50. Které protokoly popisují standardy IEEE 802.11, IEEE 802.15 a IEEE 802.16
IEEE 802.11 – WiFi, 802.11b a 802.11.g pásmo 2,4GHz, 802.11a pásmo 5GHz
IEEE 802.15 – ZigBee – bezdrátová komunikační technologie, pro sítě PAN, dosah 75 metrů, rychlost až 250 kbit/s
IEEE 802.16 – WiMAX – bezdrátová komunikace pro venkovní sítě, stále se vyvíjí

51. Co jsou to virtuální lokální počítačové sítě? Jak se tvoří a v čem spočívají jejich výhody?
Logicky nezávislá síť v rámci jednoho nebo několika zařízení.
Clem je učinit logickou organizaci sítě nezávislou na fyzické vrstvě, čímž lze usnadnit správu sítě, zvýšit její výkon a podpořit bezpečnost.

52. Co je to most, jak se liší od opakovače? Jaké jsou základní funkce mostu?
Opakovač – digitální zesilovač, pracuje na fyzické vrstvě. Nechápe význam jednotlivých bitů. Bez něj například dostah 10Gb Ethernetu, při užití kroucenné dvoulinky jen 100m, tenký koaxiál 185m.

Most – Má inteligenci, dokáže rozhodnout, zda data zůstanou jen v lokální segmentu, či je nutné je poslat dál. Most tedy ke své funkci potřebuje znát formát přenášených dat, a to alespoň natolik, aby si z nich dokázal odvodit, kdo je jejich příjemcem a kdo odesilatelem. Kromě toho pak potřebuje i informaci o tom, které uzly se nachází ve kterých segmentech.

Tuto druhou skupinu informací může most získat různými způsoby:
1, Jednou z možností je apriorní "vyplnění tabulky", kterou most ve vhodné formě dostane při svém spuštění a podle které pak pracuje, aniž by ji sám jakkoli měnil. To je jistě velmi robustní řešení, vhodné pro takové sítě, jejichž konfigurace se mění jen zcela výjimečně. V praxi je ale toto řešení používáno jen velmi málo, protože existují jiná, ještě výhodnější řešení.

2, Další možností je nechat most se tyhle informace naučit, dá si je do souvislosti adresu se segmentem. Postupně se naučí vše potřebné, používá se u Ethernetu.

53. Vysvětlete jak funguje Spanning Tree algoritmus a kdy se používá.
Most se dokáže sám učit, když mu přijde datový ráměc ze směru A, od odesilatele X, odvozí, že uzel X leží v tomto směru. Pokud je ale spojení redundantní(existují cykly v grafu popisujícím síť), přijde mu taková informace z více směrů a nemůže se rozhodnout.
Ovšem existence redundantního spojení je žádoucí, zvyšuje se tím spolehlivost sítě. Je tedy nutné, aby se mosty domluvily a vybraly takovou cestu, která nebude obsahovat žádné cykly. Mosty se tedy pomocí speciálního protokolu domluví na nejvhodnější acyklické topologii. Z této vzájemné domluvy vychází jeden most v roli tzv. kořenového mostu (root bridge), a všechny ostatní mosty vybírají ze všech svých směrů právě jeden, který prohlásí za "kořenový" (ve smyslu: vedoucí ke kořenovému mostu). Tím vzniká přísně stromovitá (a tudíž acyklická) struktura, v jejímž kořeni je kořenový most. Celý algoritmus je navíc řešen tak, aby při výpadku některého mostu či spojení dokázal využít existenci redundantních spojení a zajistil automatické zotavení celé sítě.

54. Vysvětlete jak funguje algoritmus Source Routing a kdy se používá?
A nyní již k samotné pointě: source routing není způsobem směrování, jak by slovíčko "routing" napovídalo. Místo toho jde o jeden konkrétní druh "mostění" (bridging), neboli o jeden konkrétní způsob fungování mostu. Samotný "source routing" vyvinula firma IBM pro své sítě **Token Ring**. Vše je založeno na myšlence, že způsob průchodu datových rámců skrz jednotlivé mosty se určí předem a potřebné pokyny k průchodu takto zvolenou trasou se vloží do každého jednotlivého rámce. Tyto pokyny přitom mají formu lineárního seznamu mostů, přes které má datový rámec postupně projít. Podstatná je na celé věci skutečnost, že o celé trase přenosu datových rámců rozhoduje již jejich odesilatel - odsud přívlastek "source" (doslova: od zdroje).

