# 5. Protokol IP, ICMP, ARP, IGMP a IGRP

## Teoretická část

Popište a vysvětlete IP protokol včetně pojmů: IP adresa, Maska podsítě, CIDR maska, Supernet, Wildcard maska. Popište třídy IP adres neveřejného rozsahu.

Vysvětlete a popište, k čemu slouží a jak pracuje protokol ARP s MAC adresou (včetně RARP). Vysvětlete a popište pojmy IGMP a IGRP.

Vysvětlete a popište, k čemu slouží a čeho využívá protokol ICMP.

## Praktická část

1. V CMD předveďte a popište funkce: ping, tracert, pathping, ipconfig, route a arp.
2. Nakreslete a popište, co je a jak pracuje supernet.
3. Předveďte z CIDR a změt na masku příklady /24, 255.255.0.0, /23, /10, 255.128.0.0 .
4. Nakreslete a popište, co tvoří IP adresu.

## Doplňující otázky

1. Popište protokoly IGMP a IGRP, následně uveďte, zda jsou podobného použití. Pokud ne, vysvětlete proč.
2. Převeďte následující Masky podsítě na WIldcard masky: 255.255.255.0, 255.128.0.0, 255.255.254.0, /20 .

# Teoretická část

## IP protokol

Internet Protocol  je v [informatice](https://cs.wikipedia.org/wiki/Informatika) základním [protokolem](https://cs.wikipedia.org/wiki/Protokol_(informatika)) pracujícím na síťové vrstvě (3.vrstva ISO/OSI) používaným v [počítačových sítích](https://cs.wikipedia.org/wiki/Počítačová_síť) a [Internetu](https://cs.wikipedia.org/wiki/Internet).

Protokol IP poskytuje datagramovou (paketovou) službu celé rodině protokolů [TCP/IP](https://cs.wikipedia.org/wiki/TCP/IP). Sám o sobě neposkytuje záruky na přenos dat a rozlišuje pomocí [IP adresy](https://cs.wikipedia.org/wiki/IP_adresa) pouze jednotlivá [síťová rozhraní](https://cs.wikipedia.org/wiki/Síťová_karta) (doplňující služby jsou poskytovány na vyšších vrstvách, viz [referenční model ISO/OSI](https://cs.wikipedia.org/wiki/Referenční_model_ISO/OSI)). V současné době je stále ještě používána starší verze protokolu [IPv4](https://cs.wikipedia.org/wiki/IPv4), nově se přechází na [IPv6](https://cs.wikipedia.org/wiki/IPv6).

## IP Adresa

IP adresa je logická adresa zařízení v síti IP. Skládá se ze 4 částí zvaných octety, každá část je veliká 8 bitů, a zapisuje se oddělená tečkou.

Adresa se většinou zapisuje v dekadické formě, ale pro výpočet je jasnější binární zápis. Teoreticky je tedy adresní rozsah od 0.0.0.0 do 255.255.255.255. Příkladem IP adresy je třeba 68.12.5.10.

### Třídy IP Adres:

Když vznikl protokol IPv4, byla představa, že adresní prostor je ohromný a nikdy se nemůže vyčerpat. Tento adresní prostor byl rozdělen do základních pěti tříd, kdy se zařazení do patřičné třídy určovalo podle prvních bitů adresy. Při komunikace se nepoužívaly masky podsítě, protože ty byly napevno dány adresou.



### Neveřejné rozsahy

Některé síťové rozsahy mají speciální vlastnosti, tou hlavní je, že se neroutují, tzn. neprochází do dalšího subnetu. To se využívá u privátních subnetů, které neprochází do internetu. V praxi je využívá většina firem v lokální síti a do internetu přistupují přes veřejnou adresu za pomoci NATu.

****

### Maska podsíťě

Subnet mask nám pomáhá určit rozdělení sítě na podsítě. Určuje, která část IP adresy je síťová, a která pro hosty. Zápis je stejný jako u IP adresy, ale platné hodnoty jsou pouze ty, které mají v binárním tvaru zleva jedničky a zprava nuly (pokud se zleva na některé pozici objeví nula, dále již musí následovat pouze nuly). Jedničky v masce jsou tzv. network ID a je to část, která je pro daný subnet stále stejná. Nuly jsou tzv. host ID a tedy část, která je proměnná a určuje adresu hosta v daném subnetu. Příkladem jednoduché masky je 255.255.255.0, ta určuje, že prvních 24 bitů adresy je network ID a posledních 8 bitů je hostovská část.

