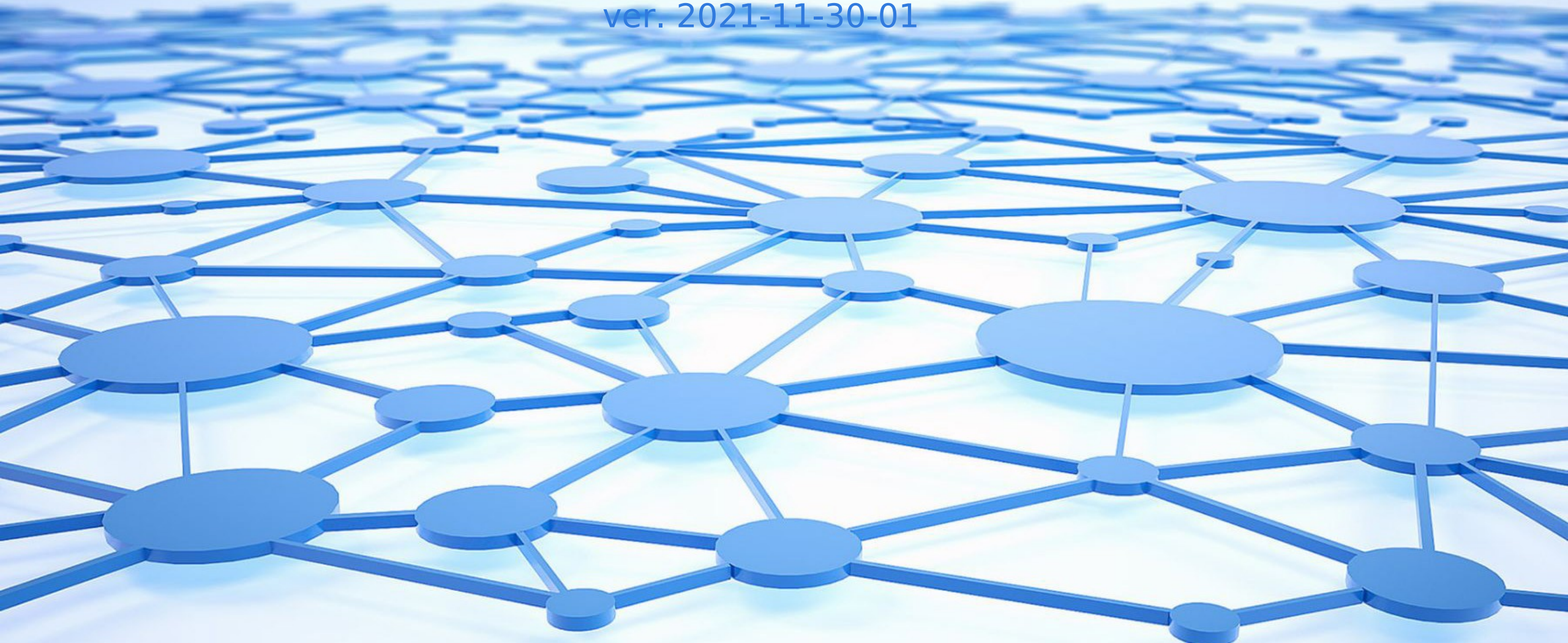
Úvod do počítačových sítí

Přednáška 9

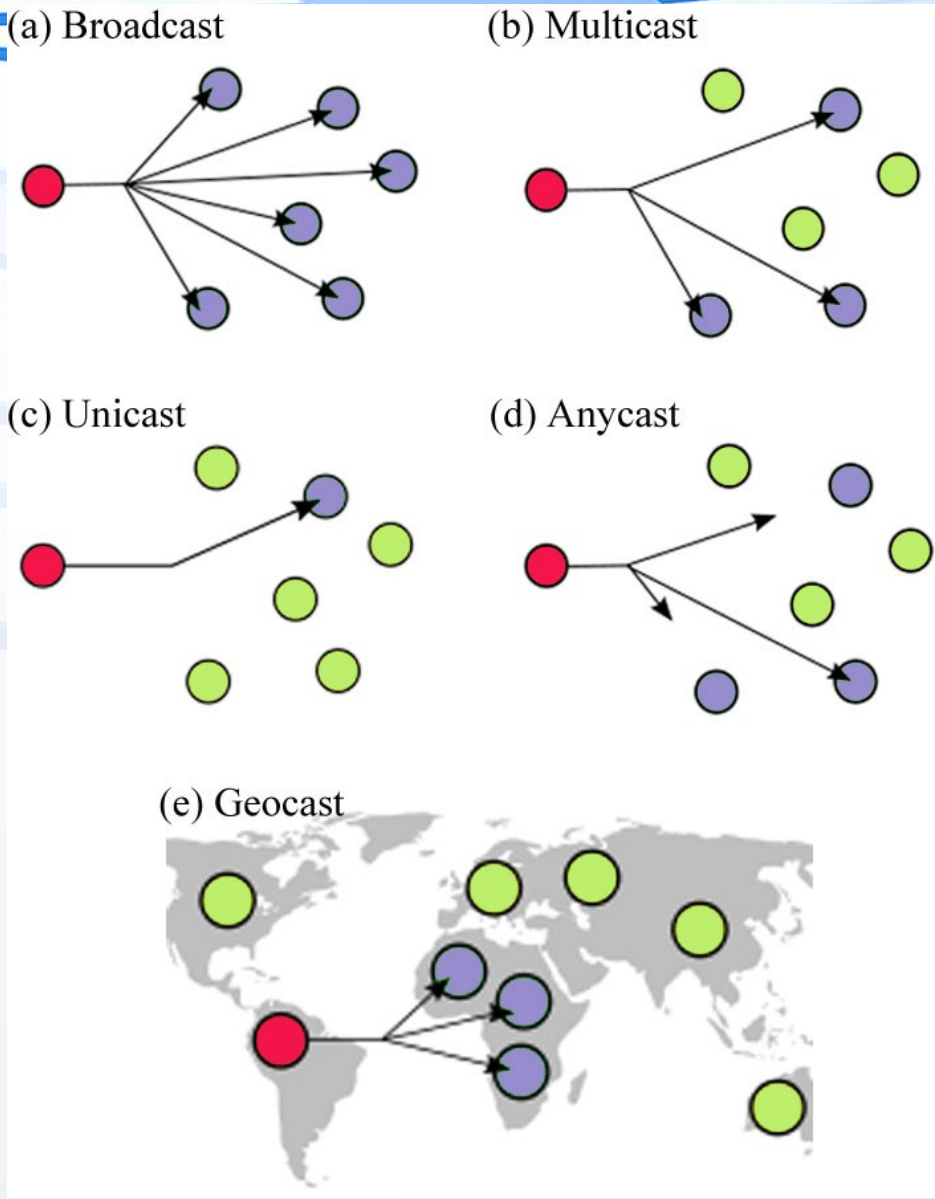
(2021/2022)

ver. 2021-11-30-01



L3 – Síťová vrstva II.

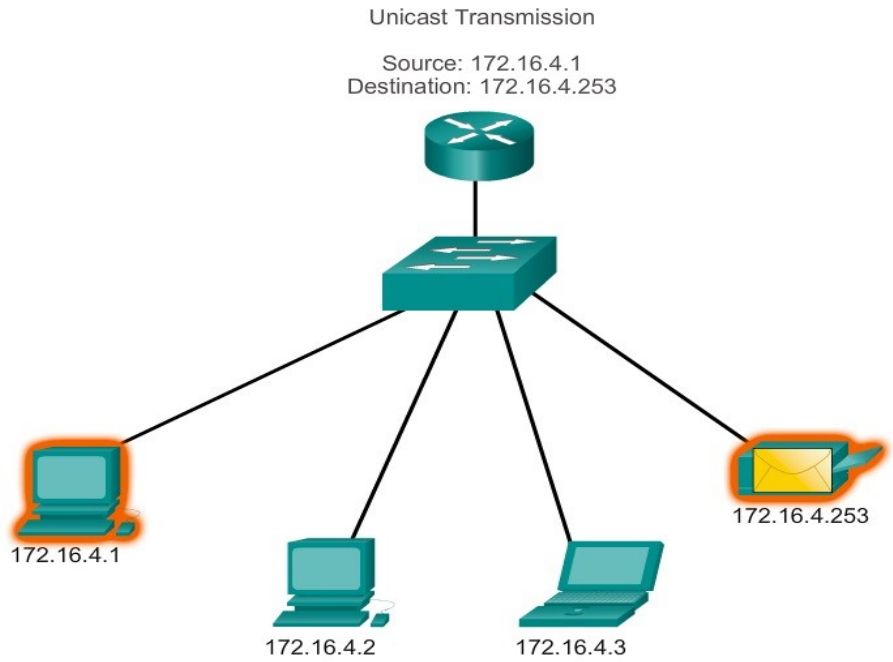
- Typy přenosů na L3
  - Unicast
    - Samostatné vysílání - „jeden s jedním“
  - Broadcast
    - Všesměrové vysílání - „jeden všem v dané sítí“
  - Multicast
    - Skupinové vysílání - „jeden všem v dané skupině“
  - Anycast
    - Skupinové vysílání nejbližšímu členovy - „jeden nejbližšímu členovy dané skupiny“
  - Geocast
    - Skupinová vysílání dané lokaci - „jeden všem v dané geolokaci“



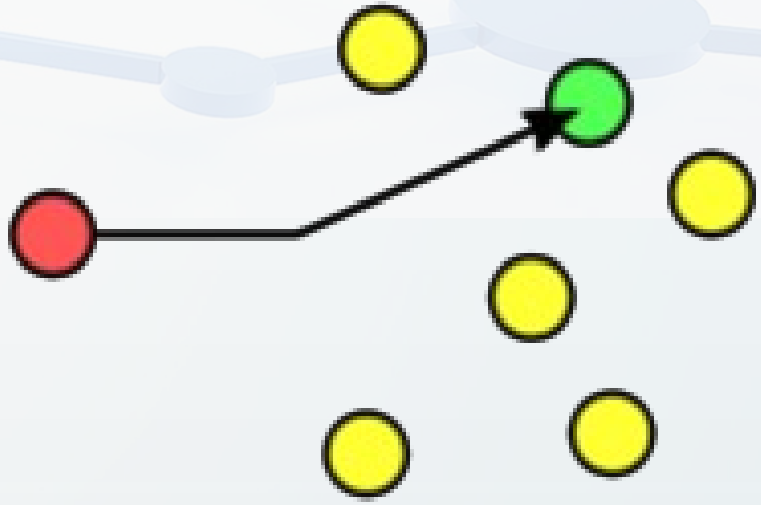
zdroj: https://www.researchgate.net/figure/Routing-Schemes-for-Wireless-Ad-Hoc-Network_fig1_266292883

Unicast

- Nejběžnější forma přenosu
- V zásadě se dá říší, že se jedná o přenos 1:1
  - Jeden účastník jednomu jinému účastníkovi
- Přenos může být realizován v rámci stejné LAN
  - Bez použití L3 směrování
- Přenos může být realizován mezi více LAN či WAN
  - S použitím L3 směrování
- Typické použití
  - Téměř veškeré běžně používané služby
    - HTTP, SMTP, POP/IMAP, FTP ….
- Nenáročný z pohledu zatížení sítě