Zajímavé je na celé věci i to, podle čeho vlastně odesilatel volí nejvhodnější trasu, kterou pak zakóduje do každého odesílaného rámce: na všechny strany vyšle speciální "průzkumný" rámec, který se sám následně šíří do všech existujících směrů, dokud nedojde k hledanému cíli. Od něj se rámec vrací zpět ke svému původnímu odesilateli a nese v sobě informaci o trase, kterou přitom prošel.

55. Jaké problémy řeší síťová úroveň?
Chtějí-li spolu komunikovat dva uzly počítačové sítě, mezi kterými neexistuje přímé spojení, je nutné pro ně najít alespoň spojení nepřímé - tedy vhodnou cestu, vedoucí přes mezilehlé uzly od jednoho koncového uzly ke druhému. Možných cest může být samozřejmě více, někdo je však musí najít, jednu z nich vybrat, a pak také zajistit správné předávání dat po této cestě. Všechny tyto úkoly má v referenčním modelu ISO/OSI na starosti síťová vrstva.
Úkoly síťové vrsty:
1, Nejdůležitějším úkolem síťové vrstvy je tedy tzv. **směrování** (**routing**), které představuje právě ono zmíněné rozhodování o směru odesílání jednotlivých paketů. Není jistě třeba zdůrazňovat, že k tomu síťová vrstva potřebuje alespoň základní informace o topologii celé sítě.

2, S tím dosti úzce souvisí i další úkol síťové vrstvy - předcházet přetížení či dokonce zahlcení částí sítě, řídit tok dat a dbát o co možná nejrovnoměrnější využití všech přenosových prostředků a kapacit.

3, Při vzájemném propojení dvou či více sítí pak přibývá síťové vrstvě ještě jeden důležitý úkol - zajišťovat nezbytné předávání paketů mezi jednotlivými sítěmi.

56. Co je to záplavové směrování, kde se používá, jaké má výhody a nevýhody?
Extrémní formou směrování je tzv. **záplavové směrování** (**flooding**). Předpokládá, že přijatý paket je znovu odeslán všemi směry kromě toho, odkud sám přišel.

Zřejmou výhodou je maximální robustnost, díky které se záplavové směrování dokáže vyrovnat prakticky s jakýmkoli výpadkem. Zaručuje také, že každý paket je vždy doručen tou nejkratší možnou cestou. Nevýhodou je ale vznik velkého množství duplicitních paketů, které výrazně zvyšují zátěž existujících přenosových cest, a které je třeba následně rušit.

V praxi se proto používá spíše tzv. **selektivní záplavové směrování** (**selective flooding**), při kterém není každý paket znovu vysílán všemi směry, ale pouze těmi, které jsou alespoň přibližně orientovány ke konečnému příjemci paketu.

57. Co je to směrování podle vektoru vzdáleností? Který směrovací protokol tuto metodu podporuje?
DVA – používá Bellman-Fordův Algoritmus. Je to směrování nejkratší cestou v počtu skoků k cíli. Maximální délka je 15, 16 je již bráno jako nekonečná vzdálenost. Používá to protokol RIP.

Vektor vzdáleností pro uzel X: minimální vzdálenost z uzlu X do všech ostatních uzlů

Každý uzel provádí následující 3 operace souběžně:

1, Posílá vektor vzdáleností svým sousedům

2, Přijímá vektror vzdáleností od svých sousedů

3, Počítá nové vzdálenosti na základě přijatých vektorů

Problém „čítání do nekonečna“:
1, Omezení horní meze pro čítání (maximální vzdálenost)

2, Split horizon (rozštěpený obzor):

X nesmí poslat do uzlu Y svou vzdálenost k uzlu Z, je-li uzel Y ve směru z X do Z.

3, Split horizon with poisoned reverse (rozštěpený obzor s otráveným zpětným směrem):

X posílá do uzlu že jeho vzdálenost k uzlu Z je ∞, je-li uzel Y ve směru z X do Z.

Bohužel, žádné z těchto řešení nezabrání cyklům

Možné řešení: Před generováním a posíláním vektoru vzdáleností, který upravuje konektivitu k jinému uzlu, počkat nějakou dobu na informace o konektivitě k tomuto uzlu od jiných uzlů

Může významně prodloužit dobu konvergence.

