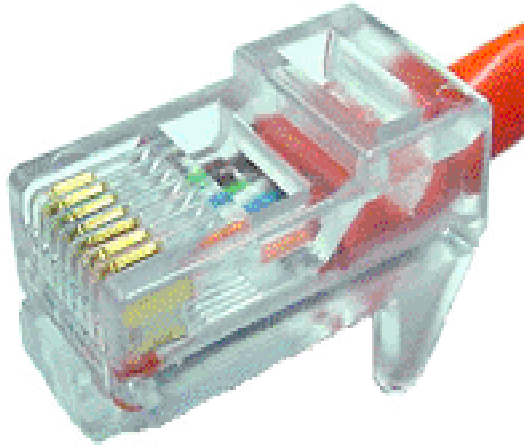
Komunikačné a informačné siete

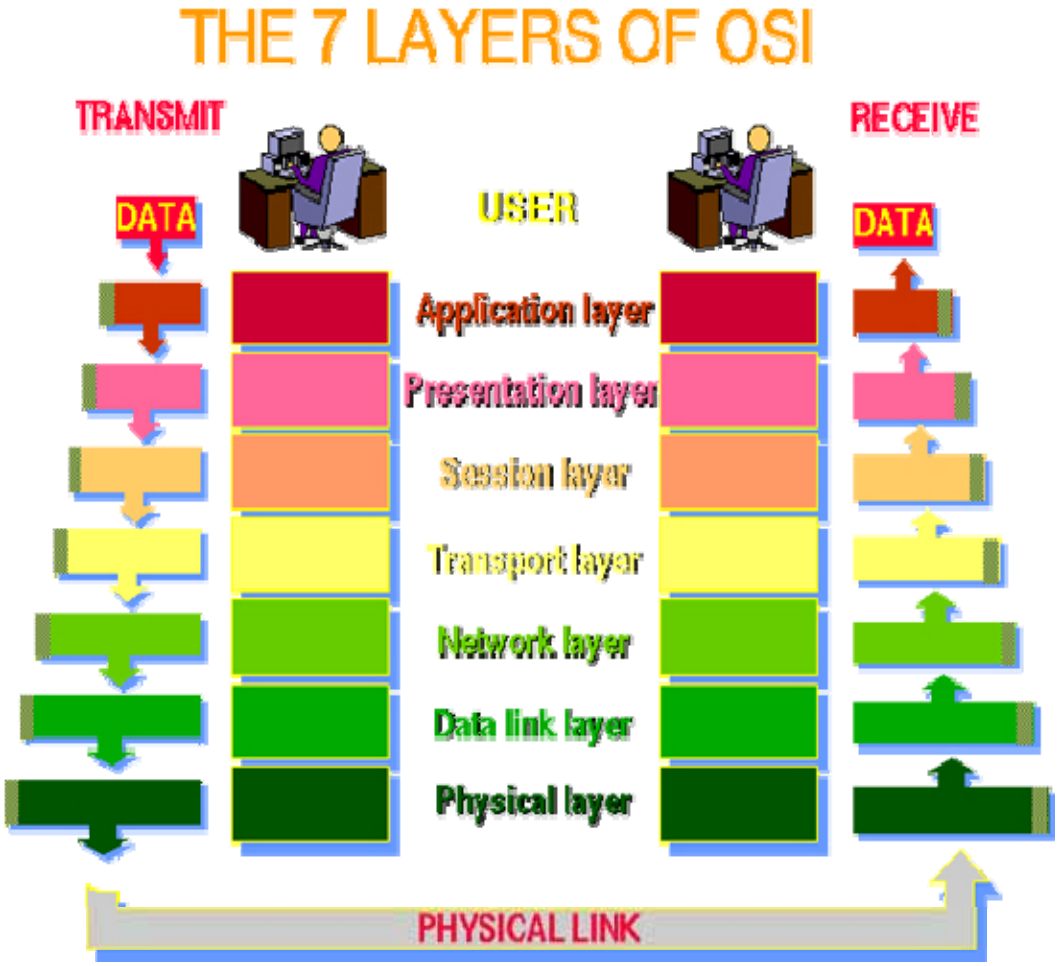
Cvičenie č. 3

Linková vrstva RM OSI

Ethernet, MAC a LLC podvrstvy



RM OSI = Reference Model Open Systems Interconnection



OSI MODEL			TCP / IP
7		**Application Layer** Type of communication: E-mail, file transfer, client/server.	FTP, SMTP
6		**Presentation Layer** Encryption, data conversion: ASCII to EBCDIC, BCD to binary, etc.	DNS
5		**Session Layer** Starts, stops session. Maintains order.	Telnet
4		**Transport Layer** Ensures delivery of entire file or message.	TCP
3		**Network Layer** Routes data to different LANs and WANs based on network address.	IP
2		**Data Link (MAC) Layer** Transmits packets from node to node based on station address.	
1		**Physical Layer** Electrical signals & cabling.	

Linková vrstva

- linková vrstva je druhá v poradí v 7-vrstvovom modeli RM OSI aj v 5-vrstvovom modeli TCP/IP
- rieši kontakt a obsluhu požiadaviek medzi fyzickou a sieťovou vrstvou
- zabezpečuje prenos údajov medzi susednými sieťovými uzlami v sieťach WAN alebo medzi uzlami na danom segmente LAN
- poskytuje prostriedky pre prenos dát medzi sieťovými uzlami a môže zabezpečovať detekciu a prípadne aj opravu chýb, ku ktorým môže dôjsť počas prenosu fyzickou vrstvou
- existuje viacero protokolov dátovej vrstvy, napr.: Ethernet, FDDI, PPP, HDLC, ATM, atď.
- linková vrstva poskytuje dáta pre prenos cez fyzickú vrstvu, pričom tento prenos môže, ale nemusí byť spoľahlivý
- niektoré protokoly linkovej vrstvy disponujú potvrdzovaním správneho prijatia rámca a nejakou formou kontrolnej sumy (CRC), niektoré protokoly však takéto potvrdzovanie ani kontrolnú sumu nepoužívajú, vtedy musia riešiť riadenie toku informácií, kontrolu chýb, potvrdzovanie a opakovaný prenos protokoly vyššej vrstvy

Linková vrstva v sieťach LAN (IEEE 802)