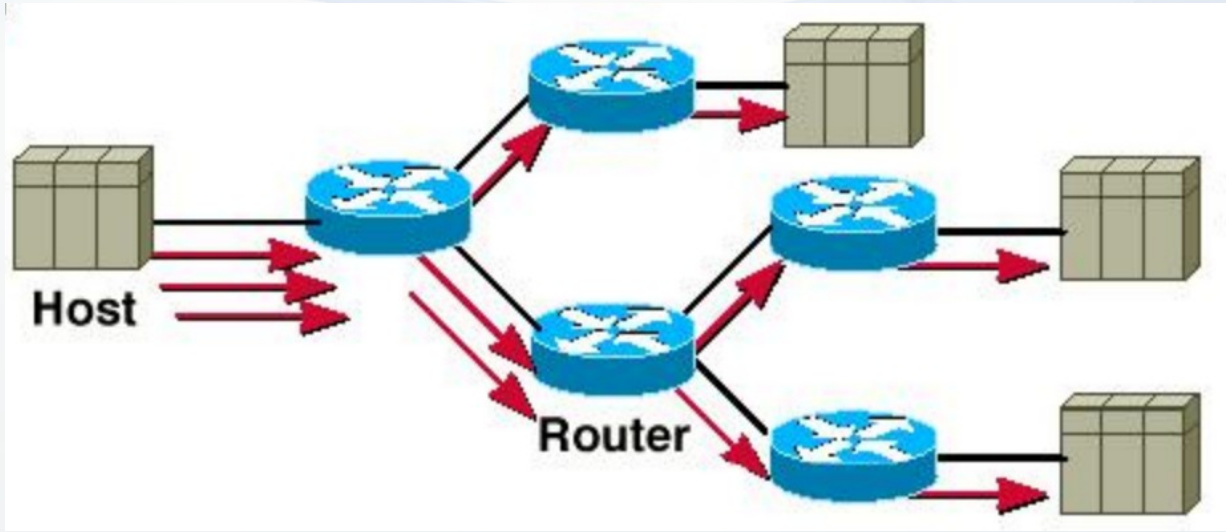
zdroj: https://www.hitechmv.com/ipv4-unicast-broadcast-and-multicast/



zdroj: https://cs.wikipedia.org/wiki/Unicastarticle.asp?p=2180210&seqNum=12

Replikovaný Unicast

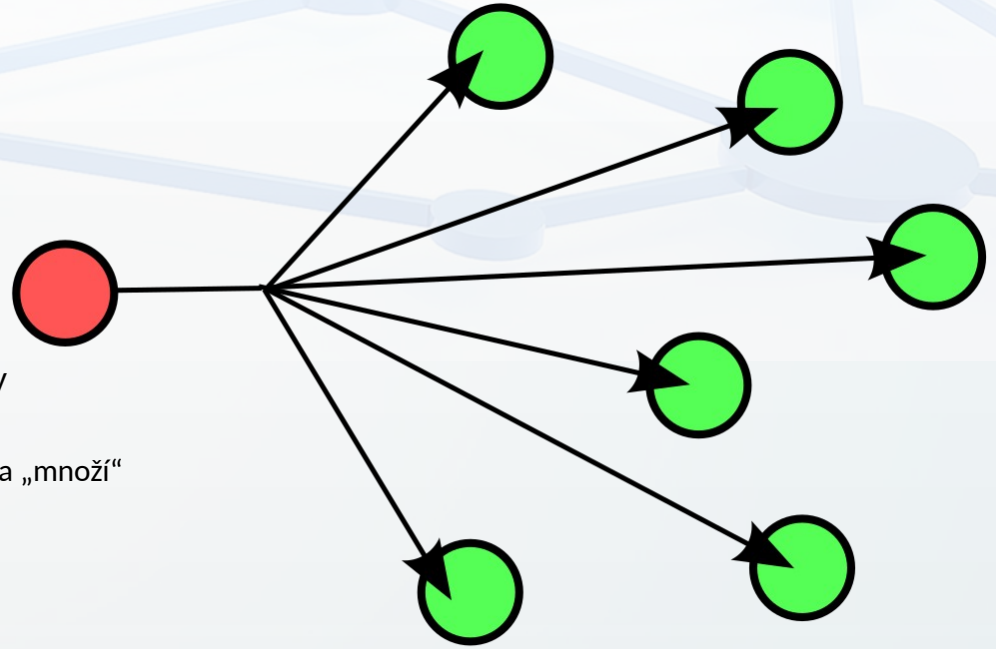
- Pokud potřebujeme odesílat data více účastníkům, musíme v případě použití unicastu přenosy opakovat
- Pro každého účastníka jsou ze zdroje odeslána vlastní data
- Výhodou je, že jednotlivé „streamy“ na sebe nejsou vázané
  - Tedy chyba v jednom nemusí ovlivnit více vysílání
    - Ale samozřejmě může, pokud je chyba ve zdroji data – např poškozený soubor
- Další výhodou je, že nepotřebuje žádné extra vybavení či adresaci
  - Proč také, jedná se o více běžných přenosů
- Nevýhod je v tomhle případě více
  - Vysílač musí znát všech přijímače
    - Všichni k němu musí být připojeni
  - Data odchází tolikrát, kolik přijímačů je připojeno
    - Což může být extrémně náročné na kapacitu linky a snadno může vést k saturaci linky a následně defakto k DDOS
      - Tolik účastníků chce čerpat data, až se zdroj stane nedostupný
  - Reálně data neodchází ve stejný okamžik
    - Zde záleží na konkrétní službě – někde to může vadit někde nemusí
      - Pro sledování video prezentace to jistě nevadí
        - Sice to uvidím každý divák v drobným posunem, ale to ničemu nevadí
      - Pro sledování on-line prezentace s možností reagovat už to problém být může
        - Ptám se na něco co reálně proběhlo před „nějakým časem“ zpět
        - Hodně bude záležet na počtu klientů



zdroj: https://havel.mojeservery.cz/mikrotik-blokovani-omezovani-multicast-provozu/

Broadcast

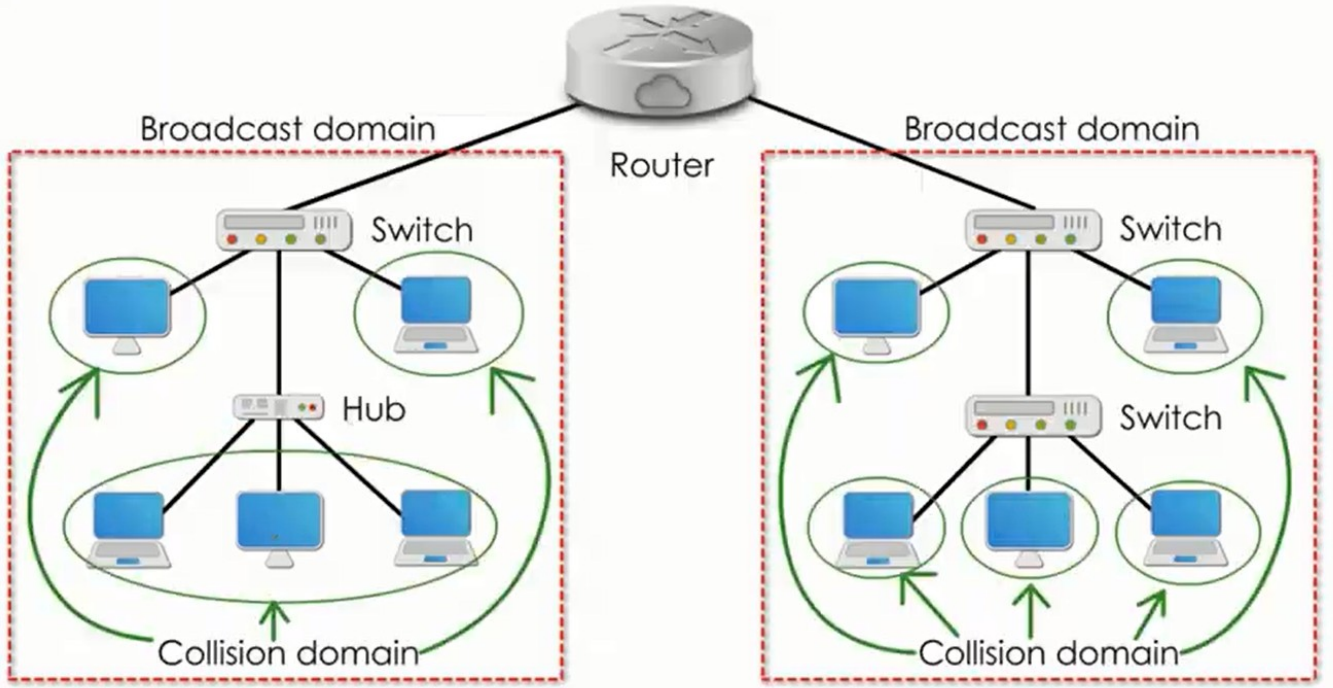
- U unicastu nastane „neřešitelný“ problém pokud budu chtít oslovit všechna zařízení v síti
  - V uvozovkách proto, že v určitých krajních situacích si mohu pomoci výčtem
    - Např pokud sem součástí sítě 192.168.1.0/29, která reálně může obsahovat stroje 192.168.1.1-6 mohu obeslat všechny, ale pokud je v LAN více sítí, oslovím zas jen část
- Řešením je broadcast – tedy vysílání „jeden všem“
  - Všem == všem na které vidím
- Výhodou je, že se odesílají jen jedna data a to na speciální adresu, která identifikuje „všechny v dané L2 síti“
  - Nemusím tedy řešit kdo vše v síti je, jen „řeknu“ VŠEM
- Velice jednoduché na realizaci – díky speciální – broadcastové – adrese
- Nevýhodou je, že data musejí v sítí přijmout a zpracovat všichni
  - Tedy i ti, kteří je nepotřebují
  - Dochází k zatěžování sítě i CPU na koncových stanicích
- Rozdíl mezi broadcastem a unicastem pro více stanic z pohledu zatížení sítě, je patrný mezi L2 prvky
  - Unicast posílá tolik dat kolik je přijímačů – pro dva propojené switche
  - Broadcast, pro dva propojené switche, posílá data jen jednou a až na jednotlivých koncových portech se data „množí“
- Využití má všude tam, kde potřebuje oslovit všechny ve stejné síti
  - DHCP – ještě nevím o síti nic a potřebuji se na nastavení zeptat, ale koho když o síti nic nevím ….?
  - ARP – nastavení sítě už znám, ale hledám převod IP x MAC
  - SMB – zjišťování okolních PC ve stejné síti



zdroj: https://cs.wikipedia.org/wiki/Broadcast

Broadcast – Broadcastová doména

- Pokud se tedy broadcast šíří všude, co jej zarazí ?
- L3 prvek - směrovač/router
- Broadcastová doména je oblast, kde se šíří broadcast a je limitovaná směrovačem
  - Kolizní doména – jak už víme – je oblast, kde může dojít ke kolizi – souběžnému a neoddělitelnému vysílání
  - Kolizní doména je
    - Jeden port switche / bridge / routeru
    - Všechny porty hubu



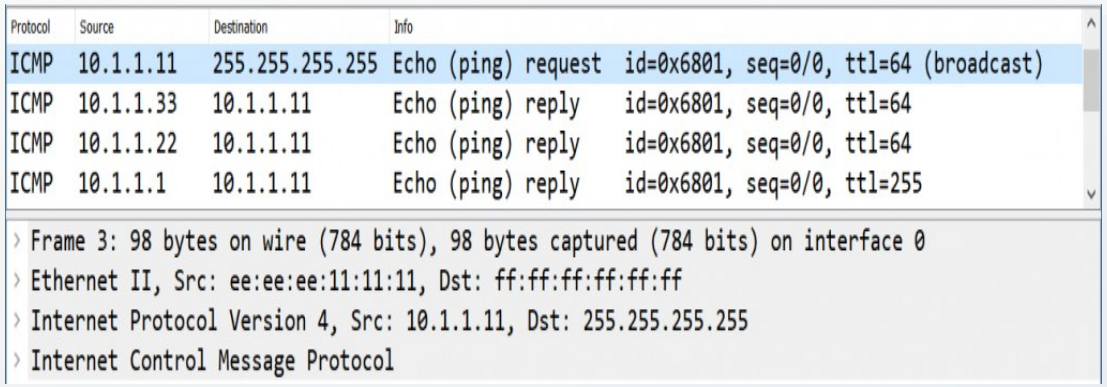
zdroj: https://medium.com/@snigdhareddy.chama/broadcast-domain-vs-collision-domain-96645a7526a1

Broadcast – typy broadcastu

- Broadcast můžeme řešit na více úrovních ISO/OSI
  - L2 a L3
- Podle použité úrovně se budou odesílat různá data na různé adresy
  - Na L2 rámce na L3 pakety
- Zároveň se bude lišit dosah broadcastové komunikace
  - Tedy kam až se může vysílaná zpráva šířit
- Rozlišuje tři typy broadcastových zprav:
  - L2 Broadcast
  - Lokální L3 broadcast
  - Cílený L3 broadcast

Broadcast – typy broadcastu: L2 broadcast

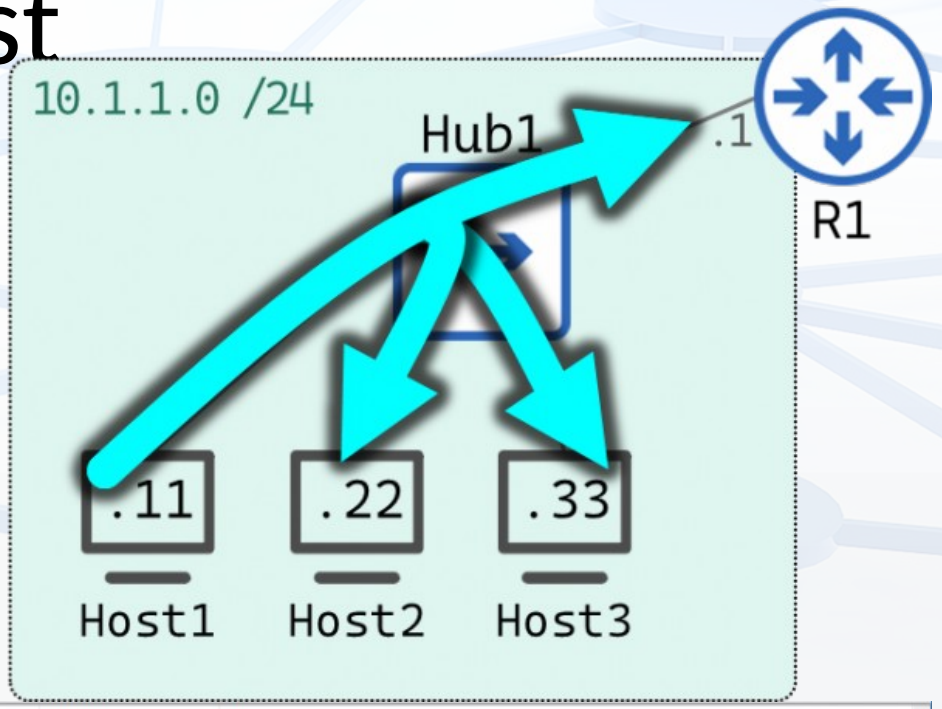
- Základní varianta vše směrového vysílání je realizována na L2 ISO/OSI
- Posílaná data mají charakter rámce / framu
- To, že se jedná o broadcast je definovanou adresou příjemce
- Pro Ethernet je MAC pro L2 broadcast FF:FF:FF:FF:FF:FF
  - Samé jedničky
- Takový rámec je
  - Na hubu kopírován na všechny porty
    - Hub to ani jinak neumí – jedná se o více-portový opakovač
  - Switch / bridge jej kopírují na všechny porty kromě příchozího
    - Kopírují rámec – ne jen signál
    - Na vše krom příchozího aby nedošlo k zacyklení – broadcastové bouři
      - Ono k ní stejně může dojít pokud je v síti smyčka, což lze řešit pomocí STP protokolu
  - Router na takový rámec odpoví, ale **dále jej nešíří**
    - Rozuměj na další porty



zdroj: https://www.practicalnetworking.net/stand-alone/local-broadcast-vs-directed-broadcast/

