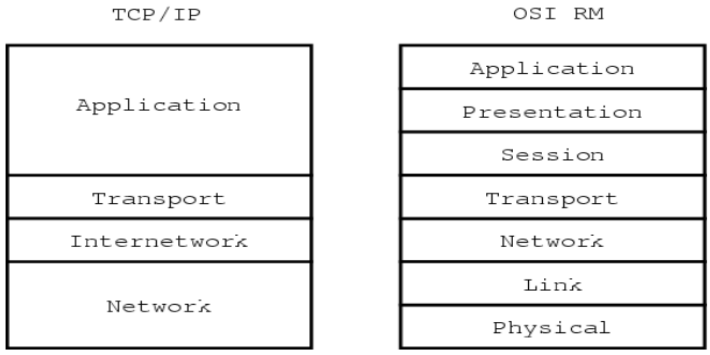
Přenosové protokoly Internetu - protokolová rodina TCP/IP

Jaké protokoly se v Internetu používají na 3. a 4. vrstvě OSI RM ?

Na třetí vrstvě se využívá protokol IP. Na čtvrté vrstvě se využívají protokoly TCP a UDP.

Srovnejte vrstvený model architektury TCP/IP s ISO OSI RM.

Tcp/ip na rozdíl od RMOSI popisuje konkrétní protokoly a jejich použití, kdežto RMOSI je jen takový „předpis." Tcp/ip mám pouze 4 vrstvy, protože bylo zjištěno že je to dostačující počet vrstev.



Jaká je délka a struktura adresy protokolu IP ? Co znamenají třídy adres ? Co jsou beztřídní adresy a k čemu se u nich používá maska podsítě (subnet mask) ?

Délka ip adresy je 32b. (X.X.X.X) maximální hodnota X je 255, minimální 0. Adresy třídy popisují jaká maska patří k dané ip adrese, podle velikosti prvního oktetu (X). Podle třídy jsme schopni určit kolik zařízení je v dané síti a zároveň tím oddělujeme adresu sítě od adresy hosta. Beztřídní adresy jsou adresy, jejichž maska se liší od masky třídy, k těmto adresám se explicitně musíme uvést jejich masku, která udává počet zařízení v síti (jaká část adresy je vyhrazena pro síť a jaká část pro hosta).

Co jsou privátní adresy a k čemu se používají ? Kdo je přiděluje ? Uveďte aspoň jeden z rozsahů, který můžete použít jako privátní adresy.

Privátní adresy jsou adresy definované uvnitř sítě takové, která s vnějším okolím (světem) nemá co dělat. Z názvu privátní vyplývá, že tyto adresy jsou soukromé. Pro komunikaci s vnějším světem jsou zpravidla překládány například pomocí NAT. Přiděluje je správce dané sítě. Příkladem je třeba 10.0.0.0 až 10.255.255.255 172.16.0.0 až 172.31.255.255

Co reprezentují IP adresy 255.255.255.255 a 127.0.0.1 ?

127.0.0.1 je adresa používaná jak localhost. Jinými slovy tím myslí daná periferie sebe samou 255.255.255.255 je univerzálním broadcastem, tedy adresou, která umožňuje zaslat paket vem stanicím v dané síti, podsíti.

Jak se formálně označí určitá IP (pod)síť jako celek ?

Jako prefix sítě za kterým následuje znak „/" a číslo dané masky například 192.168.4.0/24- říká že adresa sítě(podsítě) je 192.168.4.0 – 192.168.4.255, rozsah určuje číslo za „/"(maska).

Jak vypadá adresa broadcastu pro určitou konkrétní IP (pod)síť ?

Máme 2. Možnosti, buďto použijeme univerzální broadcast 255.255.255.255, nebo je jím adresa sítě, podsítě, jejíž část pro hosta je vyplněna samými jedničkami. Přiklad adresa sítě je 192.168.0.0/24. Broadcast takovéto sítě je 192.168.0.255.

Proč se používá podsíťování (subnetting) a v čem spočívá jeho princip ?

K přesnému rozdělení adres v dané (pod)síti. Klade důraz na využití pouze nezbytného počtu adres přidělených ISP. Umožní efektivnější rozdělení adresního prostoru pro reálné účastníky.

K čemu slouží překlad adres (NAT) , jaký je jeho princip a na jakém síťovém prvku jej lze realizovat ?

K oddělení privátní části sítě od veřejné. Je možno překládat určitou adresu vnitřní a určitou adresu vnější. Při použití dynamického NATu lze s přideleným rozsahem M vnějších adres přidělit N vnitřních adres, přičemž platí že N>M.

Jaký je princip dynamického NAT a statického NAT ?

