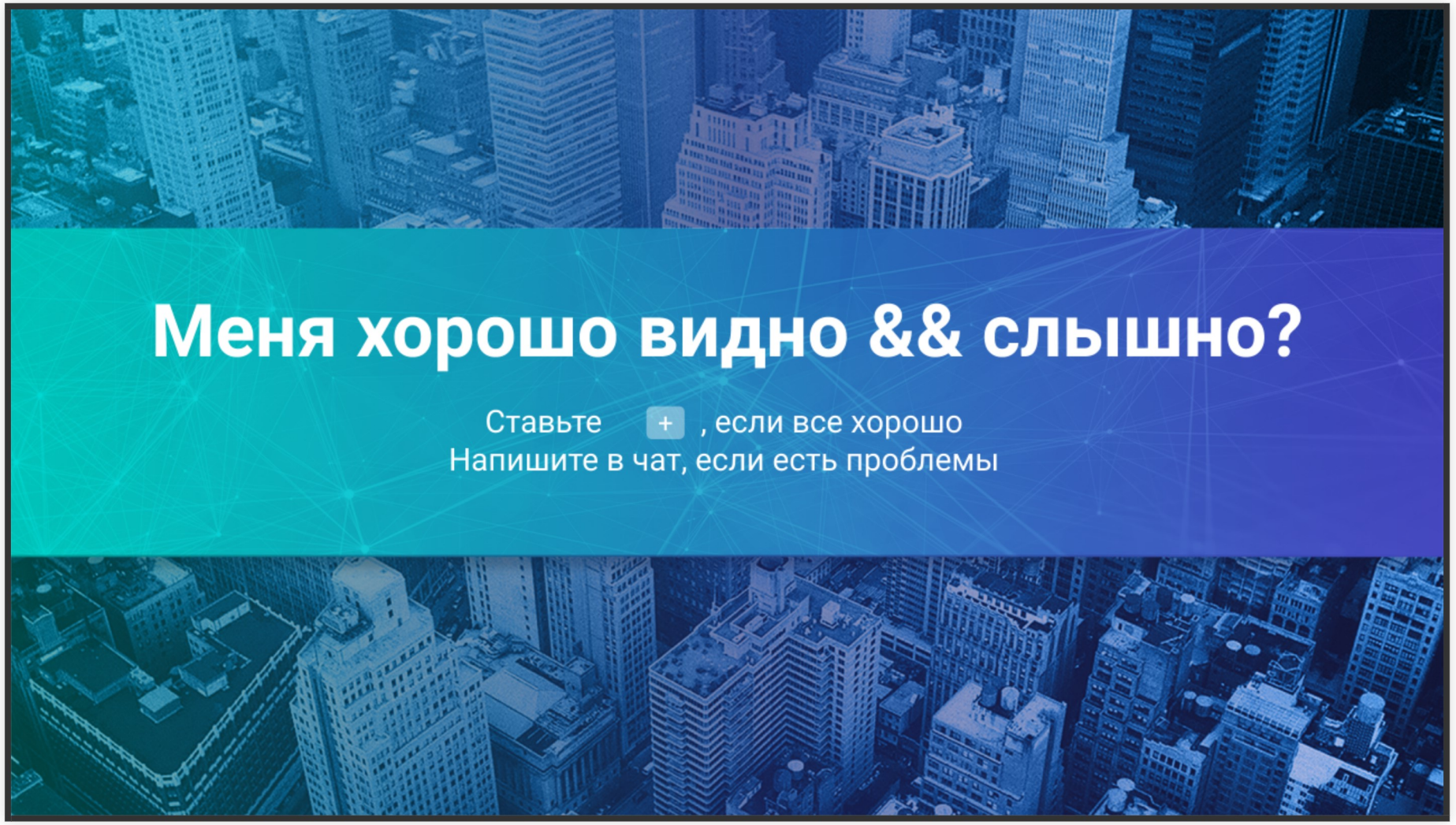

Меня хорошо видно && слышно?
Ставьте + , если все хорошо
Напишите в чат, если есть проблемы

НЕ ЗАБЫТЬ ВКЛЮЧИТЬ ЗАПИСЬ!!!

