1.1 Úlohy sieťovej vrstvy modelu OSI

Sieťová vrstva predstavuje v modeli OSI tretiu vrstvu. V modeli OSI aj v modeli TCP/IP plní sieťová vrstva zhodné úlohy, ktoré je možné zhrnúť do dvoch vzájomne úzko nadväzujúcich oblastí:

TCP/IP	OSI
transportná	transportná
sieťová	**sieťová**
vrstva sieťového rozhrania	linková
	fyzická

- Sieťové (logické) adresovanie
- Smerovanie

1.1.1 Prečo logické adresovanie?

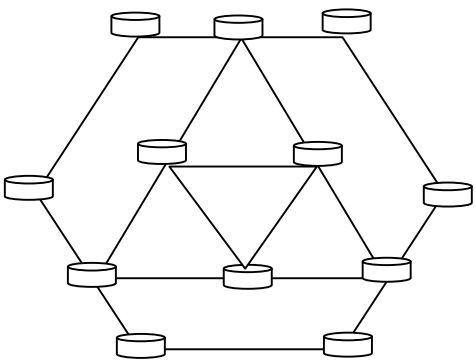
Mnohí hĺbavejší študenti si hneď v úvode položia otázku, prečo je potrebné zaviesť ďalší adresovací systém, keď každé rozhranie už má pridelenú adresu fyzického rozhrania – MAC adresu. Z povahy konštrukcie MAC adresy (pripomeňme si: prvých 24 bitov – označenie výrobcu OUI, ďalších 24 bitov v podstate výrobné číslo) je zrejmé, že **na základe fyzických adries nie je možné vytvárať žiadne logické hierarchické štruktúry**. To znamená, že nie je možné v sieti vymedziť oblasti, ktoré by boli **charakteristické nejakou vlastnosťou adresy** – napríklad aby prvých 8 bitov adresy vyjadrovalo príslušnosť ku nejakej sieti a predstavovalo základ pre rozhodovanie smerovača. (príklad – obrázok – sieť iba s MAC adresami)
Z tohto dôvodu je nevyhnutné **zaviesť logické – sieťové – adresovanie**, ktoré prideľuje administrátor siete a ktoré umožňuje vytvoriť požadované hierarchické logické štruktúry.
Najznámejším príkladom sieťového adresovania sú IP adresy, existuje ale viacero sieťových adresných systémov, napríklad adresovanie IPX, XNS, a iné.

1.1.2 Súvislosť medzi adresovaním a topológiou siete

Zopakujme si, čo vieme o malej sieti:
U malých sietí, LAN sietí sa používajú **také topológie siete, ktoré umožňujú iba jednoznačnú trasu medzi kažými dvoma uzlami siete**. Ani u typológie BUS, ani u RING, STAR alebo Extended STAR (Hierarchical STAR) nie je možné prejsť od ktoréhokoľvek uzla do iného uzla po viacerých trasách. V takejto sieti **vystačíme s fyzickým adresovaním**, pretože v každom bode siete je možné presne určiť, kadiaľ má rámec ďalej ísť, aby sa dostal ku cieľu. Na zdieľanom médiu sa rámec dostáva ku všetkým potencionálnym príjemcom rámca, u bridgeovanej, resp. switchovanej siete zabezpečuje výber trasy tabuľka priradenia MAC adresy ku konkrétnemu portu. Vždy však musí byť vytvorený rámec s MAC adresou cieľa, pretože s iným typom adresy nedokáže sieťové rozhranie pracovať.
Problém môže nastať u veľmi veľkých LAN sietí s topológiou Hierarchical Star, ak množstvo počítačov v sieti prekročí u switchov kapacitu tabuliek pre priradenie MAC adresy príslušnému portu.
Zhrnutie: V LAN sieti, ak nie je extrémne veľká, vystačíme s MAC adresami a službami fyzickej a linkovej vrstvy modelu OSI.