- inštitúcia IEEE vypracovala normy pre jednotlivé typy LAN (napr. Ethernet, Arcnet, Token Ring atď.). Tieto normy opisovali pre každý typ LAN vrstvu MAC. Takto vznikli normy IEEE 802.3 pre Ethernet, IEEE 802.4 pre Token Bus, IEEE 802.5 pre Token Ring, atď. Pre všetky systémy bola potom vypracovaná spoločná norma pre vrstvu LLC pod označením IEEE 802.2
- problematika linkovej vrstvy v ISO/OSI bola takto rozdelená do dvoch podvrstiev v IEEE normách, pričom jednotlivé normy IEEE 802 boli prevzaté aj do ISO
- spodná podvrstva, Medium Access Control (MAC) čiastočne zasahuje do fyzickej vrstvy a zaoberá sa prístupom na prenosové médium
- horná podvrstva Logical Link Control (LLC) umožňuje nadväzovať, spravovať a ukončovať logické spojenia medzi jednotlivými stanicami LAN
- protokol vrstvy IEEE 802.2 LLC môžeme používať so všetkými MAC vrstvami IEEE 802, napr. Ethernet, Token Ring, IEEE 802.11, atď, a podobne aj s niektorými MAC vrstvami, ktoré nie sú typu 802, napr. FDDI
- niektoré protokoly linkovej vrstvy, napr. HDLC, zahŕňajú obe podvrstvy, hoci niektoré ďalšie protokoly, napr. Cisco HDLC používajú MAC podvrstvu v kombinácii s odlišne definovanou LLC podvrstvou
- linková vrstva je často implementovaná softvérovo vo forme ovládača sieťovej karty. Takto má operačný systém definované softvérové rozhranie medzi linkovou vrstvou a sieťovou vrstvou.

Protokoly linkovej vrstvy

- **SLIP** - **Serial Line IP**, vkladá IP-pakety priamo do sériovej linky. Kvôli riadeniu linky sú medzi dáta vkladané tzv. Esc-sekvencie. Protokol SLIP je špecifikovaný normou RFC-1055. Jedná sa o jednoduchý protokol určený pre prenos paketov sieťových vrstiev.
- **CSLIP** - **Compressed SLIP**, varianta protokolu SLIP s kompresiou 40 bytov záhlavia protokolov TCP a IP na 3 až 16 bytov. Dáta sa nekomprimujú. Protokol je špecifikovaný normou RFC-1144.
- **HDLC**, uskutočňuje detekciu chýb aj riadenie toku dát. Je špecifikovaný normami ISO-3309, ISO-4335, ISO-7776, ISO-7809, ISO-8471 a ISO-8885. Jedná sa o rozsiahlu normu, pričom mnohí výrobcovia si ju upravujú podľa seba, takže dochádza k vzájomnej nekompatibilite, napr. CISCO HDLC, DEC HDLC, atď.
- **PPP**, využíva rámce tvaru protokolu HDLC, nevyužíva však všetky možnosti protokolu HDLC, t.j. tvorí jeho podmnožinu. Je špecifikovaný normami RFC-1661 a RFC-1662.
- **Frame Relay**, protokol linkovej vrstvy pre rozsiahle siete. Je špecifikovaný v normách I.122, I.441 a ANSI TI.606. Využíva virtuálne okruhy (obdoba pevnej linky), ktoré si užívateľ prenajíma (medzi svojimi jednotlivými lokalitami) od prevádzkovateľa siete Frame Relay.
- **ATM**, protokol orientovaný na virtuálne okruhy umožňujúci spojenie na dvojbodových spojeniach (point-to-point) a na spojoch, kde jeden odosielateľ adresuje viacero adresátov (point-to-multipoint). Prenáša zvuk, video aj rámce dátových sietí. Umožňuje emuláciu LAN pri využití vysokých prenosových rýchlostí ATM.
- **Ethernet**, v súčasnosti najrozšírenejší protokol linkovej vrstvy.
- **FDDI**, protokol lokálnej siete, v ktorej sú jednotlivé stanice zapojené do kruhu. Je špecifikovaný normou ISO-9314.

Prvky Ethernetovej siete

- LAN sieť typu Ethernet pozostáva z:
  - sieťových uzlov
  - prepájacieho média

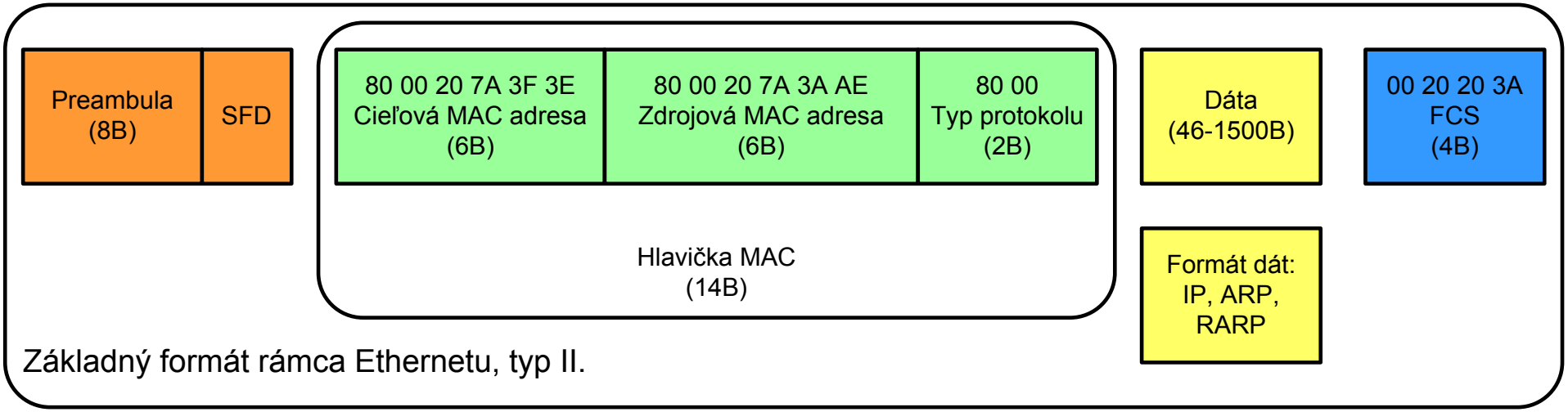
- sieťové uzly spadajú do dvoch hlavných tried:
  - Data terminal equipment **(DTE)**
    - zariadenia, ktoré sú zdrojom alebo cieľom dátových rámcov
    - zariadenia, ako napr. PC, pracovné stanice, servery,t.j. koncové zariadenia
  - Data communication equipment **(DCE)**
    - spojovacie sieťové zariadenia, ktoré prijímajú a odosielajú rámce cez sieť
    - nezávislé zariadenia - repeatre, switche, routre
    - komunikačné stykové jednotky, ako napr. sieťové karty a modemy