Администратор Linux

Александр Гаврик

Наставник OTUS

Системный администратор

Администратор локальных сетей

Internet Protocol version 6

Цель занятия

- Понимание работы протокола IPv6
- Особенности и преимущества использования
- Типы взаимодействия в IPv6
- Формирование адреса IPv6
- Получение адреса IPv6 разными способами
- Маршрутизация и firewall в IPv6

План занятия

- Сравним IPv4 и IPv6;
- Изучим методы взаимодействия узлов в IPv6;
- Рассмотрим адреса IPv6, их типы и научимся их различать;
- Поймем, почему ICMPv6 очень важен в IPv6;
- Настроим IPv6 в Linux и проверим его работоспособность;
- Демонстрация механизмов выдачи адресов IPv6 (SLAAC и DHCP);
- Обсудим основные особенности маршрутизации и firewall в IPv6.

Недостатки и особенности IPv4

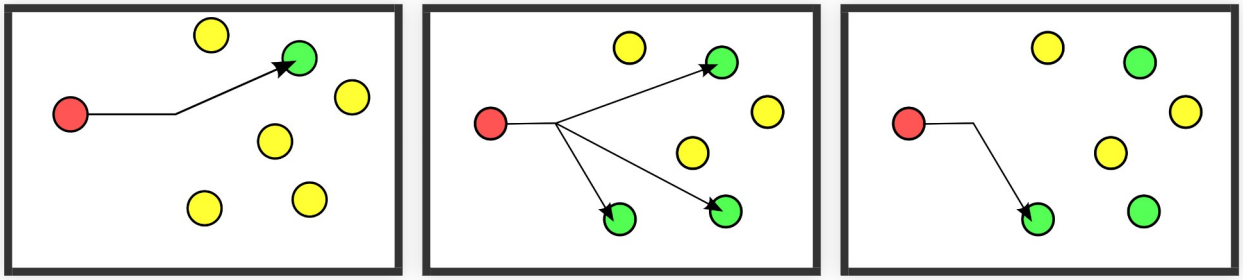
- протокол-пионер (1974 год, иная парадигма);
- недостаток адресов и классовая адресация;
- дополнительные служебные механизмы (протоколы ICMP, ARP, DHCP);
- нет автонастройки (APIPA не в счёт);
- нет встроенных механизмов защиты данных (стек протоколов IPSec);
- NAT и отсутствие сквозной связности "от края до края";
- разделение на публичные и частные адресные пространства и, как следствие, коллизии адресных пространств;
- прикрученная сверху бесклассовая адресация;
- фрагментация на маршрутизаторе.

Преимущества IP version 6

- много адресов, единое адресное пространство в сети Интернет;
- адресация похожая на "классовую", но не она, т.е. мы понимаем что это за адрес, когда смотрим на него;
- преимущества бесклассовой адресации: возможность аггрегации;
- убраны по максимуму вспомогательные протоколы, а нужные функции интегрированы в протокол;
- штатный механизм автоконфигурирования;
- штатные механизмы безопасности;
- "отсутствие" NAT и сквозная связность;
- отсутствие широковещания (убрана паразитная нагрузка на узлы сети внутри канала);
- оптимизация формата заголовка (фиксированная длина и отдельный расширяемый заголовок);
- фрагментация на отправителе.

Принципы взаимодействия

- **Unicast** - одноадресная передача одному адресату (основное взаимодействие);
- **Multicast** - многоадресная передача адресатам, которые подписались на группу;
- **Anycast** - одноадресная передача ближайшему адресату (альтернативный метод);



Unicast

Иметь несколько адресов на интерфейсе - это нормально для IPv6

По стандарту: адреса должны быть уникальны в пределах Интернет за исключением некоторых немаршрутизируемых типов адресов.
По факту: адреса должны быть уникальны в пределах какой-либо(!) сети:

- В пределах Интернет - global unicast address;
- В пределах канала - link-local address;
- Есть ещё некоторые виды.

```
ip -6 address show dev eth1
ip -6 address add ipv6address/prefixlength dev interface
```

Адрес IPv6

128 бит записанные в шестнадцатеричным виде, разделенные двоеточиями на 8 групп (по 4 разряда)

2001:0DB8:0000:00FF:0000:0000:0000:0001

Сокращенный формат (однозначное соответствие):

