Spolehlivý dvousměrný logický kanál sestavený nad protokolem TCP z rodiny protokolů TCP/IP
○ Umožnuje své uzavření pro přenos v jednom směru a další odesílaní dat ve směru druhém. Přenášená data pak již nejsou potvrzována přijmací stranou
○ Vždy zajištuje že data při přenosu nemohou být odposlechnuta
○ Vždy zajištuje že přenášená data budou před vlastním odesíláním na síti zašifrována
■ Zajištuje že přenášená data nebudou při přenosu znehodnocena chybou (zejména ztrátou tcp segmentu)
■ Umožnuje své uzavření pro přenos v jednom směru a další odesílaní dat ve směru druhém. Přenášená data pak jsou i nadále potvrzována přijmací stranou
■ Umožnuje řízení toku dat mezi odesílatelem a příjemcem pomocí propagovaní bufferu (window size) ze strany příjemce

Vyberte tvrzeni, ktera charakterizuji (globalni platnou) MAC adresu
○ Je tvorena ctyrmi osmibitovymi cisly
■ Je tvorena sesti osmibitovymi cisly
○ Slouzi k adresaci ciloveho pocitace na 3. vrstve OSI modelu
○ Obsahuje informace nutne pro smerovani paketu smerovace
■ prvni cast urcuje vyrobce, druha seriove cislo
○ Je rozdelena na adresu site a koncoveho uzlu

Ve srovnani DVA a LSA smerovacich algoritmu
■ DVA konverguji typicky dele nez LSA
○ jsou LSA na implementaci jednodusi a vypocetne mene nerocnejsi nez DVA
○ DVA i LSA algoritmy pouzivaji stejny typ metriky a tim je vzdy pocet smerovacu mezi zdrojem a cilem
○ DVA sestavuji smerovaci tabulky na zaklade znalosti topologie site, LSA algoritmy sestavuji smerovaci tabulku na zaklade smerovacich tabulek jinych algoritmu
■ smerovaci informace se v pripade algoritmu DVA mezi smerovaci siri ve stanovenych casovych intervalech . V pripade algoritmu LSA jsou sireny pouze pri jejich zmene.
○ pro rozsahle site jsou vhodnejsi DVA smerovaci algoritmy z duvodu rychle konvergence

Siti prochazi TCP segment se zdrojovym portem 100, cilovym portem 200 a s nastavenymi priznaky SYN a ACK. Tento segment predstavuje
○ zadost o navazani spojeni z klienta z portu 100 na port serveru 200
○ zadost o navazani spojeni z klienta z portu 200 na port serveru 100
○ zamitnuti zadosti o navazani spojeni na port 200 serverem
○ odpoved serveru na zadost o navazani spojeni na port 200 z klienskeho portu 100
○ zamitnuti zadosti o navazani spojeni na port 100 klientem
■ odpoved serveru na zadost o navazani spojeni na port 100 z klienskeho portu 200

Intrusion Detection System je nastroj pro
■ odhaleni utoku na sit nebo operacni sytem
○ sifrovani komunikace ve VPN tunelu
○ Smerovani IP paketu mezi VLANy

○ Sysnchronizaci primarni a sekundarni DNS
○ Prepinani ramcu mezi VLANy

Co muzeme rict o protokolu RIP
■ Predava sousedovi obsah sve smerovaci tabulky
■ Je pouzivan na smerovacich
■ Zjistuje nejkratsi cesty do vsech siti - rozhodujici je pocet preskoku
○ Predava sousedovi tabulky dvojic (MAC adresu, post)
○ Zabranuje vzniku smycek na 2.vstve ISO-OSI Referencniho modelu
○ Je pouzivan na prepinacich

Hlavicka protokolu IP (IPv4)
■ Neobsahuje cisla zdrojoveho a ciloveho portu
■ Obsahuje zdrojovou a cilovou adresu
○ Ma pevnou delku
■ Obsahuje pole TTL, inkrementovane pri pruchodu smerovaci se
■ Obsahuje bitovy priznak MF, individualni fragmentaci
○ Obsahuje kontrolni soucet ramce

Referencni model ISO-OSI
■ Definuje na 1.vrstve fyzicke parametry rozhrani
■ NA 3.vrstve popisuje komunikaci mezi ruznymi LAN pres prostredniky
○ Definuje jako standartni protokol 3. vrstvy protokol TCP
○ Obsahuje 15 vrstev
○ NA 3. vrstve popisuje komunikaci mezi primo propojenymi systememy
○ Definuje na spojove vrstve zpusoby spojovani kabelu (parametry stavu atd.)

DNS - Sluzba domenovych jmen
■ Vyuziva pro komunikaci protokoly UDP i TCP
■ Umoznuje pouzivat domenova jmena o delce komponenty max. 63 znaku
■ Umoznuje preklad IP adres na domenova jmena
○ Realizuje preklad MAC adresy na IP adresu
○ Rozlisuje mala a vekla pismena
○ Pouziva jako oddelovac komponent jmen dvojtecku

Server protokolu POP3
■ Umoznuje cteni obsahu postovni schranky pouze po predchozi autentifikaci

Moznosi sdileni prenosoveho media jsou
■ Casovy multiplex
■ Vlnovy multiplex
■ Frekvencni multiplex
○ Nelze sdilet vubec
○ Napetovym multiplex

Ktere z nasledujich tvrzeni jsou pravdiva o protokolu HTTP?
■ Je provozovan nad transportnim protokolem TCP
■ Je postaven na architekture client-server

○ Je provoznovan nad transportnim protokolem UDP
○ Slouzi pro ziskani IP adresy pri znalosti MAC adresy
○ Pouziva se pro ohlasovani chyb a zvlastnich stavu pri prenosu paketu
○ Pouziva se pro sifrovany prenos WWW stranek

Topologicka databaze, ktera reprezentuje topologii dane site
○ Se pozuva v pripade pouziti algoritmu DVA pro dynamicke smerovani
○ je pouzivana protokolem RIP
■ je vyuzita v dynamiskem smerovani k nalezeni nejkratsich cest do jednotlivych siti
○ Se v dynamickem smerovani vubec nepouziva
○ ?