1.1.3 Požiadavky na topológiu veľkých sietí

Od topológií veľkých sietí však požadujeme, aby sa dokázali vysporiadať s poruchou kabeláže či uzla na trase bez toho, že by bolo vážnejšie ohrozené prepravovanie paktov v sieti. Inými slovami, aj ak bude niektorý uzol, alebo aj viacero uzlov alebo káblových trás vyradených, musí ostať konektivita medzi neporušenými uzlami v sieti zachovaná. Na splnenie tejto požiadavky však nevyhnutne potrebujeme takú topológiu, ktorá umožní použiť pri preprave paketov medzi uzlami náhradú trasu – a lepšie, ak možných trás bude veľmi mnoho a bude možné vyberať najvýhodnejšiu z nich podľa momentálnej situácie.
Obecným predstaviteľom takejto topológie je MESH:



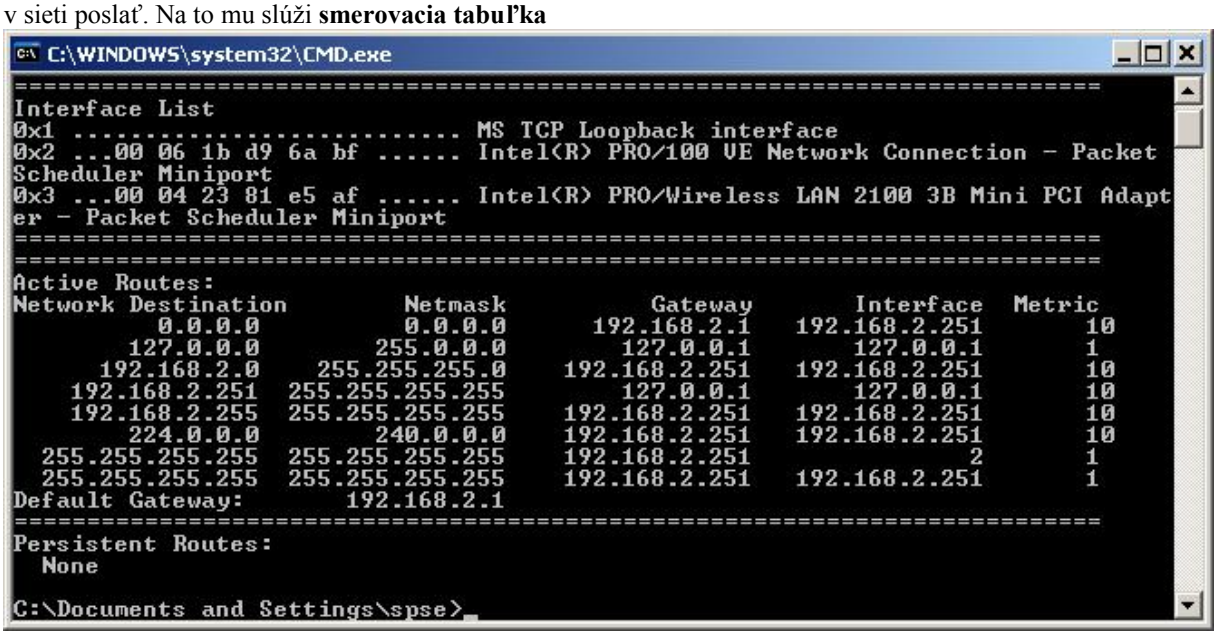
Táto topológia však okrem nesporných výhod prináša aj veľký problém: Ak existuje viacero možností, pre ktorú možnosť sa má uzol rozhodnúť? Podľa akých kritérií sa má uzol rozhodovať? Ako zohľadniť prípadné zmeny topológie – poruchy, výpadky či naopak ak pribudnú nové možnosti ?
Pri práci s fyzickými adresami je možné príslušný uzol siete – napríklad switch – vybaviť programom, ktorý sieť „prehľadá“ a trasy ku všetkým uzlom siete si uloží do tabuľky. Niektoré switche dokážu s využitím Tree Spanning Protokolu aj vyhľadať najvýhodnejšiu trasu z viacerých možných, ale stále sú ich možnosti obmedzené iba na siete s niekoľkými desiatkami či stovkami počítačov. Vo veľkej sieti je však nevyhnutné pracovať s miliónmi či miliardami rozhraní, čo je nemysliteľné, ako sme