2001:DB8:0:FF:0:0:0:1

2001:DB8:0:FF::1

Сокращенный адрес IPv6

- 1 правило: старшие нули можно убрать, если сам октет не 0 (0DB8 -> DB8, 0000 -> 0)
- 2 правило: в одном месте несколько нулевых групп можно заменить на :: (:0000:0000: -> ::)
- Второе правило можно применить только в одном месте и минимум к 2-м группам нулей

FF02:0000:0000:0000:0000:0001:FF00:0300
FF02:0:0:0:0:1:FF00:300
FF02::1:FF00:300

2001:0DB8:0000:1111:0000:0000:0000:0200
2001:DB8:0:1111:0:0:0:200
2001:DB8:0:1111::200

0000:0000:0000:0000:0000:0000:0000:0001
0:0:0:0:0:0:0:1
::1

0000:0000:0000:0000:0000:0000:0000:0000
0:0:0:0:0:0:0:0
::

Префикс IPv6

Адрес условно делится на 2 части: **Network ID** и **Interface ID**.
Граница между двумя частями определяется маской-префиксом.

2001:0DB8:0000:00FF:0000:0000:0000:0001/64
2001:DB8:0:FF::1/64
2001:DB8::/32
::1/128
::/0

Рекомендуется на конечных узлах назначать /64 (часто так и есть).
Для point-to-point можно и правильно использовать /127.
Но можно использовать любую длину, которую захочется.

Network ID. Типы адресов IPv6

- Link-local unicast - fe80::/10 - индивидуальные адреса в пределах канала
- Global unicast - 2000::/3 - глобально индивидуальные адреса
- Multicast - ff00::/8 - адреса групповой рассылки
- Loopback - ::1/128 - локальная машина
- Unspecified - ::/128 - неуказанный (неизвестный) адрес
- Unique-local - fc00::/7 (fc00::/8 + fd00::/8) - индивидуальные адреса в пределах сайта (предприятия)
- и некоторые другие...

Network ID. Link-local unicast

Уникальные НЕмаршрутизируемые адреса в пределах канала

fe80::/10 (чаще всего будут fe80::/64)

Генерируются автоматически. Генерируются обязательно.

Могут совпадать на разных интерфейсах одного устройства, т.к. будут в разных каналах. Следовательно, при их использовании обязательно указывать интерфейс.

Только для использования внутри сети (аналог IPv4 169.254/16).
Не маршрутизируются в Интернет.

Адрес IPv6 в linux

```
sysctl -a | grep ipv6.*
ip -6 address
ip -6 address add ipv6address/prefixlength dev interface
nmcli connection show System\ eth1 | grep ipv6
nmcli connection mod System\ eth2 ipv6.addresses "fd00:2000::1/64"
nmtui
vi /etc/sysconfig/network-scripts/ifcfg-eth2
```

Ручная конфигурация

```
ipv6.method manual     IPV6_AUTOCONF=no
ipv6.method auto       IPV6_AUTOCONF=yes
ipv6.method dhcp       IPV6_AUTOCONF=no
                       DHCPV6C=yes
ipv6.dns ...           DNS0=...

ipv6.addresses "2001:db8::a/64 2001:db8::1"
IPV6ADDR=2001:db8::a/64
IPV6_DEFAULTGW=2001:db8::1

ipv6.dns-search example.com     DOMAIN=example.com
ipv6.ignore-auto-dns true       IPV6_PEERDNS=no
connection.autoconnect yes      ONBOOT=YES
connection.id eth0              NAME=eth0
connection.interface-name eth0     DEVICE=eth0
802-3-ethernet.mac-address ...     HWADDR=...
```

Multicast

Зарезервированные адреса многоадресной рассылки:

- FF02::1 - все устройства;
- FF02::2 - все маршрутизаторы;
- FF02::1:2 - все DHCPv6 серверы;
- FF02::1:FFxx:xxxx/104 - solicited-node multicast, группа узлов, у которых совпадают последние 24 бита (xx:xxxx) из unicast адреса;
- FF02::5 - группа маршрутизаторов с протоколом OSPFv3;
- FF02::6 - группа маршрутизаторов с протоколом OSPFv3;

Область видимости multicast:

- 1 - интерфейс
- 2 - канал
- и другие.

```
ping6 ff02::1%eth1
```

Network ID. Unique-local unicast

Уникальные НЕмаршрутизируемые адреса в пределах сайта.

fc00::/7 (fc00::/8 + fd00::/8)

- fc00::/8 - управляются IANA (фактически не используются);
- fd00::/8 - можно выбрать самостоятельно (стандарт обязывает использовать сеть /48, выбранную по специальному алгоритму);

Только для использования внутри сети.