Server provozuje dve sluzby - DNS a TFTP. Jakym zpusobem rozlisi server, o ktery druh
zadosti se jedna v okamziku kdy prijde zadost od klienta?
■ Prichozi datagram obsahuje cilovy port, ktery urcuje, o kterou sluzbu se jedna

K cemu se v sitich IEEE 802.11 pouziva mechanizmus RTS-CTS?
■ K rezervaci kanalu na dobu zamysleneho vysilani ramce

Problem skryteho uzlu spociva v
■ Neuplne vzajemne slysitelnosti stanic

Pro sítě typu Ethernet (alespoň 10 Mbit/s) se používá následující kabelaž
□ Supervidové optické vlákno (supermode)
■ Tenký koaxiální kabel
■ FTP (kroucená dvoulinka stíněná folií)
□ UTP kategorie 1
■ Dle normy EIA/TIA 568A/B
□ Dle normy ISO 8859-2

O metodě LSA (link state algorithm) lze říci
■ Je příkladem dynamického směrování
■ Směrovače znají topologii sítě
■ Směrovače posílají sousedům směrovací tabulku
□ Pomalu konverguje
□ Je reprezentována směrovacím protokolem RIP
■ Je reprezentována směrovacím protokolem OSPF

Hlavička protokolu TCP*
■ Obsahuje čísla zdrojového a cílového portu
□ Obsahuje kontrolní součet, který ale nemusí být vyplněn
■ Obsahuje pole jednobitových příznaků určených k řízení spojení
□ Obsahuje číslo protokolu, neseného v TCP segmentu
■ Obsahuje číslo posledního správně přijatého oktetu
□ Je vkládána do rámců přímo na začátek datového pole

Přepínač (SWITCH)
■ Posílá rámec Ethernetu s MAC adresou FF:FF:FF:FF:FF:FF na všechna rozhraní.
■ Vybírá rozhraní, na něž bude rámec zaslán , podle cílové MAC adresy.
□ Směřuje pakety na základě IP adresy cíle
□ Má na každém portu přiřazenu IP adresu
■ Umožňuje definovat virtuální LAN sítě (VLANy)
■ Může posílat rámce z různých VLANů jinému přepínači pomocí TRUNK portů

SMTP server komunikuje
□ s POP3 serverem, od kterého přijímá e-maily
■ se SMTP klientem (user agent)
□ jak s POP3, tak s IMAP serverem
■ s jiným SMTP serverem.
□ s IMAP serverem
□ s IMAP klientem

Pro přenos dat se běžně používají následující typy modulací.
■ Amplitudová
□ Kvantová
■ Frekvenční
■ Fázová
□ Doplerovská
□ Binární

Metody nedeterministického přístupu ke sdílení kanálu jsou:
□ Centrální řízení
□ Distribuované řízení předávání …..
■ Aloha
□ Virtuální logický kruh
■ Metoda CSMA/CD
□ Binární vyhledávání

O metodě DVA (distance vector algorithm) lze říci:
■ Je příkladem dynamického směrování
□ Směrovače znají topologii celé sítě
■ Směrovače poskytují sousedům směrovací tabulku.
■ pomalu konverguje
■ Je reprezentován směrovacím protokolem RIP
□ Je reprezentován směrovacím protokolem OSPF

Směrovač (router)
□ Posílá rámec Ethernetu s MAC adresou FF:FF:FF:FF:FF:FF na všechna rozhraní.
□ Vybírá rozhraní, na něž bude rámec zaslán , podle cílové MAC adresy.
■ Směřuje pakety na základě IP adresy cíle
□ Zvyšuje pole TTL každého procházejícího paketu o nakonfigurovanou hodnotu.

■ Má na každém portu přiřazenou IP adresu.
□ Musí mít celou směrovací tabulku ručně definovanou administrátorem (kromě připojených sítí.)

SMTP server*
■ Přímá e-maily od poštovního klienta (user agent)
□ Odesílá e-maily poštovním klientem (user agent)
□ V případě neexistence schránky příjemce zasílá klientovy zprávu ICMP Destination Unreachabble
■ Může navazovat TCP spojení s jinými SMTP serverem.
■ Přijímá e-maily od jiného SMTP serveru.
□ Posílá e-maily jiného SMTP serveru jako UDP datagramy.

Topologie sítí jsou
■ Sběrnice
■ Hvězda
■ Distribuovaná hvězda (strom)
□ Čtverec
■ Kruh
□ Polynomiální

Topologie sítě Ethernet jsou
■ Sběrnice
■ Hvězda
■ Distribuovaná hvězda (strom)
□ Čtverec
□ Kruh
□ Polynomiální

Protokol RIP*
■ Běží mezi směrovači (ROUTERY)
□ Běží mezi přepínači (SWITCHi)
■ Předává sousedovi směrovací tabulku
□ Předává sousedovi tabulku dvojic <MAC adresa, port>
■ Počítá nejkratší (nejlevnější) cesty do všech sítí
□ Zabraňuje vzniku smyček na 2. vrstvě

Následující typy záznamů jmenných serverů mají tyto významy
□ SOA – Definuje všechny neautoritativní servery pro danou doménu.
■ NS – určuje autoritativní jmenný server pro danou doménu
□ MX – určuje WINS server (jmenný server pro protokol MS NetBios)
□ A – přiřazuje k IP adrese k doménové jméno
■ PTR – přiřazuje ke speciálnímu zápisu IP adresy doménové jméno
■ CNAME – určuje alias pro dané doménové jméno

Ve kterých situacích se posílá odesílateli ICMP zpráva?