Broadcast – typy broadcastu: Lokální L3 broadcast

- Lokální nebo také místní či běžný broadcast
- Posíláme L3 paket a posíláme jej na L3 broadcastovou adresu
  - Např pro Ipv4 je to 255.255.255.255
  - Stejně jako na L2 i na L3 se jedná o adresu, kde jsou binárně samé „1“
- Realizace bude provedena tak, že se tento paket umístí do L2 rámce s adresou FF:FF:FF:FF:FF:FF a odešle se jako L2 broadcastový rámec
- Odpovědi docházejí už na konkrétní L3 adresu odesílatele
- Hub / Switch / Bridge danou zprávu posílají dále
- Router opět jen odpovídá, ale na další porty ji nekopíruje
  - Protože ví, že se jedná o broadcast
- Stejně jako u L2 je možné realizovat jen v rámci jedné LAN
  - Logicky, protože router nás jinam nepustí



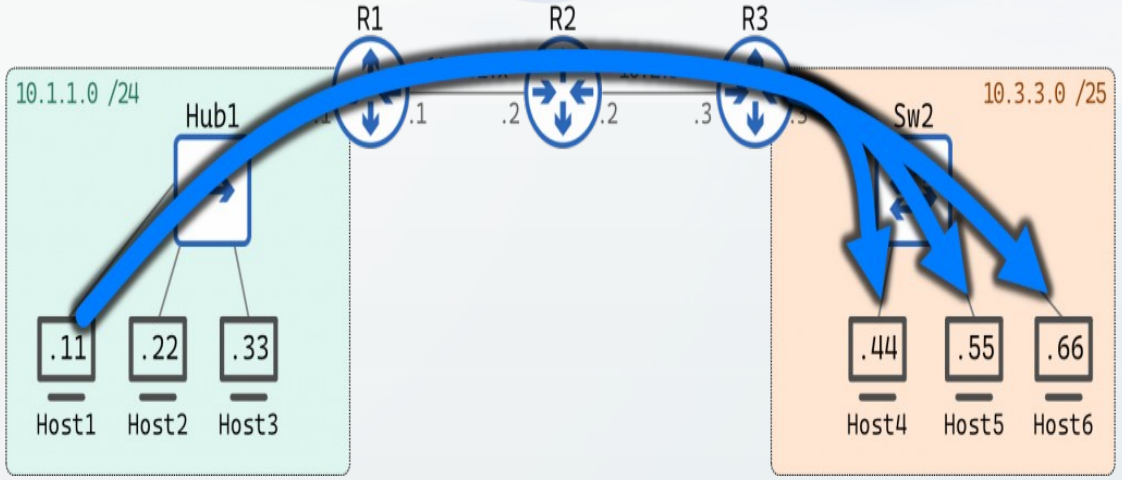
Protocol	Source	Destination	Info
ICMP	10.1.1.11	255.255.255.255	Echo (ping) request id=0x6801, seq=0/0, ttl=64 (broadcast)
ICMP	10.1.1.33	10.1.1.11	Echo (ping) reply id=0x6801, seq=0/0, ttl=64
ICMP	10.1.1.22	10.1.1.11	Echo (ping) reply id=0x6801, seq=0/0, ttl=64
ICMP	10.1.1.1	10.1.1.11	Echo (ping) reply id=0x6801, seq=0/0, ttl=255

```
> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
> Ethernet II, Src: ee:ee:ee:11:11:11, Dst: ff:ff:ff:ff:ff:ff
> Internet Protocol Version 4, Src: 10.1.1.11, Dst: 255.255.255.255
> Internet Control Message Protocol
```

zdroj: https://www.practicalnetworking.net/stand-alone/local-broadcast-vs-directed-broadcast/

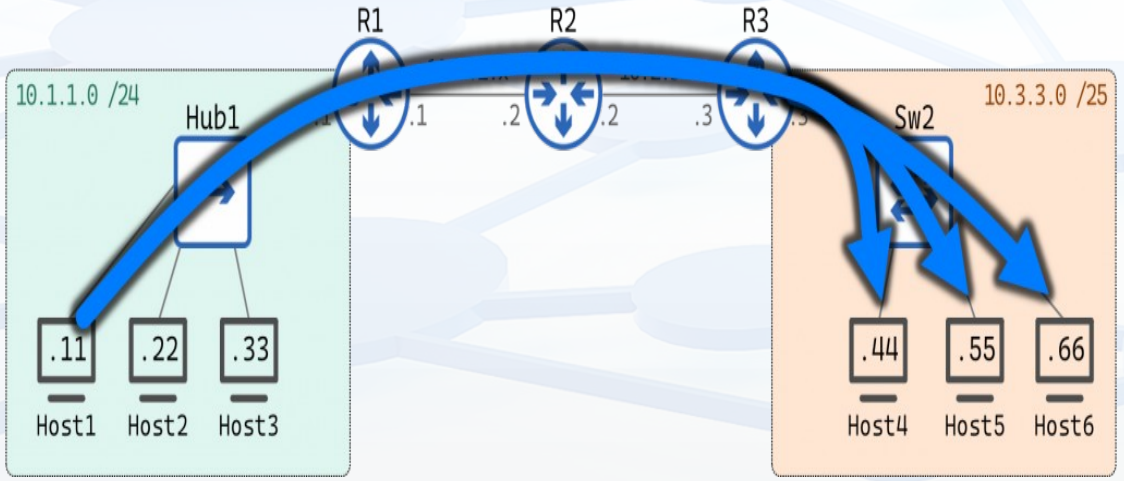
Broadcast – typy broadcastu: Cílený L3 broadcast

- Podobě jako v předchozím případě i lokálního broadcastu posíláme paket, ale zde na jinou adresu
- Už nepoužíváme obecnou adresu 255.255.255.255, ale používáme broadcastovou adresu sítě, do které chceme vysílat
  - Např u IPv4 se jedná o nejvyšší adresu v síti – síť je jak víme definovaná maskou
    - Ona může být definovaná i třídou adres pro classfull sítě, ale třídy adrese pojí s konkrétní výchozí maskou
      - A *8*, *B*/16, C/24
  - Např pro 10.1.1.0/24 bude broadcastová adresa 10.1.1.255
    - Tedy binárně opět samé „1“, ale JEN ve variabilní části adresy
- Pokud se je jedná o síť, jejíchž jsem součástí, je situace stejné jako u lokální broadcastu
- Ale pokud se nejedná o lokální síťím je situace dramaticky odlišná
  - Tento paket je v počátku šířen jako unicast
    - Logicky, protože pro 10.1.1.0/24 je 10.1.1.255 broadcast, ale pro 10.1.0.0/16 je to plnohodnotná adresa
  - Tento paket tedy projde routerem/routery až do cílové sítě
    - Na základě běžného směrování
  - A teprve až na routeru, který spravuje cílovou síť, začne být šířen jako lokální broadcast
  - Protože cílový router má na jednom interface síť 10.1.1.0/24 a tedy ví, že se jedná o broadcastovou adresu
  - L2 broadcast se použije až na posledním routeru
- Odpověď jde pak klasickým unicast paketem
  - A řídí se klasickým směrováním
- Povolení tohoto typu komunikace představuje bezpečnostní riziko
  - Mohl posílat požadavky do cizích sítí a zjišťovat živé stroje
  - Typicky se defaultně zakazuje



zdroj: https://www.practicalnetworking.net/stand-alone/local-broadcast-vs-directed-broadcast/

Broadcast – typy broadcastu:
Cílený L3 broadcast - příklad



Protocol	Source	Destination	Info
ICMP	10.1.1.11	10.3.3.127	Echo (ping) request id=0x6b01, seq=0/0, ttl=64 (no response f…
ICMP	10.2.3.3	10.1.1.11	Echo (ping) reply id=0x6b01, seq=0/0, ttl=253
ICMP	10.3.3.66	10.1.1.11	Echo (ping) reply id=0x6b01, seq=0/0, ttl=61
ICMP	10.3.3.55	10.1.1.11	Echo (ping) reply id=0x6b01, seq=0/0, ttl=61
ICMP	10.3.3.44	10.1.1.11	Echo (ping) reply id=0x6b01, seq=0/0, ttl=61

```
> Frame 13: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
> Ethernet II, Src: ee:ee:ee:11:11:11, Dst: ee:ee:10:11:11:11
> Internet Protocol Version 4, Src: 10.1.1.11, Dst: 10.3.3.127
> Internet Control Message Protocol
```

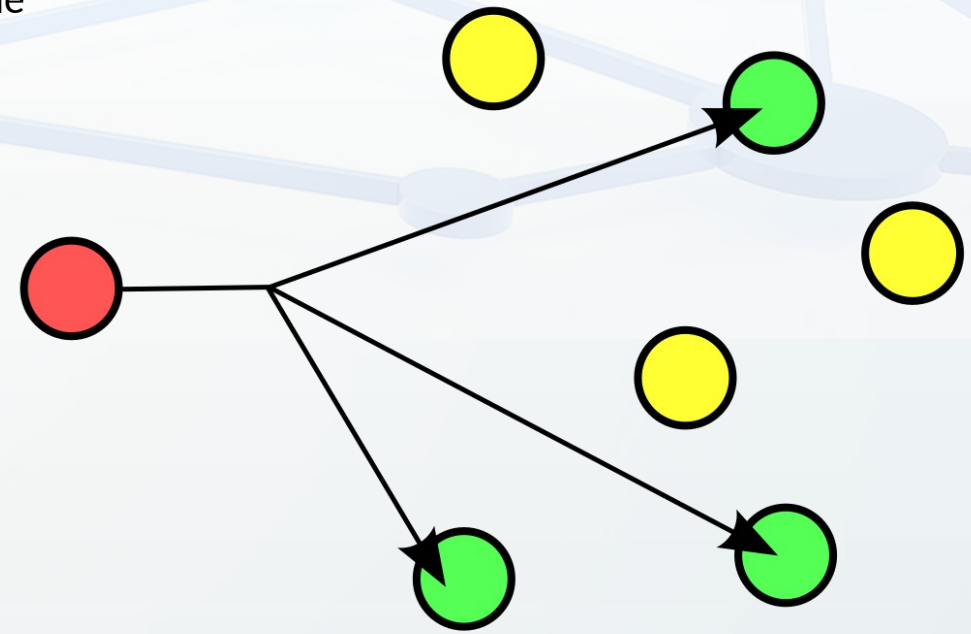
Protocol	Source	Destination	Info
ICMP	10.1.1.11	255.255.255.255	Echo (ping) request id=0x6b01, seq=0/0, ttl=61 (broadcast)
ICMP	10.3.3.66	10.1.1.11	Echo (ping) reply id=0x6b01, seq=0/0, ttl=64
ICMP	10.3.3.55	10.1.1.11	Echo (ping) reply id=0x6b01, seq=0/0, ttl=64
ICMP	10.3.3.44	10.1.1.11	Echo (ping) reply id=0x6b01, seq=0/0, ttl=64

```
> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
> Ethernet II, Src: ee:ee:10:33:33:33, Dst: ff:ff:ff:ff:ff:ff
> Internet Protocol Version 4, Src: 10.1.1.11, Dst: 255.255.255.255
> Internet Control Message Protocol
```

zdroj: https://www.practicalnetworking.net/stand-alone/local-broadcast-vs-directed-broadcast/

