



Networking
For everyone

Multicast Routing

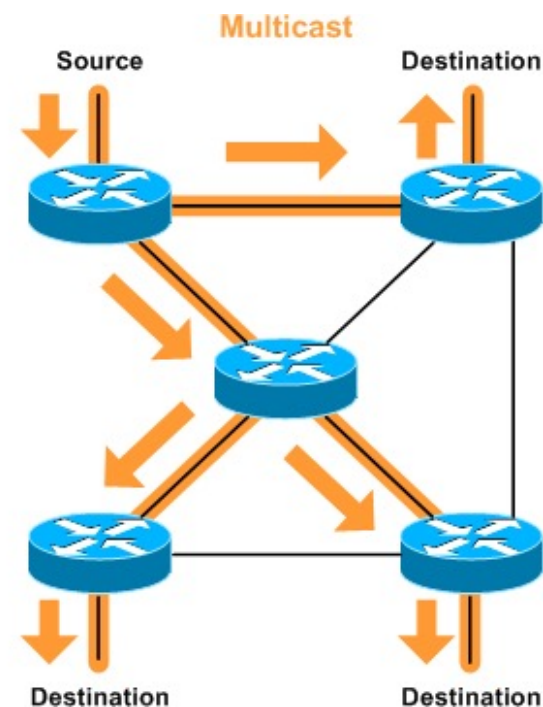
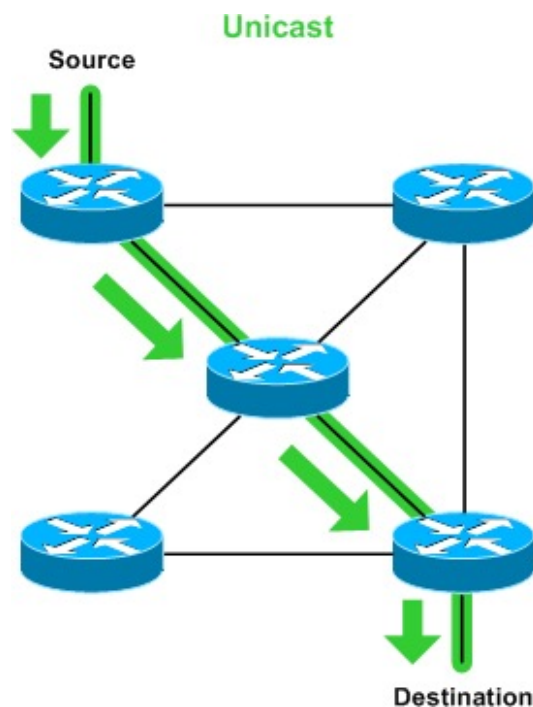


Networking
For everyone

Основы многоадресной рассылки

Когда нужна многоадресная рассылка?

- Одноадресная рассылка хорошо работает для взаимодействий вида «один-к-одному»
- Что делать если нужно передавать информацию от сервера ко многим клиентам?
 - или от большого количества серверов большому количеству клиентов
 - напр. видеоконференции
- Два подхода
 - Push
 - Pull



Многоадресная адресация (IP)

- Выделен блок IP адресов класса Д
 - $224.0.0/4 = 224.0.0.0 - 239.255.255.255$
- Внутри диапазона есть собственная классификация
 - $224.0.0.0/24$ – Local Network Control Block
 - $224.0.1.0/24$ – Internetwork Control Block
 - $224.1.0.0/16$ – Reserved
 - $224.2.0.0/16$ – SDP/SAP
 - $224.3.0.0/16, 224.4.0.0/16$ – AD-HOC
 - ...
 - $232.0.0.0/8$ – Source Specific Multicast