□ Pokud velikost paketu přesáhne 64 kB a je zakázána fragmentace.
□ Když se paket na některé lince ztratí.
□ Pokud velikost paketu přesáhne délku datového pole rámce některé linky a je povolena fragmentace.
■ Pokud velikost paketu přesáhne délku dat.pole rámce některé linky a je zakázaná frag.
■ Pokud směrovač příjme paket s TTL=1 a podle směrovací tabulky jej má přeposlat dalšímu směrovači.
□ Jako odpověď na DNS dotaz

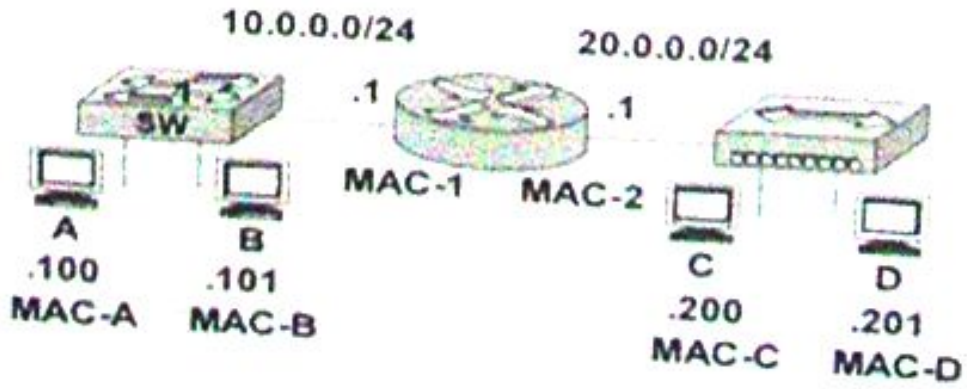
Pro odesílání a příjem elektronické pošty slouží následující protokoly
■ SMTP
□ SNMP
■ POP3
■ IMAP
□ FTP
□ BOOTP

Stanice X příjme TCP segment s nastaveným příznakem ACK a s těmito hodnotami v záhlaví:

Sequence number: 1000 Acknowledge number: 500 Window: 100

Na základě této informace stanice X smí odeslat bajty se sekvenčními čísly
a) 10001 - 1500
b) 501 – 600
c) 501 – 1000
d) 101 – 500
e) 101 – 1000

U směrovacích protokolů třídy Distance vector posílají směrovače
a) informaci o přilehlých linkách vždy při změně stavu
b) obsah své směrovací tabulky jen tehdy, když dojde k její změně
c) periodicky informaci o přilehlých linkách
d) periodicky obsah své směrovací tabulky



Síť je nakonfigurovaná podle obrázku (MAC adresy jsou označeny pro přehlednost symbolicky). Všechny stanice mají správně nakonfigurovány IP adresy, masky podsítě

i výchozí brány (default gateway). Jaké zdrojové a cílové MAC a IP adresy budou v rámci, který dorazí na cílovou stanici při zaslání paketů.

a) ze stanice A na stanici C b) ze stanice B na stanici A

	Zdrojová MAC adr.	Cílová MAC adr.	Zdrojová IP adr.	Cílová IP adr.
A – C	MAC-A	MAC-C	10.0.0.100	20.0.0.200
B – A	MAC-B	MAC-A	10.0.0.101	10.0.0.100

Referenční model ISO-OSI

□ Obsahuje 10 vrstev
■ Definuje na 1. vrstvě fyzické parametry rozhraní
□ Definuje na spojové vrstvě (link layer) způsoby svařování kabelů
■ Na 3. vrstvě realizuje směrování mezi sítěmi
■ Pro přenos dat na 4. vrstvě může využívat metodu plovoucího okénka (sliding window)
□ Definuje jako standardní protokol 3. vrstvy protokol IP

Sériový přenos

□ Je synchronní, asynchronní nebo antisynchronní.
□ Zasílá v jednom taktu hodin podle implementace slovo o délce 8, 16 nebo 32 bitů
■ V synchronním režimu udržuje neustálou časovou synchronizaci zdroje a cíle.
□ Používá vždy pro přenos dat start bity a stop bity.
□ Po vypršení časového limitu vždy znovu posílá nepotvrzené znaky
■ V synchronním režimu používá křídlových značek pro označení hranic datové jednotky.

9. Služba doménových jmen (DNS)

■ Umožňuje používat doménová jména o délce komponenty max. 63 znaků
□ Rozlišuje malá a velká písmena (je case-sensitive)
□ Používá jako oddělovač komponent jmen dvojtečku
■ Využívá pro komunikaci protokoly UDP i TCP
□ Realizuje překlad MAC adresy na IP adresu
■ Umožňuje překlad IP adres na doménová jména

10. Co se stane, když router nemůže doručit IP paket?

■ Paket je zahozen.
□ Router paket uchová v bufferu do doby, než se dobudují směrovací tabulky.
■ Je poslána chybová zpráva ICMP původnímu odesílateli
□ Je poslána chybová zpráva ICMP původnímu cíli
□ Paket je vrácen na předchozí router.
□ Paket je zaslán zpět původnímu zdroji.

