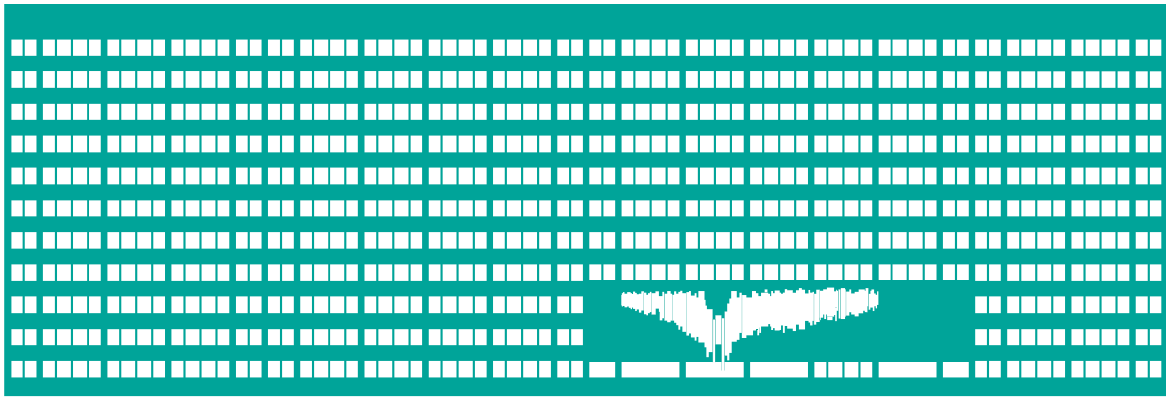
VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE | DEPARTMENT OF COMPUTER SCIENCE

Analýza protokolů rodiny TCP/IP, NAT



Počítačové sítě
7. cvičení

ARP
Address Resolution Protocol

- mapování IP adres na MAC adresy
- Při potřebě zjistit MAC adresu k IP adrese se generuje **ARP request** (broadcast), ten obsahuje požadovanou IP adresu. Stanice s touto adresou odpoví svou MAC adresou (**ARP reply**).
- Zdroj ARP dotazu si výsledek uloží do ARP cache
  - (lokální cache na stanici, udržuje známá mapování IP-MAC)
- Navíc se do **requestu** vkládá dvojice < zdrojová IP, zdrojová MAC >, každý počítač sleduje všechny ARP broadcasty a doplňuje informace ve své ARP cache

