# 9. Metody vysílání dat, navazování a ukončování spojení

## Teoretická část

**Vysvětlete a popište metody vysílání dat Unicast, Broadcast, Multicast. Vysvětlete a popište metody navazování a ukončování spojení (Handshake) 3cestný a 4cestný. Popište pozitivní a negativní navázání a ukončení spojení.**

## Praktická část

1. **Nakreslete a popište metody Unicast, Broadcast a Multicast.**
2. **Nakreslete a popište 3cestný handshake.**
3. **Nakreslete a popište pozitivní a negativní potvrzování (ACK)**

## Doplňující otázky

1. **Nakreslete a popište 4cestný handshake.**

# Metody vysílání dat

Když chceme poslat nějaká data v počítačové síti, je důležité správné adresování zprávy a s tím je svázána metoda vysílání. Záleží na tom, zda chceme data zaslat pouze jedné stanici, několika stanicím najednou nebo všem stanicím ve stejném subnetu.

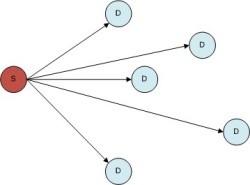
Vysílání jednoho všem = Broadcast

Vysílání jednoho jednomu = Unicast

Vysílání jednoho více uzlům = Multicast

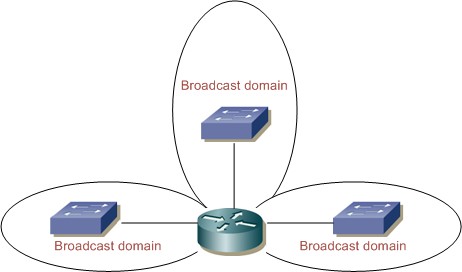
# Broadcast

**Broadcast** je jeden ze způsobů vysílání v TCP/IP síti (používá se nespojový (connectionless) protokol, jako třeba UDP). Je to vysílání jednoho všem, tedy vysílaný paket je (teoreticky) zachycen všemi zařízeními v síti, lepé řečeno v dané broadcast doméně (subnetu). Toto vysílání se používá převážně v LAN sítích (ne WAN). Broadcasty jsou dnes používány pro řadu účelů (třeba DHCP, ARP) a využívá je velké množství aplikací. Tvoří velkou část provozu v LAN síti a zatěžují aktivní síťové prvky i stanice, proto je snaha o jejich minimalizaci.



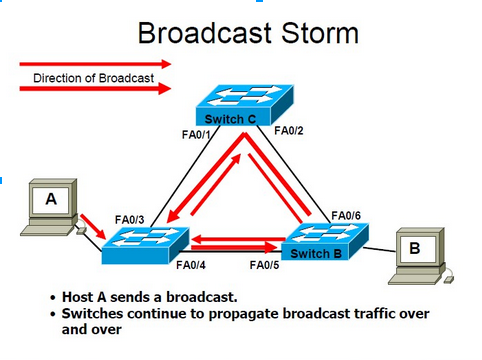
**Broadcast adresa** je adresa, na kterou se posílá komunikace v případě brodcastového vysílání. Jedná se o adresu, která má binárně samé jedničky. Na 3. vrstvě OSI modelu je to IP adresa 255.255.255.255 (občas se tak nepřesně označuje i broadcastová adresa subnetu, tedy poslední adresa v subnetu, viz dále).   
Na 2. vrstvě (fyzické) je broadcastová MAC adresa identicky adresa "se samými jedničkami" FF:FF:FF:FF:FF:FF – Používá se při WAKE ON LAN.

**Broadcast domain** je logická část sítě, ve které mohou připojená zařízení přímo komunikovat. Mělo by se tedy jednat o jeden subnet a hranicí je router, který by broadcasty neměl přeposílat.



*Pro rozdělení sítě na menší broadcast domény slouží routery nebo technologie VLAN.*

**Broadcast storm** je kritický stav, když počet broadcastů v síti je tak velký, že není možno vytvářet nová spojení a stará spojení jsou rušena. Často vzniká z důvodu smyček v síti.