11. Pro stahování binárních souborů z Internetu se běžně používají tyto protokoly

□ SNMP
■ HTTP
■ FTP
■ HTTPS

□ BOOTP
□ DHCP

7. Jednoznačnou IP adresu (Ipv4) může stanice získat následujícím způsobem
■ Pomocí protokolu DHCP
□ Pomocí protokolu HTTP
■ Protokolem BOOTP
□ Protokolem ICMP (IP address request)
□ Pomocí protokolu ARP
□ Od nejbližšího DNS serveru nalezeného pomocí zprávy vyslané broadcastem

8. Jak může router získat informace o cestách do cílových sítí?
□ Switche informují okolní routery, které sítě admin nakonfiguroval do jejich tabulek
■ Informace jsou vloženy staticky síťovým administrátorem.
□ Cesty se získávají z informací shromážděných v ARP tabulkách.
□ Routery a switche si vzájemně přeposílají informace o sítích, které znají, pomocí směrovacích protokolů.
□ Informace jsou odeslány jako broadcast switchem pokaždé, když je k němu připojen nový segment sítě.
□ Informace lze získat aktivními dotazy protokolu ARP

Jakým způsobem mohou směrovače získat informace o možných cestách k cílovým sítím
■Informace jsou vloženy staticky administrátorem
□ Cesty se získávají z informací shromážděných v ARP tabulkách
□HUBy (opakovače) informují okolní směrovače, které site administrator nakonfiguroval do jejich tabulek
□Informace jsou odeslány jako broadcast přepínačem pokaždé, když je k němu připojen nový segment site
■ Informace se předávají pomocí směrovacích protokolů
□ Informace lze získat aktivními dotazy protokolu ARP

9. V hlavičce protokolu TCP jsou obsaženy následující položky
■ Bitový příznak FIN, požadující ukončení komunikace v jednom směru
□ Bitový příznak NAK určující, že se jedná o negativní potvrzení
□ Bitový příznak NOP, definující, že se jedná o paket, udržující spojení (keep-alive)
■ Bitový příznak RST, který vynucuje ukončení spojení v obou směrech
■ Bitový příznak SYN, který se používá při navazování spojení
■ Pole určující aktuální šířku přijímacího okénka

10. Metody deterministického přístupu ke sdílenému kanálu jsou
■ Centrální řízení
■ Distribuované řízení předáváním pověření
□ ALOHA
■ Virtuální logický kruh
□ Metoda CSMA/CD
■ Binární vyhledávání

11. Které z následujících tvrzení jsou pravdivá o protokolu HTTP ?
■ Je postaven na architektuře client-server
□ Slouží pro získání IP adresy, při znalosti MAC adresy.
□ Je provozován nad transportním protokolem UDP.
□ Používá se pro šifrovaný přenos WWW stránek
□ Využívá se pro ohlašování chyb a zvláštních stavů při přenosu paketů.
■ Je provozován nad transportním protokolem TCP.

7. **MAC adresa (globálně platná)**
■ Je rozdělena na dvě části, určující výrobce a sériové číslo
□ Slouží k adresaci cílového počítače na 3. vrstvě OSI modelu
□ Je rozdělena na adresu sítě a koncového uzlu
□ Je tvořena čtyřmi osmibitovými čísly
■ Je na Ethernetu tvořena šesti osmibitovými čísly
□ Obsahuje informace nutné pro směrování paketů směrovačem

8. **Metoda Sliding window (plovoucí okénko)***
■ Ve variantě GO-BACK-N požaduje retransmisi paketů od prvního ztraceného
□ Udržuje v přijímacím okénku dosud nepotvrzené pakety.
■ Používá na odesílající straně okénka zaslané pakety
□ Vždy vyžaduje zasílání negativních potvrzení (NAK)
■ Po vypršení časového limitu ve variantě GO-BACK-N znovu posílá všechny dosud nepotvrzené pakety
□ Je použita pro přenos dat na internetu protokolem UDP

Druhy směrování jsou
■ Statické (neadaptivní) směrování
■ Hierarchické směrování
□ Geografické směrování
■ Distribuované směrování
□ Topologické směrování
■ Dynamické směrování

Co jsou to výhody použití statického směrování oproti dynamickému?
■ menší zatížení procesoru routeru
■ úplná kontrola nad výběrem použitých cest
□ menší námaha při konfiguraci
□ vyšší adaptabilita při změně topologie
■ vyšší bezpečnost než při použití směrovacího protokolu
□ možnost použití i na přepínačích s podporou VLAN

Pokud nemáte k dispozici žádný e-mailový klient, jakým způsobem si můžete nahlédnout do své emailové schránky?
□ Použiji příkaz ping s volbou –t MX a adresou serveru, kde je má poštovní schránka
□ Využiji program telnet a připojím se na port 25 (port SMTP serveru)
□ Neexistuje žádný způsob, kterým lze přečíst obsah emailové schránky-
□ Využiji program FTP a připojím se na port 110 (port POP3 serveru)
■ Využiji program telnet a připojím se na port 110 (port POP3 serveru)

□ Použiji protokolu MDP (Mail Download Protocol) pomocí příkazu mdp

Při zjišťování cesty sítí příkazem traceroute

a) odesílatel postupně zvětšuje pole TTL v hlavičce IP paketu a přijímá zprávu ICMP Echo Reply
b) odesílatel postupně snižuje pole TTL v hlavičce IP paketu a přijímá zprávu ICMP Echo Reply
c) odesílatel postupně snižuje pole TTL v hlavičce IP paketu a přijímá zprávu ICMP Time Exceeded
d) odesílatel postupně zvětšuje pole TTL v hlavičce IP paketu a přijímá zprávu ICMP Time Exceeded

Kanál je sdílen metodou distribuovaného binárního vyhledávání. V případě současného vysílání různé hodnoty více stanicemi bude na kanále logická nula. O kanál soutěží stanice A,B a C s adresami:
A: 1101010
B: 1010010
C: 1010101
Určete, při kterém bitu adresy je rozhodnuto, která stanice získá přístup ke kanálu a která to bude.

Fragmentované pakety sestavuje podle polí Identification, Fragment Offset a

a) zdrojové MAC adresy výhradně cílová stanice.
b) zdrojové MAC adresy kterýkoliv router na cestě.
c) zdrojové IP adresy výhradně cílová stanice.
d) zdrojové IP adresy kterýkoliv router na cestě.

Co lze říci o MAC adresách 00:BB:BB:BB:00 a 00:BB:BB:BB:01?

a) jde o dvě varianty broadcast adresy.
b) jde o adresy stanic na stejném segmentu sítě.
c) jde o adresy přidělené témuž výrobci.
d) jde o MAC adresy vyhrazené pro funkci protokolu ARP.