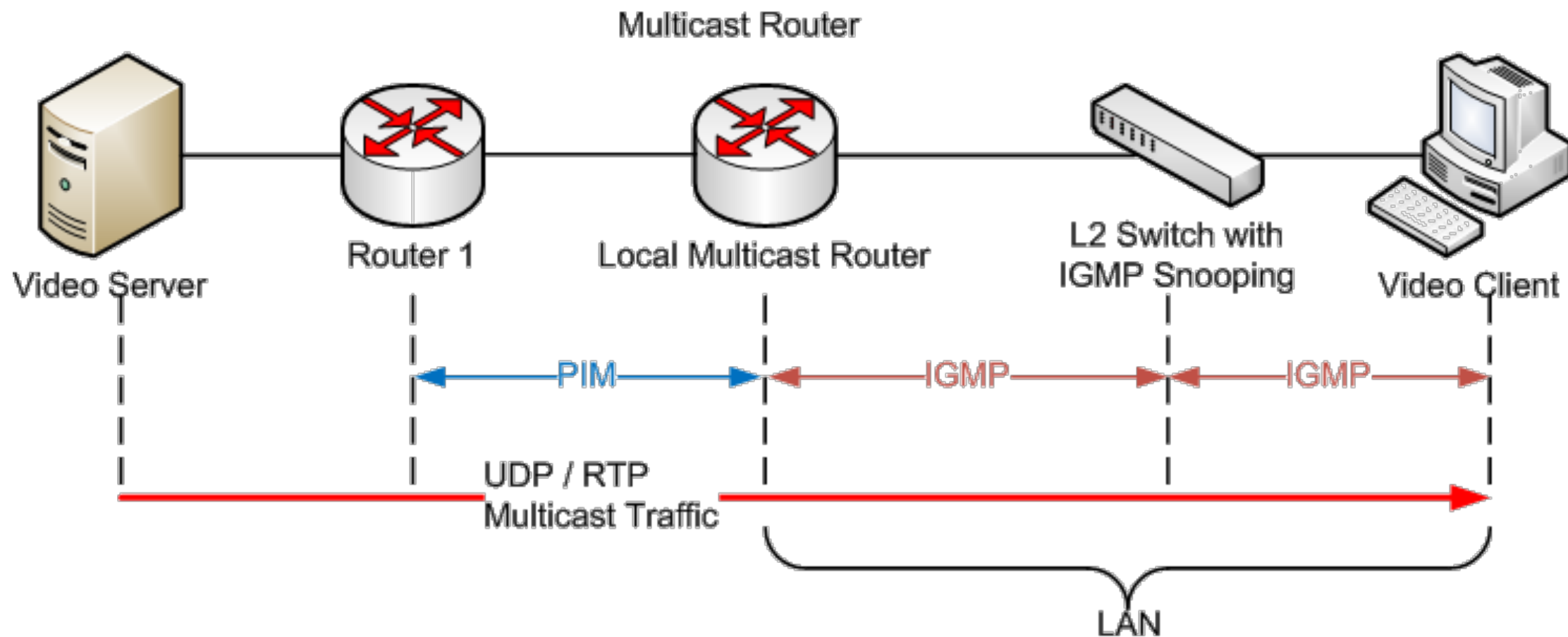


Многоадресная адресация (MAC)

- Каждому IP ставится в соответствие свой MAC
- Используется зарезервированный OUI
 - IPv4: 0100:5eXX:XXXX
 - 2^{28} многоадресных IP-адресов и 2^{23} MAC-адресов
 - IPv6: 3333:XXXX:XXXX
- Что делать коммутатору при получении пакета с таким MAC адресом получателя?



Архитектура сети





Networking
For everyone

Internet Group Membership Protocol

Кратко про IGMP

- Используется получателем чтобы сообщить о своей заинтересованности в получении многоадресной рассылки
 - на текущий момент существуют IGMPv1/v2/v3