***Smyčky v síti nám řeší STP Protokol.***

## Směrovaný broadcast na subnet - Subnet Directed Broadcast

**Subnet Directed Broadcast** je speciálním případem broadcastu, který se použije ve chvíli, kdy chceme zaslat broadcast do jiného subnetu, než v kterém se nacházíme. Funguje to tak, že rámec (frame) putuje sítí jako unicast přes routery až na router, který má cílový subnet (určený broadcastovou adresou subnetu) jako přímo připojený. Tento router upraví rámec na běžný broadcast a odešle jej na odpovídající rozhranní. Protože však tato technika byla používána k útokům, tak bývá na routerech nebo i firewallech většinou zakázána. To se týká routeru, který by měl rámec převést na broadcast, přes ostatní by měl rámec projít normálně.

**Subnet broadcast address** (broadcast adresa subnetu, někdy také nazývaná directed broadcast address) je IP adresa, která se skládá z network ID a samých jedniček v host ID. Jinak řečeno, jedná se o poslední adresu subnetu (ta se nemůže přiřadit stanici). Pro jednoduchý příklad máme počítač s adresou 192.168.10.39 a maskou255.255.255.0, podle masky vidíme, že první tři oktety tvoří network ID a poslední oktet jsou host ID, takže broadcast adresa subnetu je 192.168.10.255.

**Smurf Attack** je nejběžnějším případem útoku pomocí Subnet Directed Broadcast, který má zařídit *Denial of Services* (DoS). Útočník odesílá množství paketů  ICMP echo reply s podvrženou zdrojovou adresou jako directed broadcast, všechny stanice v subnetu odpovídají echo reply a stanice, jejíž adresa je ta podvržená, je zahlcena.

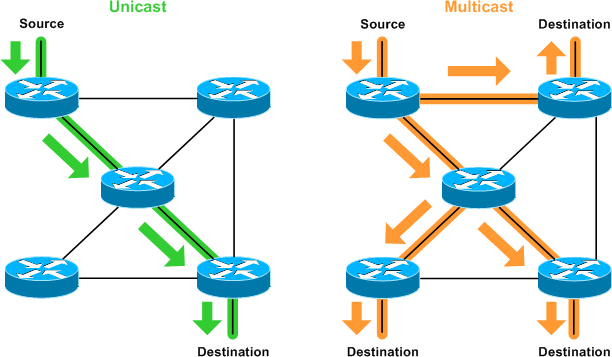
**Síťový broadcast** je [IP datagram](https://cs.wikipedia.org/wiki/IP_datagram), který je odeslán na IP adresu, která je v cílové síti broadcastem. Vysílající ani uzly, přes které síťový broadcast putuje, nemohou zjistit, že to je broadcast, protože v IP datagramu není obsažena informace o cílové síti (její číslo sítě a [maska sítě](https://cs.wikipedia.org/wiki/Maska_s%C3%ADt%C4%9B)). Proto je síťový broadcast přepravován stejně, jako jakýkoliv jiný IP datagram. Až poslední router zjistí, že cílová IP adresa je shodná s broadcastem pro daný segment sítě a proto datagram odešle jako broadcast. V ethernetové síti to znamená odeslání datagramu v rámci, jehož cílová MAC adresa je FF:FF:FF:FF:FF:FF.

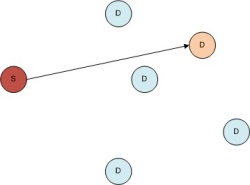
# Unicast

**Unicast** je vysílání, kdy je paket zasílán jednomu cíli. Jedná se o běžnou komunikaci, kdy spolu komunikují dvě stanice.