V TCP segmentu se zdrojovou adresou 10.0.1.10 a cílovou adresou 10.0.2.20 je nastaven příznak RST dochází k:
a) Násilnému ukončení spojení (oboustranně)
b) Jednosměrnému ukončení z 10.0.1.10
c) Jednosměrnému ukončení z 10.0.2.20
d) Upozornění na poškození

POP3 server
a) Slouží typicky k odesílání el. pošty
b) Je prvním serverem přenášející zprávu
c) Umožňuje příjem el. pošty pouze po autentizaci
d) Se připojuje k DNS serveru

SMTP server

a) Slouží typicky k příjmu el. pošty
b) Při průchodu zprávy vloží hlavičku Received určující, že zpráva prošla
c) Umožňuje zaslaní zpráv el. pošty pouze po autentizaci USER a PASS
d) **Se připojuje k DNS serveru, kde zjišťuje podle MX záznamu POP3 doménu, na nějž se připojí a odešle mu zprávu**

Příkladem protokolů 7 vrstvy modelu RM OSI (celá kombinace)

a) TFTP, HTTP, FTP, ICMP
b) TCP a UDP
c) IP a IPX
d) DNS, HTTP, TFTP

10. Ve kterých situacích se posílá odesílateli ICMP zpráva?

□ Pokud velikost paketu přesáhne 64 kB a je zakázána fragmentace.
□ Když se paket na některé lince ztratí.
□ Pokud velikost paketu přesáhne délku datového pole rámce některé linky a je povolena fragmentace.
■ Pokud velikost paketu přesáhne délku dat.pole rámce některé linky a je zakázaná frag.
■ Pokud směrovač příjme paket s TTL=1 a podle směrovací tabulky jej má přeposlat dalšímu směrovači.
□ Jako odpověď na DNS dotaz

Protokol TFTP

■ Umožňuje stanicím stáhnout soubor pro start OS ze serveru
□ Poskytuje masku podsítě
□ Vyžaduje uživatelské jméno a heslo pro autentizaci
■ Umožňuje nahrávat soubor na server
□ Využívá protokol TCP
■ Používá potvrzovacího schématu stop-and-wait

Protokol TFTP

■ Je využíván pro svou jednoduchost k načítání souboru pro start OS ze server (network boot)
■Přenáší data ze serveru ke klientovi nebo od klienta k server
□Kvůli omezení velikosti dat v UDP datagramu může přenášet pouze soubory do velikosti 64 KB
■ Používá algoritmus stop and wait
■ Využívá nezašifrované spojení

Technologie ASDL

□ Je vhodná pro poskytovatele služeb díky velkým přenosovým rychlostem
■ Umožňuje přenášet data na vzdálenosti řádově jednotek km po klasickém vedení telefonní sítě
□ Má asymetrické přenosové rychlosti rychlejší k poskytovateli pomalejší opačně
■ Přizpůsobuje skutečnou rychlost kvalitě linky
□ Vylučuje současné použití analogového telefonu
■ Používá splitter pro rozdělení pásma

Sítě typu Ethernet jsou podle normy IEEE 802.3
■ 10Base2 – sítě Ethernet na tenkém koax kabelu typu RG58
□ 100BaseSX – plně duplexní přenos po 1 metalickém vodiči
■ 10BaseT a 100BaseT – metalické sítě na kroucené dvojlince
□ 100BaseFX – optické trasy 10Mbit/s
□ 10BaseGLX – přenos po klasické telefonní dvojlince
□ 10GBaseT – optické sítě 10000 Mbps full duplex

Protokol ICMP IPv4 lze využít k
□ Přiřazení MAC adresy IP adrese (address resultion)
□ Přesměrování provozu pro určitou sít na jinou bránu
■ Kontrola dostupnosti PC (echo request)
■ Informaci o nedoručitelnosti datagramu (destination unreachable)
■ Informaci o překročení počtu směrování (time exceeded)
□ Informaci o počtu paketu zahozených směrovačem (router drop rate)

Protokol FTP
□ UDP data
□ ICMP data
■ TCP data
□ UDP řídící
□ ICMP řídící
■ TCP řídící

Použití ISDN pro přenos dat přes přípojku BRI dává tyto možnosti
□ Datový kanál s přenosovou rychlostí až 2Mbps
■ Zřízení spojení cca do 1 sekundy
□ Vetší přenosovou rychlost ve směru ke koncovému zařízeni (downstream) než ve směru do sítě (upstream)
□ Možnost svazkování až 16 kanálů
■ Možnost pomalého přenosu po kanále D pokud to operátor sítě ISDN podporuje
□ Současné použití analogového telefonu na téže lince

Virtuální privátní sítě
□ Jsou sítě založené na VLAN které používají privátních IP adres
■ Používají sdílenou veřejnou infrastrukturu
□ Lze na 3 vrstvě realizovat s použitím SSL
■ Lze na 3 vrstvě realizovat s použitím IPSec
□ Z principu nedovolují provozovaní jiných protokolů než IP
□ Jsou nákladnější na vybudování a správu než privátní infrastruktura

Překlad adres NAT
□ Při použití statického NAT je nutné použít ve vnitřní síti statického směrování
□ NAT dovoluje stanicím bez podpory protokolu IP komunikovat s Internetem
■ Zvyšuje bezpečnost skrytím vnitřní struktury sítě
□ Zvyšuje bezpečnost vnější sítě před útoky
■ Při použití čistého dynamického NAT nelze ve vnitřní síti provozovat servery přístupné z Internetu
□ Ve vnitřní síti za NAT musí být použity privátní IPadresy, jinak nebude fungovat

Protokol pro služby www
□ Ve verzi HTTP 1.0 více dokumentů v 1 spojení
■ Ve verzi HTTP 1.1 více dokumentů v 1 spojení
□ Ve verzi HTTP 1.0 data šifruje
□ Ve verzi HTTP 1.1 data šifruje
■ K šifrování dat ve verzi 1.0 i 1.1 je třeba HTTPS
□ Umožňuje přenos binárních dat až od verze 1.1