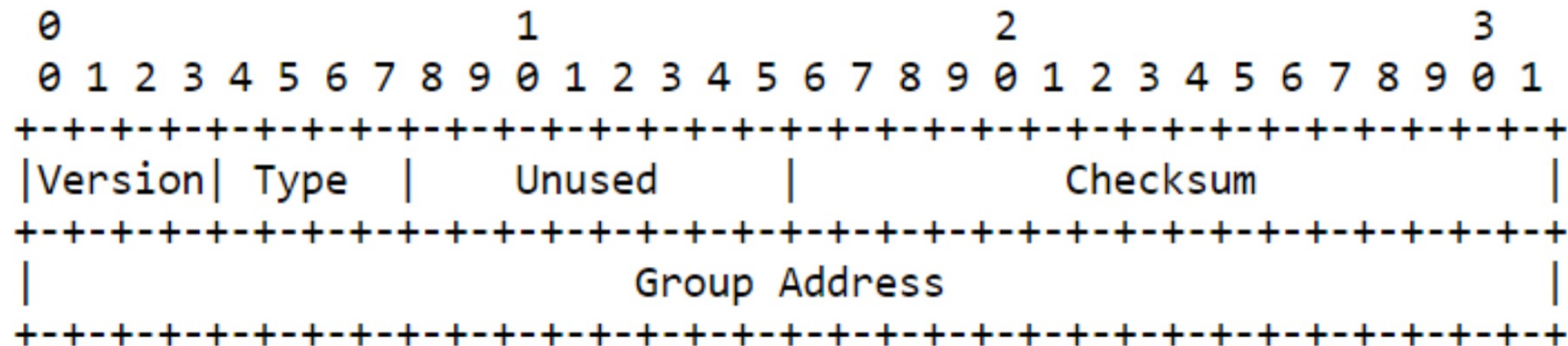
Зачем нужен IGMP?

- Если коммутатор не знает MAC адрес получателя, то пакет рассылается на все интерфейсы
 - неоптимальное использование полосы пропускания
 - клиенты получают трафик, в котором не заинтересованы
- IGMP позволяет коммутаторам и маршрутизатору (шлюзу) разумно передавать трафик клиентам



IGMPv1

- Определяет всего два вида сообщений
 - IGMP Query (General Query)
 - IGMP Report



- Query рассылаются на адрес 224.0.0.1 (все узлы) на периодической основе
 - GDA = 0.0.0.0

```
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: fa:16:3e:e4:d3:de (fa:16:3e:e4:d3:de), Dst: IPv4mcast_01 (01:00:5e:00:00:01)
Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 224.0.0.1 (224.0.0.1)
Internet Group Management Protocol
  [IGMP version: 1]
  Type: Membership query (0x11)
  Header checksum: 0xeeff [correct]
  Multicast Address: 0.0.0.0 (0.0.0.0)
```

IGMPv1

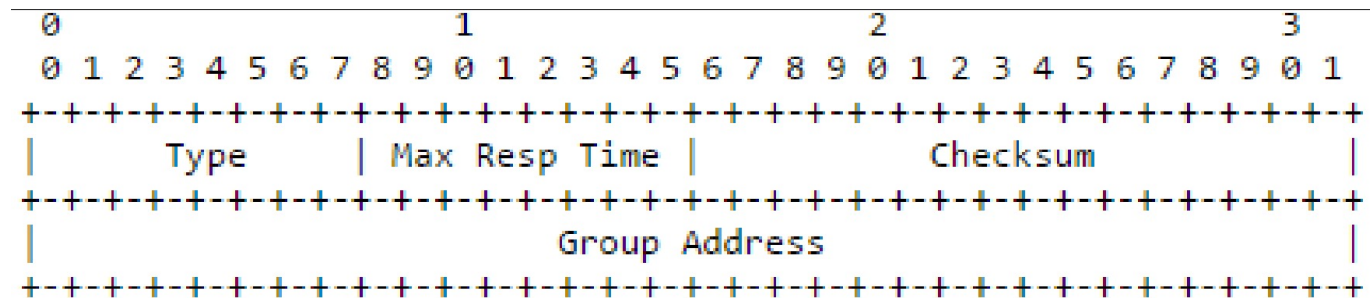
- Когда приложение на клиенте хочет получать трафик, отправляется сообщение Report

```
+ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
+ Ethernet II, Src: fa:16:3e:35:d1:43 (fa:16:3e:35:d1:43), Dst: IPv4mcast_01:01:01 (01:00:5e:01:01:01)
+ Internet Protocol Version 4, Src: 192.168.1.101 (192.168.1.101), Dst: 239.1.1.1 (239.1.1.1)
- Internet Group Management Protocol
  [IGMP Version: 1]
  Type: Membership Report (0x12)
  Header checksum: 0xfdfc [correct]
  Multicast Address: 239.1.1.1 (239.1.1.1)
```