už skôr spomenuli, bez logickej štruktúry sieťových adries. Nevyhnutné je teda zapojenie ďalšej vrstvy modelu OSI – vrstvy sieťovej.
Zhrnutie: Pri veľkých sieťach potrebujeme zaviesť ďalší adresovací systém, ktorý bude umožňovať vytváranie hierarchických štruktúr a smerovanie paktov na základe definovaných podmienok pre určitú vlastnosť adresy, a to na základe dvoch dôvodov:

- príliš veľa rozhraní v sieti – nie je možné vytvárať tabuľky so zoznamom všetkých rozhraní
- možnosť viacerých trás medzi dvoma uzlami

1.1.4 Smerovateľný a nesmerovateľný protokol

Existuje viacero adresovacích systémov, používaných na sieťovej vrstve. Z hľadiska ich použitia vo veľkej sieti je však dôležité, aby príslušný protokol – teda aj adresovací systém – bol **smerovateľný**. To znamená, že s ním musia byť schopné pracovať smerovače a na základe potrebných údajov príslušný paket nasmerovať do tej časti siete, kde sa nachádza cieľ paketu.
Protokol IP používa IP adresovanie. IP adresa pozostáva z niekoľkých skupín číslic (v prípade IP verzie 4 ide o 4 skupiny čísiel v rozsahu 0 až 255ň. IP adresa ako celok je routermi interpretovaná tak, že **časť adresy predstavuje adresu siete**, kam má byť paket doručený, a **časť adresu rozhrania (počítača)**, ktorému je paket určený. Sieť ako celok je tvorená logickým systémom adries, to znamená, že z hodnoty jednotlivých častí adresy vie router celkom presne zistiť, kde sa nachádza cieľová sieť a kam – cez ktoré svoje rozhranie - má paket ďalej v sieti poslať. Na to mu slúži **smerovacia tabuľka**