Bezestavová filtrace
■ Každý paket UDP
■ Každý paket TCP
■ Každý paket IP

Protokol UDP
■ Obsahuje čísla zdrojového a cílového portu
■ Obsahuje CRC, který nemusí být vyplněn

Přenosové medium lze sdílet
■ Frekvenčním multiplexem
■ Časovým multiplexem
■ Vlnovým multiplexem

šifrováni
■ zajištění integrity při přenosu dat, že nebyly změněny
■ symetrické šifrováni bývá rychlejší než privátní a veřejný klíč

IP adresa je
□ Je rozdělena na dvě části, určující výrobce a sériové číslo
■ Slouží k adresaci cílového počítače na 3. vrstvě OSI modelu
■ Je rozdělena na část adresy sítě a část adresy koncového uzlu
■ Je tvořena 4mi osmibitovými čísly
□ Je na Ethernetu tvořena 6ti osmibitovými čísly
□ Obsahuje informace nutné pro směrování paketu přepínačem

Spanning Tree
□ Běží mezi směrovači
■ Běží mezi přepínači
□ Předává sousedovi směrovací tabulku
□ Předává sousedovi tabulku dvojic (MAC adresu, port)
■ Počítá nejkratší (nejlevnější) cesty ke kořeni stromu
■ Zabraňuje tvorbě smyček na 2. vrstvě

Hlavička protokolu IP (IPv4)
■ Obsahuje zdrojovou a cílovou adresu
□ Obsahuje čísla zdrojového a cílového portu
□ Obsahuje zdrojový příznak FF (force fragments), vynucující fragmentaci
■ Obsahuje kontrolní součet
■ Obsahuje pole TTL (time to live), při jehož vynulování je paket zahozen

■ Může být proměnné délky

Jakým způsobem můžeme charakterizovat asymetrický kryptografický systém?
■ Používá dva klíče jako vzájemně související pár
□ Pro větší zabezpečení šifruje data na zdroji dvěmi klíči
□ Používá jeden sdílený klíč
□ Používá algoritmy DES, 3DES nebo AES
■ Používá jeden klíč pro šifrování a druhý pro dešifrování
□ Používá efektivní algoritmy, které nejsou náročné na výpočet a jsou snadno implementovatelné hardwarově

Ve srovnání DVA a LSA směrovacích algoritmů
■ Jsou DVA na implementaci jednodušší a výpočetně méně náročné než LSA
□ LSA výrazně déle konvergují než DVA
■ Směrovací informace se v případě algoritmů DVA mezi směrovači šíří ve stanovených časových intervalech (např. 30s) V případě LSA jsou šířeny pouze při jejich změně
■ LSA sestavují směrovací tabulku na základě znalosti topologie sítě, DVA algoritmy sestavují směrovací tabulku na základě směrovacích tabulek jiných směšovačů.
□ DVA i LSA algoritmy používají stejný typ metriky a tím je vždy počet směšovačů mezi zdrojem a cílem
■ Pro rozsáhlé sítě jsou vhodnější LSA směrovací algoritmy z důvodů rychlé konvergence, stability

Které z následujících protokolů můžeme pomocí ACL zakázat, aniž bychom ohrozily funkčnost zasílání a příjmu elektrické pošty?
□ POP3
□ SMTP
■ ICMP
■ FTP
□ DNS
■ TFTP

User Datagram Protokol (UDP)
□ Je protokol druhé vrstvy
□ vždy zajišťuje spolehlivý přenos dat sítí
■ je používán při přenosu dat nepotvrzovanou datovou službou
■ v hlavičce obsahuje pole kontrolního součtu
□ v hlavičce obsahuje číslo zdrojového a cílového portu. Tyto položky však nejsou povinné a nemusí být použity
□ používá se pouze pro přenos zvuku v IP sítích.

Jaká je největší vzdálenost mezi dvěma aktivními prvky u 100BaseT Ethernetu podle standartu, když používámé kabely UTP5?
a) 82 metrů
b) 100 metrů
c) 185 metrů
d) 300 metrů
e) 305 metrů

Protokol Spanning Tree slouží k
a) vyhledání nejkratších cest z každého přepínače do každého segmentu sítě
b) zablokování spojů tvořících smyčky mezi přepínači
c) vyhledání nejkratších cest z každého směrovače do každého segmentu sítě
d) zablokování spojů tvořících smyčky mezi směrovači
e) zablokování spojů mající nejdelší cestu ke kořenu stromu

Který z následujících výrazů označuje čas, mezi odesláním paketu odesílatelem a jeho přijetí příjemcem?
a) šířka pásma (bandwidth)
b) zpoždění (delay)
c) time-to-live (TTL)
d) kontrolní součet
e) rozptyl (jitter)

Metrika v algoritmech DVA (Distance Vector Algorithm)
□ je číslo, které reprezentuje kvalitu linky k sousednímu směrovači
■ je číslo, které udává počet přeskoků (hop count) na cestě od zdroje k cíli
□ určuje počet bitů IP adresy, které jsou použity pro pro adresaci sítě
■ bývá omezená maximální hodnotou, při jejímž překročení se směrovací informace považuje za neplatnou
■ se mění v závislosti počtu směrovačů ve zvolené cestě sítí
□ je zcela nezávislá na počtu směrovačů ve zvolené cestě sítí

Protokoly 7. Vrstvy OSI modelu jsou (všechny ve variantě)
a) FTP, TFTP a HTTP
b) TCP a UDP
c) IP a IPX
d) DNS, ARP, DHCP a BOOTP
e) TCP, UDP a IP

