

Network for DevOps — Recap

Факты, которые должен знать DevOps

- 90% сетевых проблем — это DNS, routing или firewall
- DevOps редко проектирует сети с нуля, но постоянно **диагностирует**
- Kubernetes, cloud и CI/CD завязаны на сеть

ТЕОРИЯ

Модель OSI (что реально важно)

- L2 — Ethernet, MAC, ARP
- L3 — IP, routing, ICMP
- L4 — TCP / UDP, ports
- L7 — HTTP, HTTPS, DNS, gRPC

! DevOps работает в основном с L3–L7

TCP vs UDP

TCP

- Connection-oriented
- Retransmission
- Order guaranteed
- HTTP(S), SSH, DB

UDP

- No connection
- Faster, no guarantee
- DNS, VoIP, streaming

3-way handshake (TCP)

1. SYN
2. SYN-ACK
3. ACK

Зачем важно:

- SYN flood
- TIME_WAIT
- Connection leaks

IP-адресация

- IPv4 vs IPv6 (на уровне понимания)
- Private ranges:
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16

CIDR и подсети

- $/24 = 256$ адресов
- $/32 = 1$ хост
- $/0 =$ весь интернет

DevOps должен уметь:

- Читать CIDR
- Понимать overlap сетей

Routing (очень важно)

- Default gateway
- Routing table
- Longest prefix match

Команды:

- ip route
- route -n

NAT

- SNAT — из private → public
- DNAT — проброс портов

Где используется:

- Cloud
- Kubernetes
- On-prem

DNS

Что делает DNS:

- Name → IP

Типы записей:

- A / AAAA
- CNAME
- MX
- TXT

DNS — частая причина проблем

- Неверный DNS server
- Кеш
- split-horizon DNS

Команды:

- dig
- nslookup
- resolvectl

Ports и services

- Port ≠ service
- 0–1023 — well-known
- 1024–65535 — ephemeral

Проверка:

- ss -lntup
- netstat

Firewalls

- Stateless vs Stateful
- Ingress / Egress

Инструменты:

- iptables / nftables
- firewalld
- cloud security groups

Load Balancing

- L4 — TCP/UDP
- L7 — HTTP

Алгоритмы:

- Round-robin
- Least connections

HTTP на сетевом уровне

- Request / Response
- Status codes
- Headers

Важно для:

- Debug API
- Ingress
- Reverse proxy

TLS / HTTPS (базово)

- Handshake
- Certificate chain
- SNI

DevOps должен уметь:

- Проверить сертификат
- Понять, почему TLS не работает

Kubernetes и сеть (overview)

- Pod IP
- Service IP
- ClusterIP / NodePort / LoadBalancer
- CNI

Где DevOps чаще всего ломает сеть

- Security Groups
- Firewall rules
- DNS
- Wrong CIDR
- NAT

ПРАКТИКА

Практика 1: Диагностика connectivity

Задача:

- Проверить доступность хоста

Команды:

- ping
- traceroute
- curl

Практика 2: DNS

- Проверить A запись
- Проверить какой DNS используется
- Проверить кеш

Команды:

- dig
- resolvectl status

Практика 3: Ports

- Запустить сервис на порту
- Проверить доступность

Команды:

- ss -lntup
- nc

Практика 4: Firewall

- Заблокировать порт
- Проверить, что сервис недоступен
- Разблокировать

Практика 5 (по желанию): Kubernetes

- Проверить доступ к Pod
- Проверить Service
- Проверить Ingress

