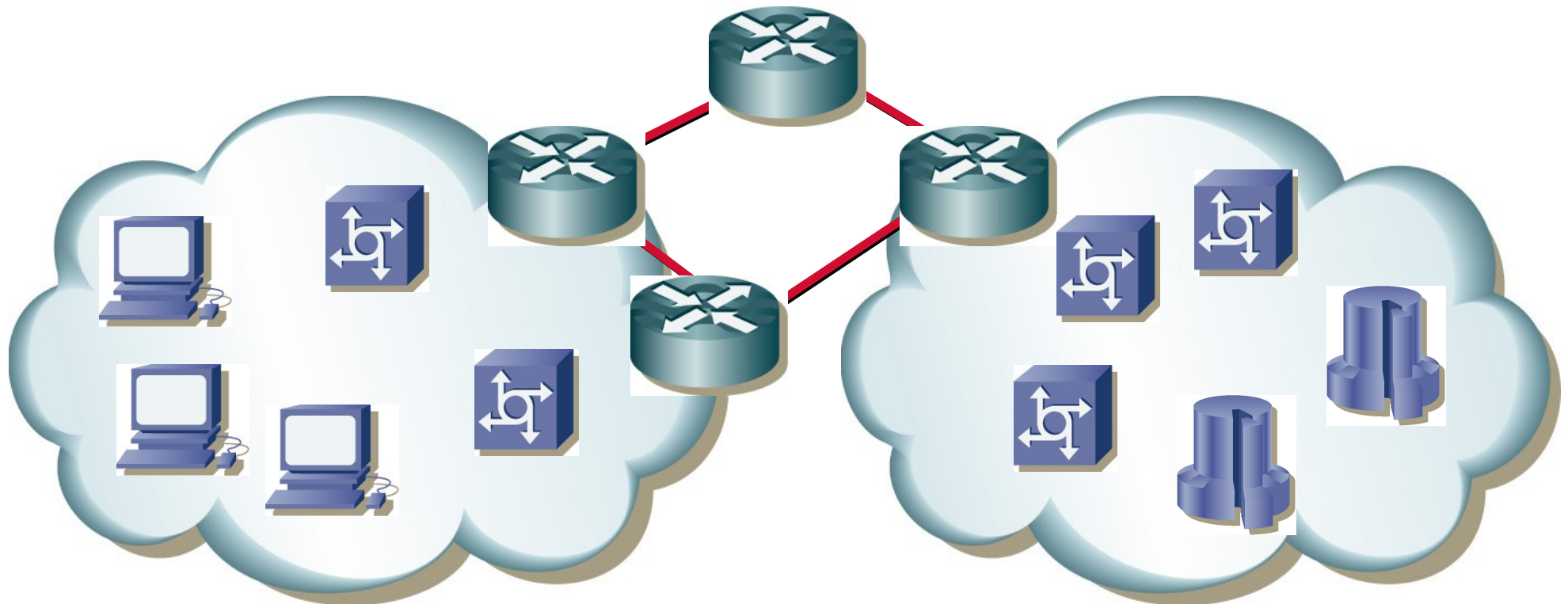


Počítačové sítě II

12. IP: pomocné protokoly (ICMP, ARP, DHCP)

Miroslav Spousta, 2006

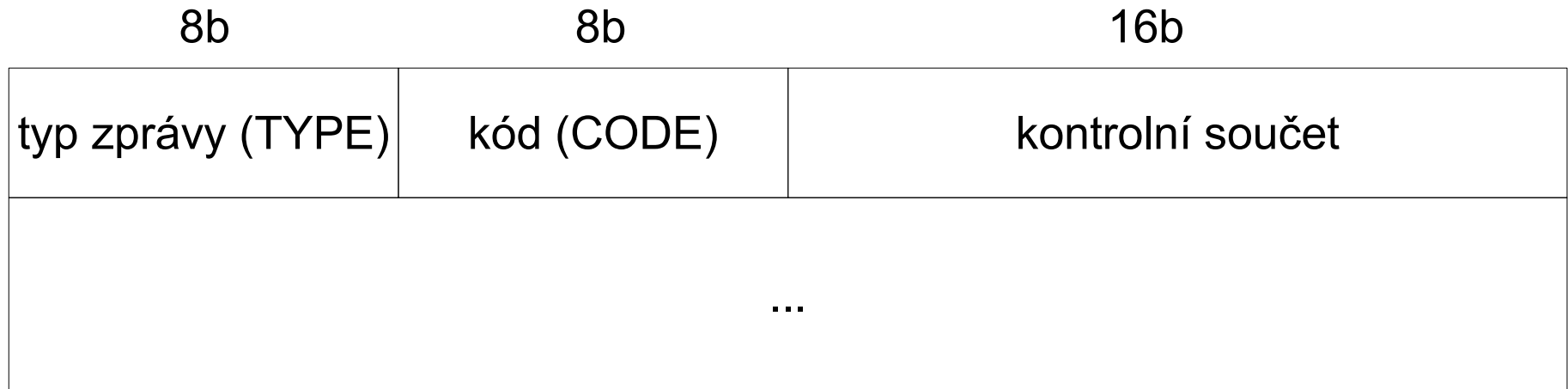
[<qiq@ucw.cz>](mailto:qiq@ucw.cz), <http://www.ucw.cz/~qiq/vsfs/>