Typy rámcov protokolu Ethernet

Existuje niekoľko typov Ethernetových rámcov:

- rámec Ethernet Version 2, resp. **Ethernet II frame**, tiež nazývaný DIX frame (skratka je odvodená od začiatočných písmen firiem DEC, Intel, a Xerox); tento rámec je **v súčasnosti najbežnejším a je často využívaný priamo v IP protokole**
- druhý typ Ethernetového rámca je variácia normy IEEE 802.3 firmy Novell ("tzv.raw 802.3 frame"), ktorý nemá hlavičku IEEE 802.2 LLC
- tretím typom je rámec IEEE 802.2 LLC
- štvrtý typ je rámec IEEE 802.2 LLC/SNAP

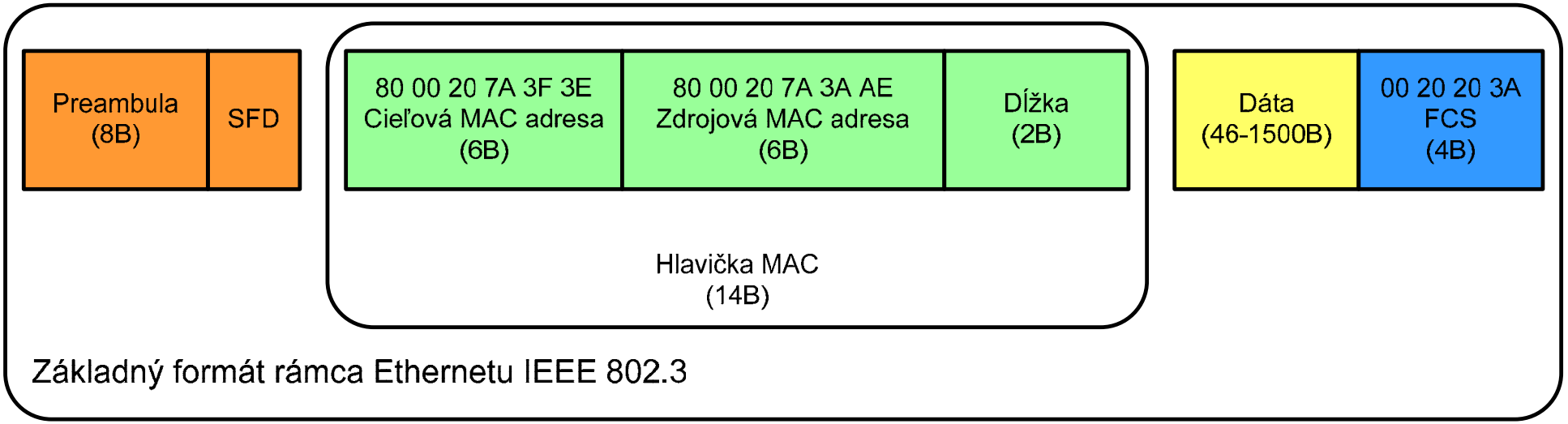
Štruktúra rámca protokolu Ethernet II.



Základný formát rámca Ethernetu, typ II.

- **rámec (Frame)** - formát dátových paketov na vedení, definovaný štandardom IEEE 802.3
- **preambula**
  - synchronizačná alternujúca postupnosť logických jednotiek a núl
  - synchronizuje všetky stanice prijímajúce rámec (označuje prichádzajúci rámec)
- **oddeľovač začiatku rámca (Start-of-Frame Delimiter - SFD)**
  - alternujúca postupnosť logických jednotiek a núl zakončená dvomi po sebe nasledujúcimi log. jednotkami
  - indikuje, že ďalší bit je MSb (Most Significant Bit) bitom MSB (Most Significant Byte) bytu cieľovej adresy
- **typ protokolu**
  - pole špecifikujúce protokol vyššej vrstvy (sieťovej), napr. IPv4, ARP, RARP
- **dátové pole**
  - musí mať minimálnu dĺžku 46 bytov; ak je potrebné prenášať menej dát, tak sa dátové pole sprava doplní bezvýznamnými dátami
- **kontrolný súčet rámca (Frame Check Sequence - FCS)**
  - umožňuje verifikáciu, či nebol rámec počas prenosu poškodený
  - obsahuje 32-bitovú hodnotu: cyclic redundancy check (CRC), ktorá je vytváraná vysielajúcou MAC podvrstvou a prepočítavaná prijímajúcou MAC podvrstvou, kvôli kontrole poškodenia
  - CRC zahŕňa polia: cieľovej a zdrojovej adresy, typu protokolu a dát

Štruktúra rámca protokolu Ethernet IEEE 802.3



Pozn.:

Niektoré staršie verzie špecifikácie rámca Ethernetu majú 16-bitové pole "dĺžka", hoci maximálna dĺžka paketu je 1500 bytov. Verzie 1.0 a 2.0 špecifikácie Ethernetu podľa Digital/Intel/Xerox (DIX), majú 16-bitové pole "typ protokolu" nazývané aj **EtherType**, v ktorom hodnoty medzi 0 a 1500 indikovali použitie originálneho Ethernetového formátu s poľom "dĺžka", kým hodnoty od 1536d (0600h) a vyššie indikovali použitie nového formátu rámca s poľom "typ protokolu".
Špecifikácia IEEE 802.3 však opäť definovala 16-bitové pole za MAC adresami ako pole "dĺžka", pričom hlavička MAC je nasledovaná hlavičkou IEEE 802.2 LLC.
Vyššie spomenutá konvencia umožňuje softvéru určiť či sa jedná o rámec typu Ethernet II. alebo rámec typu IEEE 802.3 a umožňuje tak koexistenciu oboch štandardov na rovnakom fyzickom médiu.