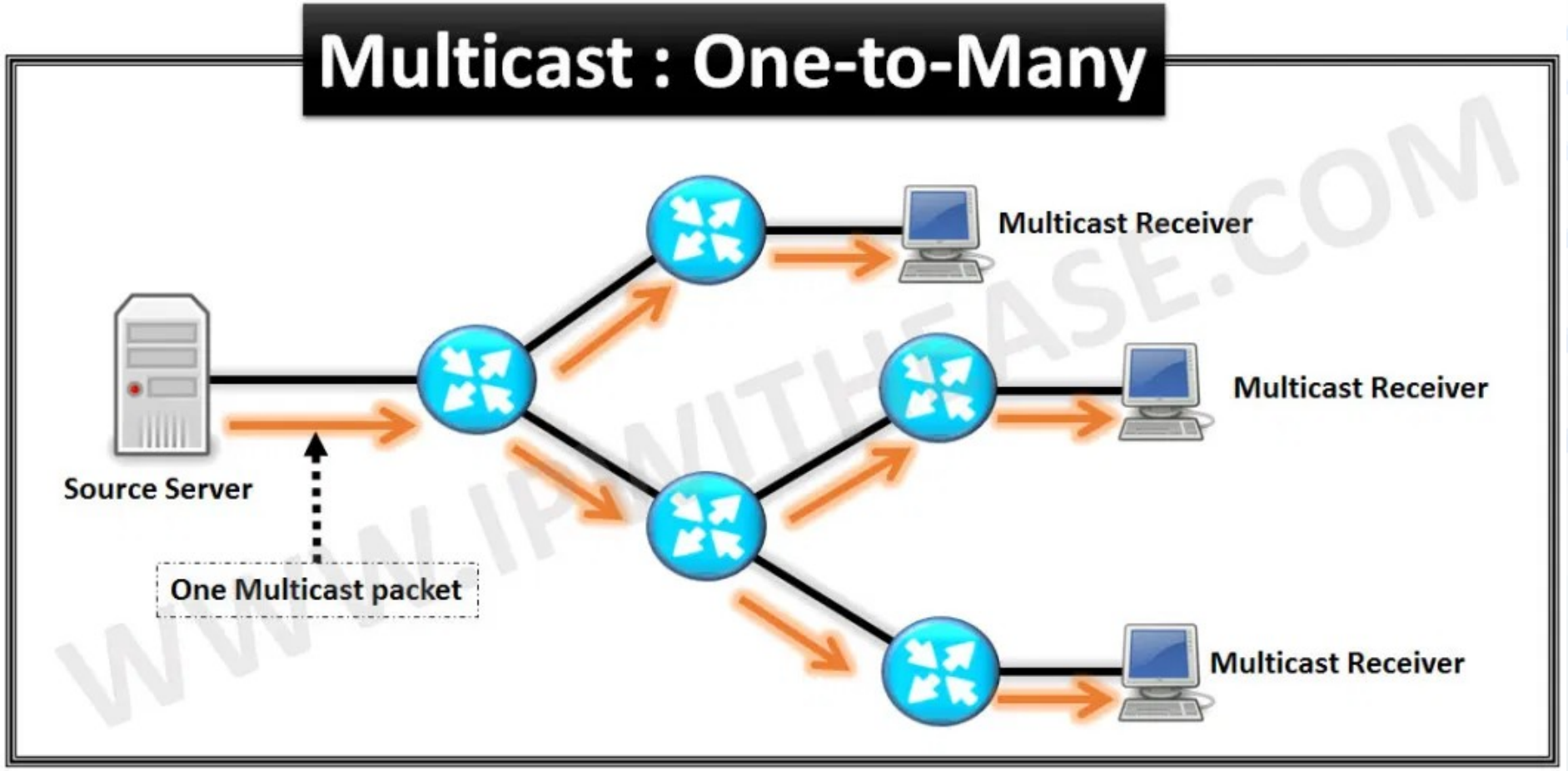
Multicast

- Broadcastová komunikace umí poslat data všem v rámci jedné LAN, ale jak řešit situaci
  - Ale data jdou VŠEM v dané LAN
- Replikovaný unicast umí poslat data na více příjemců i v různých sítích
  - Ale za cenu tolika datových toku od zdroje kolik je příjemců přenosu
- Multicast je řešení pro situace, kdy potřebuje poslat stejná data více účastníkům, ale
  - Nechceme / nemůžeme být omezeni na jednu LAN
  - Potřebujeme minimalizovat datové toky
    - To obecně chceme vždy ;)
  - Skupina příjemců není předem známa a ani nijak místně vázaná
    - Tohle neplatí tak obecně – musí být v rámci celé cesty multicast dostupný
- Multicast funguje tak, že tam kde jdou data společnou cestou, tedy v unicastu by bylo více paralelních přenosu, jsou přenášena jen jednou a teprve tam, kde se cesty dělí se kopírují na více portů
  - Ale jednou cestou / portem jde vždy jen jedna kopie data
- Multicast je nespolehlivý – aby spolehlivý byl, muselo by docházet k potvrzování a případně opakování dat – a to je problém pro „live“ data
  - Upřednostňujeme kontinuální datový tok, před jistotou doručení všech dat



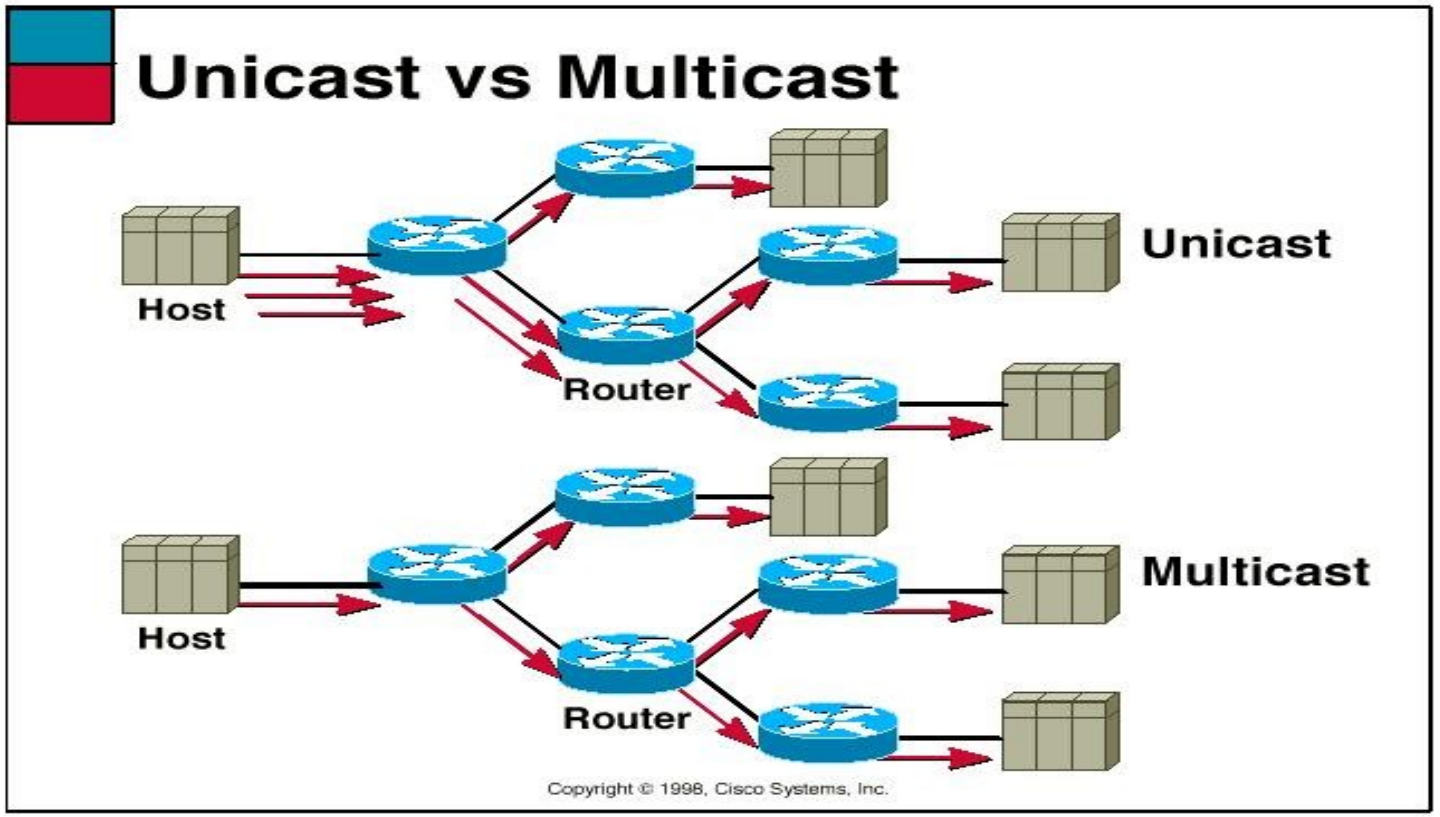
zdroj: https://en.wikipedia.org/wiki/Multicast

Multicast – příklad



zdroj: https://ipwithease.com/understanding-multicast-basics/

Multicast – porovnání s unicastem



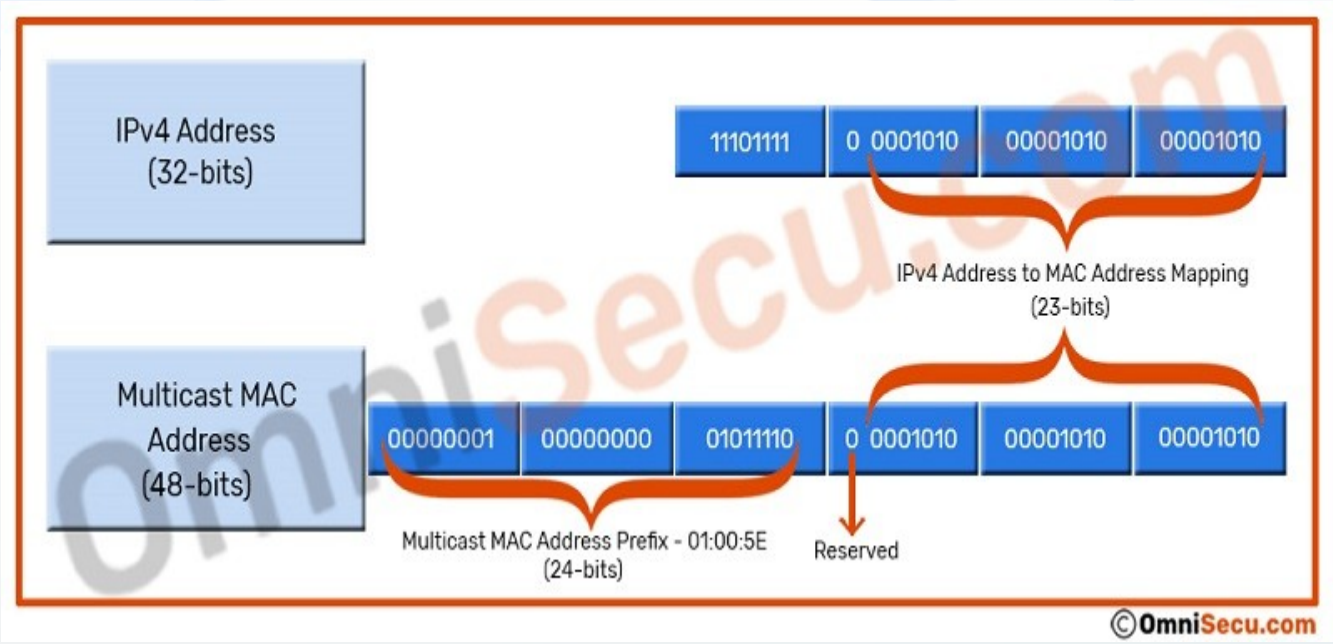
zdroj: https://havel.mojeservery.cz/mikrotik-blokovani-omezovani-multicast-provozu/

Multicast – použití

- Typicky tam, kde potřebujeme distribuovat větší množství stejných data ve stejný okamžik skupině příjemců
- Velmi často se používá pro distribuci video/zvukového vysílání
  - Stream videa
  - videokonference
- Distribuované interaktivní hry / simulace
  - Stejnou situaci potřebujeme aby vidělo naráz více účastníků
- Hromadné kopírování dat
  - Například klonování pevných disků
  - Na KIV používáme UDPCast ke klonování stanic
- Konfigurace skupin zařízení
  - Například NTP synchronizace času

Multicast – Adresace

- Multicast, podobě jako broadcast se řeší na L2 i L3 úrovni
  - A tedy pro switch i router se chová zcela jinak
- Na úrovni L2 se používají speciální MAC adresy pro multicast
  - Ty tvoří pevně daný prefix
    - Pro Ethernet je to 01:00:5E
  - A následně 23 bitů přímo z L3 IP multicastové adresy
- Na úrovni L3 má multicast vyhrazené adresy třídy D
  - 224.0.0.0/4
    224.0.0.0 až 239.255.255.255
- Jednotlivé skupiny adres mají svůj předdefinovaný specifický význam



zdroj: https://www.omnisecu.com/tcpip/multicast-ipv4-address-to-mac-address-mapping.php

Multicast – L3 adresy a jejich význam

IP multicast address range	Description	Routable
224.0.0.0 to 224.0.0.255	Local subnetwork[1]	No
224.0.1.0 to 224.0.1.255	Internetwork control	Yes
224.0.2.0 to 224.0.255.255	AD-HOC block 1[2]	Yes
224.3.0.0 to 224.4.255.255	AD-HOC block 2[3]	Yes
232.0.0.0 to 232.255.255.255	Source-specific multicast[1]	Yes
233.0.0.0 to 233.251.255.255	GLOP addressing[4]	Yes
233.252.0.0 to 233.255.255.255	AD-HOC block 3[5]	Yes
234.0.0.0 to 234.255.255.255[citation needed]	Unicast-prefix-based	Yes
239.0.0.0 to 239.255.255.255	Administratively scoped[1]	Yes