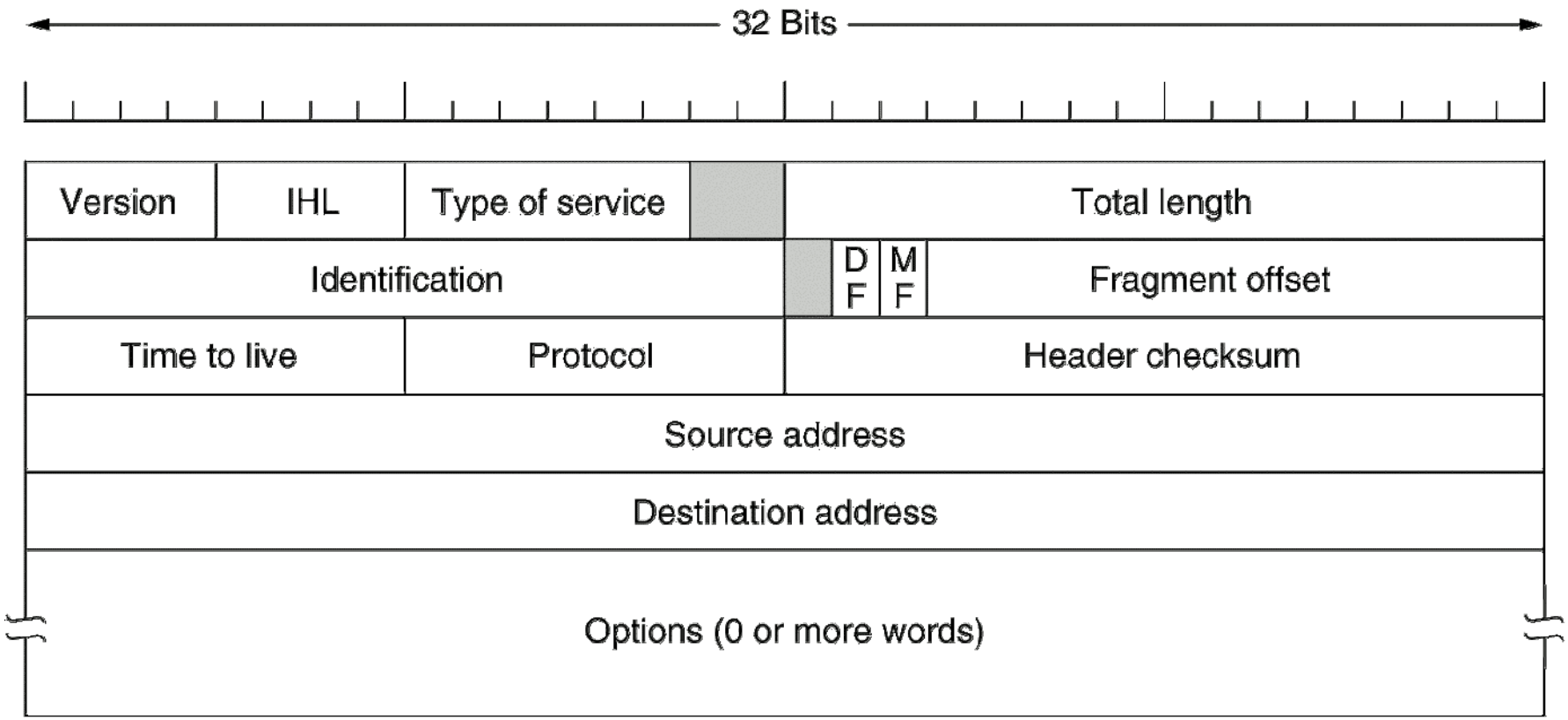
Práce s příkazem arp

- Výpis tabulky mapování MAC-IP (Linux, Win)
  - Parametry:
    - **-a** výpis všech záznamů v arp cache
    - **-s** <*IP*> <*MAC*> ruční vložení (statického) záznamu
    - **-d** <*IP*> výmaz záznamu z arp cache
  - Parametry v Linuxu:
    - **-v** detailní výpisy
    - **-n** výpisy v numerické podobě (bez DNS)

- Příklad výpisu (Windows):

```
Rozhraní: 158.196.64.66 --- 0x10004
  internetová adresa    fyzická adresa          typ
  158.196.64.1          00-0a-f3-6e-bc-0a     dynamická
  158.196.64.137        00-0c-f1-3c-54-87     dynamická
```

Hlavička IP


32 Bits
Version
IHL
Type of service
Total length
Identification
D F
M F
Fragment offset
Time to live
Protocol
Header checksum
Source address
Destination address
Options (0 or more words)