Unicast označuje v [počítačové síti](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5) zasílání [paketů](https://cs.wikipedia.org/wiki/Paket) pouze jedinému cíli (uzlu, stanici). Unicastové vysílání je opakem [broadcastu](https://cs.wikipedia.org/wiki/Broadcast" \o "Broadcast), který se vysílá do všech uzlů v síti najednou. Mezi unicastem a broadcastem stojí ještě multicasting, rozesílá pakety pouze určité skupině stanic. Pokud není možné multicast použít, musí se každý paket zasílat všem počítačům zvlášť (unicast), nebo je nutné použít broadcast, což v obou případech síť a uzly zatěžuje.

Unicast se používá pro přímou komunikaci mezi dvěma uzly v síti. V případě, že je potřeba doručit stejná data více uzlům najednou, je vhodnější použít multicast nebo broadcast (například streamování zvuku nebo videa, při konferenčních hovorech, [IPTV](https://cs.wikipedia.org/wiki/IPTV) a podobně).

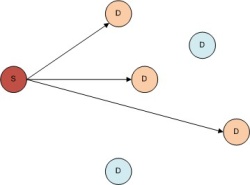


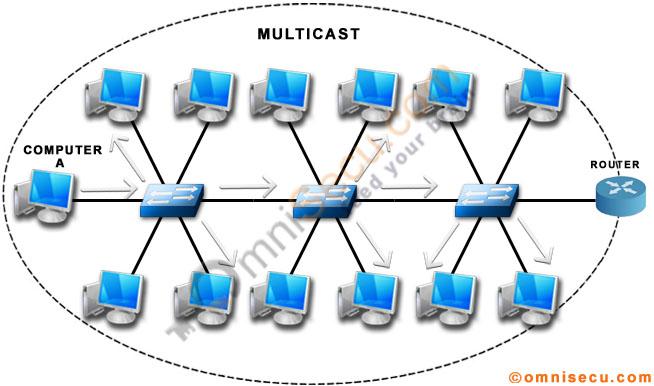


# 

# Multicast

Při této komunikaci se jedna informace doručuje skupině cílů. Multicast využívá efektivní metodu doručování, aby pakety v síti putovaly pouze jednou. Principem je, že se vytvoří mutlicastová adresa z rozsahu 224.0.0.0/4(pro LAN je určeno 224.0.0.0/24), a klienti se k této adrese zaregistrují. Pro vytváření skupina a registrování se používá protokol Internet Group Management Protocol (IGMP).





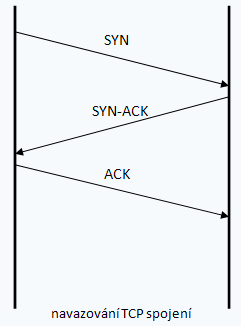
# Trojcestný handshake

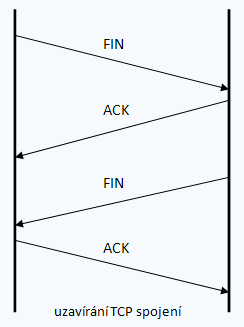
## Navázání spojení

Aby se mohla vysílat data pomocí TCP protokolu, je nejprve třeba vytvořit spojení. Pro navázání spojení se používá*třícestný handshake* (potřesení ruky). V průběhu navazování spojení se obě strany dohodnou na čísle sekvence (sequence number)odpovědi (acknowledgement number)

Navázání spojení probíhá ve třech krocích:

1. Klient pošle SYN packet s uvedeným číslem sekvence (x), číslo odpovědi 0
2. Druhá strana si uloží číslo sekvence (x) a odpoví SYN-ACK, jako číslo sekvence nastaví svoje číslo (y) a do čísla odpovědi vloží (x+1) - další očekávanou hodnotu
3. Klient odpoví ACK, číslo sekvence (x+1), číslo odpovědi (y+1)

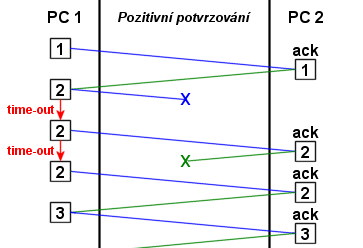




## Ukončení spojení

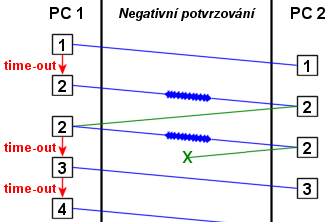
## Principy při ukončení spojení jsou podobné jako při jeho navazování. Nejčastěji se používá *čtyřcestný handshake*, kdy každá strana samostatně uzavře spojení. Zde se používá sekvence FIN s odpovědí ACK.