Urychlení konvergence: triggered update (okamžité spuštění opravy)

58. Co je to směrování podle stavu linek? Který směrovací protokol tuto metodu podporuje?

LSA, používá se v **OSPF**, prostě to vytvoří graf sítě a lokálně to Dijkstrem spočte nejkratší cestu. Nezatěžuje síť oproti **DVA**, ale zase vyžaduje větši výpočetní výkon

Link State Algorithm (LSA) – směrování podle stavu linek

● Každý uzel ví jak dosáhnout přímo spojené sousedy: lokální link-state (stav linek)

● Přerušené linky nebo nefungující sousední směrovače jsou detekovány periodickou výměnou „hellou“ zpráv

● Každý směrovač šíří vlastní stav linek do všech ostatních uzlů sítě pomocí spolehlivého záplavového doručování

● Znalost stavu linek ze všech uzlů je dostatečná pro konstrukci grafu propojení celé sítě

● Každý uzel vypočte minimální vzdálenost k ostatním uzlům pomocí Dijkstrova algoritmu

Každý uzel generuje periodicky nebo při změně stavu lokální linky **Link State** pakety (**LSP**)

Uzel, který **LSP** přijme, pošle jej všem svým sousedům, kromě toho, od kterého ji obdržel

Sekvenční číslo **LSP** musí být větší, než posledně uloženého **LSP** od tohoto uzlu

● Před posláním LSP sousedům snižuje hodnotu TTL

● Jestliže TTL LSP dosáhlo nuly, posílá je uzel dál s tím, že je to signál pro vyřazení tohoto LSP ze všech uzlů

● Pomocí TTL se měří stáří lokálně uložených LSP

● Co se stane, když sekvenční číslo LSP dosáhne maxima?

● Co se stane když se uzel rychle vypne a zase zapne bez toho, že sousedé detekují výpadek?

● Uzel si může od souseda vyžádat poslední uložené LSP

Výhody a nevýhody:

+ Rychlé ustálení po změně topologie

+ Více robustní než RIP

+ Předchází problému čítání do nekonečna

- Vyžaduje ukládání LPS v každém uzlu (týká se rozšiřitelnosti)

- OSPF se proto používá pouze pro interní směrování (omezení z důvodu škálovatelnosti – rozšiřitelnosti

59. Co je to skupinové směrování a čím se liší od směrování podle individuální adresy?
Přeposílání IP datagramů z jednoho zdroje skupině více koncových stanic.
Odešle se jeden datagram, ale přijde každému cíli.

60. Co je to Dijkstrův algoritmus a jak funguje?
Nalezení nejkratší cesty v grafu. Při každém průchodu cyklu se do množiny navštívených uzlů přidá právě 1 uzel. Průchodů cyklem je tolik, kolik má graf vrcholů.
Algoritmus:
Celý algoritmus se dá shrnout do tří kroků (ohodnocení cesty do vrcholu X budeme značit |X|):

- nalezení vrcholu s minimálním dočasným ohodnocením (nazvěme ho V)
- prohlášení vrcholu V za trvalý
- změna ohodnocení sousedů tak, že |S| = min(|S|, |V| + ohodnocení hrany z V do S), kde S je soused V.

http://www.kiv.zcu.cz/~konopik/sem/cech/index.html
(Příklad)

61. Co je to Bellman-Fordův algoritmus a jak funguje?
V případě grafů se záporně ohodnocenými hranami není Dijkstrův algoritmus použitelný. Proto nasazujeme Bellman-Fordův algoritmus, který také jako v Dijkstrovo algoritmu využívá metodu relaxace hran, která zjišťuje aktuálně nastavenou hodnotu nejkratší vzdálenosti od uzlu S. Jestliže je zjištěno
, že hodnota v uzlu je vyšší než hodnota z nynějšího uzlu plus ohodnocení hrany z nynějšího uzlu do uzlu, v kterém bychom chtěli změnit jeho hodnotu, tak tuto hodnotu změníme, respektive snížíme. Hlavní rozdíl oproti Dijkstrovu algoritmu spočívá v průchodu grafu. Jelikož Dijkstrův algoritmus jestliže projdeme všechny následníky jednoho uzlu tak tento uzel "uzavře" a poté ho už neupravuje. Toto se v Bellman-Fordovu algoritmu neděje jelikož on tyto uzly neuzavírá takto ihned ale projíždí několikrát všechny uzly a upravuje postupně hodnoty vzdáleností nejkratších cest.

62. Popište funkci protokolu RIP. Kde se používá, jaké má výhody a nevýhody. Uveďte algoritmy, které byly vyvinuté aby kompenzovaly nevýhody protokolu.