- Не предусмотрен механизм выхода из группы
 - маршрутизатор отправляет Query
 - после 3-х попыток передача трафика приостанавливается

IGMPv2

- Является улучшением v1
 - эдакий v1 на стероидах
- Основная идея появления протокола – улучшение механизма покидания группы
- Четыре типа сообщений
 - Group Membership Report
 - Group Membership Query
 - Leave
 - Group-Specific Query



v2 General Query

- Отправляется маршрутизатором на периодической основе
 - тоже самое, что и v1 Query
 - за исключением Max Resp Time

```
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: fa:16:3e:e4:d3:de (fa:16:3e:e4:d3:de), Dst: IPv4mcast_01 (01:00:5e:00:00:01)
Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 224.0.0.1 (224.0.0.1)
Internet Group Management Protocol
  [IGMP Version: 2]
  Type: Membership Query (0x11)
  Max Resp Time: 10,0 sec (0x64)
  Header checksum: 0xee9b [correct]
  Multicast Address: 0.0.0.0 (0.0.0.0)
```

v2 Membership Report

- Отправляется клиентом в случае заинтересованности получения трафика
 - IP адрес получателя = группа рассылки

```
Frame 1: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface 0
Ethernet II, Src: fa:16:3e:35:d1:43 (fa:16:3e:35:d1:43), Dst: IPv4mcast_01:01:01 (01:00:5e:01:01:01)
Internet Protocol Version 4, Src: 192.168.1.101 (192.168.1.101), Dst: 239.1.1.1 (239.1.1.1)
Internet Group Management Protocol
  [IGMP version: 2]
  Type: Membership Report (0x16)
  Max Resp Time: 0,0 sec (0x00)
  Header checksum: 0xf9fc [correct]
  Multicast Address: 239.1.1.1 (239.1.1.1)
```

- Отправляется клиентом в ответ на Query от маршрутизатора
 - клиент выжидает тайм-аут длиной от 0 до **Max Response Time**, который указан в пришедшем Query



Выход из группы

- Если клиент более не заинтересован в рассылке, он отправляет IGMP Leave
 - IP получателя = 224.0.0.2 (все маршрутизаторы)

4385	05:04:03.997093000	172.16.0.5	224.2.2.4	UDP	1370	Source port: 60603	Destination port: search-agent
4386	05:04:04.012693000	172.16.0.5	224.2.2.4	UDP	1370	Source port: 60603	Destination port: search-agent
4387	05:04:04.028293000	172.16.0.5	224.2.2.4	UDP	1370	Source port: 60603	Destination port: search-agent
4388	05:04:04.028293000	192.168.4.2	224.0.0.2	IGMPv2	46	Leave Group 224.2.2.4	
4389	05:04:04.043893000	172.16.0.5	224.2.2.4	UDP	1370	Source port: 60603	Destination port: search-agent
4390	05:04:04.059493000	172.16.0.5	224.2.2.4	UDP	1370	Source port: 60603	Destination port: search-agent
4391	05:04:04.075093000	172.16.0.5	224.2.2.4	UDP	1370	Source port: 60603	Destination port: search-agent
4392	05:04:04.090693000	172.16.0.5	224.2.2.4	UDP	1370	Source port: 60603	Destination port: search-agent

⊞	Frame 4388: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface 0
⊞	Ethernet II, Src: Microsof_0c:6e:0d (00:15:5d:0c:6e:0d), Dst: IPv4mcast_00:00:02 (01:00:5e:00:00:02)
⊞	Internet Protocol Version 4, Src: 192.168.4.2 (192.168.4.2), Dst: 224.0.0.2 (224.0.0.2)
⊞	Internet Group Management Protocol
	[IGMP Version: 2]
	Type: Leave Group (0x17)
	Max Response Time: 0,0 sec (0x00)
	Header checksum: 0x06f9 [correct]
	Multicast Address: 224.2.2.4 (224.2.2.4)