Podvrstva Media Access Control - MAC

- **Media Access Control** (MAC) - podvrstva dátového komunikačného protokolu, ktorá je časťou linkovej vrstvy modelu RM OSI
- poskytuje adresovanie a machanizmus riadenia kanálového prístupu, ktorý umožňuje niekoľkým terminálom, resp. sieťovým uzlom komunikovať v rámci mnohobodovej siete, typicky LAN alebo MAN
- protokol MAC nie je potrebný v prípade plne duplexnej point-to-point komunikácie
- v jednokanálovej point-to-point komunikácii môže byť plne duplexná prevádzka emulovaná, pričom táto emulácia môže byť považovaná za MAC vrstvu
- podvrstva MAC zabezpečuje rozhranie medzi podvrstvou LLC a sieťovou vrstvou
- podvrstva MAC poskytuje mechanizmus adresovania, ktorý označujeme ako fyzické adresy, resp. MAC adresy. Jedná sa o unikátne sériové číslo priradené každému sieťovému adaptéru. Tieto adresy umožňujú doručiť dátové pakety do cieľa v rámci podsiete, t.j. fyzickej siete bez routerov
- **Media access control** je tiež často používaným synonymom pre Multiple Access Protocol, keďže podvrstva MAC poskytuje protokol a riadiace mechanizmy, ktoré sú nevyhnutné pri niektorých metódach kanálového prístupu. To umožňuje niekoľkým staniciam zdieľať pripojenie na rovnaké fyzické médium.

Podvrstva Logical Link Control - LLC

- podľa štandardu IEEE 802 je **Logical Link Control** (**LLC**) hornou podvrstvou linkovej vrstvy RM OSI
- podvrstva LLC je rovnaká pre rôzne fyzické médiá (napr. Ethernet, token ring, WLAN)
- podvrstva LLC zabezpečuje hlavne:
  - multiplexovanie protokolov prenášaných cez podvrstvu MAC pri vysielaní a ich demultiplexovanie pri prijímaní
  - voliteľne zabezpečuje riadenie toku dát, detekciu a retransmisiu stratených paketov
- protokol LLC používaný v sieťach IEEE 802 a v niektorých iných sieťach, napr. FDDI je špecifikovaný štandardom IEEE 802.2
- niektoré protokoly, ktoré nie sú typu IEEE 802 si tiež môžeme predstaviť ako by boli do podvrstiev MAC a LLC rozdelené. Napr. kým HDLC špecifikuje funkciu MAC (tvorba rámcov z paketov) aj funkciu LLC (multiplexovanie protokolov, riadenie toku, atď), niektoré iné protokoly, ako napr. Cisco HDLC môžu používať rámcovanie ako HDLC ale vlastný LLC protokol

MAC adresy

- Media Access Control adresa (MAC adresa) predstavuje unikátny identifikátor jednoznačne určujúci každý sieťový adaptér (NIC)
- mnoho sieťových protokolov 2. vrstvy využíva jednu z troch metód číslovania, ktoré sú riadené organizáciou IEEE, jedná sa o: **MAC-48**, **EUI-48**, a **EUI-64**, ktoré sú všetky globálne unikátne; organizácia IEEE vlastní obchodné známky na mená "EUI-48" a "EUI-64". (EUI - **Extended Unique Identifier**.)
- nie všetky komunikačné protokoly využívajú MAC adresy a nie všetky protokoly vyžadujú globálne unikátne adresy
- MAC adresy (nie ako IP adresy a IPX adresy) nie sú delené na "hostiteľskú" a "sieťovú" časť, takže hostiteľ nemôže z MAC adresy iného hostiteľa určiť či sa tento nachádza na rovnakom sieťovom segmente 2. vrstvy ako posielajúci hostiteľ alebo sieťovom segmente premostenom do tohto sieťového segmentu a nemôže určiť MAC adresu routera, ktorý je na rovnakom sieťovom segmente ako posielajúci hostiteľ alebo segmente premostenom do tohoto segmentu a tak pomocť smerovať paket k cieľovému hostiteľovi
- na účely konverzie adries protokolov 3. vrstvy (napr. IP) na MAC adresy 2. vrstvy sa obvykle používa protokol ARP

MAC adresy

- pôvodné IEEE 802 MAC adresy, teraz oficiálne nazývané "MAC-48", pochádzajú z Ethernetovej špecifikácie. Pôvodní návrhári Ethernetu použili 48-bitový adresný priestor, takže celkovo je k dispozícii 2^{48} možných MAC adries
- všetky tri systémy číslovania používajú rovnaký formát a odlišujú sa len v dĺžke identifikátora
- adresy rozdeľujeme na **individuálne a skupinové**
- **individuálne adresy** môžu byť buď **univerzálne** alebo **lokálne administrované**
  - **univerzálne administrovaná adresa (universally administered address)**
    - jedná sa o adresu unikátne priradenú zariadeniu jeho výrobcom; niekedy ich nazývame "vypálené adresy (burned-in addresses)"
    - prvé tri oktety (v poradí v akom sa vysielajú) identifikujú organizáciu (výrobcu), ktorá použila identifikátor a označujú sa ako Organizationally Unique Identifier (OUI).
    - nasledujúce tri (v prípade systémov MAC-48 a EUI-48) alebo päť (v prípade systému EUI-64) oktetov identifikuje zariadenie v rámci výrobcu a zabezpečujú jedinečnosť označenia
    - organizácia IEEE očakáva, že číselný priestor systému MAC-48 nebude vyčerpaný skôr než okolo roku 2100 a priestor EUI-64s nebude vyčerpaný v dohľadnej budúcnosti
  - **lokálne administrovaná adresa (locally administered address)**
    - je priradená zariadeniu administrátorom siete softvérovým prepísaním adresy danej výrobcom
    - neobsahuje OUI
    - univerzálne a lokálne administrovaná adresa je odlíšená nastavením druhého LSb v MSB adresy; ak je bit = 0, adresa is univerzálne administrovaná, ak je bit = 1, jedná sa o lokálne administrovanú adresu. Vo všetkých OUI je bit = 0. Napr. adresa 20-00-00-00-00-01 je lokálne administrovaná adresa
- adresy MAC-48 a EUI-48 udávame obvykle v hexadecimálnom formáte, pričom každý oktet je separovaný pomlčkou, napr. "00-08-74-4C-7F-1D".

