Как работает сеть в K8s

CNI, сетевые плагины и политики в Kubernetes

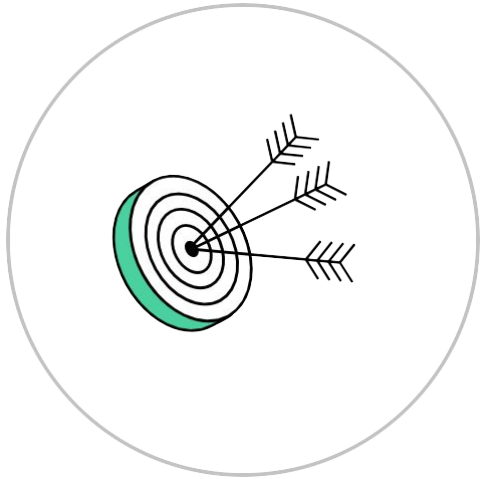
Кирилл Касаткин
DevOps-инженер, Renue

Кирилл Касаткин

DevOps-инженер, Renue

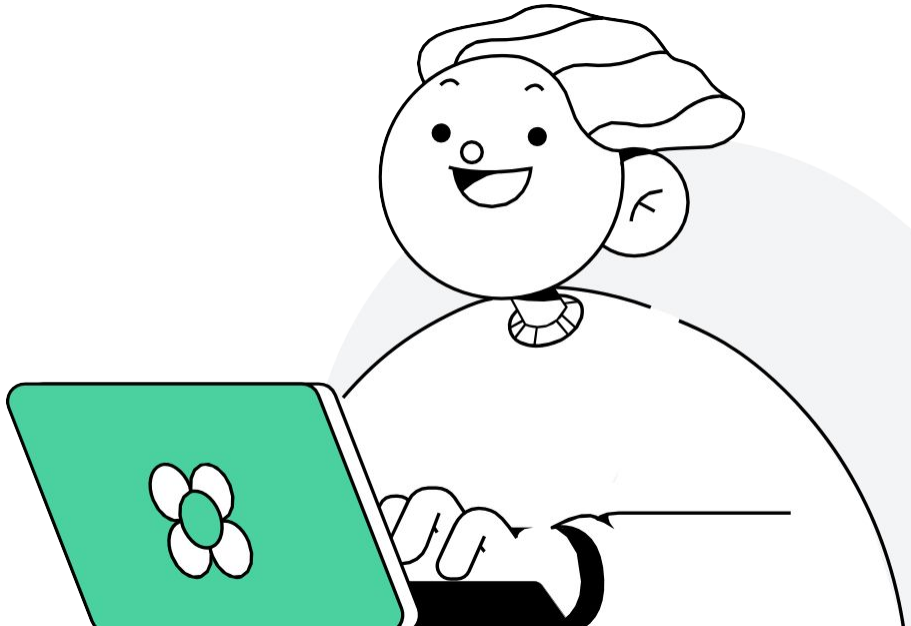
Цели занятия

- Изучить сетевую модель подов