Dynamický NAT pracuje tak, že propůjčuje vnější adresy z tzv. poolu prvkům vnitřní sítě. Tyto adresy se přidělují pouze v momentě, kdy chce vnitřní stanice vysílat ven a jejich přidělení má časově

omezenou platnost. Dynamický NAT umožňuje připojit na M vnějších adres N vnitřních zařízení, přičemž platí že N>M a najednou lze mít připojených M zařízení.
Statický NAT má pevně nadefinované pro jakou vnitřní adresu použije při překladu vnější adresu. Tyto adresy pak překládá pořád stejně.
Na jakém principu lze pomocí NAT za jedinou veřejnou IP adresu "ukrýt" větší množství vnitřních adres ?
U NAT se tím myslí Dynamický NAT. Viz. Otázka výše.
Pak existuje i PAT, ten se stará o to, aby pod jednou IP adresou bylo ukryto více zařízení, které rozeznává pomocí portu, kterým jsou připojení. Zdrojové porty jsou přiděleny dynamicky, tabulka mapuje jednotlivé Porty na vnitřní adresy.
Na které vrstvě pracuje IP protokol ? Co je jeho úkolem ?
Ip protokol pracuje na 3. Vrstvě. Posílá nezávisle směrované pakety do sítě bez navázání spojení. V Dnešní době se používá verze 4 a stále více se prosazuje 6. Je zodpovědný za nasměrování a odeslání paketu. Paket obsahující data obsahuje take tzv. Hlavičku, která nese řídicí data. (Zdroj, cíl fragmentaci,…). Představuje nesolehlivou službu.
Popište význam všech položek v hlavičce IP paketu (obrázek hlavičky si najděte ve studijních materiálech)
Verze- určuje typ použité ip (4, nebo 6)
IHL- délka hlavičky v půlbajtu
TOS-typ služby-slouží k tomu, aby mohla umožnit odesilateli, aby zvolil charakter přepravní služby ideální pro dotyčný diagram. V praxi však k realizaci nedošlo.
Celková délka- délka datagramu v bajtech.
Identifikace- odesilatel přidělí každému odeslanému paketu jednoznačný identifikátor. Pokud byl datagram při přepravě fragmentován, pozná se podle této položky, které fragmenty patří k sobě (mají stejný identifikátor).
Offset fragmentu- udává, na jaké pozici v původním datagramu začíná tento fragment. Jednotkou je osm bajtů.
TTL (Time To Live): představuje ochranu proti zacyklení. Každý směrovač zmenší tuto hodnotu o jedničku
Protokol: určuje, kterému protokolu vyšší vrstvy se mají data předat při doručení
Kontrolní součet hlavičky: slouží k ověření, zda nedošlo k poškození.
Adresa odesílatele
Adresa cíle
Volby: různé rozšiřující informace či požadavky. Například lze předepsat sérii adres
Protokol IPv4 podporuje fragmentaci přenášených paketů. Proč a za jakých okolností k fragmentaci dochází ? Kdo fragmenty opět skládá a jak pozná, které fragmenty patří stejnému paketu a v jakém pořadí ?
Dochází k ní v moment, kdy chce zdroj odeslat data o větší velikosti než je dostačující pro 1. datagram. Poté pomocí identifikátoru označí všechny související pakety a nastaví offset pro každý z nich dle jeho pořadí. Celou režii provádí router. Složení všech diagramů dohromady provádí příjemce, který většinou zřídí nějaký buffer a postupně je seskládá dohromady.
Vysvětlete úkol a princip činnosti protokolu ARP.
Vysílá se broadcastově a jeho úkolem je zajistit mapování ip adres na MAC adresy. 6adatel generuje ARP request s parametrem daného ip, stanice, která nese tuto adresu zprávu zachytí a odpoví na ní ARP reply, s obsahem MAC.
Vysvětlete, k čemu se používá protokol ICMP. Uvěďte alespoň několik typů ICMP zpráv vždy s příkladem konkrétní situace, za které se generují (vždy rovněž udejte, kdo bude zprávu generovat).
Protokol sloužící k ohlašování řídicích zpráv, například ohlašování chyb, zvláštních stavů při přenosu, žádosti o ping. Vypršení TTL, Destination-netwrk-host-port-protocol unreacheable, parametr problem, redirect. Šíří se v datové části paketu IP. Při ping se dotazuje zdrojová stanice a odpovídá cílová stanice. Při Source quench žádá cílová stanice o snížení rychlosti generování požadavků zdrojem. TTL se generuje v momentě vypršení a odešle ho adresa na které se zastavil při cestě k cíli.
K čemu se používá příkaz traceroute implementovaný ve většině OS ? Vysvětlete princip jeho funkce.

Slouží k zjištění cesty směrem od zdroje až k cíli. Využívá se TTL který se pořád inkrementuje a sledují se adresy, ze které přijde ICMP zpráva Time Exceeded. Testovací paket buď ICMP pro Microsoft a neb UDP na neexistující port pro Unix

Vyjmenujte základní rozdíly mezi IPv4 a IPv6.

Ip 4 má k dispozici mnohem menší množství adres. Je pouze 32 bitovou adresou, zapisuje se dekadicky přičemž minimální hodnota je 0 a maximální 255. Ip 6 je 128 bytová adresa a zapisuje se hexadecimálne 0 je min a max je FFFF. Ip 6 nepoužívá broadcast a ani fragmentaci. Místo toho má unicast anycast multicast a možnost vepisování dalších hlaviček. Místo TTL využívá max. skoků, je to ale jen analogie.

