zařízení tvořící LAN funguje na druhé vrstvě OSI modelu, slouží k propojenní několika počítačů, umožňuje jim komunikovat mezi sebou, je chytřejší než hub, může vytvořit vice podsítí … VLAN
   * Router … funguje na třetí vrstvě OSI modelu, slouží k propojení sítě a routování do interentu, často se mu říká default gateway, novější routry poskytují funkci NATu či firewall.
   * MAC(fyzická adresa) adresa je 48bitová rozdělená dvojtečkou na šest skupin po dvou hexadecimálních čísel, je pevně zapsaná na každém počítači u novějších ji lze změnit, výrobce zažádá o první polovinu druhou by měl sám doložit, pokud je kolize v LAN síti většinou je vyřešena virtuální změnou(u moderních počítačů)
   * Ip adresa … adresa ipv4 (32bit) nbeo ipv6 (128bit) operující na třetí vrstvě Osi modelu, používá se pro identifikaci počítače v internetu, dnes se používá výce ipv4 adresa ale plítvalo se s nimi a tak došly (řešíme pomocí NAT)
   * ARP … address resolution protocol … slouží k získání MAC adresy když známe ip adresu nejedná se o ip packet a ip datagram (ip packet je jen typ ip datagramu), arp request je poslán jako linkový broadcast (všechny počítače na LAN síti jsi zapíší počítač do své ARP cach) vlastník ip adresy posílá ARP reply.
   * Routing je určování cest datagramů v prostředí počítačových sítí. O routing se stará směřovač
4. Otazka
   * ISO/OSI (IEEE Institute of Electrical and Electronics Engineers) (Aplication / Presentation / Session / Transport / Network / Data Link / Physical) TCP/IP (Aplicaition / transport / network / network interface) (ARPANET),(6 … kódování, komprese, formát dat, 5 … vytvoří session mezi zařízeními)
   * PDU (protocol data unit) … aplikační vrstva (data), transportní vrstva (datagra … UDP, segment … TCP), network (packet), lnk (frame), phyzical (bits)
   * Zapoudření (vždy plus hedaer na dane vrstve)… aplikační vrstva (data), transport (source destination port), network (source destination ip), link (source destination MAC + patička)
   * Nespojová služba … datagram je odeslán nezávisle na ostatních, neexistuje, mezi nimi žádná přímá vazba, používá se pro přenos krátkých rychlých správ (DNS,DHCP) hlasu či videa, příkladam takového protokolu je UDP (User datagram protocol)
   * Spojovaná služba … vyžaduje aby bylo mezi dvěmi zařízeními nejprve vytvořeno spojení (three way handshake), pak jsou data odesílána jako posloupnost bloků s přidanou infromací, která je umožňuje správně seřadit, například TCP (transmission control protocol) http, pop3, imap, smtp
     1. Tcp (spolehlivost, zachování pořadí, vyšší režie)
     2. UDP (bez záruky, nezachovává pořadí, jednoduchý)
5. Otazka
   * Na začátku se využíval token ring a koaxiální cabel (jedno jádro), S příchodem etherentu a kroucené dvojlinky se od předchozí topologie upouští. Následně se přesunul a na bus topology a pak na star topology. Ethernet se komunikuje pomocí MAC address spadá do první a druhé vrstvy OSI modelu. Sourně ethernet nazýváme kabelovou technologií pro počítačové sítě běžně používané na LAN, MAN, WAN.
   * 10BaseT … rychlost, (base band … digitální signál), t….twistedpair/f…fiber optic, 1G (gigabit), Ethernet … 802.3, Fast Ethernet 802.3u, Gigabit Etherent 802.3z, 10 Gigabit ethernet 802.3ae
   * Koaxiální kabel (10Mbps) … jádro (signál) … vnitřní vodič, obal (stínění) vnější vodič, mezi nima (dielektrikum) nevodivá vrstva, nejčastěji je v něm veden stejnosměrný signal
     1. Kabelová televise, napáječ vysílacích a příjmacích antén (radio amatéři)
   * Twisted pair … tvořen dvojcemi kabelů které jsou do sebe zamotané aby zabráníli crosstalku … díky tomu se signal indukovaný vyzařovaný z kabelu z velké části vyruší, vedeme signal 1,2,3,6 a telefon 4,5 u gigabit ethernetu výše je veden signal přez všech osm, delíme je do CAT kategorií 1-8 kde se postupně vice portčí, stíní se jako celek fólií (trochu v 6 ale od cat 7 výš) tím se I zvětšáje přenosová vzdálenost a přenso dat (cat8 25GBps, cat7 10GBps, cat6 1Gpx), (S/F/U)/ (S/F/U)TP … U .. unshielded, S … shelded(opletení), F … foilded (folie), prvni (celý svazek), druhý (jednotlivé páry), používají se konektroy Rj-45, (telfoni menší RJ11), jsou dvě verze poskládání barev A a B (používá se více), můžeme zapojit jako cors over nebo jako straight true(vice používané)
   * Optické vlákno … skleněné nebo plastické vlákno přenáší prostřednictvím světla signal (je výsledek aplikace vědeckých poznatků) využívá infra-red červené světlo pro přenos dokáže přnášet 10 až 40GBps ovšem není tak robusní jako twisted pair a velmi jednoduše v něm může docházet k útlumu, mají mnohem menší ztráty na vyšší vzdálenosti
6. Otazka
   * Statické … směrování nejsou za běhu stanice záznamy ve směrovací tabulce nijak aktivně měněny.Může je zapsat zprávce nebo mohou být v konfiguračním souboru poskztnutý DHCP, využívá se na malých LAN není potřeba menít
     1. Obsah obrázku text, účtenka, Písmo, snímek obrazovky

        Popis byl vytvořen automaticky
   * Dinamické (adaptační) reaguje na změny v počítačové síti a přizpůsobuje se jim obsah směrovací tabulky
     1. RIP (Routing information Protocol) … využívá Bellmanův-Frodův algoritmus pro určení nekratší cesty v síti. Aby packet nekoloval do nekonečna je mu nastaven limit 15 hopů (ten ovšem omezuje velikost sítě), routry si navzájem posílají směrovacý tabulky nejprve co 30 sekund naraz pak se to muselo nádně rozházet
     2. Obsah obrázku text, diagram, snímek obrazovky, Paralelní