Dynamické směrování zajišťuje automatické šíření směrovací informace mezi směrovači vždy směrovačům zpřístupňuje znalost topologie síťě je jedním z přístupů, jak zajistit naplnění směrovací tabulky směrovače je jedním z přístupů, jak zajistit naplnění přepínací tabulky přepínače umožňuje vzdálenou správu přepínačů umožňuje rozšíření směrovací tabulky mezi směrovači

Která tvrzení z oblasti bezpečnosti sítí jsou platná?
□Šifrování se v praxi realizuje výhradně na prezentační vrstvě
□Vrstva SSL zajišťuje šifrování na 2.vrstvě OSI RM
■IPSec zajišťuje šifrování na 3.vrstvě OSI RM
□Pro šifrování provozu v Internetu je nejefektivnější šifrování na 2.vrstvě OSI RM
■Šifrování může být technicky realizováno i na více vrstvách OSI RM současně
■Při asymetrickém šifrování lze šifrivat privátním klíčem a dešifrovat veřejným nebo opačně

Server provozuje dvě služby – HTTP a FTP. Jakým způsobem rozliší server, o který druh spojení se jedná, v okamžiku, kdy zaregistruje pokus o připojení?
c) Příchozí segment obsahuje cílový port, který určuje, o kterou službu se jedná.

Doplňte: Protokol ARP slouží
k získání adresy 2. vrstvy na základě známé adresy 3. vrstvy OSI-RM

Ze stanice s MAC adresou 01:23:45:67:89:AB a IP adresou 1.2.3.4/24 je vysílán ARP požadavek na zjištění adresy 2.vrstvy OSI-RM stanice s IP 1.2.3.2, jejíž adresa je 0A:BC:DE:F1:23:45.
Ramec s požadavkem bude zaslán na cílovou c) MAC adresu FF:FF:FF:FF:FF:FF

Směrovací tabulka musí vždy obsahovat tyto sloupce:
■IP adresu cílové stanice sítě, kterou daný daný řádek tabulky reprezentuje
□IP adresu počítače, který adresu poslal
■Metriku, která vždy reprezentuje počet směrovačů na cestě k cíli
■Rozhraní, kterým bude paket vysílán nebo IP adresu souseda, kterému bude paket poslán
□Seznam protokolů, které daná síť podporuje
□Porty protokolu TCP, které mohou být použity v poli cílového portu v hlavičce TCP

Ve srovnání protokolů TCP a UDP platí
□Protokol TCP zatěžuje síť při přenosu malého množství daleko méně než protokol UDP
■Protokol TCP je na rozdíl od protokolu UDP schopen zajistit, že přenášena data budou k příjemci vždy doručena bez případných chyb vzniklých jejich přenosem sítí.
□Protokol UDP má mnohem delší záhlaví než protokol TCP
■Oba protokoly používají pro identifikování zdrojového a cílového portu šestnáctibitová čísla nesená v jejich záhlaví.
■Protokol UDP může mít jako cílovou adresu uvedenou adresu broadcastovou nebo multicastovou. Protokol TCP toto neumožňuje.
□Hlavička obou protokolů je stejná, zajišťuje však síťové služby

NAT
□Znamená Network Access Tunnel
□Slouží pro bezpečné vzdálené připojení do podnikové sítě
■Jedná se o překlad IP adres
■Umožňuje změnu cílového portu v TCP segmentu
■Umožňuje změnu zdrojového portu v TCP segmentu
□Šifruje data transparentní vrstvě OSI modelu

Protokol TFTP
■Používá na 4.vrstvě protokol UDP
■Je využíván pro svou jednoduchost k načítání souboru pro start OS se serveru (network boost)
□Kvůli omezení velikosti dat v UDP datagramu může přenášet pouze soubory do velikosti 64KB
□Používá sliding window
□Přenáší data pouze ze serveru ke klientovi
□Využívá zašifrované spojení

Přenos v přeloženém pásmu broadband
■ umožnuje přenášet více kanalů jedním přenosovým mediem
□ umožnuje přenos ale za cenu zhoršení využití přenosového media
□ znamena využití jiného ne definovaného přenosového media

□využívá se zejména v sitích LAN s technologií ethernet
□Využívá vždy větší šířku pásma než přenos v základním pásmu
□se používá převážně pro datové přenosy v současných sitích LAN

Protokol TFTP
■ Používá na 4.vrstvě protokol UDP
■Je využíván pro svou jednoduchost k načítání souboru pro start OS se serveru (network boost)
□Kvůli omezení velikosti dat v UDP datagramu může přenášet pouze soubory do velikosti 64KB
□Používá sliding window
□Přenáší data pouze ze serveru ke klientovi
□Využívá zašifrované spojení

Která tvrzení jsou pravdivá o protokolu DHCP

Jde o protokol pro dynamické přidělovaní MAC adres klientům
■Je postaven na architektuře klient server
Slouží ke kontrole dostupnosti cílového počítače
slouží pro zablokování smyček mezi přepínači
■Jde o protokol pro (dočasné) přidělování IP adres a ostatních parametrů …
Jde o protokol pro vybírání obsahu poštovních schránek

Pro protokol NTP platí:
□Pracuje s místními časy a časovými zónami
■Podporuje hierarchickou organizaci NTP serverů
■Je určen k synchronizaci časů v siti s proměnným přenosným zpožděním
□Je určen k synchronizaci časů pouze v síti s konstantním přenosným zpožděním
□Je použitelný pouze na synchronních WAN linkách

Při navazování TCP spojení:
□Se vždy nejdříve před otevřením dvousměrného logického kanalu jeho parametry vyjednávají pomocí protokolu UDP
□Je potřeba dohodnou počáteční sekvenční čísla použita pro potvrzování přenášených dat pro oba směry nezavisle
■Je v prvním tcp segmentu který komunikaci zahajuje, nadstaven pouze příznak SYN v jeho hlavičce
□Se nejdříve pomocí TCP segmentu s nadstaveným příznakem QOSv jeho hlavičce testuje kvalita linky
■Jsou počáteční sekveční čísla která jsou použita pro potvrzování přijatých dat generována nahodně
□Je nezbytné aby bylo číslo zdrojového a cílového portu stejné

Nad danou topologií provozujeme dynamické směrování založené na algoritmu DVA. V dané topologii jsou všechny její části vzájemně dosažitelné. Jaká omezení platí pro danou síť, pokud vzdáleností rozumíme počet přeskoků?