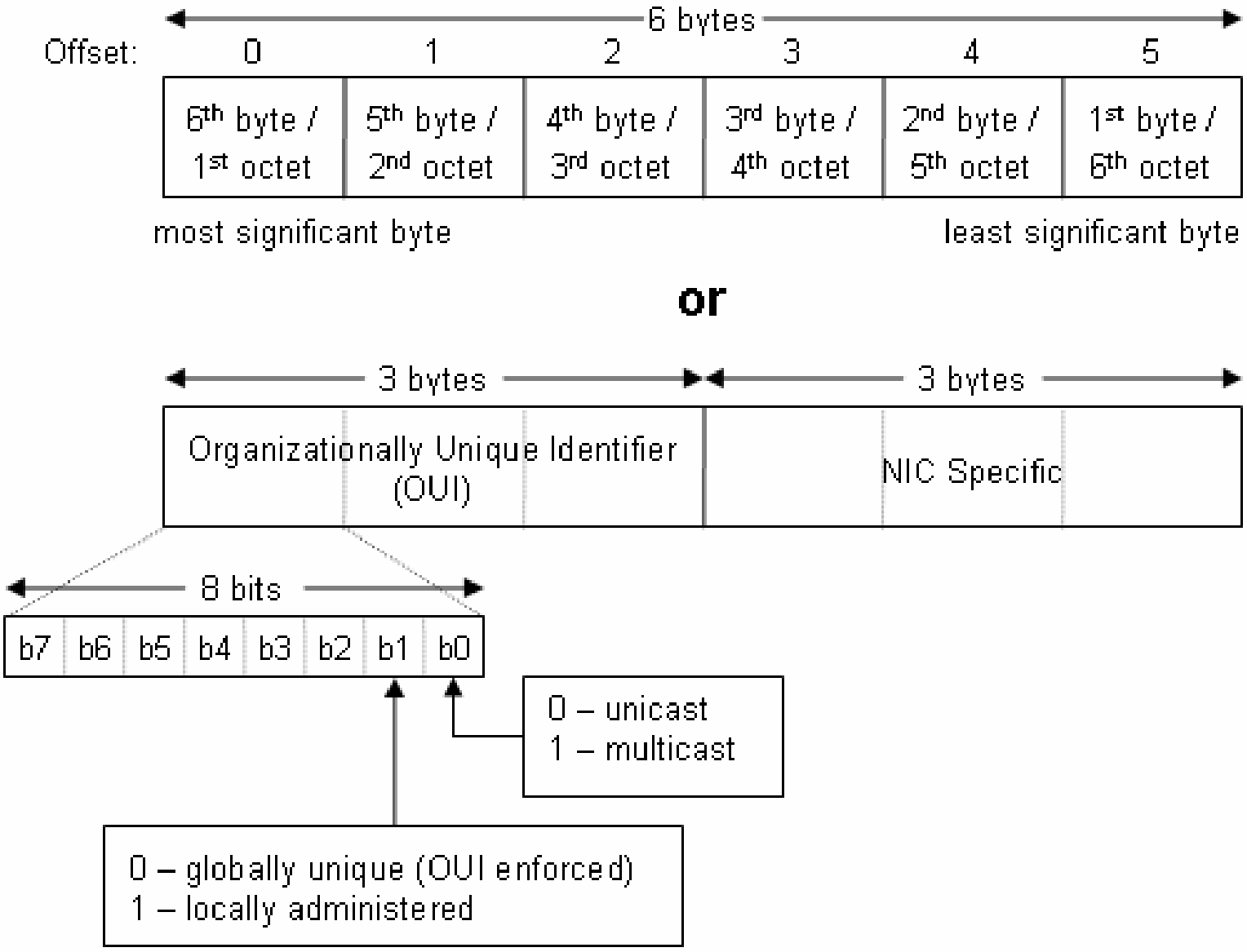
MAC adresy

- formát identifikátorov MAC-48 používajú nasledujúce technológie:
  - Ethernet a ďalšie siete typu IEEE 802
  - bezdrôtové siete WiFi 802.11
  - Bluetooth
  - IEEE 802.5 token ring
  - FDDI
  - ATM (ale len spínané virtuálne prepojenia)
- rozdiel medzi identifikátormi EUI-48 a MAC-48 je čisto sémantický: MAC-48 používame pre sieťový hardvér a EUI-48 používame k identifikácii ďalších zariadení a softvéru. Podľa definície nie je EUI-48 v skutočnosti "MAC adresa", hoci je syntakticky nerozoznateľná a priradená z rovnakého číselného priestoru
- organizácia IEEE v súčasnosti zvažuje, že pod označením MAC-48 bude chápať zastaraný výraz používaný k označovaniu špecifických typov identifikátorov EUI-48 používaných k adresovaniu hardvérových rozhraní v rámci existujúcich sieťových aplikácií typu 802 a nemal by byť používaný v budúcnosti. Namiesto toho by mal byť používaný na tento účel výhradne termín EUI-48.
- číselný formát identifikátorov EUI-64 používajú niektoré ďalšie technológie, napr.:
  - FireWire
  - IPv6
  - ZigBee / 802.15.4 bezdrôtové siete typu "personal-area"

Skupinové MAC adresy

- organizácia IEEE zaviedla niekoľko typov špeciálnych adries nazývaných **skupinové adresy (group addresses)**, aby bolo možné v danom okamihu adresovať viac ako jednu NIC:
  - **broadcast address**, umožňuje poslať pakety všetkým staniciam na danej LAN; jedná sa o adresu v hexadecimálnom tvare "FF:FF:FF:FF:FF:FF"
  - **multicast address**, umožňuje poslať pakety všetkým staniciam na danej LAN, ktoré boli konfigurované administrátorom siete tak, aby prijali pakety posielané na túto adresu
  - **functional addresses**, identifikujú jednu z viacerých NIC v sieti Token Ring, ktorá poskytuje službu definovanú v IEEE 802.5
- LSb 1. oktetu MAC adresy rozlišuje individuálne odresy od skupinových adries. Tento bit je nastavený na 0 pri individuálnych adresách a 1 v skupinových adresách
- aj skupinové adresy, podobne ako individuálne adresy, môžu byť buď univerzálne alebo lokálne administrované