        Popis byl vytvořen automaticky
     3. OSPF(Open Shortest Path First) … je hierarchický interní směrovací protokol, fungující na bázi link-state, tzn. každý směrovač zná strukturu celé sítě(přesněji oblasti … OSPF doména). Činnost OSPF je rozdělena do tří částí – správa sousedských relací, šíření směrovacích informací a určování nejkratších (optimálních) cest.
     4. Obsah obrázku text, snímek obrazovky

        Popis byl vytvořen automaticky
7. Otazka
   * Spanning tree protocol (IEEE 802.1D) … protocol který odstraňuje smičky v ethernetových LAN mezi switchi … redundatní spoje odpojí (předchází zahlcení sítě) … Broadcast storm (při poslání unicast frameu bude switch do nekonečna přepisovat MAC ardres table protože nevý jaký port poslal unicast frame)
   * 1. Elect the root bridge … všechny switche začnou poté jak nabootují posílat svě v teřiny BPDU frame každý se prohlásí za root bridge, postupně začnou swtche posílat BPDU toho kdo má nižší údaje než oni a v jednu chvíli se shodnou na root bridge
     1. BPDU (Bridge protocol data unit) … používá se při výběru root bridge, root port, designated portu a alternated portu, obsahuje: bridge priority (4bits) … nejmenší vítězí volby (ovšem všichni mají defaultně nastaveno na 32768 z rozsahu 0 – 61440 přidává se po 4096), pokud je nerozhodno hledí se na Extended system ID (12 bits) které identifikuje VLAN, pokud jsou I tyto čísla stejná pak přicházi v potaz MAC adressa (48 bits) znovu kdo má nejnižší ten vyhrává
     2. Bridge priority to exact value … (config)#spanning-tree vlan 1 priority 8192
     3. Bridge priority to 28673 … (config)#spanning-tree vlan 1 root secondary
     4. Bridge priority to 24577 … (config)#spanning-tree vlan 1 root primary
     5. Pro zobrazení prority … show spanning-tree
   * 2. Elect the root ports … jak je odhlsován root bridge tak STA algoritmus je použit pro vybrání root porů, každý switch vybírá jeden port který je nejblýže ke switch a označího jako root port
     1. Path cost … STA algoritmus vybere tu cestu která má nejnižší internal path cost … ta je vypočtena součtem všech cen vstupních portů během cesty k root bridgy (hodnota portů je přenastavitelná) gigabit je lepší než fast etherent … má menší cenu
   * 3. Elect designated ports … každý segment mezi dvěmi switchy musí mít právě jeden designated port, jsou v nejlepší cestě příjmou traffic od root bridge (sám root bridge má všechny porty designated), pokud je na jednom konci root port na druhém musí být designated, pokud neni mezi dvěma switchi ani jeden root port můžou se rozhodnou podle internal root path k root bridgy pokud je I tak stejná pošlou si navzájem BPDU a kdo vyhraje má designated port, pokud I to nerozhodne můžou se porovnat port ID
   * 4. Elected blocked port … pokud port není root ani designated stane se blocked a bude zablokovaný
   * Časy … helo timer (2 sekundy), forward delay timer … (listening learning state … 15 sekund), Max Age Timer (čas než se znovu spustí a zkontroluje topologie … 20 sekund)
   * RSTP (Rapid stp) 802.1w … jedná se o rychlejší verzi používá stejný algoritmus , zvyšuje rychlost rekalkulace pokud se topologie změní,
     1. Obsah obrázku text, snímek obrazovky, číslo, diagram

        Popis byl vytvořen automaticky
     2. Obsah obrázku text, snímek obrazovky, Písmo, číslo

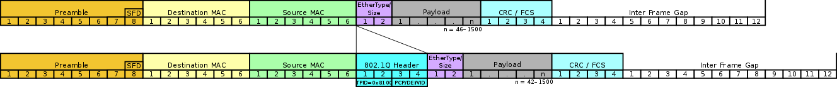
        Popis byl vytvořen automaticky
     3. Obsah obrázku text, snímek obrazovky, diagram, řada/pruh

        Popis byl vytvořen automaticky
8. Otazka
   * Je výraz pro logickou síť, zefektivní využití switche tím že v něm udělá logické podsítě na jednotlivých portech, defaultní vlan je vlan 1, všechny porty jsou defaultně na vlaně 1(Native clan, Management vlan, nemůže být přejmenována nebo smazána), Data vlan je vlan přímo pro user generated content, management vlan je nastavena výhradně pro network management traffic (SSH, TELNET), Native VLAN specifický druh valny kterým cestují framy které nejsou otagované
   * Konfigurace
     1. Obsah obrázku text, Písmo, snímek obrazovky

        Popis byl vytvořen automaticky
     2. Obsah obrázku text, snímek obrazovky, Písmo

        Popis byl vytvořen automaticky
   * Dynamic tranking … dovoluje zrychlit konfigurační process pro správce sítě port může být nastaven jako
     1. Trunking (trunk), nontrunking (access), negotiate trunking s příbuzným zařízenám
     2. Obsah obrázku text, snímek obrazovky, Písmo, algebra

        Popis byl vytvořen automaticky
     3. switchport mode { access | dynamic { auto | desirable } | trunk }
     4. Obsah obrázku text, snímek obrazovky, Písmo, číslo