Jaké protokoly se v Internetu používají na 4. vrstvě ? Jaký je mezi nimi rozdíl ? K jakým účelům je který z nich výhodnější ?

Protokoly TCP a UDP. UDP představuje nespolehlivý přenos. Typicky se hodí pro přenos videa, neb na místa kde se vyžaduje jednoduchost(dotaz odpověď např. DNS, sdílení soub. V LAN). Nezaručuje spolehlivé doručení k cíli Data se prostě mohou ztratit nebo dojít dvakrát. Hlavička obsahuje pouze source a destination port checksum UDP délku. Hodí se tam, kde nemáme čas se zabývat znovu odesláním nedoručených paketů a tam, kde se předpokládají ztráty.

TCP je spolehlivější, zajišťuje bezeztrátový přenos. Podporuje segmentaci a je rbusním protokolem pro navázání spojení a ukončení.

Popište význam položek hlavičky UDP.

Source port- zdrojový port
Destination port- cílový port
Délka – délka paketu vč. Dat
Checksum – kontrolní součet

Popište význam položek hlavičky TCP.

Source port - port procesu generujícího datagram
Destination port - určuje kterému procesu na cílovém uzlu jsou data určena
Sequence Number - sekvenční číslo prvního datového oktetu v segmentu (pokud není nastaven příznak SYN). Pokud je nastaven příznak SYN, jedná se o tzv. initial sequence number – ISN a první datový oktet má číslo ISN + 1
Acknowledgement Number - má význam pouze když je nastaven kontrolní bit ACK. Toto číslo je nastaveno na hodnotu, kterou odesílatel očekává v poli Sequence Number v následujícím paketu. Je-li ustaveno spojení, je toto číslo vždy posíláno.
Data Offset - specifikuje číslo vyjádřené 32bitovým slovem. Indikuje kde data v segmentu začínají data přenášená tímto datagramem.
Reserved - toto 6ti bitové pole je rezervované a mělo by vždy být nulové
Control Bits - kontrolní bity (příznaky) zajišťující "handshaking" a ostatní specifické procesy
URG - Urgent Pointer
ACK - Acknowledgement
PSH - Push funkce
RST - Reset spojení
SYN - synchronizace sekvenčních čísel
FIN - oznámení, že odesílající nemá žádná další data
Window - množství dat oktetech, které je potvrzováno najednou
Checksum - kontrolní součet, není povinný a v tom případě je 0
Urgent Pointer - údaj je platný pouze pokud je nastaven příznak URG
Options - pole proměnné délky určené pro volitelné parametry TCP, parametr je používán např. pro indikaci maximální velikosti segmentu, kterou je přijímají strana schopna zpracovat
Padding - specifické množství nulových bitů doplňujících hlavičku tak, aby měla 32 bitovou hranici (tj. aby byla beze zbytku dělitelná 32)

K čemu se u protokolů UDP a TCP používají porty ? Proč nestačí cílový port, ale pracuje se i se zdrojovým portem ?

Spolu s ip adresu identifikují konkrétní proces na konkrétním zařízení v internetu. Zdrojový a cílovy port se vždy udávají. 0-1023 jsou veřejně definované služby 1024-4096 klientské porty obvykle přidělované klientům ze strany OS.

Popište proceduru navázání a uzavření spojení u protokolu TCP.

Typ požadavek – potvrzení. Nejprve proběhne dohoda o startovacím sekvenčním čísle SEQ zvlášť pro oba směry. Tyto čísla jsou náhodná z důvodu zamezení ovlivnění případným zbloudilým paketem. Kounikae probíhá buďto SYN, nebo SYN+ ACK , nebo ACK.

Př: SYN(SEQ=x) pro hosta

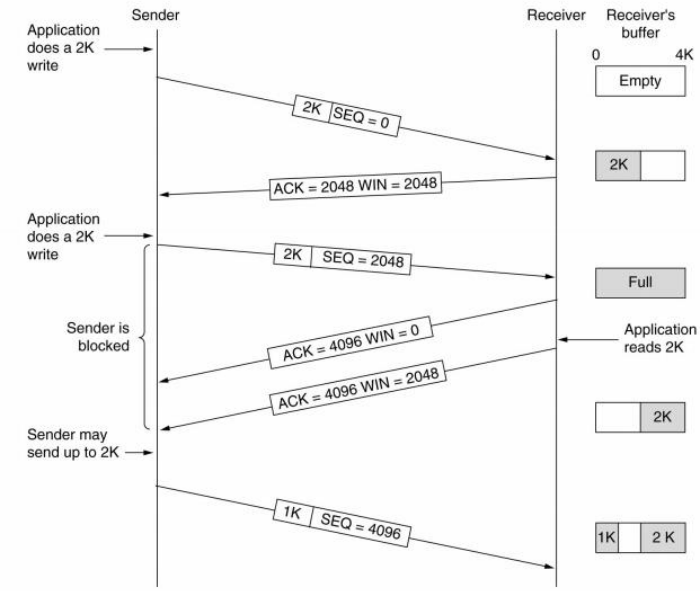
SYN(SEQ=y, ACK=x+1) od hosta

(SEQ=x+1, ACK=y+1) pro hosta (ACK)

Spojení se uzavírá z obou stran zvlášť, možnost i polovičního uzavření FIN + ACK z obou stran. Uzavírat může začít kdokoli.