Je typu **distance vector** – uzly si vyměňují aktualizace tvořené směrovým vektorem a jeho ohodnocením.

Všechny ohodnocení linek jsou nastaveny na 1 (počet mezilehlých uzlů).

Princip fungování:
Aktualizace se posílají každých 30 sekund. Pokud do 180 sekund nepřijde update od konkrétního(sousedního) routeru, jsou všechny cesty přes ně považovány jako nekonečné. Po dalších 120 sekundách jsou odstraněny z tabulky.

Výpočet cest je distribuovaný, každý počítá kousek, takže chyba jednoho ovlivní ostatní.

Aktualizace se posílají jen přímým sousedům(routerům), takže router nevidí dál, než ke svým sousedům, nezná celou topologii.

Neudržuje alternativní cesty, cesty se stejným ohodnocením ignoruje.

Zatěžuje hodně síť, ale nezatěžuje moc CPU.

Algoritmus opravy směrovací tabulky:
Pokud je nově vypočtená vzdálenost

1, Menší – opravit

2, Stejná – nic neměnit

3, Horší:

Na základě zprávy ze směrovače, který je sousední pro původní směrování – opravit (**zhoršení ocenění)**

Na základě zprávy z jiného směrovače – **nic neměnit**

63. Popište funkci protokolu OSPF. Kde se používá, jaké má výhody a nevýhody. Uveďte topologii sítě, typy směrovačů a jakou mají funkci.

Je typu link-state, každý uzel testuje dostupnost svých sousedů, každý uzek sestavuje link-state paker, ve kterém jsou údaje o dostupnosti sousedů(stav linky a ohodnocení).

Tyto pakety jsou rozesílány všem uzlům v síti, ale jne při nějáké změně, jinak každých 30 minut. Všechny uzly tedy mají úplnou informaci o jednotlivch spojích a mohou si vypočítat optimální cesty → chyby ovlivní jen sama sebe.

OSPF podporuje alternativní cesty, různé cesty pro různé druhy provozu. Také dovoluje rozdělit sítě na menší oblastí, kdy topologie není šířena mimo tuto oblast.

Směrovače v oblastěch se rozdělí takto:
- interní – zajištují směrování v rámci oblasti
- páteřní – zajištují směrování v páteční oblasti
- na rozhraní – patří do oblasti o do páteře, vyměnují info mezi nimi
- hraniční – vyměnují informace s jinými oblastmi

Směrovač monitoruje dostupnost sousedů hello paketem každých 10 sekund, pokud do 40 sekund soused neodpoví, zruší se sousedství, když do 30 miut není změna, opakuje vše.

Určení vah cest:
- Nejjednodušší (často používané)

  Všechny linky mají stejnou cenu – směrování s minimálním ohodnocením
- Cena linky – převrácená hodnota kapacity

  10Mb linka má 100 krát vyšší cenu než 1Gb linka
- Cena linky – zpoždění linky

  250ms satelitní spojení má 10 krát větší cenu než 25ms pozemní linka
- Cena linky – využití linky

  Linka s 90% využitím má 10 krát vyšší cenu než linka s 9% využitím, způsobuje oscilace.

64. Co jsou to protokoly externího směrování a kde se používají?
Používají se pro směrování mezi sítěmi, jsou to protokol pro směrování mezi autonomními oblastmi.

● BGP udržuje směrovací tabulky, šíří opravy směrování a rozhodnutí o směrování zakládá na směrovací metrice

● Vyměňuje informaci o dosažitelnosti sítě (reachability)

● Vytváří graf propojitelnosti AS (AS connectivity)

● Odstraňuje směrovací smyčky a prosazuje rozhodnutí o strategii

●BGP používá jednu metriku k určení nejlepší cesty

Linková metrika je hodnota preference přiřazená administrátorem

Je to multikriteriální funkce: počet procházených AS, strategie směrování, stability, rychlosti, zpoždění, ceny, …

● Vybírá nejlepší cestu a instaluje IP forwardovací tabulku

Path Vector protocol:
● Podobný Distance Vector Protocol
● Každý BGP směrovač posílá pomocí broadcastu sousedům celou cestu (posloupnost AS) do cíle

Dá seručně nastavit, kudy to má jit, aby síť obsluhovala jen své zákazníky a ne všechny jenom proto, že má nejvyšší rychlost; „aby to ten s dobrym pripojenim neodsral“.