        Popis byl vytvořen automaticky
   * VLAN (virtuál LAN) IEEE 802.1Q … přidává a definuje VLAN header do ethernet frameu … prvná dva oktety (TPID TAG protocol identifyer) … obsahují hodnotu 0x8100 a říkají že další dva oktety budeou nést informace o VLANě, druhé dva uktety se skládájí z PCP (Priority Code Point … 3bits) … obsahuje prioritu rámce do jaké fronty je potřeba zařadit, CFI (Canonical Format Indicator 1bit) … v jakém pořadí je rámec přenášen (kanonickým tvarem (little endian), který se používá v ethernetu, nebo nekanonickým (big endian), který se používá v Token Ringu) 0 … kanonicky, VID(VLAN identifier 12bits) … můžeme mít 4096 různých valn id … identifikuje číslo vlany
   * Smaller broadvast domain, improve security, better performance, reduce cast,
     1. 
   * VTP … je proprietární protocol cisca, který zajišťuje přenášení čísel a názvů VLAN mezi switchy do jedné domény což usnadňuje správu. Jeden přepínač je zvolen jako server ostatní budou typu klient všechny musí být ve stejné doméně na clentu nelze vytvářet VLAN nebo měnit ty stávající
     1. Summary advertisement … je posílán každých pět minut obsahuje doménu, číslo revise, čas poslední změny, pokud je správná doména a číslo revise větší než má on uložené posílá zpátky Advertisement request jinak ingoruje
     2. Advertisement request je posílán z kilenta na server, jako odpověď posílá server Subset advertisement
     3. Subset advertisement obsahuje název domény, číslo revise a informace o vlanech (číslo, aktivní/neaktivní, jméno, velikost)
     4. Nastav porty jako trunk s stejnou native vlanou
     5. Na server vtp mode server, vtp domain ahoj, vtp password ahoj
     6. Na clinetovy vtp mode client, vtp domain ahoj, vtp password ahoj
9. Otazka
   * VPN (Virtual private network) … jedná se o propojení vice počítačů prostřednictvým nedůvěryhodné sítě (interent), tak že mezi sebeou budou počítače komunikovat jako by byly an jedné privátní uzavřené síťi, protože při navazování spojení je totožnost obou stran ověřena pomocí certifikátu a celá komunikace mezi počítači je šifrovaná, prto takové spojení lze považovat za bezpečné.
   * Poskytuje … důvěrnost (pokud se někomu neoprávněnému dostane packet do ruky bude zašifrovaný), ověření odesílatele (zabraňuje neověřeným uživatlům přístup), integrita zpráv (detekce a zamítnutí instancí které se snaží manipulovat s přenášenými zprávami)
   * OpenVPN … populární opensource protocol, široce využívaný pro tovření tunelů, podporuje jak šifrování na vrstvě SSL/TLS tak ve vrstvě 2 (Ethernet frames), je schopen pracovat zkrze firewall a NAT
   * Šifrování skrije identitu, šifruje data
   * Remote access … propojení jednotlivce k datacentru pomocí šifrovvaného tunelu, Site-to-Site … propujuje dvě sítě, nebo skupiny kanceláří pomocí šifrovaného tunelu
   * Tunely … šifrované TCP spojení
   * WireGuard … modern rychlý VPN protocol, je navržen s důrazem na jednoduchost a efektivitu, je vysoce škálovatelný poskytuje vysokou rychlosta a je považovaný za bezpečný. Je psaný tak aby byl možný implementovat na jakékoliv platformě, je lehký aminimalizuje množství kódu … rychlejší a bezpečnější, asymetrická výměna symterické šifry
   * [TLS](#SSL_TLS)
10. Otázka
    * DHCPv4 (Dynamic host configuration) … přiřazuje ip adresu, subnet mask, default gateway, dns záznam. Jedná se o jednodužší konfiguraci administrátory sítě. Tuto funkci může častokrát zastoupit router, drží pů adres ze kterého na určitý časový úsek vypůjčí ip adresu pokud do vypršení se jeho vypůjčení neprodlouží bude adresa znovu nabízena jako dostupná
      1. DHCP Discover (DHCPDICOVER) … klient začne boardcastovat DHCPDISCOVER za použití (255.255.255.255) s valstní MAC adresu za účelem nalezení DHCP server
      2. DHCP offer (DHCPOFFER) … DHCP server rezervuje jednu z volných ip adres (server si vytvoří arp záznam s rezervovanou ip adresou), posílá zpátky DHCPOFFER které obsahuje MAC adresu clienta, rezervovanou ipv4 adresu, subnet mask, dobu vypůjčení a ip adresu DHCPv4 serveru
      3. DHCP Request (DHCPREQUEST) … využívá se jak pro obnovení tak pro přijmutí
         1. Přijmutí(založení) … oznamuje příjmutí informaci, tím odmítá nabýdky jakých koliv jiných server
         2. Prodloužení … předtím než dojde k vypršení si uživatel prodlouží leasing, pokud nedostane DHCPPACK po uběhnutí timeoutu začne klient broadcastovat DHCPoffer
      4. DHCP Ackknowledgment … 1. Server se pomocí ICMP pingu může ještě přesvědčit že ip adresu nikdo nepužívá, klient který příjme DHCPPACK si uloží konfigurační údaje a posílá ARP request (ujišťuje se že nikdo nemá jeho ip adresu), pokud nedostane odpověď začne ip adresu používat 2. Server potvrdí vypůjčení posláním DHCPACK message
    * Konfigurace
      1. Obsah obrázku text, snímek obrazovky, Písmo, design

         Popis byl vytvořen automaticky
      2. Obsah obrázku text, snímek obrazovky, Písmo

         Popis byl vytvořen automaticky
11. Otazka
    * IPv6 LLA adresa je automaticky počítačem vytvořena když se nabootuje, Ipv6 adresa GUA musí být přiřazena staticky (ručně) nebo dynamickyza použitím Stateless (SLAC, SLAC + DHCPv6) nebo stateful (DHCPv6) metodou. Jaký z těchto způsobů bude využit rozhoduje RA (Router advertisement message), RA se posílá co 200 vteřin, pokud počítač nedostane RA zažádá si o ní za pomocí RS (Router Solocitaion) … posílá na ff02:: all router multicast adres space
      1. RA flag … rozhoduje jaká z metod bude využita pro vytovření GUA adresy
         1. A fleg (A fleg==1) … využí SLAAC
         2. O flag (A flag==1,O fleg==1) … využí SLAC + stateless DHCPv6
         3. M flag (M flag == 1) … využí statefull DHCPv6
    * SLAAC (Stateless address auto configuration) … všechny potřebné informace počítač dostane z RA, prvních 64 bitů použije počítač stejné jako má router druhou polovinu si dovygeneruje za pomocí EUI-64 (sedmi bit invert, MAC doprostřed ff:fe) nebo randomu, následně posílá DAD(Duplicate adres detection) packet aby si ověřil že na síti nikdo danou ip adresu nema … jedná se o ICMPv6 Neighbour solicitation (NS) s speciálne zkonstruovanou multicast adresou (kopíruje 24 bitů adresy klienta) … pokud nikdo neodpoví pak je adresa unikátní (troreticky DAD neni potřeba ale je doporučeno ho využívat jak na všech typech konfigurace)
    * DHCPv6
      1. Klient posílá RS message všem routrům
      2. Router obdrží RS a odpovídá RA značící že bude potřeba zahájít komunikaci s DHCPv6 serverem
      3. Klient posílá DHCPv6 SOLICIT (aby našel dhcp) na rezervovanou adresu ff02::1:2 (posílá se na lokální síti protože má link local scope)
      4. Server odpovídá s ADVERTISE unicast message, infromuje klienta že je dostupný
         1. Stateless DHCPv6 client … vytvoří si adresu z RA a (EUI-64, random), pošle DHCPv6 INFORMATION-REQUEST message (žádajíc o dodatečné informace, DNS a podobně)
         2. Stateful DHCPv6 klient … pošle DHCPv6 REQUEST message za účelem obdržení všech potřebných IPv6 konfiguračních paramterů
      5. Server posílá DHCP REPLY klientovy, obsah zprávy záleží na tom jestli klient posílal DHCPv6 REQUEST nebo DHCPv6 INFORMATION-REQUEST message.
      6. DAD ICMPv6 NS
    * Konfigurace
      1. Obsah obrázku text, snímek obrazovky, Písmo