Выход из группы

- В ответ на получение Leave, маршрутизатор отправляется Group-Specific Query
 - отвечают только те клиенты, которые подписаны на указанную группу

4468	05:04:05.276295000	192.168.4.1	224.2.2.4	IGMPv2	60	Membership Query, specific for group 224.2.2.4	
4469	05:04:05.291895000	172.16.0.5	224.2.2.4	UDP	1370	Source port: 60603	Destination port: search-agent
4470	05:04:05.307495000	172.16.0.5	224.2.2.4	UDP	1370	Source port: 60603	Destination port: search-agent
4471	05:04:05.323095000	172.16.0.5	224.2.2.4	UDP	1370	Source port: 60603	Destination port: search-agent
4472	05:04:05.338695000	172.16.0.5	224.2.2.4	UDP	1370	Source port: 60603	Destination port: search-agent

⊞	Frame 4468: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊞	Ethernet II, Src: ca:00:13:08:00:08 (ca:00:13:08:00:08), Dst: IPv4mcast 02:02:04 (01:00:5e:02:02:04)
⊞	Internet Protocol Version 4, Src: 192.168.4.1 (192.168.4.1), Dst: 224.2.2.4 (224.2.2.4)
⊞	Internet Group Management Protocol
	[IGMP Version: 2]
	Type: Membership Query (0x11)
	Max Response Time: 1,0 sec (0x0a)
	Header checksum: 0x0cef [correct]
	Multicast Address: 224.2.2.4 (224.2.2.4)