Popište výměnu dat během TCP spojení včetně řízení toku (flow control). Zaměřte se na položky Sequence number, Acknowledgement number a Window v hlavičce TCP segmentu.

Částečně viz výše.



Směrování a směrovací algoritmy

Vysvětlete pojem směrování. Které aktivní prvky se směrováním paketů zabývají ?

Směrováním se zabývají Routery.Obsahují tzv. směrovací tabulky a podle nich odesílají pakety v síti. Tento mechanismus všeobecně slouží k nasměrování na vhodnou cestu pro paket směrem k cíli.

Vysvětlete pojem směrovací tabulka. Jaké položky (sloupce) byste očekávali v jejich jednotlivých záznamech (řádcích) ?

Tato tabulka je uložena ve směrovači. Ten si jí sestavuje buďto dynamicky a nebo jí má staticky nadefinovanou a podle ní odesílá pakety do sítě. Obsahuje hodnoty typu Cílová adresa + maska a tzv. next hop neboli výstupní rozhraní na které má paket nasměrovat. V prostředí IP se volí vždy cesta taková, která se shoduje na co největší počet míst s adresou cíle. Při směrování nutnost projít vždy celou tabulku.

Vysvětlete pojem implicitní cesty (default route).

Tato cesta se definuje implicitně. A znamená to že pokud má směrovač odeslat paket na síť, kterou nezná tak jí pošle na defaultně stanovené rozhraní (next_hop), typicky se jedná o směrovač jdoucí k ISP.

Jaký je rozdíl mezi statickým a dynamickým směrováním ?

Statické směrování je bezpečnější. Prostě je na pevno nadefinováno kam s jakým paketem. Když ale odpadne daná linka, nutný zásah pro nápravu komunikace. Užitečné pokud se topologie sítě často nemění.
Dynamické směrování automaticky reaguje na změny v topologii sítě. Směrovací tabulka je často užívána už za její samotné tvorby. Nutnost provozů směrovacích protokolů(RIP, OSPF)
Vysvětlete princip, výhody a nevýhody hierarchického směrování.
Rozdělení do hierarchicky organizovaných celků, směrovače v jednotlivých celcích znají jen topologii svého celku, cestu do vyššího celku a seznamy v síti hierarchicky nižších celcích (nikoli jejich vnitřní strukturu). Výhoda je omezení rozsahu směrovacích tabulek.
Vysvětlete pojem směrovací protokol.
Je tím myšlen protokol, který se stará o směrování tvorbu a úpravu jednotlivých směrovacích tabulek u směrovačů v dané síti. Jeho úkolem je automatizované směrování bez potřeby ručního zásahu.
Do jakých dvou základních kategorií směrovací protokoly (algoritmy) dělíme ?
Do 2. Tříd. 1 z nich se nazývá Distance Vector a 2 Link State.
Vysvětlete princip směrovacích algoritmů na bázi vektorů vzdáleností (distance vector).
Směrovače neznají topologii sítě, ale pouze adresy vedoucí k sousedům, přes které odesílají pakety do jednotlivých sítí a vzdálenosti k těmto sítím (distance vector). Zpočátku směrov. Tabulka obsahuje pouze sousedy. Při běhu se periodicky tyto tabulky zasílají sousedům, kteří si podle nich, upravují své vlastní. Pokud cesta nebyla delší dobu inzerována z tabulky se odstraní. Zde se objevuje tzv“problém počítání do nekonečna.“
Vysvětlete princip směrovacích algoritmů na bázi stavů spojů (link state).
Směrování na základě znalosti stavu jednotlivých linek. Směrovače znají topologie celé sítě a ceny jednotliv. Linek. Tyto informace drží v topol. Databázi. Každý směrovač počítá strom nejkratší cesty ke všem ostatním směrovačům. Všechny směrovače počítají na základě stejných, úplných dat. Směrovače neustále sledují stav a funkčnost k němu napojených linek. Při změně okamžitě šíří informaci ke všem ostatním směrovačům a ti si jí uloží d topologické databáze.
Srovnejte výhody a nevýhody směrovacích algoritmů tříd distance vector a link state.
Link state – každý směrovač zná celou topologii sítě, ale je schopen kožité reakce na změnu stavu linek. Tedy rychlá konvergence.
Distance vector- každý směrovač ví jen to nezbytně nutné (nemusí znát celou topologii je to zbytečné.) Problémem je to, že v případě přidání nové cesty reaguje rychle ale když cestu odebereme musíme řešit problém počítání do nekonečna. Tedy pomalá konvergence
Uveďte reprezentanty směrovacích algoritmů tříd distance vector a link state v prostředí TCP/IP.
Nejčastěji využívaný protokol Distance vector je RIP
U link state to je OSPF

Domain Name System

Jaká je struktura doménového jména ? Co znači (obvykle vynechávaná) tečka za jménem vpravo ?
Uveďte základní generické domény.
Je to hierarchická stromová struktura jmenného prostoru. Každý uzel je identifikován doménovým jménem. Je tvořeno spojením jména uzlu stromu se všemi jmény uzlů na cestě ke kořeni („.“), oddělovač je tečka.
Generické domény: .com .org .net .edu .mil .gov
Následují domény názvů států .cz .sk ….
Definujte pojem domény.
Je to jednoznačné jméno (identifikátor) počítače nebo počítačové sítě, které jsou připojené do internetu.
Definujte pojem zóna. Jaký může být vztah domény a zóny ?
Část stromu uložena na jednom DNS serveru. J spravována separátně. DNS server je autoritativní pro domény obsažené v jím spravované zóně.