         Popis byl vytvořen automaticky
      2. Obsah obrázku text, snímek obrazovky, Písmo, číslo

         Popis byl vytvořen automaticky
      3. Obsah obrázku text, snímek obrazovky, Písmo, Paralelní

         Popis byl vytvořen automaticky
12. Otazka
    * DNS (Domain name system), decentralyzovaný hierarchycký systém doménových jmen, převod domén na ip adresu, umí toho teď ale mnohem víc (slouží dnes jako distribuovaná databáze síťových informací)
    * Záznamy A záznam (ipv4 adresu), AAAA záznam (ipv6 adresu), PTR záznam (ip na doménu), MX záznam (poštovní server), CNAM záznam (alias domény), CERT (certifikace public key) … nslookup -type=mx seznam.cz
      1. Autoritativní server … je ten, na němž jsou uloženy trvale záznamy k dané doméňě(zóně), většinou je jich více (primární sekundární), každá změna je potřeba propagovat na všechny autoritativní servery(provozován registrátorem domény nebo hostingu)
      2. Rekurentní server (cash only) … nejvíce překládané ip adresy má uložen v cachy pro rychlejší přístup jedná se například o servery u ISP, záznamy tam nejsou uložené trvale
      3. Root servery … kořenové servery předsatvujízásadní část infrastruktury internetu, tyto servery poskytujý kořenové zónový soubor ostatním DNS serverům, kořenové servry popisují kde se nachází autoritativní servery pro domény vyšších úrovní
    * Top level domain (doména prvního řádu), doména druhého řádu a tak dále, když dělám dotaz jdu postupně od nejvíce obeného k nejvíce konkrétnímu, nejprese ptám serveru který který mě odkáže na server který zná doménu prvního řádu, ten mě odkáže na další která zná doménu druhého řádu, a tak dále dokud nedostanu to co hledám
    * Reverzní dotaz ip adresa je opak dns musí se tedy otočit 192.168.60.1 bude vypadat jako 1.60.168.192.in-addr.arpa, pak můžeme se postupně dotazovat znovu a dostat se až k doméně která za ip adresou stojí
    * Historicky byl DNS neexistoval pouze se udržoval jeden centrální soubor hosts který jsi člověk musel stáhnout a použít v složce (/etc/hosts), ve chvíli kdy už to nebylo udržitelné musel se vymyslet lepší alternativa … DNS (decentralizovaný sistém), dnsmasq může houstovat /etc/hosts soubor pro počítači na síty aby mohl být využit jako DNS server ne jenom lokálně na počítači ale i globálně na síti
13. Otazka
    * Firewall … filtruje provoz, zabezpečuje síťový provoz na různých úrovních … paketový filter, aplikační filter, Stavové paketové filtry, honeypot … návnada pro útočníky které se nastavuje pro sledování a včasné varování, analýza útoku na honey pot může být použita k obraně proti němu
    * Paketové filtry … nejednodužší nejstarší firewall, udává pravidla jaké jaké adrsesy a porty mohou být propustěny, konstrola se provaádí na třetí vrstvě, jsou vysoce rychlé ale pro dnešní požadavky už nedostačující, (nízká úroveň kontroly)
    * Aplikační brány (proxy firewall) … klient se připojí na proxa a ta následně k server, data od klienta filtruje a předává server data od servru pátky předává klientovy, kontrola je prováděna na 7 vrstvě, server nazná zdrojovou adresu protže je na požadavku uvedena vnější adresa brány, takže automatiky funguje jako NAT (umí ale I paketová filtry),
      1. Výhodou je poměrně vysoké zabezpoečení známých prtokolů
      2. Neváhodou vysoká náročnost na HW, celá komunikace je pomalejší, po nástupu stavovýých filtru se přesdtaly aplikační brány dale vyvýjet,každý protocol vyžaduje specializovanou proxy
    * Stavové paketov= filtry … mají stejnou funkci jako paketové filtry, navíc však ukládají informace o povolených spojeních, které pak můžou hrát roli v dalším rozhodování
      1. Urychlujeme zpracování paketů už povolených spojení, firewall sam povolí zpětnou komunikaci při povolení na známých prtokolech (stačí povolyt FTP směrem na server firwall sam povolí cestu zpět), možnost vytvářet virtuálního stavu pro nestavové protokoly jako je UDP a ICMP, stale si zachovávájí svou rychlost s poměrně slušnou úrovní zabezpečení, snadná konfigurace
    * NAT (network address translation) … jedná se o způsob síťového provozu kde dochází k přepisu zdrojové nebo cílové ip adresy I v hlavičkách protokolu na straně firwallu, routeru.používá se pro přístup vice počítačů do globální sítě přez jednu public ipadresu. Ovšem znemožňuje end-to-ent spojení a snižuje rychlost přenosu
      1. Source NAT … u ip paketu se změní source ip a zdrojového portu pokud je využit
      2. Destination NAT mění se cílová ip addresa a tcp port, zpřústupňování privátních služeb pro vřejnou ip adresu
      3. Maškaráda (NAT 1:N) … nejčastěji používaný změněné infomace jsou zapsané routrem do nat tabulky
      4. Výhody umožňuje připojit vice počítačů přez jednu ip public adresu do interetu, zajišťuje skrytí nelze považovat za zabezpečení
      5. Je náročný, spomaluje traffic, může se za ní skrývat kdokoliv
    * Antivirové program … slouží k odhalení a předejití virů na klientském zařízení
      1. Virové slovníky … kontrolujem jestli nějaký program enodpovídá paternu který máme v nich uložený, hledá známé viry
      2. Nebezpečné chování … sleduje chování všech program, a označuje nějaké cování program za nebezpečné nebo bezpečné
      3. Sandbox … spouští soubory na pískovišti a sleduje jejich chování pokud nedělají nic zákeřného tak, jsou označeny jako bezpečné
14. Otázka