Не маршрутизируются в Интернет.

Помним, что NAT "отсутствует".

Network ID. Global unicast

Уникальные маршрутизируемые адреса в пределах Интернет.
Имеют иерархию.

[2001:0][DB8]:[0000]:1111:0000:0000:0000:0200

Internet Assigned Numbers Authority (IANA)

Regional Internet Registry (RIR) - RIPE NCC

Local Internet Registry (LIR)

Internet Service Provider (ISP)
(часто ISP имеет статус LIR)

Клиенты (от /48 до /64)

Interface ID

Можно использовать любой размер Interface ID, но обычно 64 бита (/64), т.к. работает modified EUI-64 из MAC.

Interface ID может быть назначен несколькими способами:

- вручную;
- автоконфигурация modified EUI-64 (как вариант: из MAC адреса интерфейса путём вставки FFFE в середину MAC и инвертирования U-бита);
- privacy extensions (RFC4941);
- протоколом ICMPv6 через механизмы Neighbor Discovery и Router Discovery (SLAAC, stateless DHCPv6);
- протоколом DHCPv6 в режиме stateful;

У адреса, внезапно(!), есть жизненный цикл:
(tentative > preferred > deprecated > invalid)

ICMPv6

Что делает? Для чего он нужен?

- То же, что и раньше - доставляет информационные сообщения и ошибки (PMTUD и пр.);
- Узнает канальные адреса соседей (Neighbor Discovery вместо ARP);
- Делает базовую автонастройку конечных узлов (Router Discovery вместо DHCP);
- Ещё управляет multicast (Multicast Listener Discovery вместо IGMP).

Если вы всё же хотите его фильтровать и блокировать, то есть RFC4890.

ND&RD

Neighbor Discovery

(знаю адрес IPv6 соседа, но не знаю канальный: как найти?)

- Neighbor Solicitation (NS) - запрос канального адреса (LLA или ::(DAD) -> SNMA);
- Neighbor Advertisement (NA) - ответ на такой запрос (LLA -> LLA или FF02::1(DAD));
- тут же работают механизмы Duplicate Address Detection (DAD) и Neighbor Unreachability Detection (NUD);

Router Discovery

(хочу получить информацию о роутерах)

- Router Solicitation (RS) - запрос информации о роутерах (:: -> FF02::2);
- Router Advertisement (RA) - оповещение по расписанию о настройках IPv6 и ответ, если был принудительный запрос (LLA -> FF02::1).

Полезные команды

```
ip -6 neigh
ndptool monitor -i eth1
tcpdump -i eth1 -vv icmp6
tcpdump -i eth1 -vv '(udp port 546 or 547)'
```

Stateless Address Autoconfiguration

Как получить адрес? На роутере настроить radvd и ... SLAAC!

- Включить интерфейс;
- Генерируется Link-Local Address и рассылается сообщение Neighbor Solicitation на адрес Solicited-node Multicast для Duplicate Address Detection (адрес в состоянии tentative);
- Рассылается сообщение Router Solicitation на адрес ff02::2;
- Роутер отвечает на Link-Local Address, что есть такие-то доступные префиксы и настройки;
- Генерируется Global Unicast Address на основе полученного префикса и рассылается сообщение Neighbor Solicitation на адрес Solicited-node Multicast для Duplicate Address Detection (адрес в состоянии tentative);
- Применяются настройки полученные от роутера;
- Если Duplicate Address Detection отрабатывает успешно, то адреса переходят в состояние preferred.

SLAAC и DHCPv6 в linux

```
yum install radvd
man radvd
man radvd.conf
vi /etc/radvd.conf
radvdump

yum install dhcp
man dhcpd6.conf
less /usr/share/doc/dhcp*/dhcpd6.conf.example
vi /etc/dhcp/dhcpd6.conf

dhclient -6 -v
dhclient -6 -S
```

RADVD SLAAC

```
interface eth1
{
        AdvSendAdvert on;
        MinRtrAdvInterval 30;
        MaxRtrAdvInterval 100;
        AdvManagedFlag off;
        AdvOtherConfigFlag off;
        prefix 2a03:5800:fa70:76bf::/64
        {
                AdvOnLink on;
                AdvAutonomous on;
        };
        RDNSS 2001:4860:4860::8888 {};
};
```

Domain Name System

Получить адрес IPv6 по имени узла: AAAA-запись.