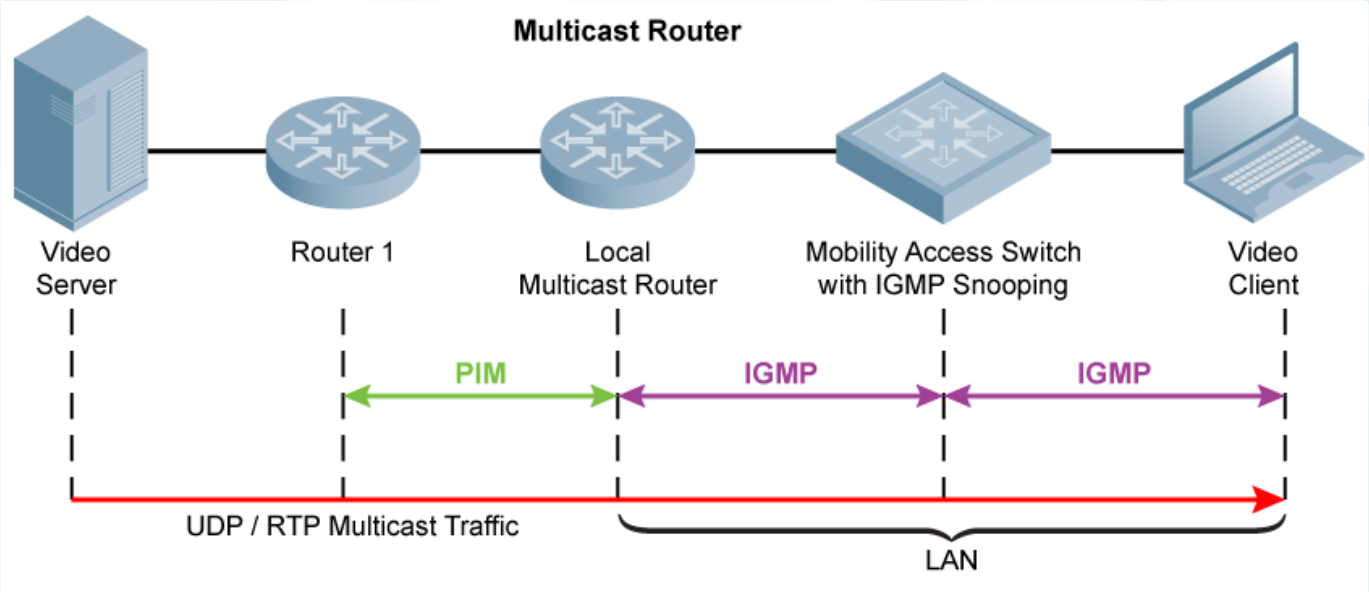
zdroj: https://en.wikipedia.org/wiki/Multicast_address

Well-Known Reserved Multicast Addresses	
Address	**Usage**
224.0.0.1	All multicast hosts
224.0.0.2	All multicast routers
224.0.0.4	DVMRP routers
224.0.0.5	All OSPF routers
224.0.0.6	OSPF designated routers
224.0.0.9	RIPv2 routers
224.0.0.10	EIGRP routers
224.0.0.13	PIM routers
224.0.0.22	IGMPv3
224.0.0.25	RGMP

zdroj: https://tutorzine.com/introduction-to-ip-multicasting/

Multicast – Princip fungování

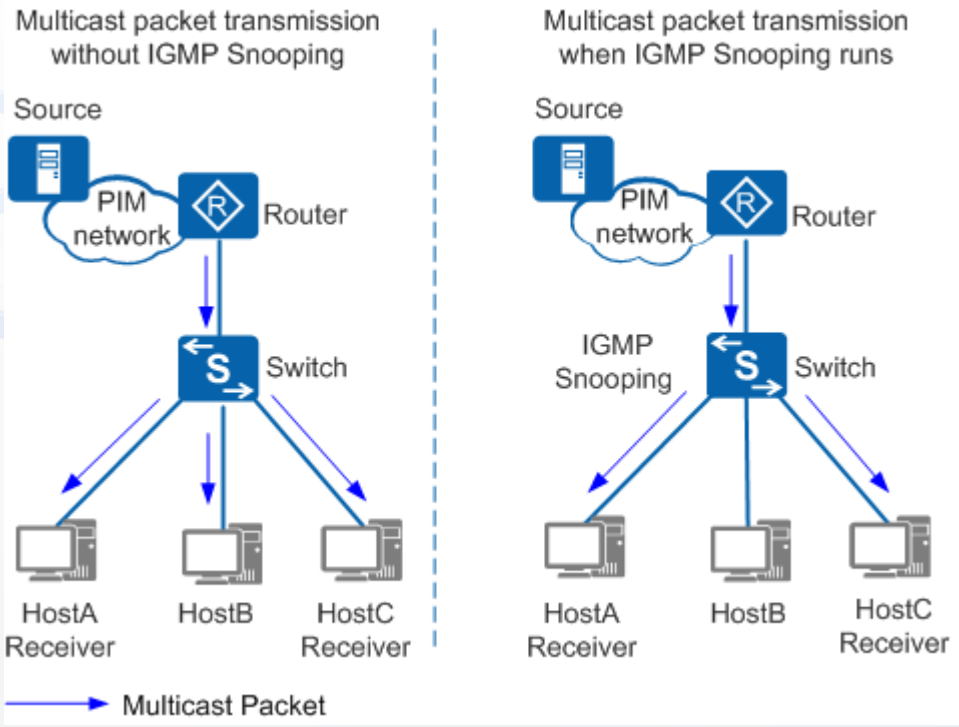
- V první řadě je nutné aby zařízení, která se mají multicastové komunikace účastnit ji podporovala a byla na nich povolena
  - S koncovými stanice obvykle problém není, ale na L2 i L3 prvcích se multicast často zakazuje
    - Důvodem je jak bezpečnost tak stabilita sítě, protože multicast může zařízení více zatěžovat
- Následně je nutné, aby se koncová stanice registrovala alespoň do jedné multicastové skupiny
  - Samozřejmě může i do více
  - Registrací stanice vyjadřuje přání přijímat data skupiny
  - K registrace s využívá protokol IGMP
- Samotný přenos se liší v rámci LAN a WAN
  - v L2 se použije multicastová MAC
  - V L3 je třeba použít multicastové směrování k doručování dat
    - Jedná se např o PIM-SM, PIM-DM, DVMRP, MOSPF



zdroj: https://community.arubanetworks.com/blogs/arunhasan11/2020/10/20/how-to-configure-verify-and-troubleshoot-igmp-and-pim-sm-functionality

Multicast – Chování na L2 a L3

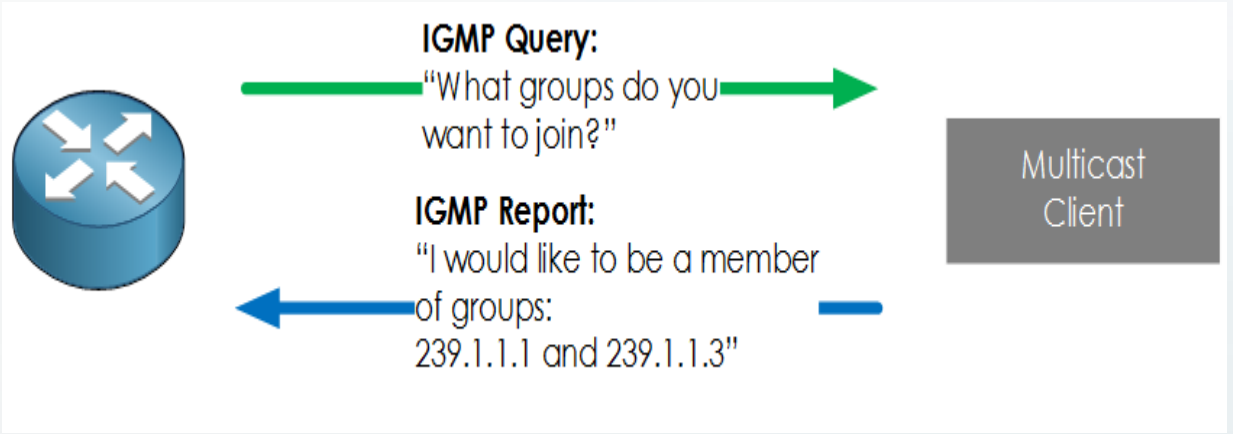
- Chování na L2
  - Velice podobné broadcast
  - Pro switch jsou dvě možné varianty
    - Bez IGMP Snoopingu – data se kopírují na všechny porty kromě příchozího
      - Opět je třeba řešit zacyklení - STP
    - S IGMP Snoopingem – data se kopírují jen na porty, kde je o daný multicast zájem
  - Na rozdíl od broadcastu se ale nezpracovává na všech stanicích, ale jen na těch, které mají o data zájem – jsou součástí skupiny
    - To poznají na základě MAC, ve které je část IP adresy
- Chování na L3
  - Zde je situace proti unicastu složitější, protože paket může být nutné zaslat na více portů
  - Je nutné předcházet zacyklení – proto se vytváří distribuční strom a data se posílají jen do větví
    - Kořenem stromu je buď první router u zdroje nebo například dohodnutý router



zdroj: https://support.huawei.com/enterprise/en/doc/EDOC1100116611/a0355a52/igmp-snooping

Multicast – Registarace do skupiny: IGMP

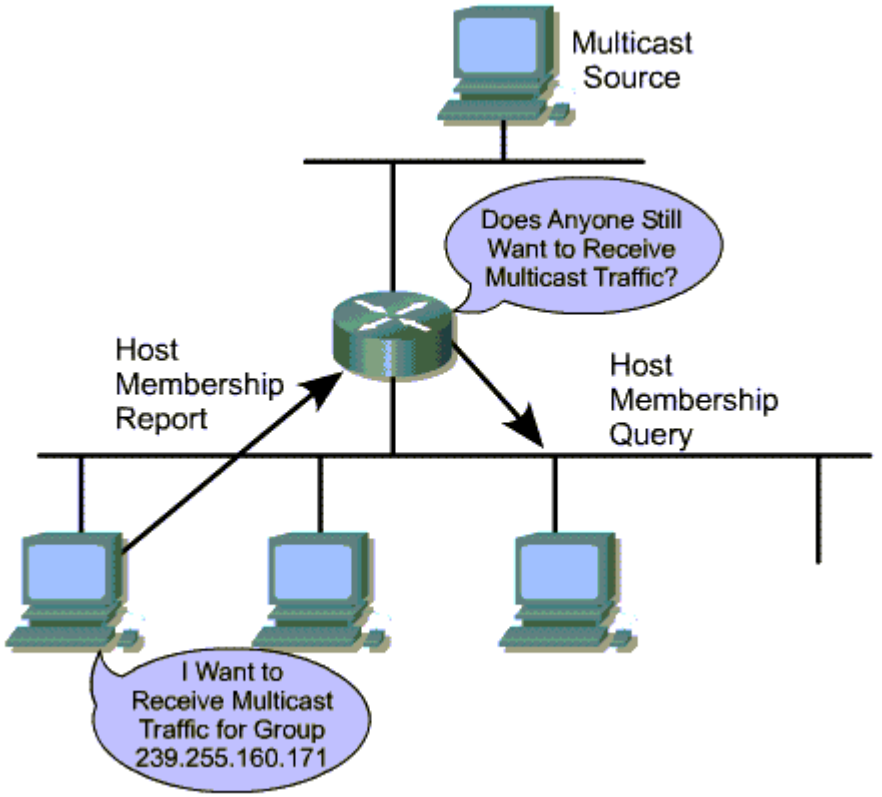
- IGMP - Internet Group Management Protocol
- Slouží ke komunikaci mezi lokální stanicí a místním routerem
- Pokud stanice chce přijímat multicast protokol, musí se zaregistrovat na lokálním routeru
- Router musí vědět, že na daném portu – odkud přišel požadavek – je někdo kdo chce přijímat multicast data dané skupiny
- Zároveň routeru umožňuje zjišťovat, zda registrovaná zařízení mají o členství stále zájem
  - Aby se detekovaly mrtvé stanice /aplikace
  - A aby se tím snížil zbytečný trafik
  - Zjišťování probíhá opakovaně – protože se mění v čase
- Existují tři veze IGMP
  - IGMPv1
  - IGMPV2
  - IGMPv3



zdroj: https://www.fir3net.com/Networking/Protocols/what-is-igmp.html

Multicast – Registarace do skupiny: IGMPv1

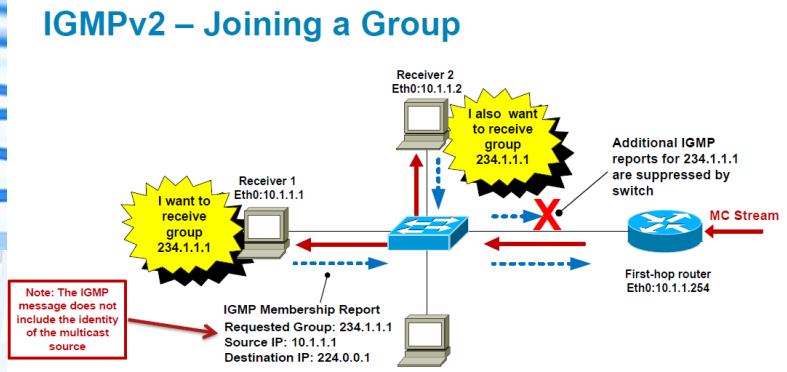
- Obsahuje dva typy zpráv
  - Reportovací
    - Klient informuje lokální router o tom, že chce být člen skupiny
  - Dotazovací
    - Router se ptá klientů, zda jsou stále ještě součástí skupin do kterých se
      - Cílem je eliminovat zbytečné přenosy
      - Pokud neodpoví nikdo, skupina na routeru zanikne
      - Dotaz se posílá každých 60s, s tím že timeout je 180s
      - Dotaz se posílá na 224.0.0.1 s TTL=1
        - » Neopustí lokání síť
      - Vzniká zde problém, že router se nedozví o tom, že stanice opustila skupinu
        - » Například proto, že klient ukončil aplikaci