ICMP

- Internet Control Message Protocol
 - doslova protokol řídicích hlášení
 - RFC 792
- pomocný protokol IP, vlastně součást IP protokolu
 - přenáší se přímo v IP datagramech
 - problémy s ICMP datagramy se nehlásí
- používá se většinou pro informování o nějakém nestandardním stavu při doručování IP datagramů
- generují se např. při zahození datagramu
 - IP se nestará o nápravu
 - ale informuje odesilatele, že se tak stalo
- ICMP zprávy se zpracovávají v IP stacku odesilatele

ICMP



- typ vyjadřuje o jakou zprávu jde
 - echo request, echo reply, redirect, ...
- kód udává parametry konkrétní zprávy
 - např. z jakého důvodu se nepodařilo datagram doručit
- další formát zprávy závisí na typu
- často následuje původní IP hlavička + 64 bitů dat z původního datagramu
 - pro TCP a UDP jsou tam uloženy porty, umožňuje to identifikovat problémové spojení³

ICMP Destination Unreachable

8b	8b	16b
TYPE = 3	CODE	kontrolní součet
nepoužito		
IP hlavička původního datagramu + 64 bitů dat		

- **CODE**

- 0: síť nedostupná (net unreachable) – směrovač nenašel cestu k síti
- 1: stanice nedostupná (host unreachable) – nelze se spojit se stanicí
- 2: protokol nedostupný (protocol unreachable)
- 3: port nedostupný (port unreachable)
- 4: fragmentace nutná, ale byl nastavený příznak DF (Don't fragment)
- 5: špatné zdrojové směrování (source route failed)

- 2, 3 od cílové stanice, 0, 1, 4, 5 od směrovače

ICMP Time Exceeded

8b	8b	16b
TYPE = 11	CODE	kontrolní součet
nepoužito		
IP hlavička původního datagramu + 64 bitů dat		

- **CODE**
 - 0: Time to Live Exceeded – TTL kleslo na nulu (příliš mnoho směrovačů po cestě)
 - 1: Fragment Reassembly Time Exceeded – vypršel čas na sestavení datagramu z fragmentů; pokud nedošel fragment 0, nic se neposílá
- **TTL brání zacyklení**
 - je nutné vždy při skoku ve směrovači přepočítat kontrolní součet IP hlavičky
- **kód 0: od směrovače, kód 1: od stanice**

traceroute, tracepath

- zasílání zpráv od směrovače, pokud TTL klesne na 0 lze využít pro stopování cesty datagramů sítí
- nastavíme TTL na 1 a vyšleme datagram k cíli
- vrátí se nám od prvního směrovače => zjistíme adresu prvního směrovače
- nastavíme TTL na 2, ...
- běžně se používá TTL kolem 64
- počet přeskoků („hopů“) z ČR do USA běžně kolem dvaceti
- traceroute a tracepath jsou programy, které zjišťují cestu k cíli
- traceroute používá UDP pakety, případně může používat ICMP echo request datagramy