65. Co je to zahlcení v sítích, čím vzniká a jak se mu bráníme.
Přepojovací uzel nestačí přepojovat přenášená data v reálném čase → hromadí se ve frontě → zvyšuje se čas obrátky → překročí se kapacita front → nové bloky jsou zahazovány → mechanismy potvrzování snažící se zajistit spolehlivost posílají data znova → zvýšení provozu v síti → zhoršuje ještě více stav → zahlcení sítě
Ošetření: uzly mají možnost upozornit na hrozící nebezpečí; „disciplína“ odesílatelů; AIMD - pomalu posílám a čekám co se stane → pomalu tím zvyšuju rychlost → jakmile zjistím ztrátu tak spadnu dolů - v nejhorším případě na 0 a zase pokračuju

66. Co je to tunelování a kde se používá. Uveďte příklady.
Používá se pro zapouzdění jednoho, či více síťových spojení do jiného. Například budu komunikovat pomocí Ipv6, ale půjde to přes síť, který umí jen IPv4, takže Ipv6 pakety obalím IPv4 a pošlu je.
Jiným běžným využitím je tunelování přes SSH spojení - pokud jím protunelujete jiné síťové spojení, zaručíte, že internetem budou data procházet zašifrovaně, i když protokol tunelovaného spojení šifrování nepodporuje.

67. Co je to mobilní IP a jak funguje.
Mobilní IP adresa umožňuje stanicím s IP adresou ze sítě o daném rozsahu IP adres být připojeny a komunikovat v sítích o jiném rozsahu IP adres.
Technologie Mobile IP udržuje stejnou IP adresu mobilního zařízení a podporuje jeho komunikaci, zatímco se přemisťuje z jedné sítě do druhé. IP zařízení komunikuje v síti, i když jeho trvalá IP adresa může být odlišná od adresy sítě.

68. Popište formát IPv4 adresy. Co jsou to podsítě a proč se zavádí?
délka adresy – 32 bitů;
5 tříd – A 0
B 10
C 110
D 1110
E 1111
Adresa rozdělena na 4 úseky po 8 bitech. Např. u A –první úsek značí síť, zbytek určuje PC v síti → státní organizace; běžný uživatel má C; E - speciální

Podsítě - nejdřív začali s třídama (A,B,C,D). Třeba u A bylo první číslo síť a ostatní čísla stanice atd. Začaly ale nedostačovat adresy, tak se přešlo na CIDR. Tam může bejt třeba IP/21, kde zleva překreješ IP adresu 21 jedničkama a zbytek ip adresy je pro stanice.

69. Co je to maska sítě a implicitní adresa směrovače?
Maska sítě:

Rozděluje adresu na část síťovou a část pro hostitelský systém

Např. 255.255.255.0

147.228.67.0 * 255.255.255.0 dává stejný výsledek pro všechny adresy začínající 147.228.67

Důvodem rozdělení na dvě části je minimalizace počtu položek ve směrovačích (jedna položka zahrnuje více adres počítačů)

CIDR (ClassLess InterDomain Routing)

Umožňuje použít pro adresování v podsíti takový počet bitů, který není na hranici 8.

Adresa se udává ve tvaru adresa/počet bitů síťové části

Implicitní směrování (Default Routing) se používá tehdy, když je zdrojová síť připojená na IP intersíť přes jediný směrovač, takže přes něj musí procházet všechny paket nepřímého směrování. V tomto případě není potřeba směrovací tabulka a stačí znalost IP adresy **implicitního směrovače**.

70. Jak se v lokální (mnohabodové) síti převede síťová adresa na fyzickou adresu počítače?
Pomocí ARP; pošle se ARP paket se zdrojovou síťovou i fyz. adr. a cílovou síťovou => cíl odpoví doplněním své fyzické adresy. Když je cíl mimo LAN, tak by směrovač doplnil svou fyz., protože to stejně půjde přes něj.