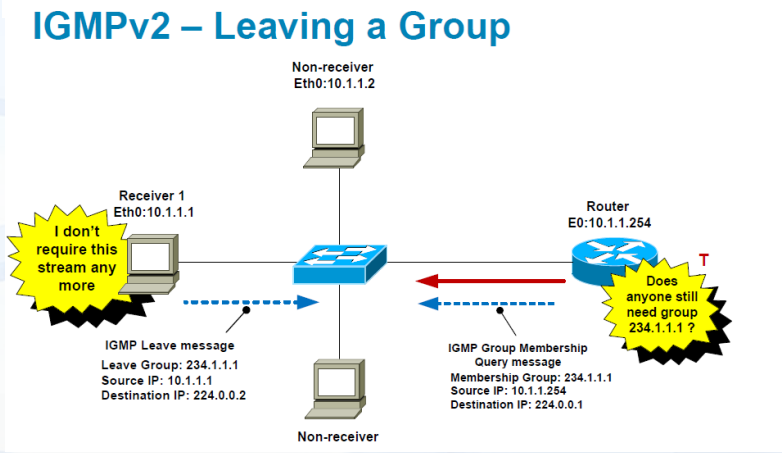


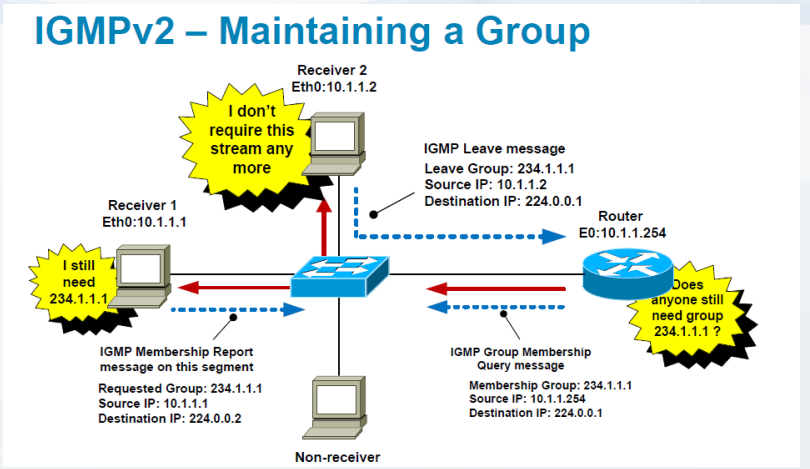
zdroj: http://www.cs.vsb.cz/grygarek/SPS/lect/multicast/multicast.html

Multicast – Registarace do skupiny: IGMPv2

- Vychází s IGMPv1 snaží se řešit jeho nedostatky
- Zavádí proti IGMPv1 čtyři novinky:
  - Zavádí Leave message, kde klient informuje server, že už není členem skupiny
    - Ta se posílá na IP 224.0.0.2
    - Urychluje ukončení zbytečných streamů a zároveň zánik prázdných skupin
  - Upravuje timeouty
    - Dotaz na hosty se posílá každých 125s
  - Zavádí volbu hlavního routeru v dané sítí
    - Pokud je jich v jedné LAN více
    - Router s nejnižší IP (porovnáno binárně)
    - Pokud zaslechnu dotazovací zprávu od routeru s nižší IP, přestane své zprávy na 400s posílat, pokud pak další neuslyší považuje původní stanici za mrtvou a začne posílat dotazy – čímž dojde k nové volbě
  - Zavádí specifická dotazy pro danou skupinu
    - Dokáže nově adresovat hosty v jednotlivých skupinách



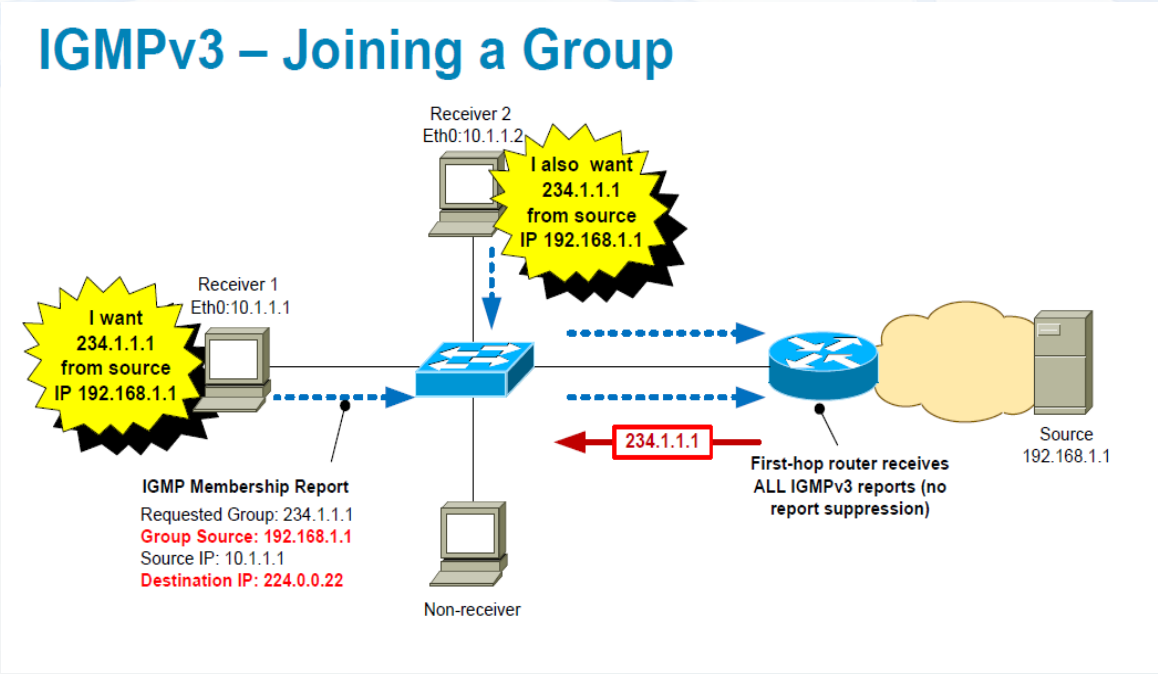




zdroj: https://mrncciew.com/2012/12/25/igmp-basics/

Multicast – Registarace do skupiny: IGMPv3

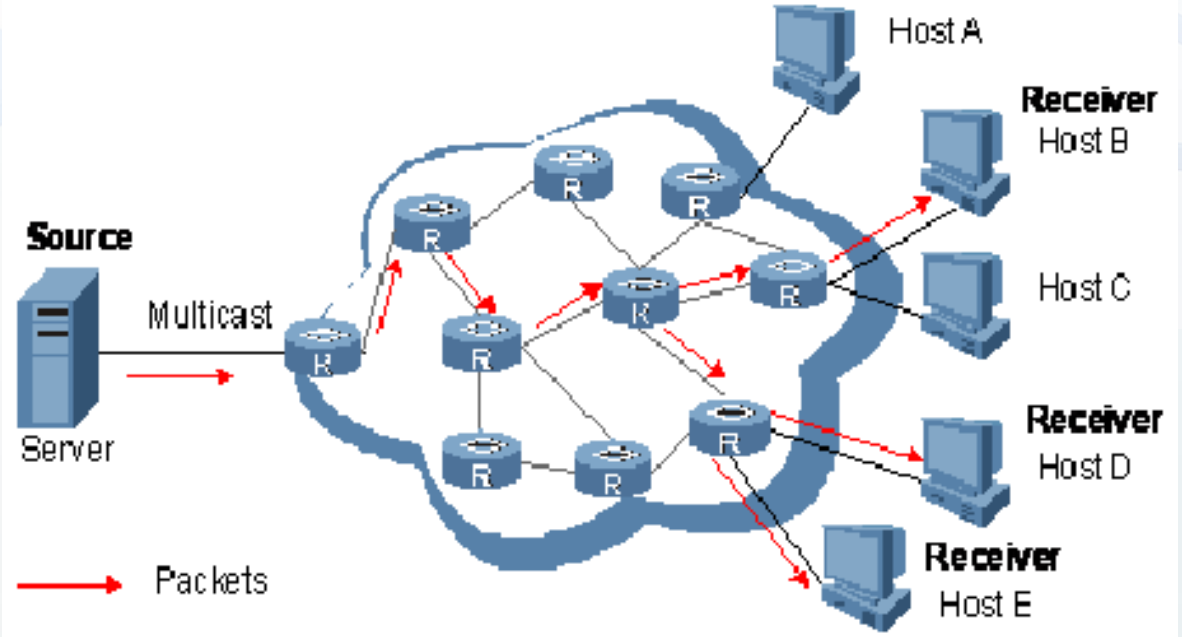
- Opět vychází z IGMPv1 a IGMPv2 a je s nimi zpětně kompatibilní
- Info o opuštění skupiny posílá na 224.0.0.22
- Nově zavádí možnost více zdrojů v jedné skupině
  - Tedy už nemusí být jen jeden zdroj dat, ale může jich být více
  - Nepřipojuji se tedy jen ke skupině, ale i ke konkrétnímu zdroj
  - Nově tedy rozlišujeme dva modely
    - ASM – Any source multicast
      - Sice může být více zdrojů v jedné skupině, ale nerozlišují se
    - SSM – Source specific multicast
      - Může být více zdrojů, které jsou ale nově – díky IGMPv3 rozlišitelné a je tedy možné si zvolit skupiny i zdroj



zdroj: https://mrncciew.com/2012/12/25/igmp-basics/

Multicast – Skupinové směrování

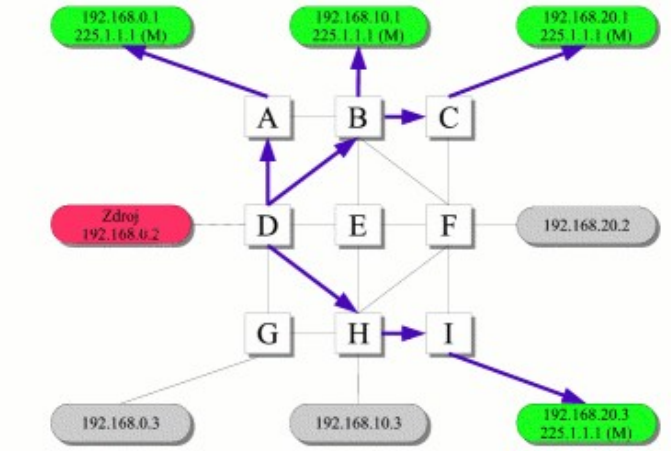
- IGMP nám vyřešilo registraci stanic do jednotlivých skupin na lokálních routerech
- Dalším krokem je přenos a směrování data mezi zdrojem a přijímačem
- S běžnými směrovacími metodami zde nevystačíme
  - Protože cílů kam data směruje může být více – dle příslušnosti přijímačů ve skupinách za jednotlivými porty routeru
- Nad sítí, což je zdroj/e, seznam příjemců a seznam routerů, se snažíme vytvořit strom
  - Aby bylo možné společnou cestou posílat data jen jednou
  - Stromy jsou dvojího typu **source-base** a **shared-base**
- Směrovacích protokolů v multicast je více:
  - DVMRP
  - MOSPF
  - PIM-DM
  - PIM-SM
  - CBT

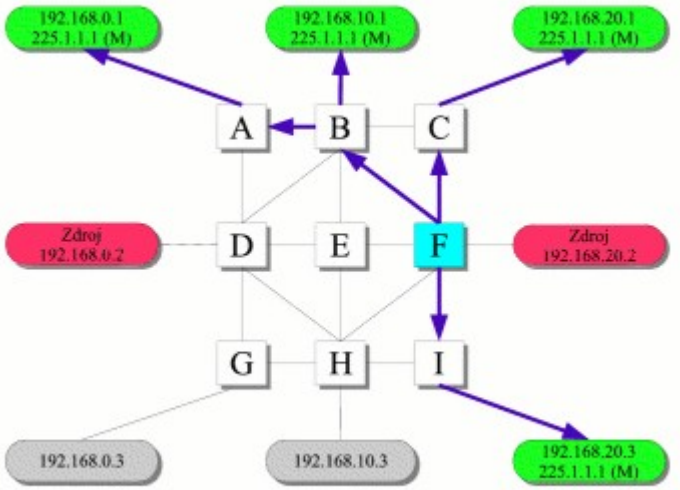


zdroj: https://www.researchgate.net/figure/Classification-of-Multicast-Routing-Protocols_fig2_278023165