Opis štruktúry MAC adresy



Zmena MAC adresy

- napriek tomu, že fyzická MAC adresa je permanentne uložená v pamäti sieťovej karty výrobcom, existuje niekoľko mechanizmov umožňujúcich modifikáciu MAC adresy (niekedy sa tento úkon označuje ako "spoofing")
- existuje niekoľko prípadov, kedy potebujeme zmeniť MAC adresu
  - ochrana súkromia, napr. v prípade pripojenia k WiFi hotspotu,
  - niektorí poskytovatelia internetových služieb viažu svoje služby na špecifickú MAC adresu; ak potom užívateľ zmení svoju sieťovú kartu alebo plánuje inštalovať router, služba nebude naďalej pracovať. Zmenou adresy nového zariadenia obvykle môžeme takýto problém riešiť, za predpokladu, že poskytovateľ služby nedetekuje zmenu MAC adresy a nezakazuje ju.
  - niektoré softvérové licencie sú tiež viazané na danú MAC adresu.
- softvérovo orientované zmeny MAC adresy modifikujú konfiguračné dáta operačného systému a nie sú teda trvalé
- hardvérovo orientovaná zmena je permanentá a je založená na zmene fyzickej adresy uloženej v EEPROM pamäti na sieťovom zariadení
- keďže MAC adresu môžeme zmeniť, nie je vhodné spoliehať sa na ňu ako na jedinú metódu autentifikácie. Štandard IEEE 802.1x predstavuje vhodnejšie riešenie autentifikácie zariadení na nižšej úrovni.

Prenos rámca

1. MAC podvrstva prijme žiadosť o vyslanie rámca spolu s adresou a dátami od LLC podvrstvy
2. podvrstva MAC zostaví rámec na základe informácií od LLC
3. podvrstva MAC presunie zostavený rámec do bufra MAC rámcov
4. začne prenos cez fyzické médium pri využití prístupovej metódy CSMA-CD

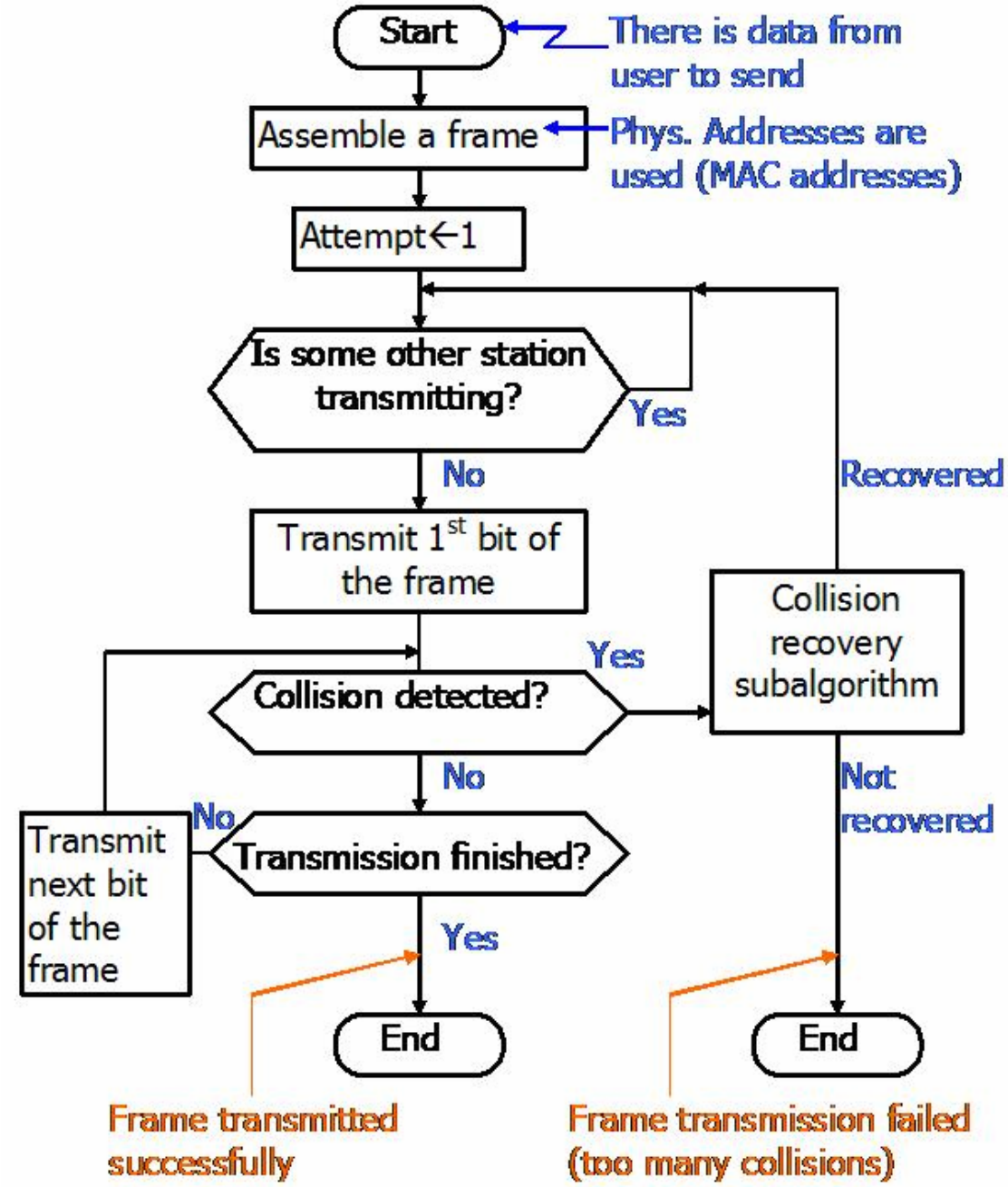
Prístupová metóda CSMA-CD
Carrier Sense Multiple Access with Collision Detection

- každá Ethernetová MAC podvrstva určuje sama sebe, kedy bude možné vysielať rámec
- **Carrier sense:** každá stanica kontinuálne sleduje vysielanie (traffic) na médiu, aby mohla určiť medzeru medzi vysielanými rámcami
- **Multiple access:** stanice môžu začať vysielanie v ktoromkoľvek časovom okamihu po detekcii, že na sieti nikto nevysiela
- **Collision detect**
  - dve alebo viac staníc na rovnakej sieti CSMA/CD (tzv. collision domain) začnú vysielať **v približne rovnakom čase**
  - bitový tok z vysielajúcej stanice zapríčiní interferenciu (kolíziu) s každým ďalším vysielaním, t.j. **všetky prenosy budú nečitateľné**
  - každá vysielajúca stanica musí byť schopná detekovať kolíziu **predtým ako dokončí posielanie svojho rámca**
- **Detekovaná kolízia - riešenie**
  - každá stanica musí ukončiť vysielanie okamžite po detekcii kolízie a potom musí čakať počas intervalu s náhodnou dĺžkou predtým ako sa pokúsi opäť vyslať svoj rámec