    * WLAN … bezdrátový přenos signálu … v pásmech 2.4GHz(IEEE 802.11b zůstavá v pasmu není kompatibilní s 802.11) a 5GHz(IEEE 802.11b), jedná se o přenosy v bezlicenčním pásmu, WIFI (standard IEEE 802.11), bezlicenční pásma můžu začít využívat bez žádosti o licenci
      1. Na licenčním pásmu operuje jeden člověk … držitel licencemá parvo na ochranu před zneužitím, licence je zpoplatněná
      2. Bezlicenčním pásmu býcá vice uživatelů, je zdarma, kdokoliv, běží zde WIFI
    * 2.4 GHz (2400 MHz – 2483 MHz) (83.5MHz), funguje na něm I Bluethoot, mikrovlné trouby, bedrátové telefony, nelze zabránit rušení
      1. 14 kanálů šířky 22Mhu, se vzájemným odstupem 5Mhz, (v EU se používá jen prvních 13 čtrnáctí již zasahuje do licenčního pásma), v EU se nepřekrývají 1,7,13
    * 5 GHz (není spojité) (5150 – 4340 MHz (200 MHz) … pouze pro indoor vyzářený výkon 200mW, 55470 – 5725 MHz (225MHz) … pouze pro outdoor vyzářený výkon 1W
      1. O šířce a rozestupu 20MHz josu nalepené na sobě ale nepřekrývají se indoor 8 outdoor 11
    * Techniky přenosu
      1. zvyšují odolnost proti rušení … Frequence hoppimg … chvíly vysílá na jednom kanálu následně na jiném příjmce ho napodobuje, DSSS … místo jednoho bitu se posílá celý vzorek … příjemce hledá I podobné vzorky k přeušenému vzorku nemusí přesahovat úroveň šumu klient ví co má hledat
      2. Zvíšení eketivnosti … MIMO (many inputs many outputs) … vysílá a přímá na vvíce anténách, Beamsteering … používá směrové antény místo všesměrových
    * Čím je vlna delší tak má větší dosah menší přenos a naopak, rádiovévlny (kome 300GHz 101 – 108 Hz), mikrovlné vlny (3-300GHz, 109 – 1011 Hz), infračervené (1012 – 1014 Hz), Ultrafialové (1015 – 1017Hz), rentgenové(1017 – 1020 Hz), gama záření 1020 a vice
    * Anténna … jedná se o elektromagnetické zařízení které vysílá rádiové vlny, ideální bodová antenna vysílá do všech směrů stejně (neexistuje)
      1. Všesměrové antény max 1km zisk 2 až 6 dBi
      2. Sektorová 30 až 12 stupňů, zisk 10 až 20 dBi, max jednotky kilmotrů
      3. Směrové antény 8 až 15 stupňů, 13dBi výše , větší dosah
    * Vysílací výkon je výkon který vystupuje z zařízení do antény, vyzážený výkon je výkon který v určitém směru z antény vystupuje, omezení vyzářeného výkonu se týká místa kde je vyzářený výkonn největší
    * Čím je nižší frekvence … lépe proniká překážkemi a větší vzdálenost, čím je vyšší bývá k dispozici vice místa může přenést vice dat, čím je kanál širší, tím větší přnosové rychlosti jde dosáhnout (max rychlost je lineárně závislá na na šířce pásma)
      1. Na blýzkých překrývajících se frkvencích může probíhat vice paralelních přenosů
    * Amplitudovou modulaci (informace je zakódována změny aplitud nosného signálu), frkvenční modulaci (informace je zakódovaná změnou frkvence nosného signálu), ON/OFF modulaci, fázová modulace (jako frekvenční , používá se u digitálního signálu)
    * Autentifikace … zabezpečení wfi za pomocí WPA,WPA2,WPA3 (Wifi protection acccess) nahrazuje zastaralé šifrování WEP
      1. WPA … z jednoho výchozího šifrovacího klíče generuju nové a rychle je střídám (pokud by někdo rozluštil jednu část komunikace klíč už nebude uplatnitelný na jiné části), používá prtokol TKIP (ukázalo se že je slabý a zranitelný), zajištění integrity se používá protocol Michael
      2. WPA2(802.11i) … využívá CCMP jak pro šifrování tak pro zaištění integrity dat proti změně … zavádí dva režimi autentifikace
         1. WPA Enterprise(firmy) … je potřebný autentifikační server, přístupvý bd ho využívá pro ověření jednotlivých uživatel, složitější konfigurace
         2. WPA personal … zde s klient prokazuje předem znalostí předem nasdíleného pre-shared klíče přístupovému bodu
15. Otazka
    * HTTP (hypertext transfer text protocol) … jedná se o internetový potokol pro komunikaci na WWW server. Slouží k přenosu HTML, XML a jiných typů souborů používá port TCP/80 (https 443), společně s elektronickou poštou je jeden s nejvyužívanějších protokolů. Pomocí aplikačních bran může spřístupnit další síťové protokoly jako jsou SMTP, FTP.
    * HTTP1.1 … jedná se o plain text protocol
      1. Obsah obrázku text, snímek obrazovky, Písmo

         Popis byl vytvořen automaticky
    * Headers je list řetězců které obdrží jak klient tak server (jsou pro klienta neviditelné), jsou CaseSensitive, jedná se o dodatečé informace a požadavky, jsou ve formátu key:value oddělené CRLF sekvencí, konec je označen prádným polem. U HTTP1.x jsou posílány na konci request nebo response, v HTTP2 a výše jsou již zakódovány do jednoho HEADER a 0 až vice CONTINUATION frames za pomužití komprese HPACK (HTTP2)
      1. Accept-Language: en
      2. Authorization Basic key
      3. Content-Length: 500
      4. Content-Type: application/json
      5. Host: site.i.am.currently.on.com
      6. Vlastní heardy by se měli označovat za pomocí anotace X-My-Header:value
    * Authetifikace … pokud cheme zajistit bezpečný přenso autentifikačních údajů měl by se pto takové potřeby vytvořit šifrovací kanál za pomocí TLS (použít HTTPS).
      1. Basic … jedná se o zašifrování username(ID) a password za pomocí Base64 … Následně s Basic slovem jako hodnota Authorization header … Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
      2. Bearer jedná se o http autentifikaci za pomocí security tokenu můžem taky chápat jako dej přístup nositely daného tokenu. Může se jednat například o API key je vedle Bearer slova jako value Authorization header … Authorization: Bearer <token>
    * Obsah obrázku text, snímek obrazovky, Písmo