Multicast – Skupinové směrování: Stromy

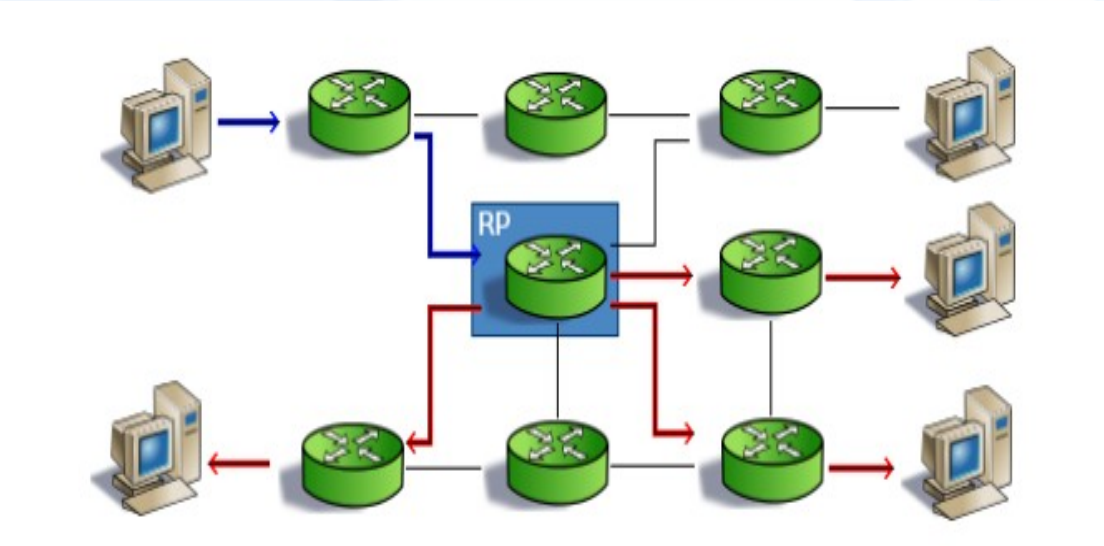
- **Source-base tree** – Source tree – Zdrojový strom
  - Kořen je vysílač, listy jsou příjemci
  - Pro různé zdroje v jedné skupině budou různé stromy
    - Označují se (S,G), např (192.168.1.1, 225.1.1.1)
  - Využívají jej Dense mode protokoly (husté)
- **Shared-base tree** – Shared tree – sdílené stromy
  - Kořen stromu pro danou skupinu je vždy na jednom místě bez ohledu na zdroj dat
  - Kořen je označován jako RP – Rendesvous point
  - Označované jako (*, G), např (*, 225.1.1.1)
  - Existuje ve dvou variantách
    - Jednosměrný - data jsou unicastem poslána na kořen a ten pak zajišťuje jejich distribuci
    - Obousměrný – zdroj posílá data směrem ke kořeni a zároveň směrem k listům
  - Využívají jej Sparce mode protokoly (řídké)
  - Vzniká problém při výpadku RP



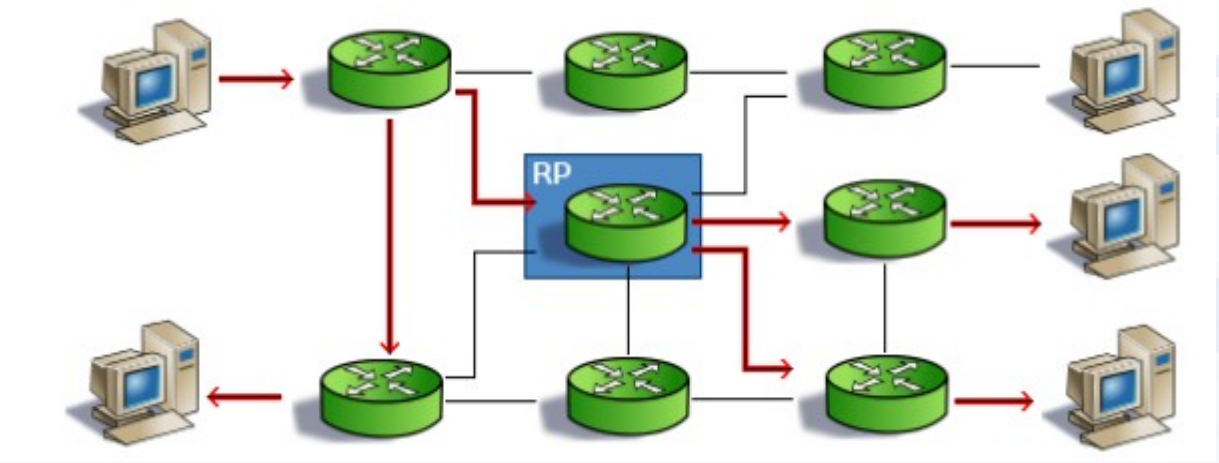


zdroj: https://www.lupa.cz/clanky/uvod-do-ip-multicastu-dil-treti/

Multicast – Skupinové směrování: Stromy: Jednosměrný a obousměrný



Jednosměrný doručovací strom

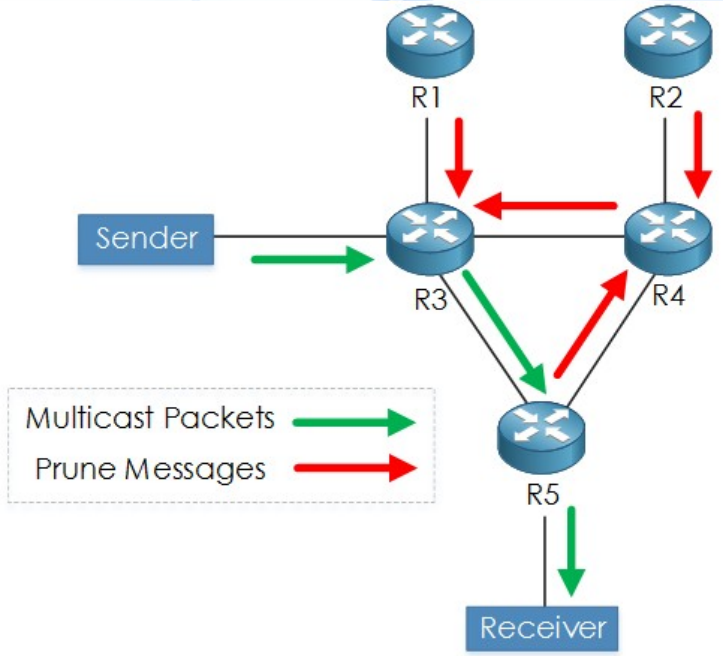


Obousměrný doručovací strom

zdroj: https://adoc.pub/univerzita-pardubice-fakulta-elektrotechniky-a-informatiky-t4ceb6f9f1ddc6f8dd65a6ee730f8606d57035.html

Multicast – Skupinové směrování: Typy protokolů

- **Dense mode**
  - Využívají zdrojové stromy
    - Kořen stromu je zdroj dat
  - Využívají „push“ principu
    - Primární předpoklad, že data jsou třeba všude – do všech větví stromu
    - Tam, kde jsou větve bez účastníka multicastového provozu, je poslána pro danou větech „prune“ zpráva
      - Ta má jen omezenou platnost
    - Po přijetí „prune“ už nejsou do dané větve posílána data dané multicastové skupiny
      - Větev byla „oříznuta“ - „ořezávání větví“
  - Používá se tam, kde předpokládáme, že většina směrovačů bude součástí multicastu - „husté zastoupení“ / „hustý provoz“
    - Nejde o množství dat, ale zastoupení směrovačů
  - Příkladem jsou protokoly DVMRP a PIM-DM
- **Sparce mode**
  - Využívá sdílené stromy
    - Kořen stromu může být libovolný
  - Využívají „pull“ principu
    - Snaží se šetřit přenosy, takže posílá data jen tam, kde jsou požadována
    - Pokud se přijímač přihlásí přes IGMP do multicastové skupiny, router pošle toto info směrem ke kořeni stromu
      - Platnost přihlášení je časově omezena
      - Pokud v dané větvi není žádný živý přijímač je „oříznuta“
  - Používá se tam, kde se předpokládá řídké zastoupení směrovačů v multicastové komunikaci – proto „řídký“
  - Příkladem jsou protokoly PIM-SM či CBT

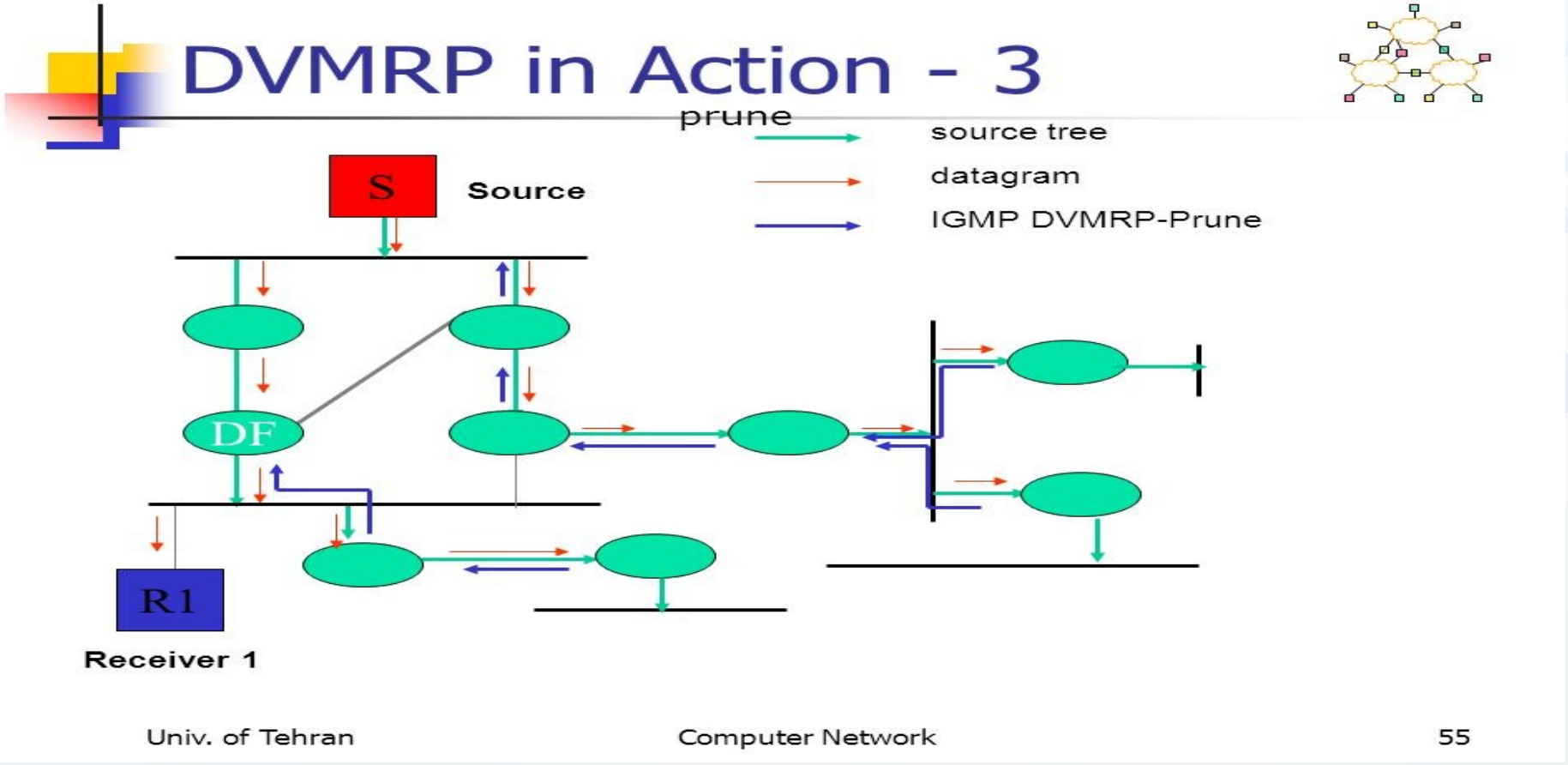


zdroj: https://www.packetflow.co.uk/what-is-pim-protocol-independent-multicast/

Multicast – Skupinové směrování: DVMRP

- DVMRP - Distance Vector Multicast Routing protocol
- Používá source base stromy a tedy se jedná o dense mode protokol
  - „hustý režim“
- Používá záplavové doručování a ořezávání hran
- Vychází z RIP protokolu, ale je výrazně složitější
- Sám si podobně jako RIP sestavuje i unicastovou směrovací tabulku
  - Je v tomhle ohledu nezávislý
- Strom vytváří pomocí Reverse Path Multicasting (RPM)
  - Pokud přijme zprávu pomocí RP a unicastové směrovací tabulky zkontroluje zda se jedná o nejkratší možnou cestu
    - Pokud ano, pošle data dále na všechny rozhraní krom toho odkud přišel
    - Pokud ne, data zahodí
- Pokud v dané podsíti – za routerem - už není žádná živá multicastová stanice, posílá **Prune** a dočasně se odpojuje od stromu