Možné hodnoty jednotlivých octetů pro masku:

### Zkrácený zápis masky - Classless Inter-Domain Routing (CIDR) notace

Subnet mask se může zapisovat také ve zkrácené formě, které se říká CIDR notace. Ta se zapisuje jako IP adresa následovaná lomítkem (/) a číslem, které reprezentuje počet jedničkových bitů v masce podsítě v binární formě. Protože celkový počet bitů v masce je 32, tak počet nul je 32 - počet jedniček. Příklad CIDR notace je 10.0.5.2/20 a tedy maska je 255.255.240.0.



### Supernet

Občas se také používá termín supernet, který označuje skupinu několika sdružených po sobě jdoucích subnetů. Jedná se vlastně o technologii CIDR a používá se například pro agregaci routovacích záznamů.

Příklad: Máme dva subnety 192.168.0.0/24 a 192.168.1.0/24, z nich můžeme vytvořit jeden supernet 192.168.0.0/23.

### Wildcard mask

Wildcard mask nebo také inversní maska je speciální zápis síťové masky, který používá například Cisco u Access listů. Jedná se o opak ke klasické masce, počítají se zde nuly místo jedniček. Takže například ke klasické masce 255.255.255.240 je inverzní maska 0.0.0.15. Inverzní masku dostaneme tak, že normální masku zobrazíme binárně, provedeme inverzi a převedeme na dekadickou hodnotu. Nebo jednodušeji stačí, u každého octetu spočítat255 - hodnota. Tedy v našem příkladě 255-255=0, 255-240=15.

## ARP

Standardizovaný protokol, který hledá MAC adresu k zadané IP adrese. Jedná se o protokol, který běží na síťové vrstvě TCP/IP modelu (2. vrstva), tedy na stejné úrovni jako IP protokol.

### Princip funkce ARP

Jako zdrojovou stanici označuji ten stroj, který hledá MAC adresu podle IP adresy. Cílová stanice má nastavenu hledanou IP adresu.

* zdrojová stanice sestaví ARP žádost (request) a odešle ji jako broadcast
* všechny stanice na lokálním segmentu přijmou žádost, a pokud nemají tuto IP, tak ji ignorují
* cílová stanice sestaví ARP odpověď (response) a odešle ji jako unicast zdrojové stanici

Jako broadcastová adrese se používá ff:ff:ff:ff:ff:ff

### Reverse ARP

Protokol Reverse ARP (RARP), podobně jako InARP, slouží k nalezení IP adresy k MAC adrese.

RARP ovšem hledá IP adresu pro sebe sama. Tato metoda se již dnes nepoužívá, protože byla

nahrazena nejprve pomocí BOOTP (Bootstrap protocol) a dnes DHCP (Dynamic Host

Configuration Protocol). Pro RARP musely být na serveru manuálně nastaveny přiřazení  
MAC adresy a IP adresy, navíc to není protokol nad IP, ale samostatně na stejné úrovni.

# IGMP

IGMP (Internet Group Management Protokol) je protokol, který rozšiřuje požadavky na implementaci protokolu [IP](https://cs.wikipedia.org/wiki/Internet_Protocol) (IPv4) o podporu [IP multicastu](https://cs.wikipedia.org/wiki/IP_multicast). Využívá se pro dynamické přihlašování a odhlašování ze skupiny u [multicastového](https://cs.wikipedia.org/wiki/Multicast) routeru ve své lokální síti.

Vysílač (zdroj dat) odesílá pakety na multicastovou adresu (která neslouží k identifikaci příjemce, ale skupiny), zdrojová adresa je jeho normální unicastová adresa. Na routerech se pak paket odesílá do všech směrů, kde je nějaký příjemce (provádí se duplikace paketu). Mezi routery se multicast pakety přenáší pomocí multicast směrovacího protokolu (nejčastěji) PIM. Ten vytváří distribuční strom skrze síť a provádí přeposílání paketů.Příjemci (stanice) se musí zaregistrovat do multicast skupiny pomocí protokolu IGMP. Tok paketů je určován příjemci, detaily závisí na použitém směrovacím protokolu (případně variantě PIM protokolu).



l

# IGRP

Je to routovací protokol typu IGP – Distance Vector. Používá se pro výměnu informací v autonomních systémech. Je to proprietární protokol a byl vyvinut na základě toho, že dřívější RIP (Routing Information Protocol) nebyl již dostačující (Měl omezený počet skoků na 15).