      Popis byl vytvořen automaticky
      1. S multiplexem je spojena priorita dotazování (úroveň 0 až 7), aby nebyly zadržovány pakety které klient potřebuje kvůli pomalému spojení
      2. HPACK hlavně HEADERS compression
      3. Server push … server sám začne posílat data I když si je klient nevyžádal
      4. Server hint … server může jenom upozornit klienta o potřebných datech klient pak může rychle zarágovat a na data se dotázat
    * HPACK využívá techniky … Statická tabulka která obsahuje nejběžněji používané hlavičky a jim odpovídající kódy, Dynamická tabluky … udržjí se v ní nedávno použité hlavičky a kód jim odpovídající, HUfmenovo kódování … pro zakódování často používaných řetězců
    * Http requests: GET, POST, PUT, DELETE, OPTIONS
    * Status code (Slouží k označení situce která vzešla z poslaného request pomocí čísla): 1xx … informational (100 Continue), 2xx Successful (200 OK. 201 Created), 3xx … redirected (300 Multiple choice), 4xx … client error (400 bad request, 401 Unauthorized, 404 Not found, 408 Request timed out, 403 Forbidden, 418 I am tea pot), 5xx … server error (500 internal server error, 501 not implemented)
    * Webové služby … webserver … node expers, python flesk, Apache, Nginx (apach a nginx za nás řeší určité věci jako šifrování, správa připojení apod.)
16. Otazka
    * SSL(secure socket layer)/TLS(Transport layer security) jedná se o kryptografický protocol a jeho předchůdce(SSL) mají za úkol navázat bezpečnou komunikaci přez interent. Pužívá se v HTTPS, VLAN, FTP. Samotné SSL se už moc nepužívá (v legacy aplikacích) jeho pojmenování ale zůstalo pro certifikát (SSL cetifikát), moderní svět přešel na TLS.
    * Symetrické/Asymetrické … šifrování má za úkol převod čitelných dat an data nečitená (zpětně se jedná o dešifrování), je velká šance že někdo zachití data které jsou přenášena přez internet ovšem šance že někdo zneužije šifrované data je malá
      1. Symetrické … tentýž klíč se používá jak k zašifrování tak k dešifrování, odesílatel a příjemce se nejdříve domluví na klíči (sekvence znaků), odesílatel zašifruje příjemce rozšifruje
      2. Asymetrická … používá dva klíče jeden pro zašifrování který může být volně dostupný pro kohokoliv (veřejný klíč) a jeden pro rozšifrování který nikdy nesmí spatřit světlo světa (privátní klíč)
         1. RSA (iniciály Rivest–Shamir–Adleman) … jeden z nejstarší public-key kryptografických systémů, který se používý pro bezpečný přenos dat, používá se I dnesa a při dostatečné délce klíče je považován za bezpečný
         2. Obsah obrázku text, snímek obrazovky, Písmo, řada/pruh

            Popis byl vytvořen automaticky
    * SSL/TLS handshake … určuje jaká verze TLS se bude používat, Určuje jaký ciper suite se bude používat (sada algoritmů která vytváří šifrované spojení), autentifikuje server za pomocí SSL certifikýtu a public key, generuje session key za účelem symetrické šifry (na konci handshakeu)
      1. 1. “client hello” message … obsahuje podporovanou TLS verzi, podporovaný ciper suit, “client random” … řetězec náhodných bajtů
      2. 2. “server hello” message … odpověď na client hello message … obashuje SSL certificate, server podporovaný ciper suit/TLS, “server random” máhodně vygenerovaný random tentokrát serverem
         1. Klient si ověří SSL certifikát server za pomocí certifikační authority, klient se přizpůsobuje ciper suitu pokud server využívá jiný
      3. 3. “premaster secret” message … klient vygeneruje další náhodný řetězec bajtů, “premaster secret” následně zašifruje za pomocí public key (který klient získal z SSL certifikátu)
         1. Server dešifruje “premaster secret”
         2. Oba klient is server vytvoří session key za pomocí “client random”, “server random” a “premaster secret” (měli by být stejné)
      4. Client/Server is ready … klient pošle “finished” message která je zašifrovaná session key server pošle “finished” message zašifrovanou session key
         1. Handshake je u konce komunikace bude dál probíhat za pomocí session key simetrické šifry
    * CA (certifikační autority) … podepisují za pomocí privátního klíče certifikáty, protože v dnešní době jsou už public key certifikačních autrit nahrané defaultně v prohlížečích může si uživatel ověřit provost certifikátu. Stále privátní klíč musí být utajený. Funguje take na základě principu přenosu důvěry v danou certifikační autoritu, tedy že důvěřujeme že by certifikační autorita nepodepsala podvonou stránku.
17. Otazka
    * SMTP (Simple mail transfer protocol) smtp 25, smtps 465 … slouží k odesílání a příjmání pošty, může vytvořit relay a předávat si zprávu, jedná se o plaintext protocol (1982), autentizace zde v základu není, vždy je potřeba se server prokázat že vskutku jsme ti za které jse vydáváme, pokud checem aby bylo SMTP šifrované šifrování musí proběhnout už před odesláním a dešifrace až po přijetí,
    * U SMTP server je potřeba řešit spam aby někdo nezneužil náš smtp server pro posílání spamu, server by byl po chvíi připsán na black list poštovních server a z stejné ipadresy a domény by už jsme email neposlaly, pro nalezení mail server si musí smtp vyžádat MX DNS záznam aby věděl kam musí zprávu směřovat
    * Obsah obrázku text, snímek obrazovky, Písmo, číslo