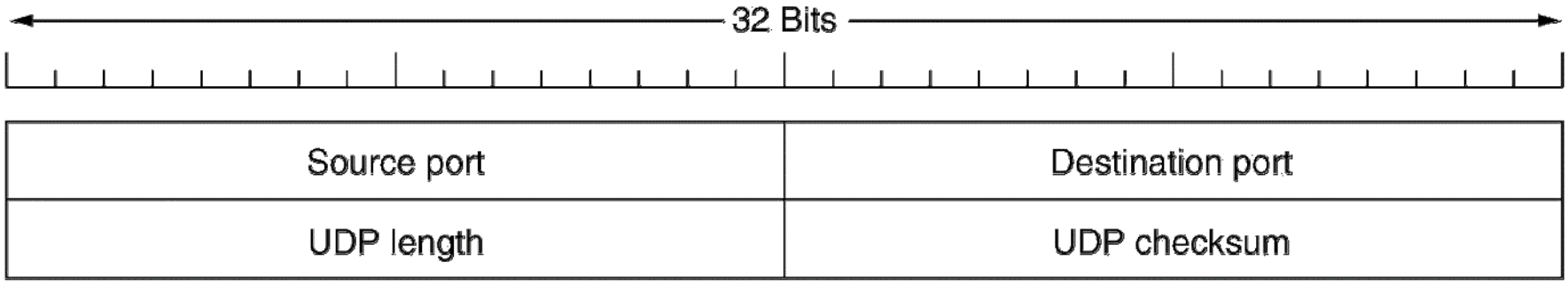
Zprávy ICMP

- „Klasické“ zpravy
  - **Echo request** , **echo reply**
  - **Destination unreachable**
    - (network, host, port, protocol unreachable, zakázaná, ale nutná fragmentace)
    - + administratively prohibited
  - **Time exceeded** (TTL=0 nebo vypršel čas pro refragmen.)
  - **Redirect**
  - **Parameter problem**
- Novější (a ne vždy podporované) zprávy
  - **Source quench** - žádost cílové stanice o snížení rychlosti generování zpráv zdrojem (přeplňují se buffery)
  - **Address mask request**, **Address mask reply** - zjištění síťové masky rozhraní
  - **Router solicitation**, **Router advertisement**