71. K čemu slouží protokol ICMP? Znáte programy, které jej využívají? Znáte princip?
Protokol IP, který je hlavním přenosovým protokolem na úrovni síťové vrstvy, funguje tzv. nespolehlivě - když zjistí, že se něco při přenosu poškodilo, nepovažuje za svou povinnost postarat se o nápravu (ale počítá s tím, že o ev. nápravu se postará někdo jiný, a to vyšší vrstvy). Protokol IP tedy má právo zahodit taková data, u kterých zjistí že jsou nějakým způsobem poškozena (samozřejmě je nezahazuje bezdůvodně). I když nemá povinnost postarat se o nápravu, přesto se snaží alespoň informovat o tom, že se něco špatného stalo. Právě k tomuto účelu pak využívá další z "doprovodných" protokolů, protokol ICMP. Ten je jakýmsi "poslem špatných zpráv" - sám nenapravuje žádné chyby či závady nebo jiné nestandardní situace, ale pouze přenáší zprávy o tom, že něco je v nepořádku.
ICMP se posílá v IPpaketu, IPpaket - hlavička, IPpaketdata a v ní ICMP paket
Využívá ho **PING**.

72. Co je to Network Address Translation (nebo Network Address and Port Translation)? Kde se používá a jaké má výhody a nevýhody?
Způsob úpravy síťového provozu přes router přepisem výchozí nebo cílové IP adresy. Adresy

lokální sítě se přeloží na jedinečnou adresu, která slouží pro vstup do jiné sítě (www...), překládanou adresu uloží do tabulky pod náhodným portem, při odpovědi vyhledá port a pošle pakety na přiřaženou IP. Používá se v Internetu.
Výhody – připojení více PC na jedné veřejné IP; vyšší bezpečnost
Nevýhody – ztráta rychlosti připojení

73. Kde se používá a jak funguje protokol ARP?
Mechanismus dynamického budování a udržování převodních tabulek mezi IP a fyzickou adresou. Využívá broadcast → vyšle info o tom, koho hledá → hledaný mu odpoví infem o sobě.
V sítích Ethernet.

74. Vysvětlete postup doručení paketu v síti internet mezi dvěma počítači, připojenými do lokálních počítačových sítí různého typu, propojených internetem (směrovači).
Pakety odeslány na server (poskytovatele připojení), server určí ideální trasu → Každý paket může putovat internetem zcela jinou trasou, a proto je jeho součástí informace o adrese odesílatele a příjemce, dále údaje označující bezchybnost data a pořadové číslo paketu, díky němuž se dá ve finále původní soubor znovu poskládat do výchozí podoby, protože jednotlivé pakety jsou doručovány v různém pořadí. → cíl odpoví a celý proces běží od cíle ke mě

75. K čemu slouží protokol BOOTP? Jak funguje?
Přiděluje stanicím parametry jako IP adresa, maska sítě, brána...-> tyto informace jsou na BOOTP serveru.
Startující stanice vyšle dotaz „kdo jsem?“ broadcastem, BOOTP server najde v tabulce podle MAC adresy příslušné údaje a odpoví
Protokol BOOTP slouží právě tomuto účelu, a vychází vstříc dokonce i bezdiskovým stanicím, kterým umožňuje tzv. počáteční zavedení jejich operačního systému (tzv. bootstrap, odsud také jeho název) - protokol BOOTP poskytne startující (tzv. bootující) stanici přesný odkaz na místo, odkud si může vyzvednou svůj operační systém a vše, co potřebuje ke svému startu (tzv. boot image).

76. K čemu slouží protokol DHCP? Jak funguje?
Dovoluje dynamické přidělování parametrů (IP, maska sítě, brány...); parametry jsou vztaženy k segmentu počítačové sítě;
přidělování IP – statické - máme jí doopravdy zaregistrovanou; dynamické - napořád nebo na dobu určitou (pronájem)

Protokol DHCP (stejně jako BOOTP) přitom vychází z architektury klient/server a počítá s existencí konfiguračního serveru (DHCP serveru), který poskytuje potřebné konfigurační informace uzlům, které vůči němu vystupují jako jeho klienti. Jednou z jeho odlišností oproti protokolu BOOTP je například to, že dokáže "propůjčovat" svým klientům IP adresy pouze dočasně, jen na dobu jejich skutečné potřeby, a pak je zase odebírat a využívat jinak.

77. Co je to protokol IPv6, jaké má základní vlastnosti, kde se používá? Jak se liší od Ipv4?
– je síťová vrstva pro mezisíťový přenos paketů
– 128bitů dlouhé adresy => spoooooousty adres
– bezstavová autokonfigurace adres
– lepší podpora multicastu
– adresy místní linky
- lépe řeší fragmentaci a defragmentaci
– jumbogramy – packety větší než 64KiB, velikost až 4GB
– rozdíly: velikost packetu, počet možných adres...