      Popis byl vytvořen automaticky
    * Imap(imap 143 imaps 993) a pop3(pop3 110, pop3s 995) … oba jseou protokoly na OSI vrstvě 7 a běží za pomocí TCP protokolu, POP3 (Post Office Protocol) … je starší mail stáhne lokálně ze schránky ve které následně mizí (pop jako v programování), imapl (internet message access prtocol) … připojuju se na server kde čtu maily a prohlížím svou poštovní schránku bez toho abych musel nějaké maily mazat
      1. Výhody:
      2. Stálé připojení (POP3 se připojí stáhne a odpojí) … je připojený tak dlouho dokud je aktivní user prostředí, pro uživatele s mnoha velkými emaily je to rychlejší
      3. Více současných klientů … POP3 dovoluje puze připojení jednoho uživatele ke schránce, IMAP vice uživatelů, vidí změny které si navájem provádějí
      4. IMAP navíc dovoluje na server vyhledávat a vytvářet pojmnovávat a mazat složky
      5. Je podporován službami jako je google (imap)
      6. Nevýhody:
      7. Imap je oproti POP3 velmi komplikovaný protocol, jeho implementace je značně složitější a je tedy náchylnější k chybám, prohledávání velké schránky může zatížit značně server,
    * SMTP … postfix, sendmail
    * Imap a pop3 … devcot
18. Otázka
    * Hardware, Jádro (Správa procesoru, Správa paměti, správa procesů), OS (správa periférií), uživatelské program,
    * Uživatelské program jsou procesy a aplikace pomocí kterých uživatel může vykonávat určitou činost, pokud potřebuje komunikovat s jádrem využívá k tomu systémová volání (system calls) … jedná se o rozhraní mezi uživatelským procesem a jádrem povoluje záskat přístup ke jádrovým funkcím (síťová komunikace, souborový systeém) … system cals vyžadují operace jako otevýrání a zavírání souborů, zápis a čtení souborů, síťové operace, správa paměti
    * OS … má za úkol dohlížet na uživatelsé program, zajistit efektivní využití HW, učinit počítač (snáze) použivatelný pro běžbého uživatele
    * Jádro je spuštěno jako první část když nabýhá operační system, přebýrá kontrolu and hardware,
      1. Správa prostředků … přiděluje paměť, případně procesy, správa souborů, způsob ukládání a přístup knim
      2. Správa procesů … vytváření a rušení procesů, potlačení a obnovení, synchornizace a jejich vzájemní komunikace (Proces … činnost řízená programem, provádění programu, k realizaci potřebuje nějaké zdroje CPU, paměť, I/O zařízení)
      3. Plánování procesů (musí podporovat multitasking, multithreading) … jedná se o úkol jádra které musí rozhodnout jakému procesu bude přidělen processor a na jak dlouho … využívá při tom praralelismu (souběžně vice proceů) a pseudoparalelismu (jedno vlákno procesy se rychle střídají vypadá jako paralelní)
         1. Dlouhodobé … má za úkol naplánovat úlohy tak aby byl počítač maximálně využit, např: vhodný mix úloh jsou náročné na I/O nebo CPU
         2. Krátkodobé … jedná se o plánování který z procesů bude přidělen procesoru (využívají všechny multitaskingové systémy)
         3. Střednědobé … používají systémy s virtuálí paměťí … jedná se o výběr který blokovaný nebo připravený process bude odsunut z vnitřní paměti na pevný disk, jeli v vnitřní paměti nedostatek.
    * Pseudoparalelismus … vy víceúlohových sistémech většinou běží víe procesů než máme procesorů k dispozici v tu chvíli se využívá. Jedná se o zdánlivý paralelizmus, přepíná mezi procesy dochází k přepnutí 100-1000krát za sekundu. Při přerušení jednotlivého procesu je nutné uložit jeho aktuální stav aby až na process přijde řada mohli jsme pokračovat tam kde jsme zkončily. KOmpletní uložeí stavu … context save a obnovení … context restore. Při uložení kontextu jednoho procesu a načtení jiného … context switch.
    * PCB (tabulka popisu procesů) … jedná se o tabulku v jádře keré uchovává data potřebná k běhu procesu, každá process má svojí PCB, která je využita při změně procesu
    * Monolitické jádro … je velké mohutné obsahuje všechny potřebné služby a ovladače mezi kterýma je závislot (pokud je nějaký špatně napsaný shodí celý systém). Jedná se o preferovaný způsob vývoje (jednodužší vývoj, extrémně účinná)
    * Mikro jádro obshauje v sobě jen základní funkce a všechny osattní systémové ovladače už nejsou zabudované přímo v jádru ale mimo něj. Mikro jádra jsou jednodužší než monolitická tedy méně zranitelnější musí být dobře navrženy (těžké vyvynout)
19. Otazka
    * Jedná se o poskytování služeb či program server doustupnými z internetu s tím, že uživatelé k nim mojou přistupovat vzdáleně (webový prohlýžeč) uživatel tedy neplatí za hardware v datacentrech ovšem jen za výkon který ne tomto hardwaru použil nebo za licence program které na tomto hardwaru použil.
    * Dovolují nám obrovskou škálovatenost a elasticitu … umožňí uživateli podle potřeby změnit výpočetní zdroje, pay as you go, up-to-date … všechen software vždy aktualizovaný, přístup přez niternet odkudkoliv
    * Typy cloudu:
      1. Veřejný cloud … cloud poskytovaný datacentry pro jakékoliv uživatele, s multitenant architekturou (a to že I když máme data vedle dat jiných na dat jiných nevidíme) která snižuje náklady, nejlevnější možnost. Často se nemusíme o nic starat protože všechnu udržbu a administraci za nás dělá datacentrum (né všechnu)
      2. Privátní cloud … veškeré deikované prostředky jsou používany jenom jedním uživatelem (firemní), and prstředky běží tedy jediný tenant, hardware běží na privátní síti a neběží tam softvare nějakého zákazníka, je bezpečný majitel and ním má naprostou kontrolu a zároveň možnost škálovatenosti a žízení prostředků. Vyšší počáteční náklady, náklady na správu, není až tak flexibilní při škálování prostředků stale máme omezený hardware.
      3. Hybridní cloud … data a interní infromace zůstávají na interním privántím cloudu a veřejný cloud je používán pro svojí škálovatnost a operace které nejsou privání. Jedná se o postupnou migaci do veřejného cloudu nebo veřejný cloud můžem používat jenom jako dodatečnou výpočetná sílu.
      4. Multi cloud … využvářešení vice dodavatelů veřejného cloudu, minimalizace rizik, zmenšení závislostí na konkrétním dodavateli nebo vytvoření nátlaku na nižší cenu. Je těžší údržba musíme mít větší znalost jendotlivých technologií.
      5. Komunitní cloud … infrastruktura cloudu je sdílena mezi několika organizacemi, tedy skupinou lidí, kteří ji využívají. Může je spojovat bezpečnostní polityka, stjná oborzájmu apod.
    * Distribuční model … vypovídá o tom, co je v rámci služby nabízeno – zda jde o software, hardware či jejich kombinaci.
      1. IaaS (Infrastructure as a Service) … pokstuje infrastrukturu, o veškeré problémy ohledně, jedná se například o virtuální stroj (server) který si bude uživatel sím spravovat, newteork administratory
      2. PaaS (Platform as a Service) … poskytuje prostředky pro vývoj a deployment aplikace, obsahuje IDE, databzi, různé programovací jazyky, určené pro vývojáře
      3. SaaS (Software as a Service) … aplikace (licencovaná služba), potřbujeme k ní přístup odkudkoliv, nepotřebujeme tak výkoné zařízení, Microsoft 360, Google Apps, určené pro end usery (kancelářní)
    * Výhody: absence nutnosti nákupu HW, znalosti principu HW a SW, jednoduchost uživatlské rozhraní, možnost okamžitého zvýšení výkonu datováho centra, přispůsobitelný IT potřebám a růstu uživatele, minimální provozní náklady
    * Nevýhody: závisost na interentovém připojení, závislost na poskytovateli, odlišný právní řád u klienta
20. Otázka
    * Hardware, Jádro (Správa procesoru, Správa paměti, správa procesů), OS (správa periférií), uživatelské program
    * Shell název textového uživatelského rozhraní, které je předchůdce grafického, shall je spuštěn po přihlášní uživatele, vytvoří příkazoví řadek skrze který dovoluje počítač ovládat a uknočen je až po uživatelově odhlášní mezi shally patří sh, bash, csh, ksh a mezi grafický interface patří například GNOME a KDE
    * Správa programového vybavení pomocí balíčkovacího systému, joud dva základní dpkg (Debian, ubuntu) a rpm (readheat), slouží k nainstalování balíčku do systému nástavba jako apt … spravuje repositáře balíčků a umožňuje je přímo ztahovat z internetu kde následně znovu pomocí rpm nebo gkpg jsou nainstalovány
    * Probíhá POST (power on self test) nejdříve počítač načte Master Boot Record (512bajtů), ten odkazuje na bootloader který by v aktuálním režimu real mode (16-bitový, neposkytuje memory protection, multitasking, nebo privilegia) režim nebyl viděl (je vidět 1 MBajt paměti) ten by měl zavést do paměti a spustit GRUB bootloader, ten má za úkol načíst kernel do paměti a následně mu předat kontrolu a připravit souborový sistém, se příchodem kernel s epočítač přepíná do pretected režimu (32-bitový, dovoluje využívat virtuální paměť, paging a bezpečný multitasking, pracuje s privilegii a ochrana paměti uděluje procesu nějakou část paměti tím zabraňuje aby si procesy ovlivňovaly). Ve chvíli jak jse načte kternel spuští int nebo system první process který následně spouští další procesy, ten znovu od krernlu přebírá kontrolu. Systemd následně sspouští každý jeden porces v nějakém run levelu (GUI 5 runlevel, MCD 3 runlevel) a mountuje file system.
    * Souborový system je hierarchický system
21. Otazka
    * Dovoluje redundatní spojení mezi zařízeními, které nebude blokovat STP, jedná se o port link aggregation převážně na Cisco switchy. Shlukuje vice portů do jedné logické linky. Zvyšuje rychlost přnosu. Můžeme takto zkobinovat až osm portů (800Mbit/s, 8Gbit/s) … výsledný virtuální interface je nazýván port channel. Snaží se traffic rovnoměrně rozložit mezi vybraných n portů. Za předpokladu že jeden z porů vypadne Etherchanel by měl předistribuovat zátěž na zbylé porty (tento process zaber eméně než vteřinu). Nemůžeme shlukovat porty s rozdílnou přenosovou rychlostí.Nastavení etherchanelu se musí shodovat na obou stranách (např trunk pory musí mít stejnou nativní vlanu).
    * PAgP (Port Aggregatio Protocol) Cisco proprietární … maximálně osm aktivních portů
      1. Etherchannel PAgP frame je posílán každých třicet vteřin, aby zkontroloval konzistenci konfigurace a vyřešil nastale nedostatky nebo výpadek a dpomáhá vytvářet Etherchanel link pomocí detekce konfigurace na obou stranách, aby s eujistil že jsou kompatibilní.
      2. Desirable nevyjednává, auto přistupuje, one jde jen s on
      3. Obsah obrázku text, snímek obrazovky, Písmo, číslo