Co je DNS server ? Čím se liší primární a sekundární server domény ? Co je to kořenový (root) DNS server ?

tento server obsahuje nebo se stará o vyhledání (překladu) domény na adresu, nebo naopak. DNS server může hrát vůči doméně (přesněji zóně, ale ve většině případů jsou tyto pojmy zaměnitelné) jednu z těchto rolí:

Primární server je ten, na němž data vznikají. Pokud je třeba provést v doméně změnu, musí se editovat data na jejím primárním serveru. Každá doména má právě jeden primární server.

Sekundární server je automatickou kopií primárního. Průběžně si aktualizuje data a slouží jednak jako záloha pro případ výpadku primárního serveru, jednak pro rozkládání zátěže u frekventovaných domén. Každá doména musí mít alespoň jeden sekundární server.

ROOT servery představují zásadní část technické infrastruktury Internetu, na které závisí spolehlivost, správnost a bezpečnost operací na internetu. Tyto servery poskytují kořenový zónový soubor (*root zone file*) ostatním DNS serverům. Jsou součástí DNS, celosvětově distribuované databáze, která slouží k překladu unikátních doménových jmen na ostatní identifikátory.

Vysvětlete, jak probíhá vyhledání záznamu odpovídajícího zadanému doménovému jménu v DNS (postupně od root serveru).

Pokud počítač hledá určitou informaci v DNS (např. IP adresu k danému jménu), obrátí se s dotazem na tento lokální server. Každý DNS server má ve své konfiguraci uvedeny Ip adresy kořenových serverů (autoritativních serverů pro kořenovou doménu). Obrátí se tedy s dotazem na některý z nich. Kořenové servery mají autoritativní informace o kořenové doméně. Konkrétně znají všechny existující domény nejvyšší úrovně a jejich autoritativní servery. Dotaz je tedy následně směrován na některý z autoritativních serverů domény nejvyšší úrovně, v níž se nachází cílové jméno. Ten je opět schopen poskytnout informace o své doméně a posunout řešení o jedno patro dolů v doménovém stromě. Tímto způsobem řešení postupuje po jednotlivých patrech doménové hierarchie směrem k cíli, až se dostane k serveru autoritativnímu pro hledané jméno, který pošle definitivní odpověď.

Jaký protokol transportní vrstvy se používá pro komunikaci s DNS serverem ?

Běžné dotazy řeší protokol UDP . Dlouhá data a transfer zóny z primárního na sekundární server nad TCP

Jaké typy záznamů databáze DNS znáte ? K čemu se jednotlivé typy používají ?

A (**a**ddress record) obsahuje IPv4 adresu přiřazenou danému jménu, například když jménu *cosi.kdesi.cz* náleží IP adresa 1.2.3.4, bude zónový soubor pro doménu *kdesi.cz* obsahovat záznam cosi IN A 1.2.3.4

AAAA (IPv6 address record) obsahuje IPv6 adresu. Zmíněnému stroji bychom IPv6 adresu 2001:718:1c01:1:02e0:7dff:fe96:daa8 přiřadili záznamem cosi IN AAAA 2001:718:1c01:1:02e0:7dff:fe96:daa8

CNAME (**c**anonical **name** record) je alias - jiné jméno pro jméno již zavedené. Typicky se používá pro servery známých služeb, jako je například WWW. Jeho definice pomocí přezdívky umožňuje jej později snadno přestěhovat na jiný počítač. Pokud náš *cosi.kdesi.cz* má sloužit zároveň jako *www.kdesi.cz*, vložíme do zónového souboru www IN CNAME cosi

MX (**m**ail e**x**change record) oznamuje adresu a prioritu serveru pro příjem elektronické pošty pro danou doménu. Tentokrát jsou parametry dva - priorita (přirozené číslo, menší znamená vyšší prioritu) a doménové jméno serveru. Pokud poštu pro počítač *cosi.kdesi.cz* přijímá nejlépe počítač *mail.kdesi.cz* a případně jako záložní i *mail.jinde.cz*, bude zónový soubor obsahovat záznamy (všimněte si použití jmen s tečkou a bez tečky) cosi IN MX 10 mail; IN MX 20 mail.jinde.cz

NS (**n**ame **s**erver record) ohlašuje jméno autoritativního DNS serveru pro danou doménu. Bude-li mít doména *kdesi.cz* poddoménu *obchod.kdesi.cz*, jejímiž servery budou *ns.kdesi.cz*(primární) a *ns.jinde.cz* (sekundární), bude zónový soubor pro *kdesi.cz* obsahovat