■maximální vzdáleností mezi směrovači v síti je vždy omezena na hodnotu, ´která je dána maximální velikostí metriky považované směrovacím protokolem za platnou

□maximální počet směrovačů v síti je omezen tím, jak směrovací protokol ve svých zprávách reprezentuje hodnotu metriky

□maximální vzdálenost mezi směrovači v síti není nijak omezena

□maximální počet směrovačů v síti je vždy omezen na hodnotu , která je dána maximální velikostí metriky považované směrovacím protokolem za platnou

□maximální vzdálenost mezi směrovači v síti je rovna polovině počtu směrovačů v této síti

■maximální počet směrovačů v síti není směrovacím protokolem omezen (pokud není technicky omezena velikost směrovací tabulky)

Překlad adres (NAT) má následující vlastnosti

□ Ve vnitřní síti za NAT musí být vždy použity privátní IP adresy, jinak NAT nebude fungovat

□ Při použití statického (cílového) NATu je nutné použít ve vnitřní síti statické směrování

■ Může mapovat adresy vnitřní sítě na několik adres z vnější sítě

□ Při použití statického (cílového) NATu nelze ve vnitřní síti provozovat servery přístupné z Internetu

□ NAT dovoluje stanicím bez podpory protokolu IP komunikovat s Internetem

■ Mírně zvyšuje bezpečnost skrytím vnitřní struktury sítě

Standard IEEE 802.11i definuje

□ Rádiovou vrstvu pro přenos přes infračervené světlo

■Bezpečnostní mechanizmy pro bezdrátové sítě

□ Standart AES jako potvrzovací schema pro přenost rámců

□ Rádiovou vrstvu pro přenos metodou FHSS

□ Rádiovou vrstvu pro přenos metodou DSSS

□Podmínky provozu sítí v pásmu 5GHz

Vyhledávání v DNS může probíhat takto

□Při dotazu na jméno, které není pod správou dotazovaného NS, NS zkusí odpověď z náhodně vybraného DNS serveru

□Při dotazu na jméno, které není pod správou dotazovaného NS, může NS dotaz odmítnout

■Při dotazu na jméno, které není pod správou dotazovaného NS,může NS použít rekurzivní vyhledávání a vrátit neautoritativní odpověď

□Vyhledávání v DNS databázi provádí SW klienta (resolver) nebo rekurzivní DNS server

■ Pokud dotazovaný DNS server je autoritativní pro dotazované jméno, odpoví přímo tento server.

■ Klient může mít přiřazení IP adresy k některým doménovým jménům předkonfigurované staticky. V tomto případě se DNS server vůbec nekontaktuje.

Protokol Spanning tree mohou provozovat

□přepínače a směrovače společně pro každý VLAN

□rozbočovače a přepínače společně pro každý VLAN

■přepínače pro každý VLAN

□rozbočovače a přepínače samostatně pro každý VLAN
□ přepínače a směšovače samostatně pro každý VLAN

Asynchronní (arytmický) sériový přenos:
□ znamená, že pro každý směr je definována jiná přenosová rychlost
□ vyžaduje linku pro hodinový signál
□ vyžaduje pouze start bit
□ udržuje stálou synchronizaci hodin mezi vysílačem a přijímačem
■ potřebuje start/stop bity
■ přenáší data po jednotlivých znacích

Bezestavová filtrace provozu má následující charakteristiky
□ Každý paket TCP protokolu je kontrolován s ohledem na ostatní pakety téhož spojení
□U TCP spojení nelze rozlišit, zda jde o první paket spojení
■Každý paket UDP protokolu je kontrolován bez vazby na ostatní pakety
□ Neumožňuje rozlišit různé typy zpráv protokolu ICMP
□Je špatně škálovatelná, protože její efektivita závisí na počtu TCP spojení procházejících routerem provádějícím filtraci
■Každý paket IP protokolu je kontrolován bez vazby na ostatní pakety

Nejdelší použitelná maska podsítě při podsíťování je
a) 255.255.255.252
b) 255.255.255.255
c) 255.255.255.250
d) 255.255.255.248
e) 255.255.255.254

Příkladem protokolů 3.vrstvy OSI modelu jsou (všechny protokoly ve variantě)
a) FTP,TFTP,HTTP
b) IP,TCP,UDP
c) IP
d) IP,ARP,DHCP
e) TCP a UDP

Ve kterých typech Ethernetu může dojít ke kolizi
□ 100BaseT full duplex
■10Base2
□ 10BaseT full duplex
■ 100BaseT half duplex
□ 10GBaseT
■ 10Base5

Které činnosti musí vykonávat spanning tree pro správnou funkčnost
□Každé zařízení počítá strom nejkratších cest ke všem ostatním zařízením (a k nim připojeným sitím) pomocí Dijkstrova Algoritmu

□Donutí směrovače vyměnit si své směrovací tabulky se svými sousedy, z těchto informací směrovač zjistí topologii sítě a ví které rozhraní má zablokovat
■Každé 2 sekundy root generuje zprávu která se šíří po stromu směrem dolů
□Každý směrovač sleduje stav a funkčnost linek připojenýmch k němu při změně okamžitě šíří informace všem ostatním směrovačům
■Vytvoření stromu nejkratších (nejlevnšíjších) cest od kořene ke každému mostui (respektive přepínači)
■Nejprve si zvolí kořen stromu. Vyběr se provádí podle nakonfigurovaných priorit a v případě shody podle jednoznačného pevného Bridge ID