Multicast – Skupinové směrování: DVMRP: Příklad



zdroj: https://slideplayer.com/slide/8070416/

Multicast – Skupinové směrování: MOSPF

- MOSPF – Multicast OSPF
- Používá source base stromy a tedy se jedná o dense mode protokol
  - „hustý režim“
- Vychází a používá OSPF
  - Unicastové
- Každý MOSPF router v paměti drží info o celé topologii sítě
- Do ceny cest – a tedy následně do výpočtu – se zohledňuje i počet stanic stanic na dané cestě
  - Čím více stanic tím lépe – tím více požadavků odbavím jednou kopií dat
- Je to patrně jediný zástupce link state protokolů pro multicast, ale reálně se příliš nepoužívá
  - Problém je v náročnosti přepočtu po každé změně v síti

Multicast – Skupinové směrování: PIM-DM

- PIM-DM – Protokol Independent Multicast – Dense Mode
- Používá source base stromy a tedy se jedná o dense mode protokol
  - „hustý režim“
    - Stejně jako DVMRP předpokládá, že všichni chtějí přijímat
- Může být použit libovolný směrovací protokol pro zjištění reverzní cesty (RPF – Reverse Path Forwarding) pro zjištění nejkratší cesty / eliminaci smyček
- Ve výchozím stavu používá záplavové směrování s následným ořezáváním hran
  - Flood-and-prune
- Existenci ostatních směrovačů zjišťuje pomocí Hello zpráv, které cyklicky každých 30s posílá ostatním směrovačům
  - Tím eliminuje čas, po který by posílal data směrem, kde už nejsou potřeba

Multicast – Skupinové směrování: PIM-SM

- PIM-SM – Protokol Independent Multicast – Sparse Mode
- Používá shared base stromy a tedy se jedná o sparse mode protokol
  - „řídký režim“
  - Jako RP je použitý router s nejvyšší IP a je označován jako DR -Designated Router
- Používá Join zprávy
- Nalezení reverzní cesty (RPF) je nezávislé na konkrétním směrovacím protokolu
- Doručovací stromy se budují mezi příjemcem a RP (Randevous Point) – univerzální (ASM – Any Source Multicast) strom
- Pokud je cesta ke konkrétnímu zdroji kratší, přechází PIM-SM od ASM ke SSM (Source Specific Multicast)

Multicast – Skupinové směrování: CBT

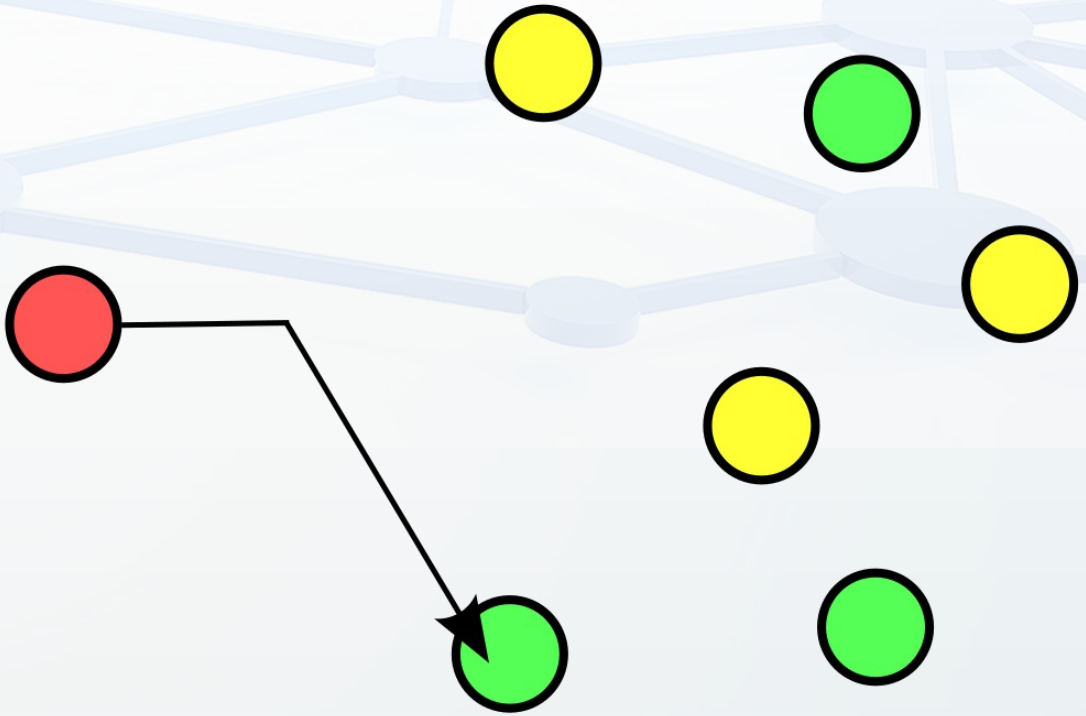
- CBT – Core Base Tree
- Přebírá charakteristiky PIM-SM
- Řídký režim, explicitní připojení, sdílené doručovací stromy
- Efektivnější při vyhledávání zdrojů než PIM-SM
- Rozděluje síť na jednotlivé Area a vytváří infrastrukturu (páteř) pro doručování multicast zpráv
  - V každé oblasti je jeden „páteřní router“
- Není komerčně používán

Multicast – Směrování :Porovnání směrovacích protokolů

Protocol	Dense Mode?	Sparse Mode?	Implicit Join?	Explicit Join?	(S,G) Source-base tree –	(*,G) shared tree?
DVMRP	Yes	No	Yes	No	Yes	No
MOSPF	Yes	No	No	Yes	Yes	No
PIM-DM	Yes	No	Yes	No	Yes	No
PIM-SM	No	Yes	No	Yes	Yes, maybe	Yes, initially
CBT	No	Yes	No	Yes	No	Yes

Anycast

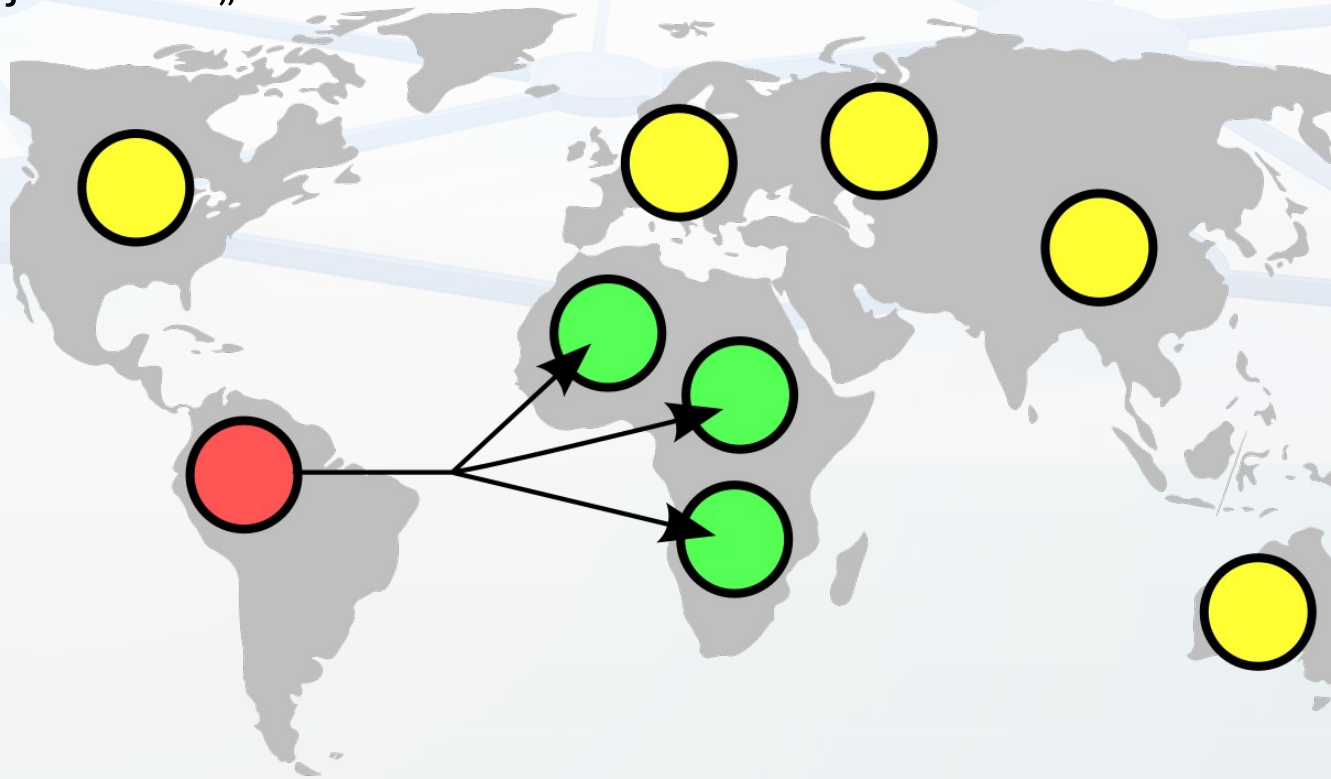
- Specifický typ přenosu dat a směrování, kde cílem není
  - Jeden konkrétní stroj (unicast)
  - Všechny stroje v dané síti (broadcast)
  - Všechny stroje v dané skupině (multicast)
- Cílem je jeden stroj ze skupiny
- Směrování záleží na zadaných konstantách zdrojů a aktuálním stavu zatížení sítě
- Typické použití je připojení na CDN
  - CDN – Content delivery network
    - Sítě poskytující obsah – například obrázky
    - Data jsou typy uložena násobně
    - Je „jedno“, který z dostupných zdrojů použiji
    - Vybírám tedy jeden z množiny



zdroj: https://en.wikipedia.org/wiki/Anycast

Geocast

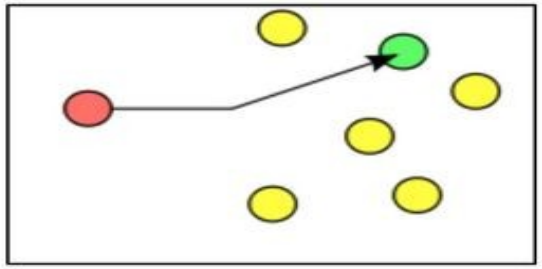
- Specifická varianta multicastu
- Specifický typ přenosu, kde cílem jsou všechny stroje v dané „lokalitě“
  - Tedy například všechna zařízení v Africe
  - Nemusí jít o opravdu všechna, ale může jít o všechna má zařízení v Africe
  - Není nutné vázanou na kontinenty
- Adresa geocastu může mít tři podoby
  - Bod
  - Kruh se středem a poloměrem
  - Mnohoúhelník – defakto seznam bodů



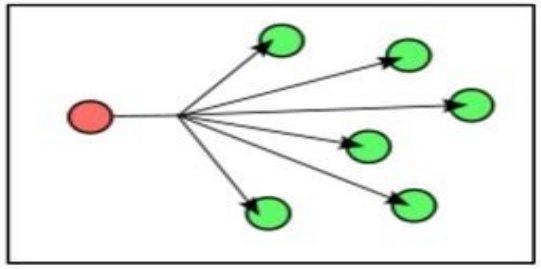
zdroj: https://en.wikipedia.org/wiki/Geocast

Porovnání typů přenosů

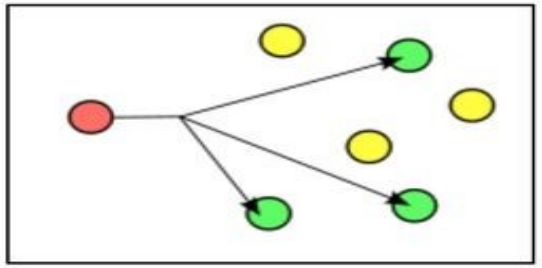
Unicast, Broadcast, Multicast, Anycast



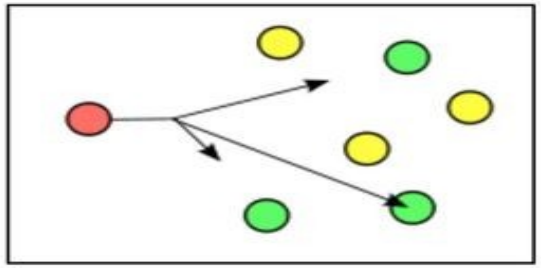
Unicast:
One specific receiver



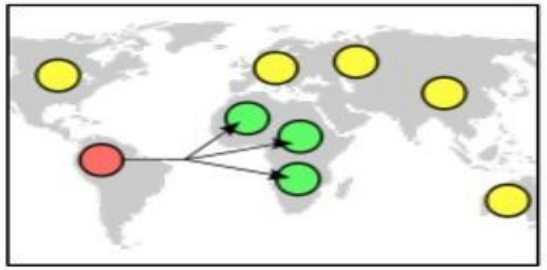
Broadcast:
Many receivers, all on the network



Multicast:
Many receivers, all of a specific group



Anycast:
One receiver, "nearest" of a specific group



Geocast:
Many receivers, all of a geographic region

Pictures: Wikipedia

http://docplayer.net/1821448-Outline-part-i-web-technologies-for-interactive-mm-part-ii-content-oriented-base-technologies-part-iii-multimedia-distribution-services.html