Obchod IN NS ns
IN NS ns.jinde.cz

PTR (**p**oin**t**e**r** record) je speciální typ záznamu pro reverzní zóny. Obsahuje na pravé straně jméno počítače přidělené adrese na straně levé (adresa je transformována na doménu výše popsaným

postupem). Držme se našeho příkladu pro záznam typu A - v souladu s ním by zónový soubor pro doménu *3.2.1.in-addr.arpa* měl obsahovat (zónový soubor definuje reverzní doménu, proto je třeba psát na pravé straně kompletní jméno s tečkou, jinak by za ně připojil reverzní doménu)
4 IN PTR cosi.kdesi.cz.
SOA (**s**tart **o**f **a**uthority record) je zahajující záznam zónového souboru. Obsahuje jméno primárního serveru, adresu elektronické pošty jejího správce (zavináč je v ní ale nahrazen tečkou) a následující údaje: *Serial* — sériové číslo, které je třeba zvětšit s každou změnou v záznamu. Podle něj sekundární server pozná, že v doméně došlo ke změně. Pokud jej zapomenete zvětšit, rozejde se obsah sekundárních serverů s primárním, což rozhodně není dobré. Pro přehlednost často ve formátu YYYYMMDDHH.
Refresh — jak často se má sekundární server dotazovat na novou verzi zóny (v sekundách).
Retry — v jakých intervalech má sekundární server opakovat své pokusy, pokud se mu nedaří spojit s primárním.
Expire — čas po kterém označí sekundární servery své záznamy za neaktuální, pokud se jim nedaří kontaktovat primární server.
TTL — implicitní doba platnosti záznamů.
Vysvětlete, jak se provazuje hierarchie DNS serverů pomocí NS záznamů.
NS (**n**ame **s**erver record) ohlašuje jméno autoritativního DNS serveru pro danou doménu. Bude-li mít doména *kdesi.cz* poddoménu *obchod.kdesi.cz*, jejímiž servery budou *ns.kdesi.cz*(primární) a *ns.jinde.cz* (sekundární), bude zónový soubor pro *kdesi.cz* obsahovat
Obchod IN NS ns
IN NS ns.jinde.cz
Vysvětlete, jak probíhá přemapování známé IP adresy na odpovídající doménové jméno.
Reverzní doména provede mapování IP adres na doménová jména pak rozdělí na NS nižších úrovní po bajtech.
Vysvětlete, k čemu slouží záznam SOA a MX.
Viz výše

Protokoly služeb Internetu

- K čemu se používá protokol Telnet ? Který port služba používá ? V čem spočívají bezpečnosní rizika Telnetu ? Čím lze službu Telnet nahradit pro omezení těchto rizik ?

23tel 22ssh tcp

- Jak se dá Telnet klient využít k ladění jiných služeb s textově orientovaným protokolem (kterých například) ?

Klientským programem telnetu se lze pro testovací účely připojit na jinou textově orientovanou službu Internetu. Lze tak například simulovat činnost webového prohlížeče. jednoduchým postupem můžeme snadno v případě problémů zjistit, zda nějaká služba vůbec běží a zda alespoň v základních rysech funguje.

- K čemu slouží protokol FTP ? V čem spočívají jeho bezpečnosní rizika ?

Hesla jsou odesílána jako běžná data tedy nejsou šifrována což snižuje bezpečnost nicméně už exituje i řešení.

- Jaké dva typy kanálů se při práci FTP vytváří a jaké porty se k tomu používají ? Kterými příkazy protokolu se zajistí přečtení a uložení souboru ? K čemu slouží příkaz PORT ? Jak se přenáší obsah adresáře (příkaz list) ?

Řídicí 21 a datový 20
MGET – přenos více souborů ze serveru (příkaz klientského software ftp)

LIST – získání seznamu souborů. K získání tohoto seznamu se musí otevřít datové spojení. Pokud parametr tohoto příkazu je adresář, získá se výpis tohoto adresáře, pokud je to soubor, získají se informace o tomto souboru a pokud příkaz nemá parametr, je vrácen výpis aktuálního adresáře. Výpis příkazu list však závisí na systému a je určen především pro člověka.
PORT - specifikuje počítač a port pro datové spojení. Klient pošle tento příkaz a bude na daném portu čekat na datové spojení.

- Co obnáší FTP přenos v režimu textovém nebo binárním ?

  Přenos může být *binární* nebo *ascii* (textový). Při textovém přenosu dochází ke konverzi konců řádků – CR/LF (DOS, Microsoft Windows) nebo jen LF (unixové systémy), pokud jsou koncové systémy rozdílné. Při binárním přenosu není do dat nijak zasahováno.

- Co znamená pasivní režim FTP ?

Znamená to, že spojení nenavazuje server přes port 20 ale host přes svůj daný port definovaný v příkazu na port 20. Pro aktivaci tohoto režimu nutno zadat příkaz PASV

- K čemu se používá protokol TFTP a jak se technicky liší od FTP ?