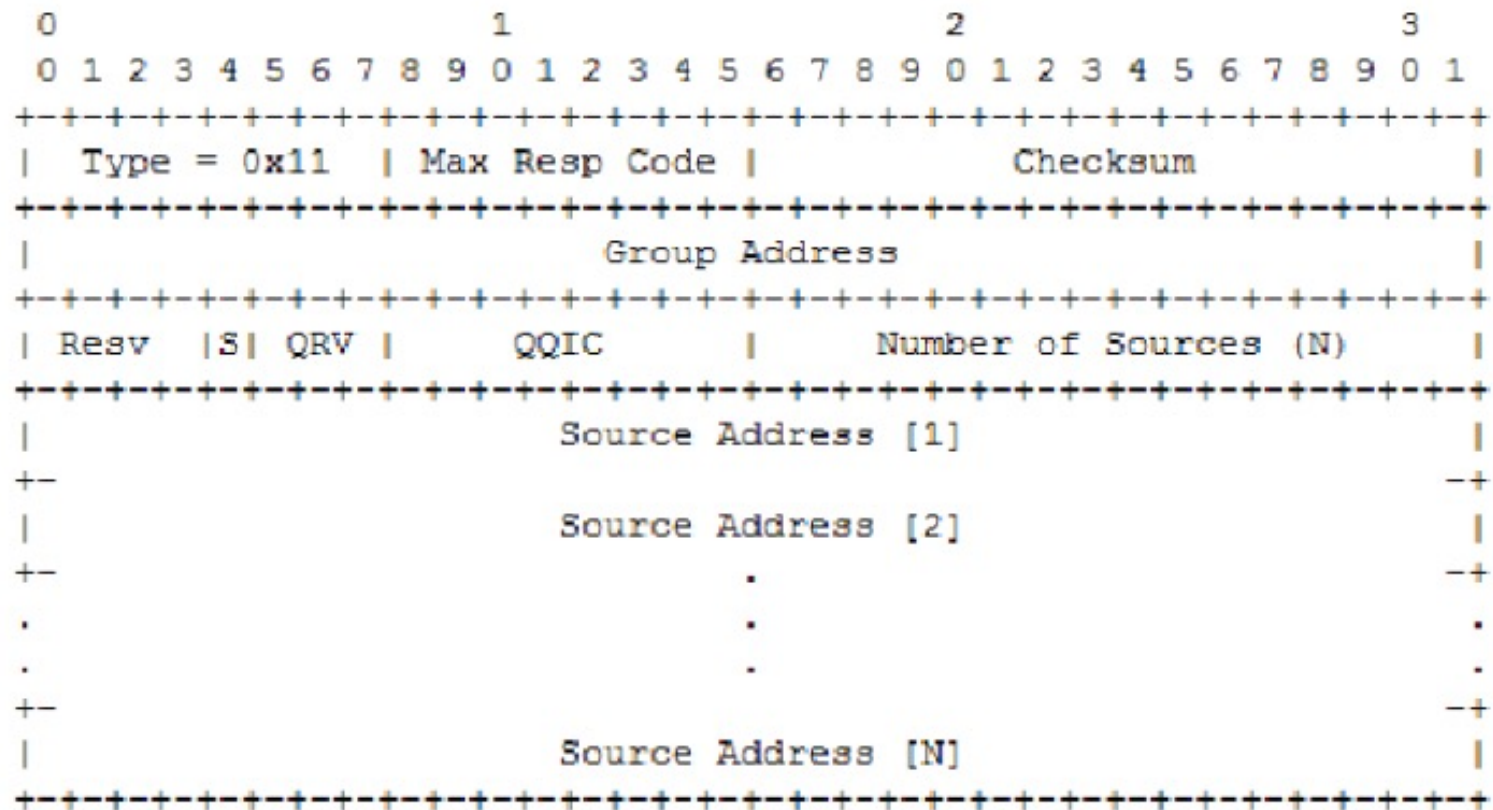
IGMP Querier

- А если маршрутизаторов в сегменте больше одного?
- Выбирается Querier
 - принцип: меньше IP адрес = лучше
- Переход роли контролируется таймером «Other Querier Present Interval»
- Если Querier получает Query с меньшим адресом, он складывает с себя роль
 - Querier'ом становится другой маршрутизатор, у которого IP меньше.



IGMPv3

- Предназначается для Source-Specific Multicast
- Подразумевается, что клиентское приложение точно знает IP адрес источника





Networking
For everyone

IGMP Snooping

Идея

- Коммутатор может прослушивать и анализировать все проходящие IGMP сообщения
 - MAC получателя
 - MAC многоадресной рассылки
 - IP многоадресной рассылки
 - Port + VLAN получателя



Snooping Proxy

- На IGMP Query отвечает только один клиент. Как быть?
 - запретить прохождение Report между клиентскими интерфейсами 😊
- Report перенаправляются с клиентского интерфейса только в сторону маршрутизатора



Snooping и выход из группы

- При получении IGMP Leave
 - коммутатор создаёт General Query
 - ответ ожидается в течение 1 сек
 - (config)#ip igmp snooping last-member-query-interval
 - не получен ответ на Query?
 - удалить запись из базы данных
 - перенаправить Leave в сторону маршрутизатора
- Мгновенный выход

(config-if)#ip igmp snooping fast-leave

(config)#ip igmp snooping vlan {VLAN_ID} immediate-leave



Snooping Mrouter интерфейс

- Чтобы IGMP Snooping корректно работал, коммутатор должен различать клиентские интерфейсы и интерфейс к маршрутизатору
- Multicast Router (Mrouter) интерфейс может быть определён динамически или статически
 - основываясь на получении IGMP Query или PIM

```
(config)#ip igmp snooping vlan {VLAN_ID} mrouter interface {INTERFACE}
```



IGMP Snooping и STP TCN

- При получении TCN коммутатор начинает «флудить» весь многоадресный трафик в рамках VLAN в течение 3 Query интервалов
- Создаётся специальное IGMP Query Solicitation
 - IGMP Leave на группу 0.0.0.0
- Основная цель деяния – максимально быстро начать передавать трафик по новой топологии





Networking
For everyone