Остальные записи (NX, NS, SRV, CNAME) тоже должны уметь работать с AAAA.

```
ipv6.l.google.com. IN AAAA 2a00:1450:4010:c0d::64
```

Получить имя узла по адресу IPv6: PTR-запись.

```
4.6.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.0.c.0.0.1.0.4.0.5.4.1.0.0.a.2.ip6.arpa
IN PTR lq-in-x64.1e100.net
```

Чтобы по SLAAC выдать клиенту DNS-сервер нужно использовать опцию RDNSS.

DHCPv6 - для чего он нужен?

DHCPv6 нужен, т.к. в SLAAC ограничен набор предлагаемых опций.

Если вы хотите, к примеру, загрузку по сети или передавать опции NTP, то вам нужен полноценный сервер DHCPv6.

Варианты:

- stateless DHCPv6 = SLAAC (сеть, префикс и шлюз) + DHCPv6 (опции);
- stateful DHCPv6 (клиент принципиально не слушает RA от роутера и обращается к серверу DHCPv6).

Stateless DHCPv6

В radvd устанавливаем флаги рассылаемого сообщения RA:

- Autonomous = on (можно назначить адрес из присылаемого в RA префикса);
- Managed = off (не запрашиваем адрес у сервера DHCPv6);
- OtherConfig = on (но получаем опции у сервера DHCPv6);

Очевидно, что в сети должен присутствовать работающий сервер DHCPv6.

RADVD stateless DHCPv6

```
interface eth1
{
        AdvSendAdvert on;
        MinRtrAdvInterval 30;
        MaxRtrAdvInterval 100;
        AdvManagedFlag off;
        AdvOtherConfigFlag on; #отличие от SLAAC only
        prefix 2a03:5800:fa70:76bf::/64
        {
                AdvOnLink on;
                AdvAutonomous on;
        };
        RDNSS 2001:4860:4860::8888 {};
};
```

Stateful DHCPv6

Если сообщения RA рассылаются, то:

- Autonomous = off (не назначаем адрес из префиксов RA)
- Managed = on (запрашиваем адрес у сервера DHCPv6)
- OtherConfig = on (получаем опции у сервера DHCPv6)

Если RA не рассылаются, то клиент всегда может самостоятельно обратиться к серверу DHCPv6 по FF02::1:2

Помним, что клиент отправляет сообщение с порта 546/UDP серверу на порт 547/UDP.

В идеальном случае, DHCPv6 сервер ещё добавляет соответствующие записи в зону DNS.

stateless/stateful DHCPv6

```
subnet6 2a03:5800:fa70:76bf::/64 {
 #range6 2a03:5800:fa70:76bf::1000 2a03:5800:fa70:76bf::2000;
 option dhcp6.name-servers 2001:4860:4860::8844;
 option dhcp6.domain-search "example.net";
}
```

RADVD stateful DHCPv6

```
interface eth1
{
        AdvSendAdvert on;
        MinRtrAdvInterval 30;
        MaxRtrAdvInterval 100;
        AdvManagedFlag on; # отличие от stateless
        AdvOtherConfigFlag on;
        prefix 2a03:5800:fa70:76bf::/64
        {
                AdvOnLink on;
                AdvAutonomous off; # отличие от stateless
        };
        RDNSS 2001:4860:4860::8888 {};
};
```

Машрутизация и firewall

В маршрутизации всё как и у IPv4:

- статическая маршрутизация;
- динамическая IGP: RIPng и OSPFv3;
- динамическая EGP: BGP.

```
ip -6 route
ip -6 route add ipv6network/prefixlength dev interface
```

Firewall как, впрочем, и IPv4, если в сети не было NAT:

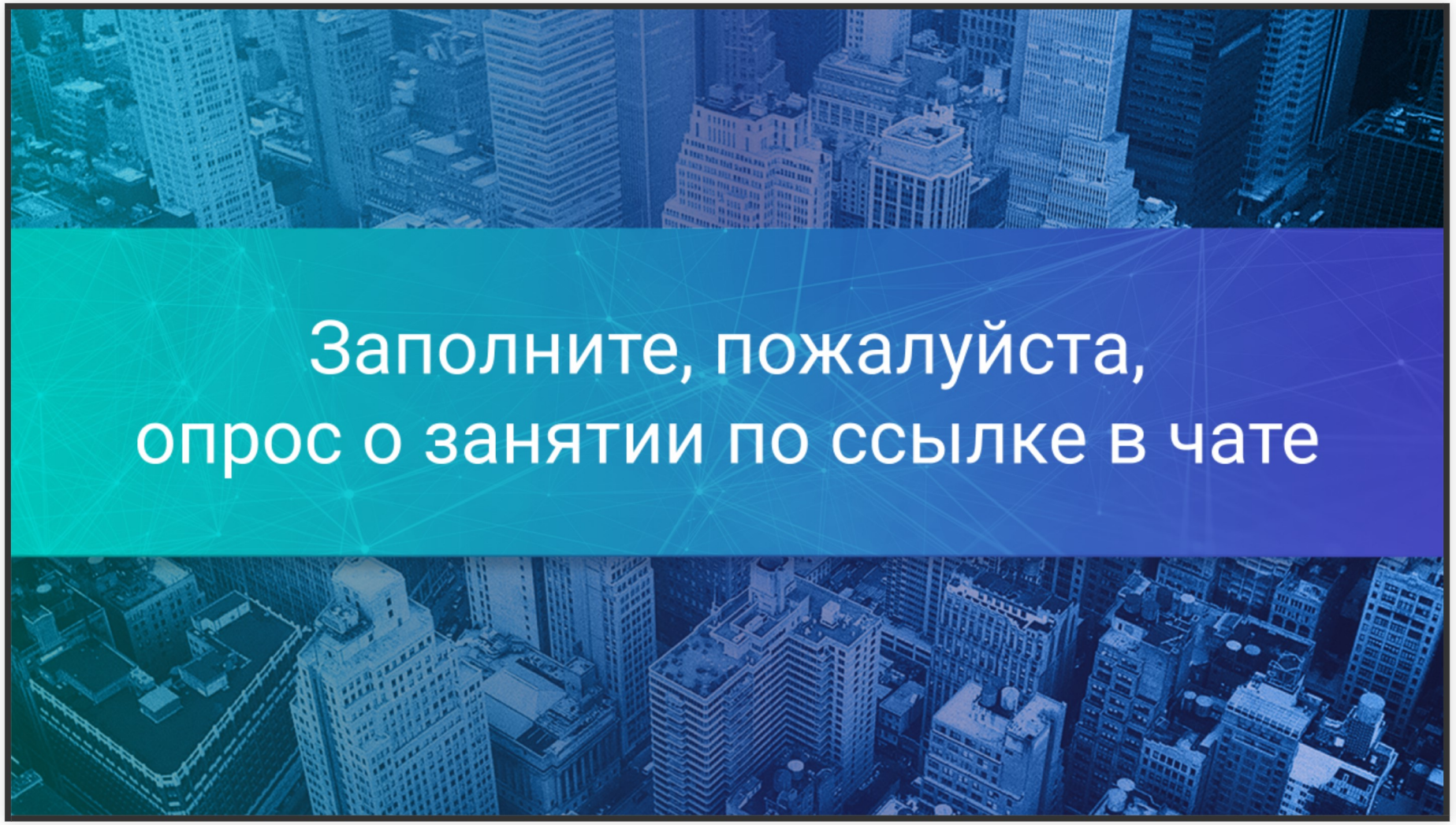
- в INPUT разрешаем только ICMPv6/DHCPv6/SSH и прочее нужное;
- фильтрация FORWARD на маршрутизаторах при желании;
- фильтрация OUTPUT при желании (чётко понимать зачем).

```
less /usr/lib/firewalld/services/dhcpv6-client.xml
firewall-cmd --add-service="dhcpv6-client"
ip6tables -L -n -v
```

Рефлексия

Отметьте 3 пункта, которые вам запомнились с вебинара

Что вы будете применять в работе из сегодняшнего вебинара?


Заполните, пожалуйста,
опрос о занятии по ссылке в чате