Je to jednoduchá implementace přenosu souborů nad UDP Používající často pro upload SW, konf. síťových prvků, nebo zavedené bootovací image stanice. TFTP je určen pro přenos souborů v případech, kdy je běžný protokol FTP nevhodný pro svou komplikovanost
musí obsahovat vlastní řízení spojení. Koncepce sezení je jednoduchá: v jednom spojení lze přenést jen jediný soubor, při komunikaci se na síti pohybuje vždy jen jediný paket (po odeslání jednoho paketu program čeká na jeho potvrzení a teprve poté posílá další). Kvůli tomuto zjednodušení poskytuje protokol na linkách s velkoulatencí jen malou přenosovou rychlost. TFTP používá portu 69 (FTP používá spojovaný protokol TCP a port 21).
Oproti FTP má různá omezení a odlišnosti:
Nelze procházet adresáře.
Neumožňuje přihlášení uživatele ani zadání hesla.
Je používaný pro čtení nebo zápis dat na vzdálený server.
Podporuje tři odlišné přenosové módy: *netascii* (pro text v ASCII s úpravami z protokolu Telnet), *octet* (pro syrová binární 8bitová data) a *mail* (pro zaslání e-mailové zprávy; tento mód by se už neměl používat).
Maximální velikost přenášeného souboru je 32 MB.
Kvůli nedostatečnému zabezpečení je nebezpečné používat tento protokol k výměně dat přes internet, používá se výhradně v lokálních sítích, kde nehrozí takové nebezpečí zcizení nebo poškození dat

- Vysvětlete pojmy User Agent, Message Transfer Agent a Mailbox.

UA je používán jako entita přijímající zprávu. Zpravidla na straně příjemce.
MTA je entita pracující na straně serveru s příjemcem. Jeho úkolem je jménem serveru převzít od odesílatele zprávu a uložit jí na Mailbox, který se rovněž nachází na daném serveru, od tud může být zpráva odeslána dále příjemci. Nachází se i čistě na přijímací straně za předpokladu že po cestě není žádný server.
Mailbox – plní funkci poštovní schránky.

- Jaké protokoly se používají pro odesílání zpráv elektronické pošty a jaké pro vzdálené vyzvedávání zpráv z poštovních přihrádek ? Jaký protokol transportní vrstvy se při tom využívá ?

Pro odesíláni zpráv se standardně využívá protokol SMTP pracující na tcp portu 25
Pro vzdálené přijetí se používá protokol POP3 na portu 110 u tcp.

- Jaká je úroveň autentizace a šifrování v běžných protokolech pro odesílání a stahování pošty ?

Všechny jsou to textttově orientované protokoly a neprovádí šifrování SMTP pracuje dokonce bez autentizace.
POP, IMAP zpravidla autentizaci provádí pomocí cleartextových hesel nebo MD5.
Lze však šifrovat POP3 a IMAP pomoci SSL tedy získáme POP3S IMAPS

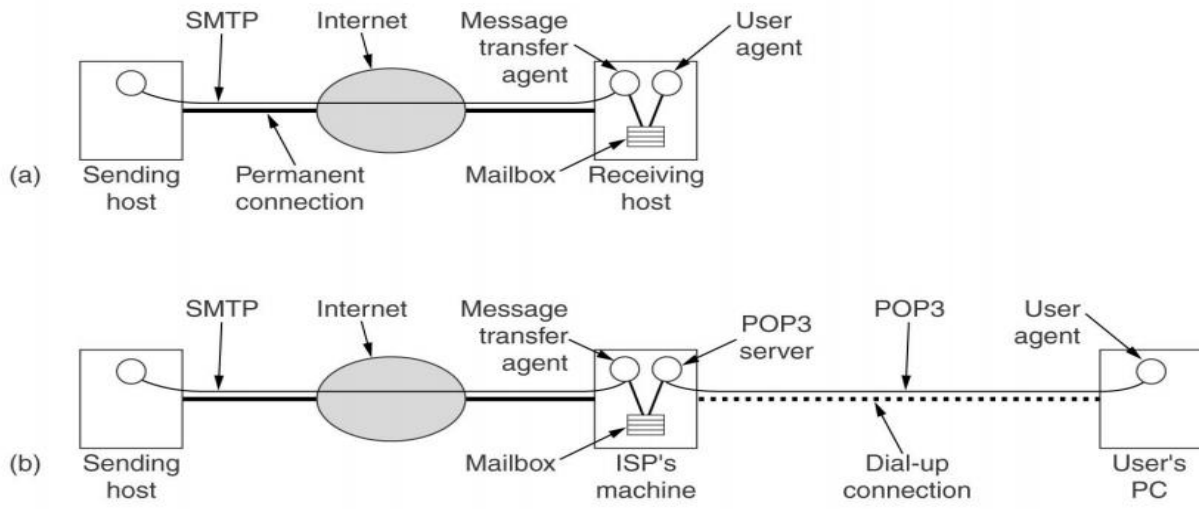
- Jaká je struktura zprávy elektronické pošty ? Uveďte příklady údajů v hlavičce zprávy. Kdo smí modifikovat hlavičku zprávy ?