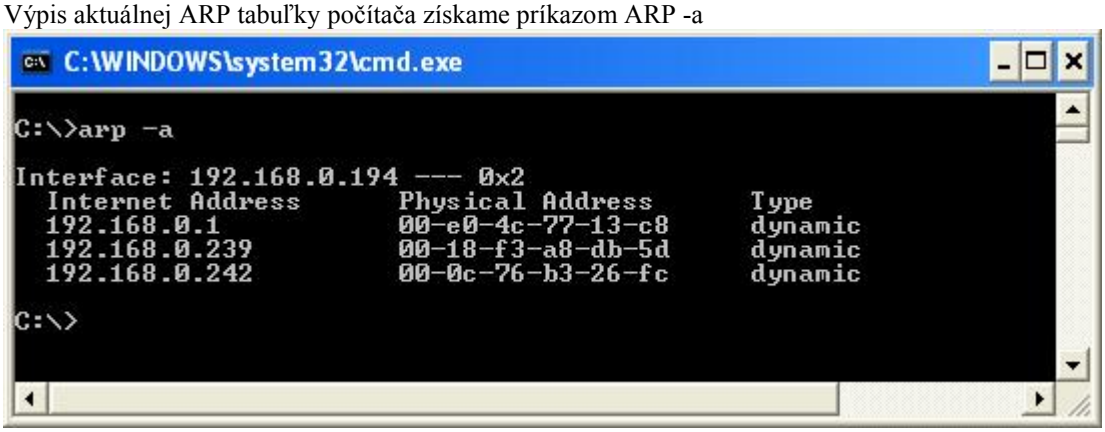


Ak chceme v sieti smerovať **pakety viacerých protokolov**, napríklad potrebujeme smerovať aj pakety typu IP aj IPX, musíme zabezpečiť, aby **smerovače vedeli s obidvoma protokolmi pracovať** – musia byť schopné smerovať aj IP aj IPX pakety a pre každý typ paketov musia mať vytvorené smerovacie tabuľky.
Príkladom smerovateľných protokolov sú TCP/IP, IPX, AppleTalk, SNA, XNS, DECnet a iné. Najrozšírenejším je IP zo sady TCP/IP.
Príkladom nesmerovateľného protokolu je NetBIOS. Tento protokol bol vyvinutý už v r. 1983 pre sieť IBM PC Network. Neskôr bol implementovaný firmou Microsoft pod názvom NetBEUI pre sieťové služby operačných systémov na báze Windows 3x a 9x. Pracuje na linkovej vrstve. Jeho hlavnou úlohou je preklad MAC adries počítačov na názvy počítačov (napríklad PetrovPC, Centrala, PrintServer a pod.), vďaka čomu je možné pracovať v sieti s logickými menami počítačov. ďalej umožňuje zoskupovať počítače do pracovných skupín (Students, Teachers), zobrazovať zoznamy dostupných počítačov po kliknutí na ikonu počítače v sieti , ale pôsobnosť protokolu bola iba v dosahu segmentov pripájaných prvkami prvej a druhej vrstvy modelu OSI. Neumožňuje smerovanie, preto nezabezpečuje konektivitu s počítačmi, ktoré sa nachádzajú za bránou (na segmentoch siete, pripojených routerom). Router nedokáže s paketmi NetBEUI pracovať – NetBEUI je nesmerovateľný protokol.
Protokol bol veľmi zraniteľný a zneužiteľný z hľadiska bezpečnosti komunikácie v sieti. V súčasnosti bol nahradený protokolom TCP/IP a prakticky sa používa iba vynímočne.
Iným príkladom nesmerovateľného protokolu je DEC's LAT, dnes už nie je používaný.

1.1.5 Preklad medzi sieťovými a fyzickými adresami

Zavedenie sieťových adries so sebou ale prináša aj nevyhnutnosť nástroja, ktorý bude zabezpečovať preklad medzi sieťovými a fyzickými adresami. Túto službu poskytuje protokol ARP.
Tento protokol má význam v najmä nasledujúcich situáciách:

Paket s IP adresou dorazil na cieľový router a ten musí zostaviť rámec, ktorý odošle cieľovému počítaču. Rámec musí byť opatrený MAC adresou cieľa. Túto MAC adresu však musí zistiť buď RARP dopytom, alebo prečítať z ARP tabuľky, uloženej v pamäti.
PC odosiela paket inému PC v lokálnej sieti, pričom aplikačná vrstva adresuje cieľový počítač prostredníctvom IP adresy. Vtedy stanica neodosiela rámec bráne, ale musí zostaviť rámec priamo s MAC adresou cieľového PC. Príslušnú MAC si musí zistiť zo svojej ARP tabuľky, alebo RARP dopytom. ARP tabuľka v systémoch Windows má iba časovo obmedzenä platnosť.
Rozhranie, ktoré si vytvára prípadne doplňuje ARP tabuľku, vyšle broadcastové volanie do siete, tzv. ARP request (RARP rámec). Odpoveďou je ARP rámec, ktorý obsahuje informáciu o sieťovej adrese rozhrania, ktoré bolo oslovené.
Výpis aktuálnej ARP tabuľky počítača získame príkazom ARP -a



Tabuľka býva v pravideľných intevaloch refreshovaná
ARP služba bola pôvodne navrhnutá pre TCP/IP protokol, ale dnes sa využíva na preklad medzi MAC adresami a viacerými inými sieťovými adresnými systémami.