- anycast – jedna IP adresa přidělenena více uzlům současně

78. Vysvětlete princip DVA, jakým způsobem se konstruují směrovací tabulky, co je to čítání do nekonečna a jaké algoritmy se používají pro urychlení konvergence.
Viz. 57

79. Vysvětlete, jak fungují jmenné servery, proč je systém doménových jmen decentralizovaný a jak se převádí jméno počítače na adresu a naopak. Účastní se také jmenné servery doručování elektronické pošty? Pokud ano, pak jak.
Jmenné servery (DNS) – převádí jméno (www.pepa.cz) na IP adresu (123.123.12.45)
Domény:
Je potřeba zajistit, aby se nesesli stejné adresy (pepa.cz).
Zavádí se hierarchie, kdy v rámci cz domény smí být
pepa.cz jenom 1x (v rámci com domény opět 1x apod).
pepa se následně dále může dělit na subdomény, ale každá
opět pouze 1x (honza.pepa.cz; franta.pepa.cz)

Použití pro el. poštu – určuje kam a jakým zp. má být doručena pošta; *pet@dcit.cz* → na tento server chodí pošta pro adresata pet, ten ji ovšem chce přijimat na *pet@frode.dcit.cz* → není vhodné mít ovšem takovouto adresu, např. pokud by se změnila subdomena frode, byla by pošta v kelu → proto se posila na globalni domenu dcit.cz → DNS ma info o tom, ze pro uzivatele pet se ma pošta přijimat na frode. Pokud se změni frode za xy, pouze se prepise DNS zaznam, ale jinak vše jede pořad stejně.

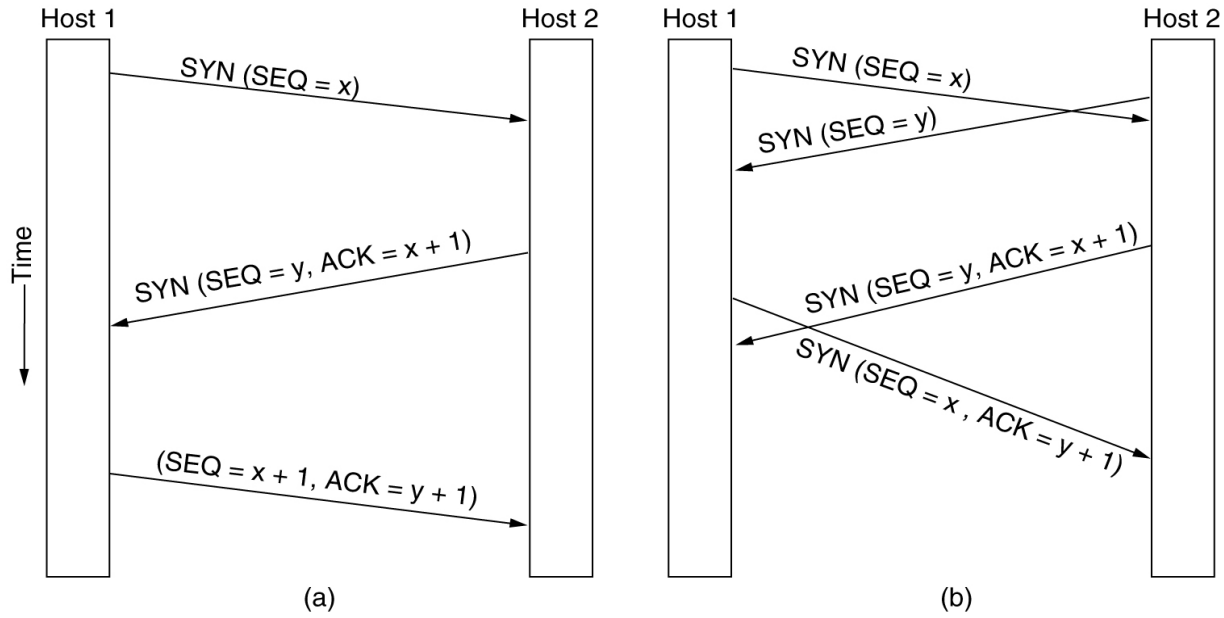
80. Vysvětlete, jak se podílí ARP na komunikaci mezi dvěma vzdálenými počítači, připojenými do Internetu prostřednictvím rozhraní Ethernet.
ARP – zabezpečuje přiřazení IP adresy fyzickým adresám linkové vrstvy → vlastní komunikace v síti pomocí fyzických adres;
2 funkce – získání MAC adres; udržování tabulek přiřezených MAC adres k IP adresám
Když IP protokol získá z vyšší vrstvy adresu → prohledá tabulku → nenajde-li cílovou adresu → vyšle požadavek → odpoví mu vlastník IP adresy → aktualizace tabulky