Prístupová metóda CSMA-CD
Analýza najhoršieho prípadu (Worst case study)

- **dve najvzdialenejšie stanice na sieti** potrebujú obe vyslať rámec
- **druhá stanica** začne vysielať presne v okamihu, kedy ju dosiahne rámec vyslaný prvou stanicou, t.j. druhá stanica detekuje kolíziu takmer okamžite
- **prvá stanica** nebude schopná detekovať kolíziu, až kým poškodený signál šírením neprejde celú cestu späť k nej
- **neskorá kolízia (late collision)** - nastáva vo chvíli, keď kolízia dosiahne vysielaciu stanicu až potom, keď táto vyslala celý rámec, t.j. vysielacia stanica počas vysielania vôbec nedetekuje kolíziu
- **kolízne okno**
  - maximálny čas potrebný k detekcii kolízie
  - približne rovnaké dvojnásobku času šírenia signálu medzi dvomi najvzdialenejšími stanicami na sieťovom segmente
  - k pojmu kolízneho okna sa priamo vzťahujú minimálna dĺžka rámca a maximálna dĺžka segmentu kolíznej domény

Prístupová metóda CSMA-CD - algoritmus



Prijatie rámca

- proces reverzný k vysielaniu rámca
- podvrstva MAC porovná cieľovú adresu prijatého rámca so zoznamom adries stanice:
  - MAC adresou
  - skupinovou adresou
  - broadcast adresou
- ak je výsledok porovnania pozitívny
  - skontroluje dĺžku rámca
  - porovná hodnotu poľa FCS s hodnotou FCS, ktorá bola vygenerovaná počas prijímania rámca
- ak je dĺžka rámca v poriadku a kontrola FCS neukáže poškodenie rámca, je rámec rozobraný a posunutý na ďalšie spracovanie vhodnej vyššej vrstve

Diagnostické nástroje - *ipconfig*

Opis

Umožňuje zobraziť aktuálnu konfiguráciu TCP/IP siete a aktuálne nastavenia pridelené protokolmi Dynamic Host Configuration Protocol (DHCP) a Domain Name System (DNS).

Ak použijeme príkaz ipconfig bez parametrov, zobrazí IP adresu, masku podsiete (subnet mask), a prednastavenú bránu (default gateway) pre všetky aktívne sieťové adaptéry.

Syntax

ipconfig [**/all**] [**/renew** [*Adapter*]] [**/release** [*Adapter*]] [**/flushdns**] [**/displaydns**] [**/registerdns**] [**/showclassid** *Adapter*] [**/setclassid** *Adapter* [*ClassID*]]

Diagnostické nástroje – *ipconfig, opis parametrov*

/all : zobrazí úplnú konfiguráciu TCP/IP všetkých adaptérov. Adaptérom môže byť fyzické rozhranie, ako napr. inštalovaná sieťová karta, alebo logické rozhranie, napr. dial-up pripojenie.

/renew [*Adapter*] : obnovuje DHCP konfiguráciu všetkých adaptérov (ak nie je adaptér bližšie špecifikovaný) alebo špecifického adaptéra, ak zadáme parameter *Adapter*. Parameter je použiteľný, samozrejme, len na počítačoch, ktorých adaptéry sú konfigurované tak, aby získavali IP adresu automaticky. Meno adaptéra získame použitím príkazu **ipconfig** bez parametrov.

/release [*Adapter*] : pošle správu DHCPRELEASE DHCP serveru, aby uvolnil aktuálnu konfiguráciu DHCP a zrušil IP adresu buď pre všetky adaptéry (ak adaptér nie je špecifikovaný), alebo konkrétneho adaptéru, ak zadáme parameter *Adapter*. Zároveň tento parameter zakáže TCP/IP všetkých adaptérov, ktoré sú konfigurované tak, aby získavali IP adresu automaticky.

/flushdns : odstráni a resetuje cache obsah DNS klienta. Počas riešenia problémov s DNS je možné použiť túto procedúru k odstráneniu neželaných záznamov z cache, podobne ako aj iných záznamov, ktoré boli automaticky pridané.

/displaydns : zobrazí obsah cache DNS klienta, ktorá zahŕňa záznamy uložené na local hoste a všetky nedávno získané záznamy zdrojov. Služba DNS klienta používa tieto informácie k rýchlej identifikácii často zadávaných mien predtým, než bude adresovať požiadavku na zistenie adresy prislúchajúcej danému menu svojmu určenému DNS serveru.

/registerdns : začne manuálnu dynamickú registráciu DNS mien a IP adries, ktoré sú konfigurované na počítači. Tento parameter je možné použiť pri riešení problémov so zlyhávaním registrácie DNS mien alebo pri riešení problémov s dynamickým obnovovaním medzi klientom a DNS severom bez potreby rebootovania klientského počítača.

/showclassid *Adapter* : zobrazí identifikáciu ID DHCP triedy pre daný adaptér. Ak chceme zobraziť ID DHCP triedy, použijeme hviezdičku (*) na mieste parametra *Adapter*. Parameter je použiteľný len na počítačoch, ktorých adaptéry sú konfigurované tak, aby získavali IP adresu automaticky.

/setclassid *Adapter* [*ClassID*] : konfiguruje ID DHCP triedy daného adaptéra. Pre nastavenie ID DHCP triedy všetkých adaptérov, použijeme hviezdičku (*) na mieste parametra *Adapter*. Parameter je použiteľný len na počítačoch, ktorých adaptéry sú konfigurované tak, aby získavali IP adresu automaticky. Ak nešpecifikujeme ID DHCP triedy, príkaz odstráni aktuálne ID triedy.

/?: zobrazenie nápovedy

Diagnostické nástroje - *ping*

Opis

Verifikuje konektivitu počítača na úrovni IP s iným počítačom s protokolom TCP/IP vysielaním správy Internet Control Message Protocol (ICMP) Echo Request. Zobrazí príjem korešpondujúcich správ Echo Reply, spolu s časom vybavenia požiadavky (round-trip time). Ping je základný príkaz protokolu TCP/IP, ktorý používame k riešeniu problémov s konektivitou a dosiahnuteľnosťou. Bez použitia parametrov zobrazuje príkaz ping nápovedu.