1.1.6 Smerovanie (routing)

Smerovanie je činnosť, ktorou smerovače (routery) v sieti preposielajú pakety s informáciami medzi sieťami tak, aby boli čo najefektívnejšie doručené k cieľovému rozhraniu. Podkladom pre rozhodovanie smerovača je vždy smerovacia tabuľka.
Smerovaciu tabuľku môže **vytvoriť** buď **sám administrátor** príslušného uzla tak, že ju sám zapíše do pamäti routera, v takom prípade hovoríme o **statickom smerovaní**, alebo bude tabuľka **vytváraná a opravovaná samotným routerom** na základe routovacích protokolov, a vtedy hovoríme o **smerovaní dynamickom**.
V období začiatkov pokusov so smerovaním sa ešte experimentálne skúšali iné metódy, napríklad kopírovanie a odosielanie paktov na všetky rozhrania okrem rozhrania, na ktoré paket prišiel („záplavové smerovanie“), alebo náhodné smerovanie – preposielanie paktov na náhodne vybrané rozhranie s predpokladom, že raz paket dorazí do cieľovej siete. Na prvý pohľad sú tieto metódy v súčasných rozľahlých sieťach nepoužiteľné.

1.1.6.1 Statické smerovanie

Smerovacia tabuľka je vytvorená administrátorom ručne a zmeny môže opať urobiť iba administrátor. Hodí sa pre **menšie siete**, kde sa nepredpokladá veľa porúch a **nemení sa ich topológia**.

1.1.6.2 Dynamické smerovanie

Smerovaciu tabuľku vytvárajú smerovače za pomoci smerovacích protokolov a priebežne ju upravujú na základe pravideľných testov siete.
Smerovače v režime dynamického smerovania vykonávajú súbežne dve činnosti:

- prieskum okolitej siete a jej parametrov a na základe výsledkov vytváranie a editovanie smerovacej tabuľky
- smerovanie paktov s dátami na základe smerovacej tabuľky

Prieskum siete a úpravy smerovacej tabuľky vykonáva smerovač na základe smerovacích protokolov. Tieto protokoly môžu pracovať na základe troch skupín algoritmov:

1.1.6.2.1 Distance Vector Alghoritm – DVA:

Meria „vzdialenosť“ ku cieľovému rozhraniu, pričom vzdialenosť vyjadruje počtom smerovačov po trase – „skokov“ (hops). Ako najvýhodnejšiu zvolí trasu s najmenším počtom skokov.
Typickými príkladmi smerovacích protokolov, pracujúcich na algoritme DVA, sú RIP alebo IGRP

1.1.6.2.2 Link State Alghoritm – LSA:

Vyhodnocuje okrem počtu skokov aj ďalšie parametre trasy: Prenosové rýchlosti jednotlivých úsekov, časy odozvy, momentálne zaťaženie siete či poplatky za prenájom trasy od cudzieho providera. Výsledkom je bezrozmerné číslo, ktoré vyjadruje „výhodnosť" danej trasy a toto číslo sa označuje výrazom „cena" (v skutočnosti však neide o cenu v eurách či dolároch, ale číslo vyjadrujúce kvalitatívne parametre danej trasy)
Typickým príkladom smerovacieho protokolu pracujúceho na LSA algoritme je OSPF.
Protokol EIGRP používa metódy prevzaté z obidvoch algoritmov.