81. Co víte o náhodných metodách sdílení komunikačního kanálu?
Aloha – stanice nezjišťuje, jestli se něco přenáší, či ne, prostě začne vysílat. Pokud nedostane potvrzení, pošle zprávu znova. Dá se aplikovat pouze do 20% zatížení sítě.
Taktovaná Aloha – zahájit vysílání lze pouze v pěvně stanovených časových okamžicích.
CSMA – viz. předchozí otázky.

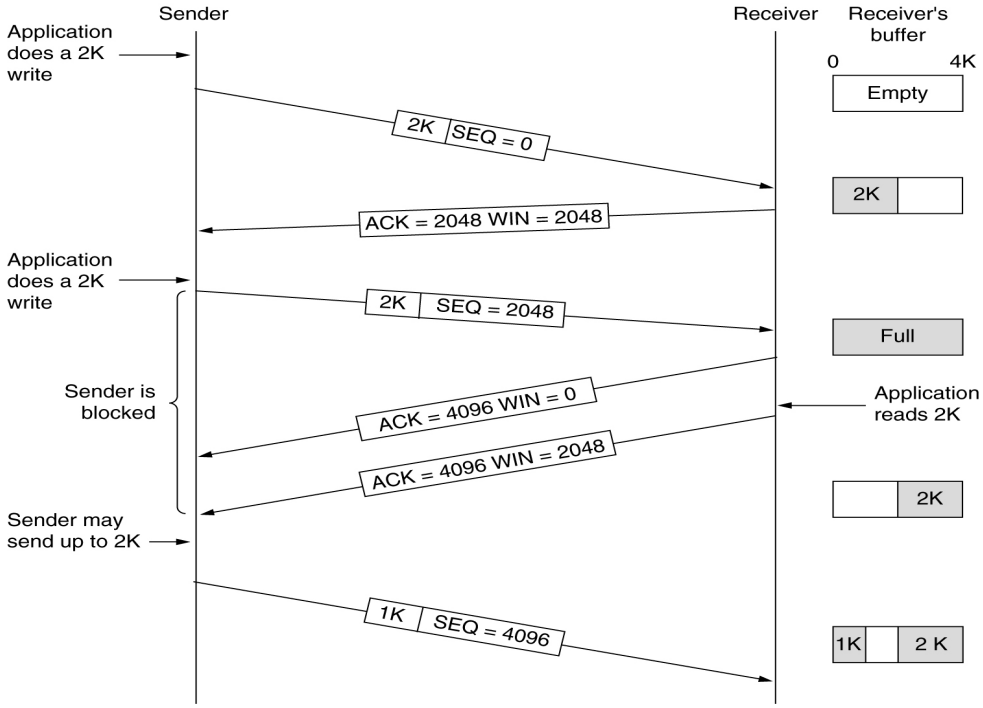
82. Co víte o standardech 802.11 (WiFi) a 802.15 (Bluetooth)?
IEEE 802.11 – WiFi, 802.11b a 802.11.g pásmo 2,4GHz, 802.11a pásmo 5GHz
IEEE 802.11 – Bluetooth, bezdrátová síť pro propojení například mobilů, pda atd. Max. Dosah 100 metrů(teoretický), rychlost 2Mbit/s, v pásmu 2,4GHz

83. Popište, jak se navazuje spojení, ruší spojení a přenáší data v protokolu TCP.

Vytváření spojení:



Přenos dat:



84. Co je to BOOTP protokol, k čemu slouží, jaký je rozdíl mezi BOOTP (bootstrap protokol) a DHCP (Dynamic Host Configuration Protocol).
Viz. Předchozí otázky.

85. Jakou funkci má relační úroveň.
Smyslem vrstvy je organizovat a synchronizovat dialog mezi spolupracujícími relačními vrstvami obou systémů a řídit výměnu dat mezi nimi. Umožňuje vytvoření a ukončení relačního spojení, synchronizaci a obnovení spojení, oznamovaní výjimečných stavů. Do této vrstvy se řadí: NetBIOS, AppleTalk, RPC, SSL. K paketům přiřazuje synchronizační značky které využije v případě vrácení paket (např. z důvodu, že se během přenosu dat poškodí síť) k poskládání původního pořadí.