- Рассмотреть сетевые плагины Flannel и Calico



План занятия

1. Сетевая модель
2. Сетевые плагины
3. Итоги
4. Домашнее задание

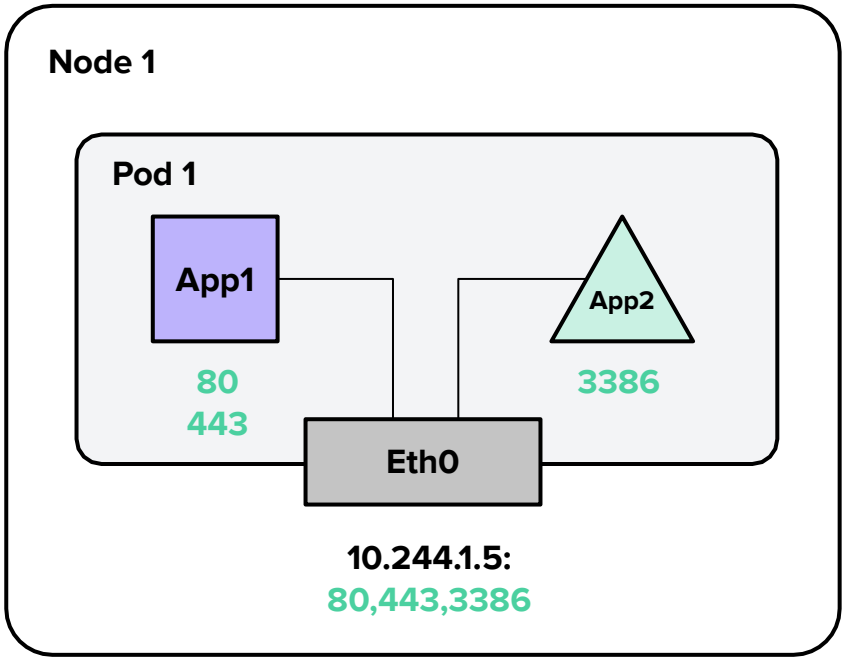


Нажмите на нужный раздел для перехода

Сетевая модель

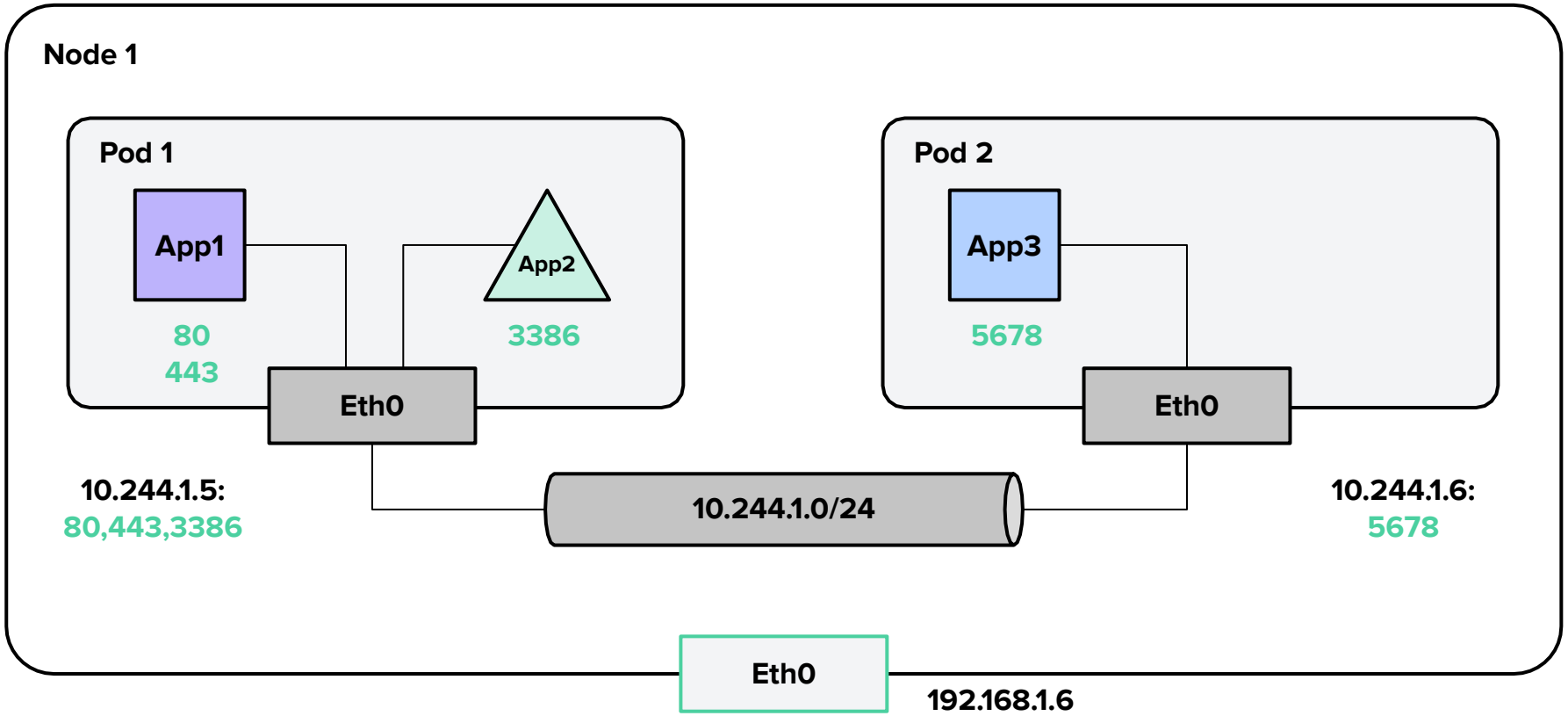
1

Сетевая модель пода (pod)