1.1.6.2.3 Path Vector Algorithm

(path vector protocol)
je podobný DVA, ale líši sa tým, že poskytuje vysoké práva administrátorovi, aby rozhodol, aké dátové toky budú smerované cez jeho sieť. Označuje sa ako ***Policy Based***, čím sa zdôrazňuje **prvoradá priorita kontroly administrátora nad zostavovaním routovacej tabuľky** a tým **vysokej bezpečnosti** (na rozdiel od DVA alebo LSA, ktoré bývajú označované ako ***Metric Based***. Administrátor ovšem nezostavuje routovacie tabuľky, ale ovplyvňuje ich zostavovanie zadaním pravidiel a priorít, ktoré majú byť zohľadňované.
Na stratégii Path Vector sú založené napríklad protokoly BGP (Border Gateway Protocol, v súčasnosti je veľmi rozšírený) a IDRP (v minulosti konkuroval BGP, neskôr bol považovaný za prekonaný, v súčasnosti sa opäť objavuje s nástupom Ipv6).
Predchodcom BGP bol EGP (Exterior Gateway Protocol), ale EGP nedokázal pracovať v sieťach s viacerými možnými cestami, dnes nemá význam.

1.1.7 Protokoly na zisťovanie zaťaženia siete

Na zisťovanie parametrov spojenia slúži v sieti Internet protokol ICMP. Tento protokol je využívaný najmä prostredníctvom služby PING. Na ICMP správach je založená funkcia mnohých diagnostických nástrojov siete. Najčastejšie typy datagramov ICMP protokolu:

- Echo Request … požiadavka na odpoveď, každý prvok v sieti pracujúci na sieťovej vrstve by na túto výzvu mal reagovať. V súčasnosti mnohé prvky z bezpečnostných dôvodov na túto požiadavku neodpovedajú.
- Echo Reply … odpoveď na požiadavku
- Destination Unreachable … informácie o nedostupnosti cieľa, obsahuje ďalšieí upresňujúce informácie
  - Net Unreachable … nedostupná cielová sieť
  - Host Unreachable … nedostupný cielový stroj
  - Protocol Unreachable … informácie o nemožnosti použiť vybraný protokol
  - Port Unreachable … informácie o nemožnosti pripojiť sa na vybraný port
- Redirect … presmerovanie – vyhľadá lepšiu trasu ako je trasa cez defaultnú bránu
  - Redirect Datagram for the Network … informuje o presmerovaní datagramov do celej siete
  - Redirect Datagram for the Host … informuje o presmerovaní datagramov pre jediný stroj
- Time Exceeded … vypršal časový limit
  - Time to Live exceeded in Transit … TTL klesol na 0 kým bol datagram doručený
  - Fragment Reassembly Time Exceeded … nepodarilo sa zostaviť fragmentovaný paket

Ďalším štandardným nástrojom umožňujúcim diagnostiku siete je príkaz TRACEROUTE. Tento nástroj umožňuje detailné mapovanie siete, na ktoré využíva chybové hlásenia ICMP protokolu. Príkaz je implementovaný do väčšiny Unixovských systémov a do systémov Microsoft Windows v podobe príkazu ***Tracert***.
Nástroje PING a TRACERT sú vyvinuté na uľahčenie správy sietí a implementované do mnohých systémov, ale v dôsledku častého zneužívania týchto nástrojov hackermi sú mnohé routery aj firewally nakonfigurované tak, že na žiadosti o odpoveď týmto službám neodpovedajú.

PING : Umožňuje použitie nasledovných parametrov:
-t opakovane odosiela ping, až do ukončenia stlačením CTRL+C
-a prekladá ip adresy na názvy hostiteľov
-n umožňuje nastaviť požadovaný počet pingov (default n=4)
-l umožňuje nastaviť veľkosť testovacieho paketu v bajtoch
-f nastavuje parameter nefragmentovať
-i umožňuje zadať požadovanú hodnotu TTL (ttl = time to live; čas života; udáva koľko skokov môže paket vykonať kým nie je zrušený)
-v typ služby
-r zaznamená cestu pre zadaný počet smerovačov
-s times, špecifikuje čas pre načítanie skokov
-w časový limit čakania na odpoveď (ms)

-j, -k umožní definovať kadiaľ má ping prechádzať

TRACERT: Umožňuje použitie nasledovných parametrov:
-w umožňuje nastaviť časový limit
-j voľné smerovanie medzi určenymi hostiteľmi