Protokol IGRP patří do rodiny protokolů distance vector, a vnitřních protokolů (Interior Gateway Protocol (IGP)). IGRP používá kompozitní metriku vypočítanou z několika položek, jako jsou zpoždění sítě (delay), šířka pásma (bandwidth), spolehlivost (reliability) a zatížení (load). Správce sítě může nastavovat závažnost faktorů pro každou z těchto metrik, ačkoli zásah do těchto nastavení se musí dělat s velkou opatrností. IGRP poskytuje širokou škálu nastavení metriky.

# ICMP

Internet Control Message Protocol je jeden z nejdůležitějších protokolů ze [sady protokolů internetu](https://cs.wikipedia.org/wiki/TCP/IP). Používají ho [operační systémy](https://cs.wikipedia.org/wiki/Operační_systém) počítačů v síti pro odesílání chybových zpráv, například pro oznámení, že požadovaná služba není dostupná nebo že potřebný počítač nebo [router](https://cs.wikipedia.org/wiki/Router) není dosažitelný.

CMP zprávy se konstruují nad IP vrstvou; obvykle z IP datagramu, který ICMP reakci vyvolal. IP vrstva patřičnou ICMP zprávu zapouzdří novou IP hlavičkou (aby se ICMP zpráva dostala zpět k původnímu odesílateli) a obvyklým způsobem vzniklý datagram odešle.

Například každý stroj (jako třeba mezilehlé [routery](https://cs.wikipedia.org/wiki/Router)), který přeposílá IP datagram, musí v IP hlavičce dekrementovat políčko [TTL](https://cs.wikipedia.org/wiki/Time_to_live) („time to live“, „zbývající doba života“) o jedničku. Jestliže TTL klesne na 0 (a datagram není určen stroji provádějícímu dekrementaci), router přijatý paket zahodí a původnímu odesilateli datagramu pošle ICMP zprávu „Time to live exceeded in transit“ („během přenosu vypršela doba života“).

## Praktická část

1. V CMD předveďte a popište funkce: ping, tracert, pathping, ipconfig, route a arp.

**p**ing - testuje spojení se vzdáleným PC, měří dobu odezvy (latenci)

*ping 192.168.10.5 - cílový PC podle IP*

*ping -t komp1 - cílový PC podle DNS jména (provede se překlad) a neskončí po 4 paketech*

tracert- funkce traceroute, sleduje cestu k cíli (přes jaké uzly/hopy)

*tracert www.google.com - pingá jednotlivé hopy*

**pathping**- kombinace funkcí ping a traceroute, rychle projde cestu k cíli a vypíše hopy, pro každý hop provede statistiku pomocí pingu

pathping -q 10 www.google.com - dotaz na cíl podle DNS, 10 dotazů pro každý hop (zkrátí se délka provedení)

**ipconfig** - konfigurace síťových adaptérů (zobrazení TCP/IP hodnot)

**ipconfig /all**- podrobný výpis

**ipconfg /renew** - obnoví IP adresu rozhranní

**ipconfig /registerdns** - obnoví DHCP pronájem a znovu zaregistruje adresu u DNS

**ipconfig /flushdns** - vyprázdní DNS cache

**ipconfig /displaydns**- zobrazí DNS cache

**route**- informace o routovací tabulce

route print - vypíše routovací tabulku

**arp** - práce s ARP tabulkou (mapování IP adres na MAC adresy)

**arp -a** - vypíše ARP tabulku

**arp -d** 157.55.85.212 - smaže záznam

**arp -s** 157.55.85.212 00-aa-00-62-c6-09 - vloží záznam

2. Nakreslete a popište, co je a jak pracuje supernet.

Viz. Nahoře.

3. Předveďte z CIDR a zpět na masku příklady /24, 255.255.0.0, /23, /10, 255.128.0.0

/24 – 11111111.11111111.11111111.000000000 – 255.255.255.0

255.255.0.0 – 11111111.11111111.00000000.00000000 - /16

/23 – 11111111.11111111.11111110.00000000 – 255.255.254.0

/10 – 11111111.11000000.00000000.00000000 – 255.192.0.0

255.128.0.0 – 11111111.10000000.00000000.00000000 - /9

4. Nakreslete a popište, co tvoří IP adresu.

Viz. Nahoře

## Doplňující otázky

1. Popište protokoly IGMP a IGRP, následně uveďte, zda jsou podobného použití. Pokud ne, vysvětlete proč.

Viz. Nahoře

1. Převeďte následující Masky podsítě na WIldcard masky: 255.255.255.0, 255.128.0.0, 255.255.254.0, /20 .

255.255.255.0 – 0.0.0.255

255.128.0.0 – 0.127.255.255

255.255.254.0 – 0.0.1.255

/20 – 255.255.240.0 – 0.0.15.255