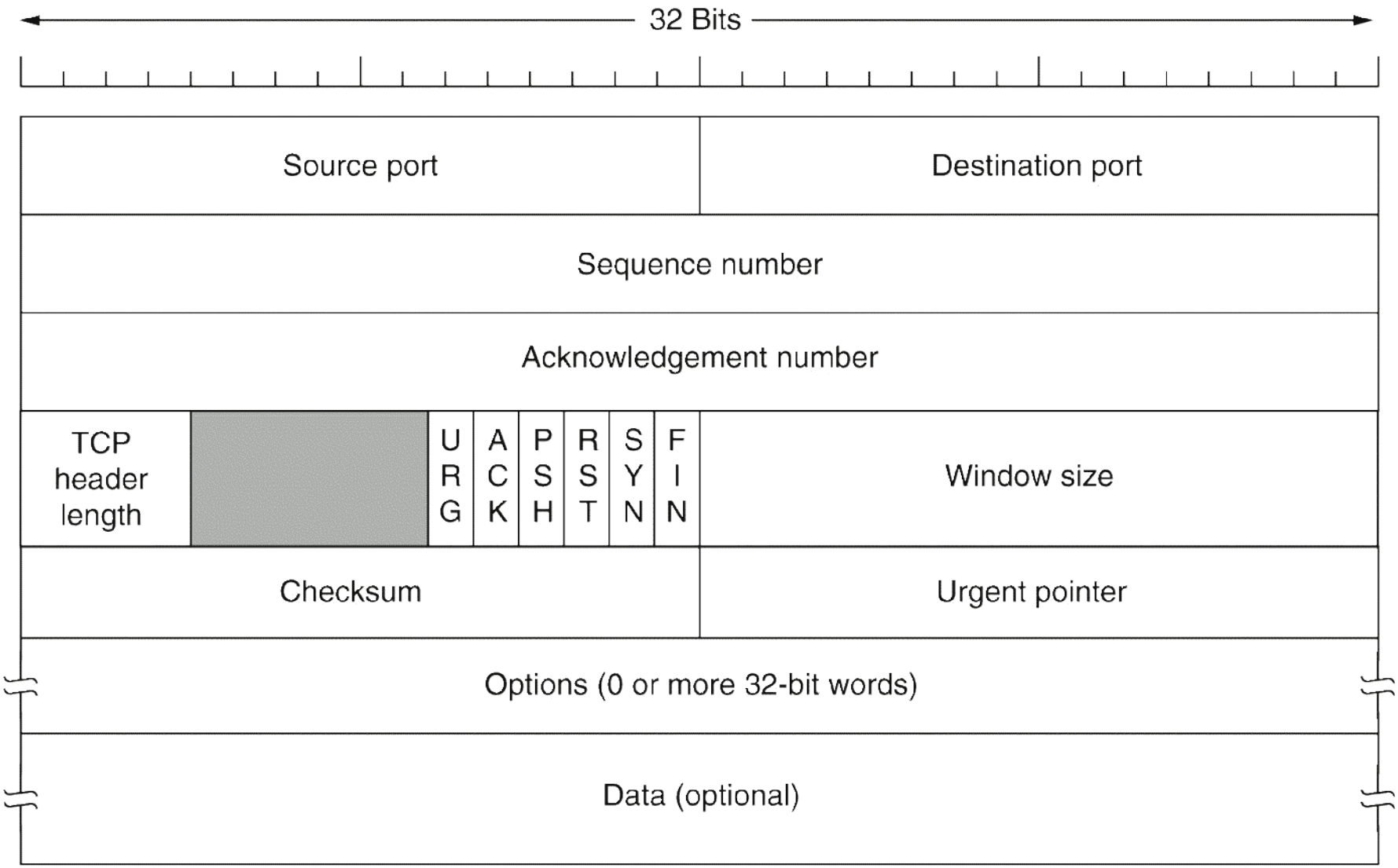
Porty

- Spolu s IP adresou identifikují konkrétní proces (službu) na konkrétním zařízení v Internetu
- 16bit (0-65535), zvlášť pro TCP a UDP
  - 0-1023: Veřejně definované služby (well-known)
  - >1024 (4096) – klientské porty, obvykle přidělování volných portů operačním systémem
- Vždy cílový i zdrojový port