Pozitivní potvrzování  
Příjímací stanice v případě, že převzala datový paket bez chyby, vyšle speciální potvrzovací paket. Na chybně přijatý paket a samozřejmě i na nepřijatý paket příjímací stanice nereaguje. Vysílací strana po zaslání paketu musí čekat určitou dobu na příchod potvrzovacího paketu. Teprve po jeho příjmu může pokračovat vysíláním dalšího paketu. Nepřijde-li potvrzení ve vymezené době, opakuje se vysílání paketu znovu. Dokáže se vyrovnat se ztrátou paketu, ale ne se ztrátou potvrzovacího paketu -> dochází k duplicitě vysílání původního paketu.



1. Vysílací stanice vyšle první paket. Ten přes přenosové médium v pořádku dorazí k přijímací stanici.
2. Ta odešle potvrzení zpět, že paket číslo jedna úspěšně dorazil.
3. Vysílací stanice obdrží potvrzení a pošle paket číslo dva.
4. Ten ale k přijímací stanici nedorazí.
5. Vysílací stanice čeká po určenou dobu na potvrzení, po time-outu vysílá znovu paket č. dva.
6. Ten dorazí k přijímací stanici, která vyšle potvrzení, které ale nedorazí.
7. Vysílací stanice po time-outu opět vyšle paket číslo dva.
8. Přijímací stanice přijme paket číslo dva a vyšle potvrzení, že došel v pořádku. Přijímací stanice přijme potvrzení a posílá paket číslo tři…

Negativní potvrzování  
Základní princip této metody vychází z toto, že vysílací strana je upozorněna pouze na chybně přijatý paket. Tato metoda rychle reaguje na chybně přijatý paket, ale nedokáže se vyrovnat s jeho ztrátou. Proto se obvykle kombinuje s pozitivním potvrzováním. V této kombinaci pak rychle reaguje na chybně přijatý paket.



1. Vysílací stanice vyšle první paket. Ten přes přenosové médium v pořádku dorazí k přijímací stanici.
2. Vysílací stanice čeká po určenou dobu, zda nedostane od přijímací stanice zprávu o poškození paketu.
3. Po vypršení time-outu odešle druhý paket.
4. Druhý paket se cestou poškodí.
5. Přijímací stanice pošle zprávu zpět vysílací stanici o poškozeném paketu č. dva.
6. Ta paket číslo dva pošle znovu.
7. Na obrázku je vidět, co se stane, pokud paket dorazí poškozen a zpráva od přijímací stanice nedorazí zpět k vysílací stanici. Vysílací stanice začne po time-outu posílat následující paket. Proto se tato metoda musí kombinovat ještě s jiným potvrzováním.

### Skupinové potvrzování - okénkové potvrzování

Jedná se vlastně o takové potvrzování, kdy se například po každých 20 paketech vyšle potvrzení. Když je pozitivní tak se pokračuje dále, jestliže je negativní, tak se oznámí číslo porušeného paketu a vysílací stanice začne vysílat znovu od porušeného paketu dále. Tento systém se opakuje, dokud neskončí přenos. Schopnost takového potvrzování obstarává opět software. Uživatel o ničem neví. Pokud je spojení mezi počítači kvalitní může se nastavit velké okno (1000 paketů), pokud je linka nekvalitní nastaví se malé okno, aby se nemuselo moc opakovat.