traceroute, tracepath

traceroute to 195.113.31.123 (195.113.31.123), 30 hops max, 38 byte packets

```
1  s1.chello.upc.cz (62.24.84.1)  86.565 ms  48.663 ms  21.908 ms
2  cz-prg01a-ra2-ge0-0-0-v20.aorta.net (213.46.172.9)  17.375 ms  14.643 ms  5.852 ms
3  at-vie01a-rd1-pos-1-0-0.aorta.net (213.46.160.53)  10.940 ms  25.298 ms  11.238 ms
4  at-vie02a-ril-pos-4-0.aorta.net (213.46.173.6)  12.161 ms  27.251 ms  11.681 ms
5  Wien1.ACO.net (193.171.16.162)  24.182 ms  12.473 ms  12.142 ms
6  195.113.179.149 (195.113.179.149)  13.623 ms  15.295 ms  11.803 ms
7  r92-r41-oc48.cesnet.cz (195.113.156.126)  14.339 ms  13.646 ms  13.179 ms
8  geovc-cesnet.pasnet.cz (195.113.69.53)  12.408 ms  35.663 ms  41.404 ms
9  geruk-geovc.pasnet.cz (195.113.68.237)  12.076 ms  13.161 ms  13.301 ms
10 flor-ruk.pasnet.cz (195.113.69.118)  12.803 ms  13.360 ms  12.571 ms
11 karlingw-c.karlin.mff.cuni.cz (195.113.31.130)  12.472 ms  12.701 ms  12.412 ms
12 k5gw.karlin.mff.cuni.cz (195.113.31.137)  12.682 ms  12.995 ms  12.428 ms
13 atrey.karlin.mff.cuni.cz (195.113.31.123)  13.067 ms  12.311 ms  19.759 ms
```

ICMP Parameter Problem

8b	8b	16b
TYPE = 12	CODE	kontrolní součet
pointer	nepoužito	
IP hlavička původního datagramu + 64 bitů dat		

- nastala „jiná chyba“ a datagram byl zahozen
 - např. chybná data v hlavičce
- pokud je CODE = 0, pointer ukazuje do původního datagramu, kde nastala chyba

ICMP Source Quench

8b	8b	16b
TYPE = 4	CODE = 0	kontrolní součet
nepoužito		
IP hlavička původního datagramu + 64 bitů dat		

- směrovač je zahlcen a musí zahazovat datagramy
- za každý zahozený datagram vygeneruje tuto zprávu
- může generovat zprávy i dříve (datagramy mohou být doručeny, i když pro ně byla vygenerovaná zpráva Source Quench)
- jedná se vlastně o žádost o snížení toku dat, které generuje zdrojová stanice
- neexistuje inverzní zpráva (zahlcení pominulo)

ICMP Redirect

8b	8b	16b
TYPE = 5	CODE	kontrolní součet
adresa nové brány (gateway)		
IP hlavička původního datagramu + 64 bitů dat		

- CODE
 - 0: přesměrovat datagramy pro síť
 - 1: přesměrovat datagramy pro stanici
 - 2: přesměrovat datagramy pro TOS a síť
 - 3: přesměrovat datagramy pro TOS a stanici
- pokud první směrovač zjistí, že stanice má lepší cestu k danému cíli, pošle tuto zprávu
- filtrovat na vnějších rozhraních sítě!

ICMP Echo Request/Echo Reply

8b	8b	16b
TYPE = 8/0	CODE = 0	kontrolní součet
identifikátor		sequence number
data...		

- žádost o odpověď (TYPE = 8) je vyslána k cíli
- cílový uzel zamění adresy, přepíše TYPE na 0 odešle zpět (data zůstávají stejná)
- umožňuje detekovat:
 - funkčnost IP stacku cílové stanice
 - počet hopů, MTU po cestě (nastavením velikosti dat)
 - RTT (Round Time Trip) – doba přenosu dat tam a zpět

ping

```
qiq@bug:~$ ping -s 5000 195.113.31.123
PING 195.113.31.123 (195.113.31.123) 5000(5028) bytes of data.
5008 bytes from 195.113.31.123: icmp_seq=1 ttl=53 time=892 ms
5008 bytes from 195.113.31.123: icmp_seq=3 ttl=53 time=114 ms
5008 bytes from 195.113.31.123: icmp_seq=4 ttl=53 time=578 ms
5008 bytes from 195.113.31.123: icmp_seq=5 ttl=53 time=154 ms
5008 bytes from 195.113.31.123: icmp_seq=6 ttl=53 time=133 ms
5008 bytes from 195.113.31.123: icmp_seq=7 ttl=53 time=122 ms
5008 bytes from 195.113.31.123: icmp_seq=8 ttl=53 time=103 ms
5008 bytes from 195.113.31.123: icmp_seq=9 ttl=53 time=100 ms
5008 bytes from 195.113.31.123: icmp_seq=10 ttl=53 time=99.3 ms
5008 bytes from 195.113.31.123: icmp_seq=11 ttl=53 time=103 ms
5008 bytes from 195.113.31.123: icmp_seq=12 ttl=53 time=105 ms
--- 195.113.31.123 ping statistics ---
12 packets transmitted, 11 received, 8% packet loss, time 11010ms
rtt min/avg/max/mdev = 99.376/227.984/892.493/248.939 ms
```

ICMP Timestamp

8b	8b	16b
TYPE = 13/14	CODE = 0	kontrolní součet
identifikátor		sequence number
čas odeslání (zdroj)		
čas příjmu (cíl)		
čas odeslání (cíl)		