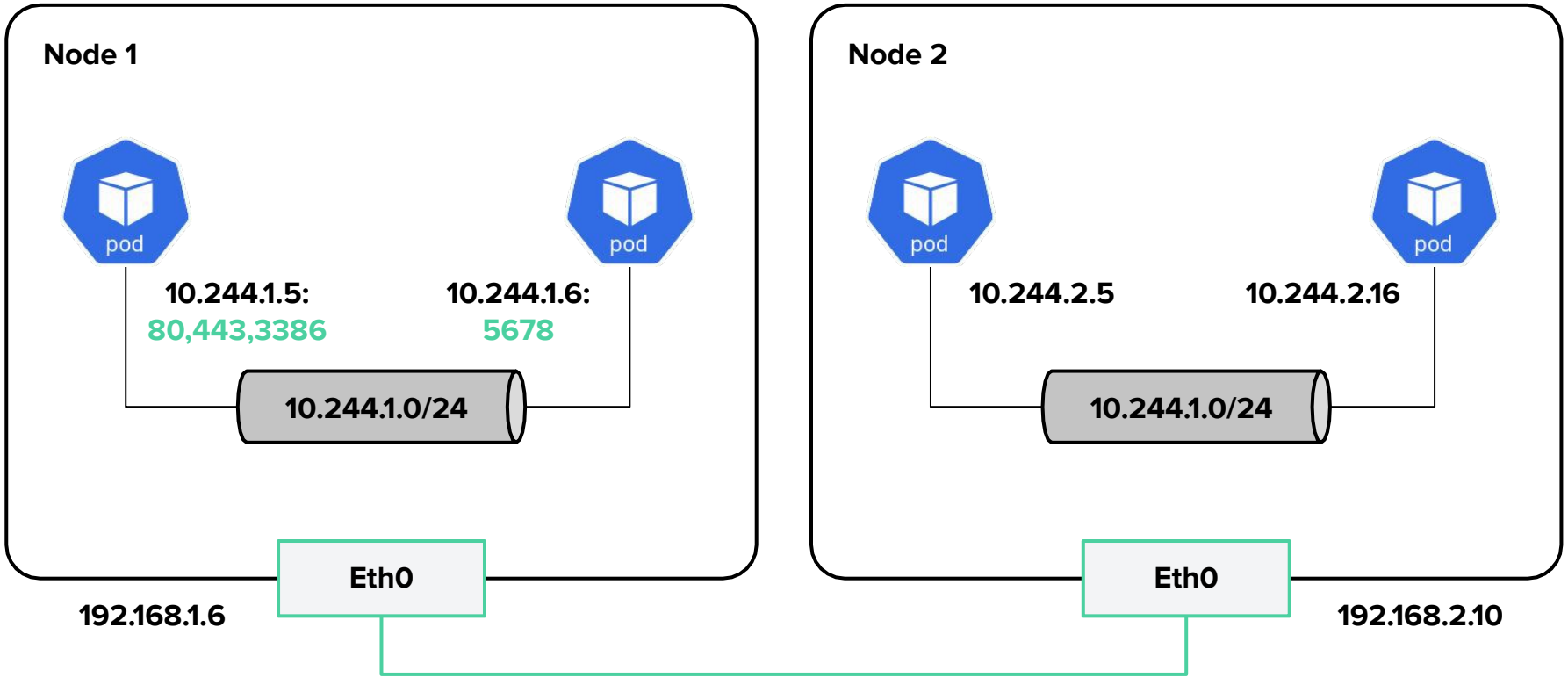


- У всех контейнеров внутри пода один и тот же IP-адрес
- Внутри все контейнеры видят друг друга как localhost
- У каждого пода есть уникальный в рамках всего кластера IP-адрес
- Сеть между подами организована без применения NAT