Syntax

ping [**-t**] [**-a**] [**-n** *Count*] [**-l** *Size*] [**-f**] [**-i** *TTL*] [**-v** *TOS*] [**-r** *Count*] [**-s** *Count*] [{**-j** *HostList* | **-k** *HostList*}] [**-w** *Timeout*] [*TargetName*]

Diagnostické nástroje – *ping, opis parametrov*

-t : ping bude kontinuálne posielať správy Echo Request do cieľa až do prerušenia jeho činnosti. K prerušeniu činnosti príkazu a zobrazeniu štatistiky je potrebné stlačiť CTRL-BREAK. K prerušeniu a ukončeniu treba stlačiť CTRL-C.

-a : na cieľovej IP adrese dôjde k spätnému určeniu mena hostiteľa. Ak bol proces úspešný, ping zobrazí korešpondujúce meno hostiteľa.

-n *Count* : špecifikuje počet správ Echo Request, ktoré bude ping posielať. Prednastavený počet je 4.

-l *Size* : špecifikuje dĺžku dátového poľa posielanej správy Echo Request v bytoch. Prednastavená hodnota je 32. Maximálna veľkosť je 65,527.

-f : špecifikuje, či budú správy Echo Request posielané s príznakom Don't Fragment flag v hlavičke IP nastaveným na 1. Potom router nemôže správu Echo Request na ceste k cieľu fragmentovať. Parameter je použiteľný pri riešení problémov s Path Maximum Transmission Unit (PMTU).

-i *TTL* : špecifikuje hodnotu poľa TTL v hlavičke IP správ Echo Request. Prednastavená hodnota je 128. Maximálna hodnota *TTL* je 255.

-v *TOS* : špecifikuje hodnotu poľa Type of Service (TOS) v hlavičke IP posielaných správ. Prednastavená hodnota je 0. *TOS* môže nadobúdať dekadické hodnoty od 0 do 255.

-r *Count* : špecifikuje, či bude použitá voľba Record Route v hlavičke IP pre záznam cesty správy Echo Request a korešpondujúcej správy Echo Reply. Každý skok v ceste bude potom zaznamenaný. Ak je to možné, je vhodné špecifikovať *Count* tak, aby jeho hodnota bola rovná alebo väčšia než počet skokov medzi zdrojom a cieľom. Hodnota *Count* musí byť v rozsahu od 1 do 9.

-s *Count* : špecifikuje, či bude použitá voľba Internet Timestamp v hlavičke IP pre záznam času príchodu správy Echo Request a korešpondujúcej správy Echo Reply pri každom skoku. Hodnota *Count* musí byť v rozsahu od 1 do 4.

-j *HostList* : špecifikuje či budú správy Echo Request používať voľbu Loose Source Route v hlavičke IP s nastavením medziľahlých cieľov daných v *HostList-e*. Pri routovaní „loose source“, môžu byť za sebou idúce medziľahlé ciele separované jedným alebo viacerými routermi. Maximálny počet adries alebo mien v HostList-e je 9. HostList tvorí séria IP adries (dekadická notácia separovaná bodkami) separovaných medzerami.

-k *HostList* : špecifikuje či budú správy Echo Request používať voľbu Strict Source Route v hlavičke IP s nastavením medziľahlých cieľov daných v *HostList-e*. Pri routovaní „strict source“, musí byť ďalšia medziľahlá destinácia priamo dosiahnuteľná (t.j. musí byť susedom na rozhraní routera. Maximálny počet adries alebo mien v HostList-e je 9. HostList tvorí séria IP adries (dekadická notácia separovaná bodkami) separovaných medzerami.

-w *Timeout* : špecifikuje hodnotu času v milisekundách, počas ktorej bude ping čakať na správu Echo Reply korešpondujúcu k vyslanej správe Echo Request. Ak ping neprijme správu Echo Reply v danom časovom intervale, zobrazí chybu "Request timed out". Prednastavená hodnota time-out(u) je 4000 ms (4 s).

TargetName : špecifikuje cieľ identifikovaný buď IP adresou alebo menom hostiteľa.

/? : zobrazí nápovedu.

Diagnostické nástroje - *tracert*

Opis

Určuje cestu k cieľovému hostiteľovi vyslaním správy Echo Request pomocu protokolu Internet Control Message Protocol (ICMP) s inkrementálne rastúcou hodnotou poľa Time to Live (TTL). Zobrazená cesta je zoznamom najbližších rozhraní routerov v ceste medzi zdrojom a cieľom. Pod pojmom najbližšie rozhranie routera rozumieme rozhranie, ktoré je najbližšie k vysielajúcemu hostiteľovi v ceste. Príkaz bez parametrov zobrazí nápovedu.

Syntax

tracert [**-d**] [**-h** *MaximumHops*] [**-j** *HostList*] [**-w** *Timeout*] [*TargetName*]

Diagnostické nástroje – *tracert, opis parametrov*

-d : pri použití tohto prepínača príkaz nebude zisťovať mená medziľahlých routerov z ich IP adries. Táto voľba zvyšuje rýchlosť sledovania a získavania výsledkov.

-h *MaximumHops* : špecifikuje maximálny počet skokov v ceste pri hľadaní cieľa. Prednastavená hodnota je 30 skokov.

-j *HostList* : špecifikuje či budú správy Echo Request používať voľbu Loose Source Route v hlavičke IP s nastavením medziľahlých cieľov daných v *HostList-e*. Pri routovaní „loose source“, môžu byť za sebou idúce medziľahlé ciele separované jedným alebo viacerými routermi. Maximálny počet adries alebo mien v HostList-e je 9. HostList tvorí séria IP adries (dekadická notácia separovaná bodkami) separovaných medzerami.

-w *Timeout* : špecifikuje hodnotu v milisekundách, počas ktorej príkaz čaká na ICMP Time Exceeded alebo správu Echo Reply korešpondujúcu k vyslanej správe Echo Request. Ak nedôjde k žiadnemu príjmu počas time-out(u), príkaz zobrazí hviezdičku (*). Prednastavená hodnota time-out(u) je 4000 ms (4 s).

TargetName : špecifikuje cieľ identifikovaný buď IP adresou alebo menom hostiteľa.

-? : zobrazí nápovedu.

Referencie

- www.windowsnetworking.com
- www.wikipedia.org
- www.cisco.com
- www.ethermanage.com