- odesílatel zaznamená čas odeslání
- příjemce čas přijetí a čas odeslání zpět
- slouží k zjištění doby přenosu dat k cílové stanici

ICMP Router Discovery Protocol

8b	8b	16b
TYPE = 9	CODE = 0	kontrolní součet
počet adres	velikost adresy (2)	životnost (s)
Router address 1		
Preference 1		
Router address 2		
Preference 2		

- RFC 1256
- 9: Router Advertisement
 - inzerování adresy směrovače, směrovač periodicky (nebo na žádost) inzeruje svoji adresu v síti a posílá ji na broadcast/multicast adresu všem připojeným uzlům
- 10: Router Solicitation
 - žádost stanice o adresu směrovače
 - jednoduchý datagram s TYPE = 10

ICMP

- další zprávy ICMP:
 - v dnešní době zastaralé, nahrazené RARP, BOOTP, DHCP
- 17/18: Address Mask Request/Reply
 - žádost o masku sítě
- 14/15: Information Request/Reply
 - žádost o adresu sítě

Překlad adres

symbolické jméno

DNS

IP adresa

ARP

MAC adresa

- MAC adresy jsou přiřazeny zařízením, používají se k adresaci na linkové úrovni, jsou závislé na zařízením, slouží k rozlišení uzlu v rámci *lokální sítě* (např. V Ethernetu)
- IP adresy jsou *univerzální v celé síti*, nezávislé na použité síťové technologii
- komunikující uzel má obě adresy, je potřeba mít mechanismus, jak zajistit převod mezi adresami
- Address Resolution (IP => MAC)
- Reverse Address Resolution (MAC => IP)

ARP

- Address Resolution Protocol, RFC 826
- protokol, který dokáže zjistit MAC adresu uzlu, pokud známe jeho IP adresu
- kdy se to hodí? Posíláme datagramy na určitý uzel (koncovou stanicí nebo směrovač) v lokální síti, neznáme její linkovou (MAC) adresu
- dynamický, distribuovaný protokol, schopný reagovat na změny v síti
 - informace se podle potřeby obnovují
 - překladová tabulka obsahuje většinou pouze dočasné položky
- pokud chce stanice znát MAC adresu jiného počítače v dané síti, vyšle linkový broadcast – ARP dotaz
- stanice, která rozpozná svoji IP adresu odpoví linkovým unicastem – ARP odpověď

ARP

- ARP pracuje „mezi“ linkovou a síťovou vrstvou
 - používá rámce linkové (tedy nikoli IP datagramy), ale přenáší IP adresu
 - v Ethernetu používá typ rámce 0x0806 (IP používá 0x0800)
- žádost vyšle IP vrstva když zjistí, že je potřeba odeslat rámec a není známá MAC adresa příjemce
 - vyšle se jen jeden ARP dotaz, i když rámců k vyslání je víc
 - pokud odpověď nepřijde do timeoutu, ohlásí chybu (host unreachable)

6B	6B	2B	28B
cílová MAC	zdrojová MAC	typ	ARP žádost/odpověď

ARP

- typ média: Ethernet: 1, ATM: 16
- protokol: pro IP 0x0800
- délka MAC adresy: 6
- délka IP adresy: 4
- operace: žádost: 1, odpověď: 2
- zdrojová MAC a IP adresa
 - adresy odesilatele žádosti nebo toho, kdo odpovídá
- cílová MAC a IP adresa
 - adresa příjemce (v případě žádosti je MAC adresa broadcast (všechny 1))

Typ média	
Protokol	
Délka MAC adresy	Délka IP adresy
operace	
Zdrojová MAC adresa	
Zdrojová IP adresa	
Cílová MAC adresa	
Cílová IP adresa	

ARP algoritmus

- počítač chce poslat data (IP datagram) jinému počítači v síti
 - potřebuje zjistit MAC adresu příjemce
 - podívá se do cache, je-li tam položka => OK
 - není, musí se použít ARP protokol
- vyšle rámeček s broadcast cílovou MAC adresou (a s vyplněnými ostatními)
- příjemce zkontroluje, jedná-li se o jeho IP adresu, ne => rámeček zahodí
- vyplní svoji MAC adresu a prohodí páry adres, aby odpovídaly odesilateli/příjemci
- odešle rámeček zpět (unicastem)
- do ARP tabulky si přidá adresu tazatele (pravděpodobně s ním bude komunikovat)