Obálka obsahující identifikaci odesílatele a příjemce
Hlavička obsahuje seznam dvojic „jméno: hodnota“
Od těla zprávy oddělena prázdným řádkem. Mezilehlé poštovní servery mhou hlavičku modifikovat MTA
Tělo dříve využití NVT dnes MIME

- Jak lze pomocí elektronické pošty posílat zprávu s netextovým (multimediálním) obsahem a zprávy složené z více částí (s "přílohami") ?

S využitím protokolu MIME

- Popište, jak se z poštovního klienta vaší pracovní stanice dostane zpráva k příjemci prostřednictvím Internetu. Předpokládejte, že klient používá server odchozí pošty (proč je to výhodné ?)



- Co je to URL ? Jaká je obecná struktura URL ?

(„jednotný lokátor zdrojů“) je řetězec znaků s definovanou strukturou, který slouží k přesné specifikaci umístění zdrojů informací (ve smyslu dokument nebo služba) na Internetu.
Tvar URL adresy a slova obsažená výrazně ovlivňují váhu webu přisuzovanou vyhledávači. Pokud URL adresa obsahuje klíčová slova, která jsou součástí hledaného výrazu, přikládají stránce vyhledávače větší význam.
Měla by být trvalá, popisná krátká, pamatovatelná jednoduhá

- Jaký protokol se používá pro čtení WWW stránek (HTML) ? Nad jakým transportním protokolem a se kterým číslem portu pracuje ?

http využívaící protocol TCP port číslo 80 v případě šfrvané komunikace HTTPS to je port 443 ale stejný protoTCP

- Vysvětlete, k čemu v protokolu HTTP slouží metody GET, POST a HEAD.

GET získání dokumentu specifikovaného zadanou cestou URL.

HEAD získání hlavičky dkumentu
POST, PUT zaslání formuláře na server.

- Vysvětlete, proč odpověď WWW serveru na žádost o určité URL obsahuje nejen obsah samotného zdroje, ale i hlavičku. Uveďte příklady údajů, které se mohou v hlavičce vyskytovat.

Hlavička poskytuje důležité informace k samotnému obsahu. Př výčet servere podporovaných příkazů, kódování dokumentů jazyk dokumentu, délka dokumentu MIME typ těla zprávy MIME verze, Datum zaslání dkumentu, Last Modified, platnost dokumentu.

- Vysvětlete, proč i HTTP požadavek obsahuje hlavičku. Uveďte příklady údajů, které mohou být uvedeny v hlavičce požadavku HTTP.

Hlavička obsahuje důležité informace směrem k serveru. Např. typ klienten akceptovatelného média, klienten akcept. Znakov sady, kódování , jazyk , autentizační údaje , If-Modified-Since, User-Agent – jméno a verze WWW prohlížeče.

- Jak se realizuje autentizace uživatelů při přístup na WWW stránky ?

Pomocí http hlavičky.

- Co jsou a k čemu lze použít Cookies ?
- malé množství dat, která WWW server pošle prohlížeči, který je uloží na počítači uživatele. Při každé další návštěvě téhož serveru pak prohlížeč tato data posílá zpět serveru. Cookies běžně slouží k rozlišování jednotlivých uživatelů, ukládají se do nich uživatelské předvolby apod.
- Uveďte základní rozdíly mezi HTTP 1.0 a 1.1.

http 1.0 spojení navazuje klient a ukončuje server po odeslání odpovědi. Pokud se stránka skládá z více dokumentů, každý se získává zvlášť po zvláštním TCP spojení.
http 1.1 klient může požádat o podržení spojení TCP po vyřízení požadavku serverem. Podpora „virtual hosts“, tedy více log serverů na stejnou IP adresu.
Možnost přenosu části dokumentu při výpadku spojení a novém načtení. Podpora kmprese dat

- Jak lze zajistit šifrování a autentizaci při přenosu WWW stránek ?

Pomocí HTTPS

- Vysvětlete, k čemu se používá protokol DHCP. Jaké parametry lze jeho prostřednictvím předat ? Jaká je výhoda oproti statické konfiguraci stanice ? Popište sekvenci zpráv protokolu během přidělování IP adresy dynamicky konfigurovatelné stanici.

Slouží k automatickému přidělování adres v rámci sítě z tzv. poolu adres. Tento pool označuje pole adres, které může přidělit. Po skončení spojení se adresa opět vrací do poolu. Tedy pokud bychom měli staticky definované adresy tak kdybychom chtěli připojit jiné zařízení v omentu, kdy je staticky definované zařízení vypnuté tak buď plýtváme adresami, nebo se ani nepřipojíme, protože už můžou být vechny adresy vyčerpané. Žádost se provádí pomocí UDP přez broadcast. Nejdříve stanice vyšle
DHCP Discaver – k nalezení dhcp serveru v okolí
DHCP Offer – DHCP nabízí své služby
DHCP Request klient žádá o rezervování jedné z adres
DHCP ack daný server potvrzuje rezervaci

- Proč je problémem,když DHCP server není na stejném segmentu jako klienti ? Jak lze tuto situaci řešit ?