         Popis byl vytvořen automaticky
    * LACP (Link Aggregation Control Protocol) … IEEE Ethernet standards … maximálně osm aktivních maximálně osm stand by (pokud nějaký aktivní link vypadne stand by ho nahradí)
      1. Active vyjednava, pasiv pristoupi kdyz nekdo vyjednava, on jde jen s on
      2. Obsah obrázku text, snímek obrazovky, číslo, Písmo

         Popis byl vytvořen automaticky
    * Konfigurace (switce podporují protocol, porty maj stejnou rychlost a typ, jsou na stejné vlaně, podporují stejné allowd vlany)
      1. Obsah obrázku text, snímek obrazovky, Písmo

         Popis byl vytvořen automaticky
22. Otazka
    * HSRP (hot standby router protocol) … jedná se o cisco proprietární protocol pro založení fault-tolerant default gatewaye. Protocol založí spojení mezi routrama v případě že hlavní routeru vypadne záložní router se ujme vedení.
    * Router s největší prioritou na sebe vezme funkci defaultní gateway a s předdefinouvanou ip addresou a virtuální mac adresou bude odpovídat na packet ARP nebo ND. Pokud primární router odpoadne což zjistí sekundární router tak že mu primární router deset sekund už neposlal Hello message (hello message obsahuje prioritu routeru). Sekundární router převezme na sebe virtuální MAC a IP adresu a bude se chovat jako minulý router.
    * Obsah obrázku text, snímek obrazovky, Písmo

      Popis byl vytvořen automaticky
    * Obsah obrázku text, snímek obrazovky, Písmo

      Popis byl vytvořen automaticky
    * Konfigurace
      1. Nastaveni ip adres na routrech podle poditi
      2. R1(config-if)# standby 1 ip 192.168.1.254
      3. R1(config-if)# standby 1 priority 150