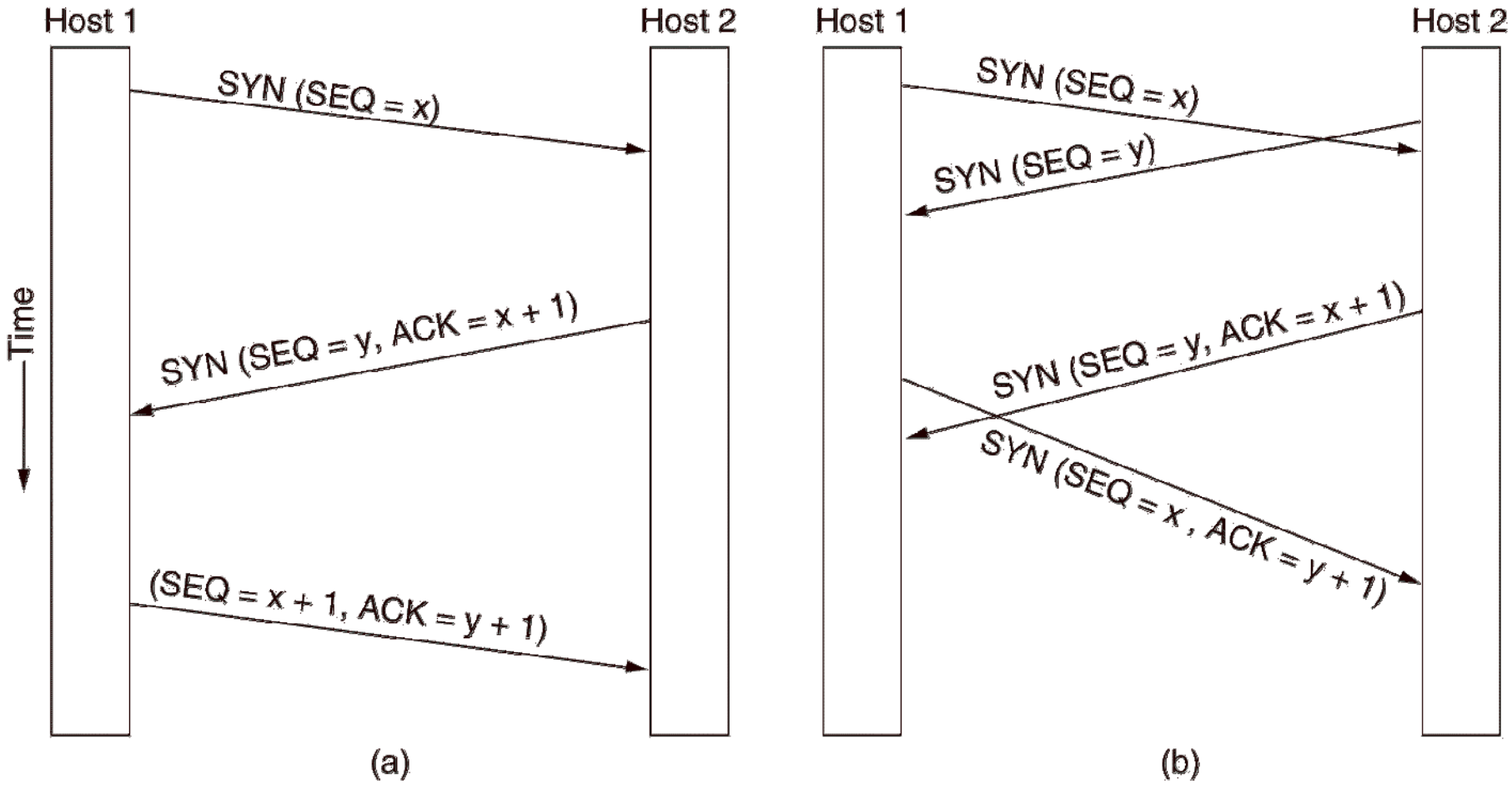
Hlavička UDP



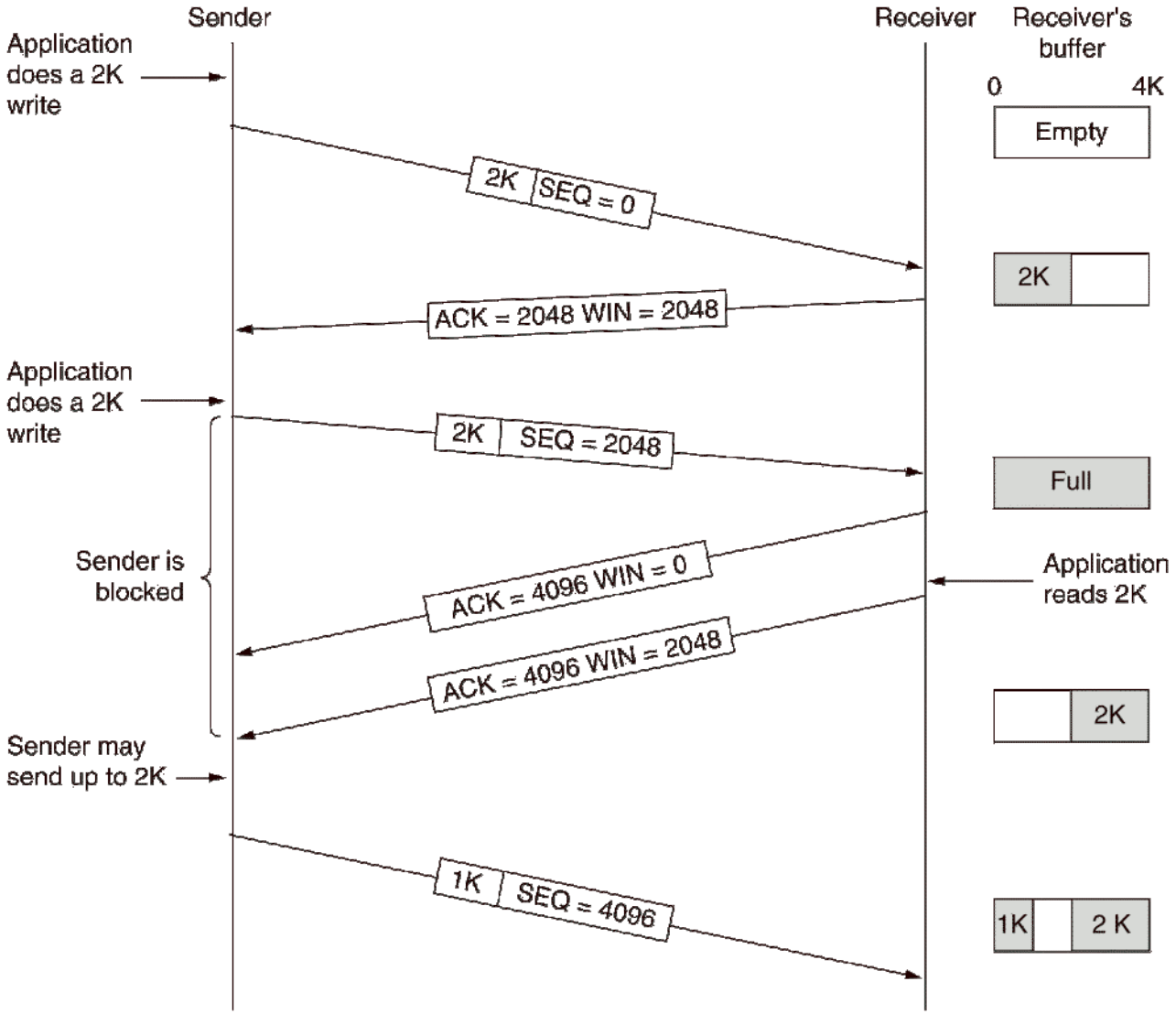
Hlavička TCP



Navazování TCP spojení



Průběh TCP spojení - řízení toku dat



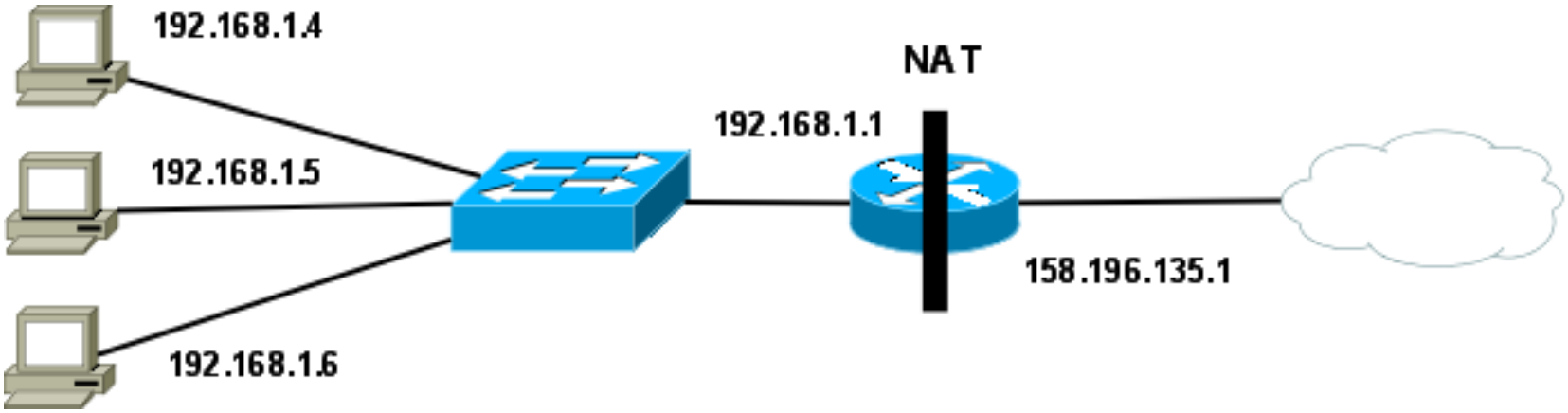
Práce s příkazem netstat

- Výpis aktivních připojení (Linux, Windows)
  - Parametry:
    - **`-a`** výpis všech spojení a naslouchajících serverů
    - **`-r`** výpis směrovací tabulky
    - **`-v`** detailní výpisy
    - **`-n`** výpis spojení v číselném formátu (bez DNS)
  - Parametry ve Windows:
    - **`-p`** *<protokol>* jen daný protokol (tcp, udp, …)
    - **`-b`** název programu, který soket využívá
  - Parametry v Linuxu:
    - **`-u`** | **`-t`** | **`-w`** jen daný protokol (tcp, udp, raw, …)
    - **`-p`** PID a název programu, který soket využívá