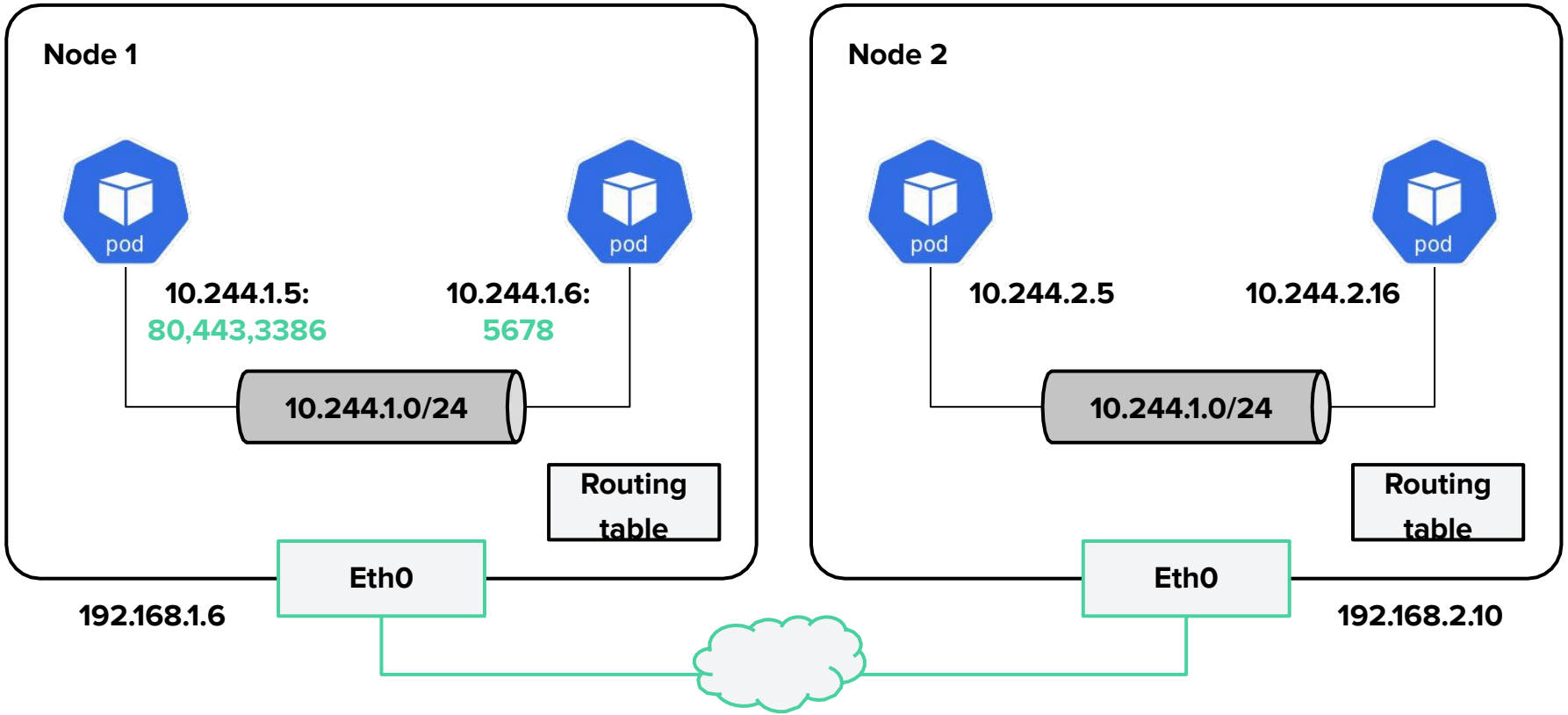
Сетевая модель подов внутри Node



Сетевая модель подов между Node



Сетевая модель подов между Node

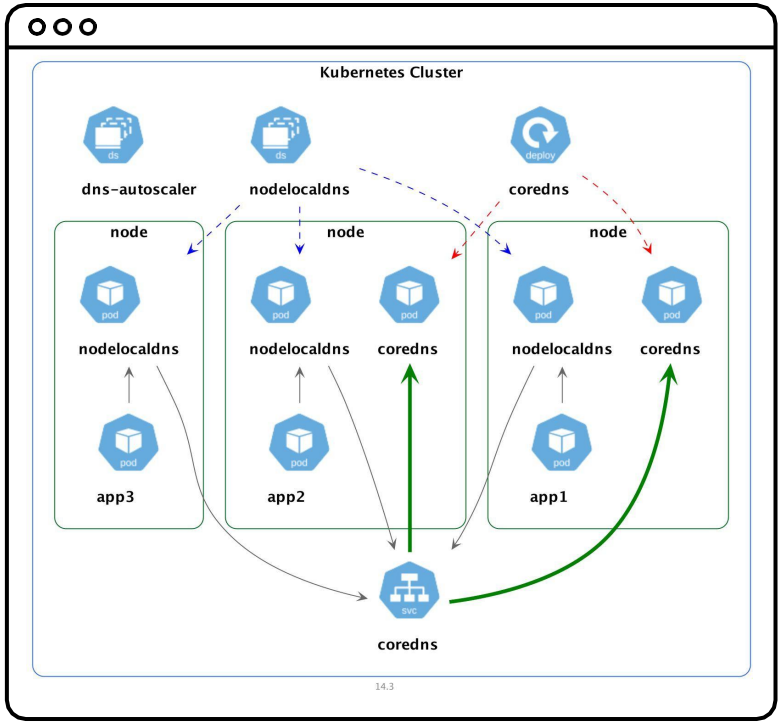


Особенности

- При инициализации кластера выбирается размер подсети для всего кластера
- Каждой ноде выделяется своя подсеть для подов. IP-адрес для пода выделяется из этой подсети
- IP-адрес ноды тоже выделяется из этой подсети. Кроме этого, у ноды есть IP-адрес на физическом интерфейсе
- **Kube-proxy** создаёт на ноде правила iptables. Схема правил хранится в etcd
- Трафик между нодами проходит с помощью CNI-плагина
- Трафик между нодами могут запретить сетевые политики (network policies), если это предусматривает CNI-плагин

Схема работы CoreDNS

CoreDNS — внутренний DNS-сервер кластера.



- CoreDNS устанавливается на нескольких нодах в формате Deployment для отказоустойчивости
- На каждой ноде установлен кеширующий DNS-сервер в формате DaemonSet
- Поды обращаются к своему кеширующему DNS-серверу, а тот, в свою очередь, обращается к CoreDNS
- Обращение к CoreDNS происходит через Service
- В Calico есть отдельный элемент dns-autoscaler, который отвечает за количество реплик CoreDNS в случае изменения нагрузки

Сетевые плагины

2

Сетевые плагины. Flannel

Особенности:

- минимальный бинарник
- хранит конфигурации в etcd
- работает на 3-м уровне OSI

Достоинства:

- поддерживает IPsec encryption
- простая установка и конфигурация

Недостатки:

- не поддерживает network policies

Источник

Сетевые плагины. Calico

Особенности:

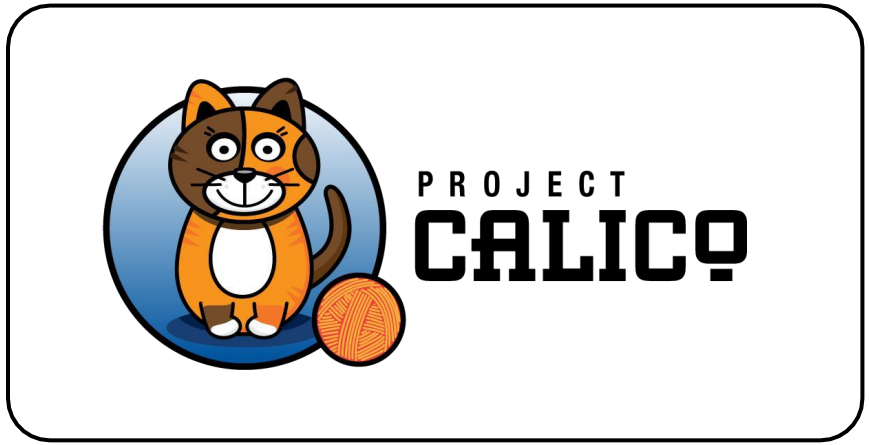
- скорость работы
- гибкая настройка политик

Достоинства:

- поддерживает network policies
- высокая производительность сети
- поддерживает SCTP

Недостатки:

- не поддерживает multicast



Источник

Прочие сетевые плагины

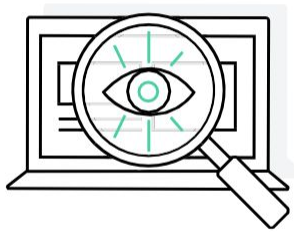
Источники: 1 2 3

Сетевые плагины. Сравнительная таблица

	Flannel	Calico	Cilium	Weave Net	Canal
Mode of deployment, способ развёртывания	DaemonSet	DaemonSet	DaemonSet	DaemonSet	DaemonSet
Encapsulation and routing, инкапсуляция и маршрутизация	VXLAN	IPinIP, BGP, eBPF	VXLAN, eBPF	VXLAN	VXLAN
Support for network policies, поддержка сетевых политик	–	+	+	+	+
Datastore used, хранилище данных	Etcd	Etcd	Etcd	–	Etcd
Encryption, шифрование	+	+	+	+	–
Ingress support, поддержка входа	–	+	+	+	+
Enterprise support, корпоративная поддержка	–	+	–	+	–

Демонстрация работы

Flannel, Calico, сетевые политики



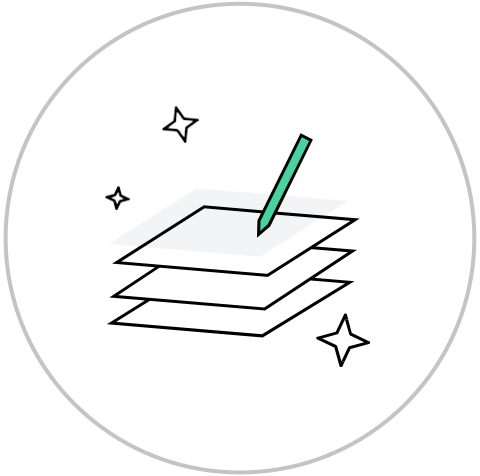
Итоги

- Узнали, как работает сеть в кластере K8s
- На примере Flannel и Calico посмотрели, как работает сеть
- Рассмотрели реализацию сетевых политик

Домашнее задание

Давайте посмотрим ваше домашнее задание.

1. Вопросы по домашней работе задавайте в чате группы
2. Задачи можно сдавать по частям
3. Зачёт по домашней работе ставится после того, как приняты все задачи



Дополнительные материалы

- Статья об устройстве сетей в K8s
- Иллюстрированное руководство по устройству сети в Kubernetes
- Статья о сети в Kubernetes
- Описание работы с Calico
- Сравнение производительности сетевых решений в Kubernetes
- Статьи со сравнением сетевых плагинов: 1 и 2

Задавайте вопросы и пишите отзыв о лекции

Кирилл Касаткин
DevOps-инженер, Renue