Proxy ARP

- některý prvek v síti (směrovač) odpovídá na ARP dotazy za uzel, který je „skrytý“ za ním
- odpovídá svojí adresou (a datagramy poté směřuje správným směrem)
- vlastně rozšiřuje lokální síť přes směrovač
- směrovač v síti „není vidět“

RARP

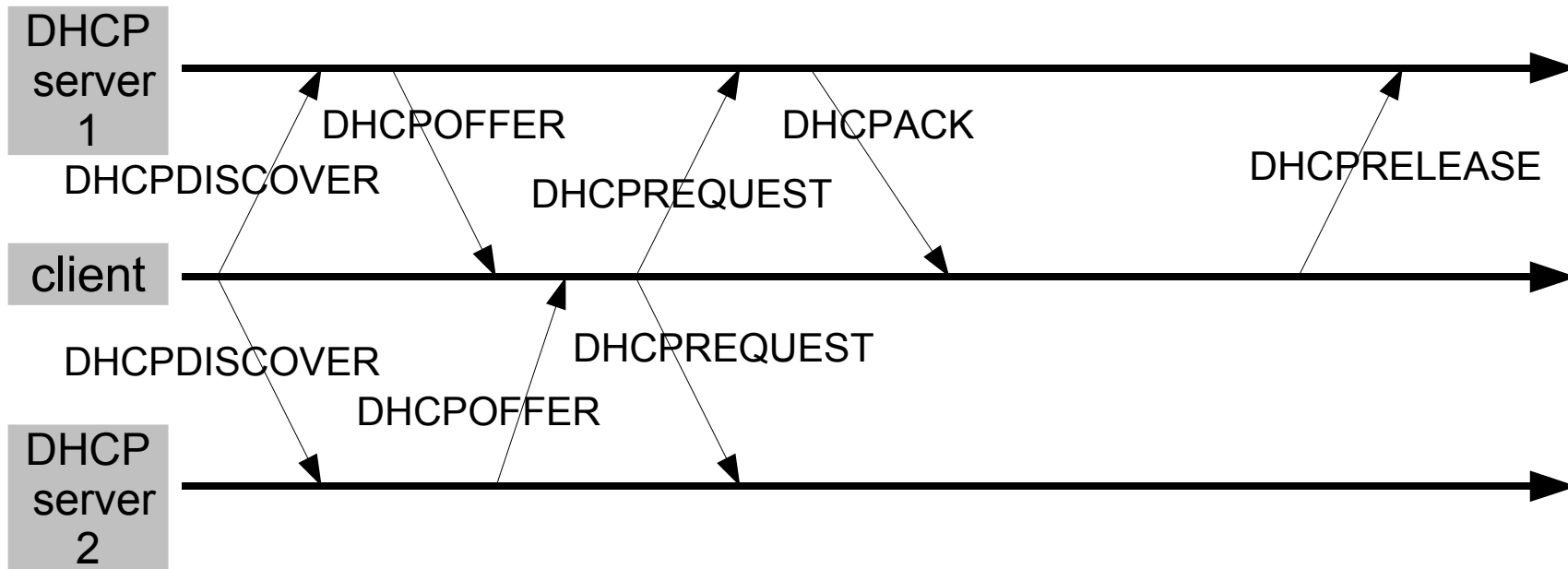
- Reverse Address Resolution Protocol, RFC 903
- IP adresa bývá na uložena v konfiguračním souboru na disku
 - MAC bývá v ROM na síťové kartě (nebo ekvivalentu)
 - vzniká problém s bezdiskovými stanicemi – znají MAC, ale ne IP adresu
- formát rámce stejný jako u ARP, ale operace je 3 pro žádost, 4 pro odpověď
- typ v ethernetovém rámci je 0x8035

Typ média	
Protokol	
Délka MAC adresy	Délka IP adresy
operace	
Zdrojová MAC adresa	
Zdrojová IP adresa	
Cílová MAC adresa	
Cílová IP adresa	

DHCP

- Dynamic Host Configuration Protocol, RFC 2131
- rozšíření staršího protokolu BOOTP
- umožňuje automatickou konfiguraci sítě stanic
- centrální přidělování IP adres a dalších informací o síti
 - maska sítě, implicitní směrovač, DNS server, WINS server
- tyto informace se periodicky obnovují
- klient i server si pamatují minulý stav => klient dostává stejnou IP adresu (pokud je to možné)

DHCP



- DHCP serverů může být v síti několik
- klient pošle DISCOVER zprávu, dostane odpověď DHCPOFFER
- klient si vybere, který server použije
- odpoví DHCPREQUEST a dostane přidělenou adresu DHCPACK
- pokud chce adresu vrátit, vyšle DHCPRELEASE