NAT

- Network address translation (translator)
  - Překlad adres (dynamický, statický) – IP→IP
  - Statický překlad
    - překladová tabulka konfigurována staticky
  - Dynamický překlad
    - překladová tabulka se vytváří za provozu
    - adresy se propůjčují z rezervoáru (pool) adres
  - Typický příklad překladu
    - z vnitřní privátní adresy na vnější veřejnou adresu

Příklad překladové tabulky s použitím portů



Zdrojová IP	Zdroj. port	Zdrojová IP	Zdroj. port
192.168.1.4	2345	158.196.135.2	2345
192.168.1.5	4589	158.196.135.2	4589
192.168.1.4	5678	158.196.135.2	5678
192.168.1.6	5678	158.196.135.2	5679

NAT v IOS

- Určení vnitřního a vnějšího rozhraní:
  - Vnitřní: **`(config-if)# ip nat inside`**
  - Vnější: **`(config-if)# ip nat outside`**
- Definice adres, KTERÉ budou překládány (typicky privátní adresy)
- Definice adres, NA KTERÉ bude překládáno (typicky veřejné adresy)
- Svázání definic dohromady

Statický NAT

- Překlad zdrojové adresy:
  - **(config)#ip nat inside source static** *<local_IP> <global_IP>*
- Překlad cílové adresy (pro defiovaný L4 port):
  - **(config)#ip nat inside source static** {**tcp**|**udp**} *<local_IP> <local_port> <global_IP> <global_port>*

Dynamický NAT – definice adres

- Definice rezervoáru (pool) adres (tzn. NA CO překládám):
  - **(config)# ip nat pool** <*NAZEV*> <*start_IP*> <*stop_IP*> **netmask** <*maska*>
    - Př.: `ip nat pool MujNATPool 20.0.0.1 20.0.0.100 netmask 255.255.255.0`
- Vybrání překládaných adres – pomocí ACL (tzn. CO se má překládat):
  - **(config)# access-list** <*ACL číslo 1-99*> **permit** <*IP*> <*wildcard*>
    - Př.: `access-list 1 permit 10.0.0.0 0.0.0.255`

Dynamický NAT

- Překlad na adresy z poolu:
  - **(config)# ip nat inside source list** <*ACL číslo*> **pool** <*NAZEV*> [**overload**]
    - Př.: ip nat inside source list 1 pool MujNATPool overload
- Překlad na adresu vnějšího rozhraní:
  - **(config)# ip nat inside source list** <*ACL číslo*> **interface** <*jméno rozhraní*> [**overload**]
    - Př.: ip nat inside source list 1 interface fa0/1 overload

NAT – zobrazení překladové tabulky

- Zobrazení překladové tabulky:
  - **#sh ip nat translations**
- Vymazání překladové tabulky:
  - **#clear ip nat translations** *
- Změna doby, kdy záznam zůstává v tabulce:
  - **(config)# ip nat translations timeout** *<počet_sekund>*
  - **(config)# ip nat translations icmp-timeout** *<počet_sekund>*
- Debug výpisy NAT překladu
  - **#debug ip nat**

NAT – příklad

- Propojte 3 směrovače za sebou (řetěz)
- Ke každému připojte stanici
- Prostřední směrovač simuluje síť s veřejnými adresami (všechna jeho rozhraní mají veřejné adresy)
- Postranní směrovače mají stanice zapojeny v privátní síti a realizují NAT
  - NAT pool je propagován do směrovacího protokolu
  - Překlad adres v obou směrech