1.1.8 OTÁZKY NA OPAKOVANIE:

1. Aké sú hlavné úlohy sieťovej vrstvy?
2. Prečo pri smerovaní potrebujeme adresný systém logických adries, založený na hierarchických pravidlách?
3. Aké topológie v princípe nevyžadujú smerovanie? Aké sú ich typické vlastnosti? Vymenujte ich!
4. Prečo je vhodné použiť smerovanie na topológii hierarchická hviezda, ak sieť obsahuje vysoký počet počítačov?
5. Aké sú požiadavky na topológiu veľkých sietí?
6. Prečo je nevyhnutné používať smerovanie na topológii mesh?
7. Ako súvisí typ použitej adresy s rýchlosťou spracovania rámca rozhraním?
8. Za akých okolností je potrebné v sieti zaviesť sieťové adresovanie?
9. Uveďte príklady dvoch sieťových adresovacích systémov!
10. Uveďte príklad smerovateľného protokolu!
11. Vysvetlite, čo rozumieme pod pojmami smerovateľný a nesmerovateľný protokol!
12. Uveďte príklad nesmerovateľného protokolu!
13. Vysvetlite rozdiel medzi smerovacím a smerovateľným protokolom!
14. Uveďte základné možnosti vytvárania smerovcej tabuľky!
15. Vysvetlite rozdiel medzi statickým a dynamickým smerovaním!
16. Aké procesy prebiehajú vo smerovači, ak pracuje na báze dynamického smerovania?
17. Vysvetlite vlastnosti troch hlavných smerovacích algortimov!
18. Aké hlavné kritérium pre rozhodovanie smerovača používa algoritmus DVA?
19. Aké hlavné kritérium pre rozhodovanie smerovača používa algoritmus LSA?
20. Aké hlavné kritérium pre rozhodovanie smerovača používa algoritmus PVA?
21. Priraďte príklady protokolov ku smerovacím algoritmom!
22. Akou metódou zistí systém MAC adresu rozhrania, ak pozná jeho IP adresu?
23. Uveďte príklady, kedy musí systém priradiť MAC adresu IP adrese?
24. Ako môžete na Vašom počítači zistiť MAC adresy rozhraní vo vašel LAN? Aké je obmedzenie pri zisťovaní MAC adries v LAN?
25. Ktorý protokol používa systém na zistenie dostupnosti sieťového uzla a testovanie parametrov siete?
26. Pomocou ktorých príkazov môže užívateľ toto testovanie vykonať sám?
27. Aké možnosti poskytujú dané príkazy?

1.1.9 PRAKTICKÉ ÚLOHY:

1. Zistite MAC adresu PC udaného vyučujúcim
2. Zobrazte aktuálnu smerovaciu tabuľku na vašom PC
3. Zistite, či je dostupný server www.infovek.sk a ďalšie uzly podľa zadania vyučujúcim. V prípade nedostupnosti cieľa identifikujte (analyzujte) podľa druhu chybového hlásenia druh problému
4. Zistite maximálnu veľkosť nefragmentovaného paketu v sieti v rámci učebne
5. Zistite počet skokov ku serveru www.infovek.sk . Na zistenie použite parameter TTL príkazu PING.
6. Zistite trasu a výpis názvov routerov ku serveru cisco.netacad.net
7. Zistite čas odozvy serverov www.svspn.sk, www.infovek.sk, cisco.netacad.net. Vysvetlite rozdiely v nameraných hodnotách.
8. Zistite IP adresy uvedených serverov.
9. Zistite, či pri viacnásobnom trasovaní toho istého vzdialeného servera bude použitá rovnaká trasa. Vysvetlite na základe Vašich pozorovaní vlastnosti smerovacích algoritmov!
10. S využitím programu NeoTrace zistite parametre spojenia s rôznymi servermi podľa zadania vyučujúceho. Určte presnú geografickú polohu uvedených serverov. Využite údaje aj GPS a Google Earth.