CH38
怎麼使用 tcpdump 與 Wireshark 分析網路流量

Agenda

- CH38 overview
- tcpdump
- Wireshark
- How to analyze network traffic?
- Lab
- Reference

CH38 overview

- Network analysis tool like tcpdump & Wireshark are common chose to troubleshoot network issue.
- tcpdump only supports command line. On the other hand, Wireshark GUI can handle complex network environment.

- PTR (pointer record) provides the IP address associated with a domain name.
- PTR common uses for reverse DNS include:
  - Anti-spam
  - Troubleshooting email delivery issues
  - Logging
- Email service:

  Gsuite, AWS SES, SendGrid, MailGun

tcpdump

- A powerful command-line packet analyzer
- tcpdump group github
- tcpdump relate project
- How about other command-line?
- Wireshark CLI tools & scripting youtube

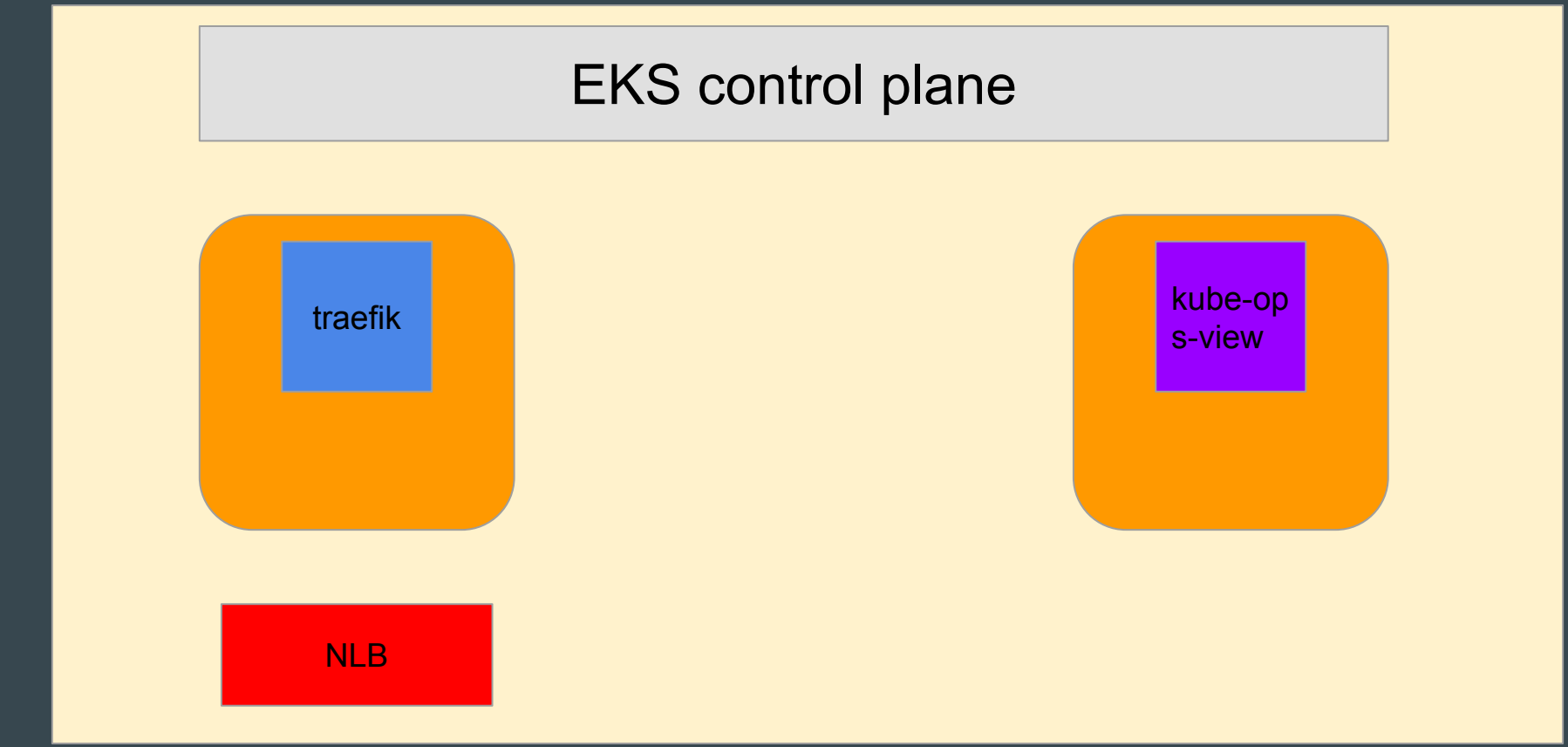
Wireshark

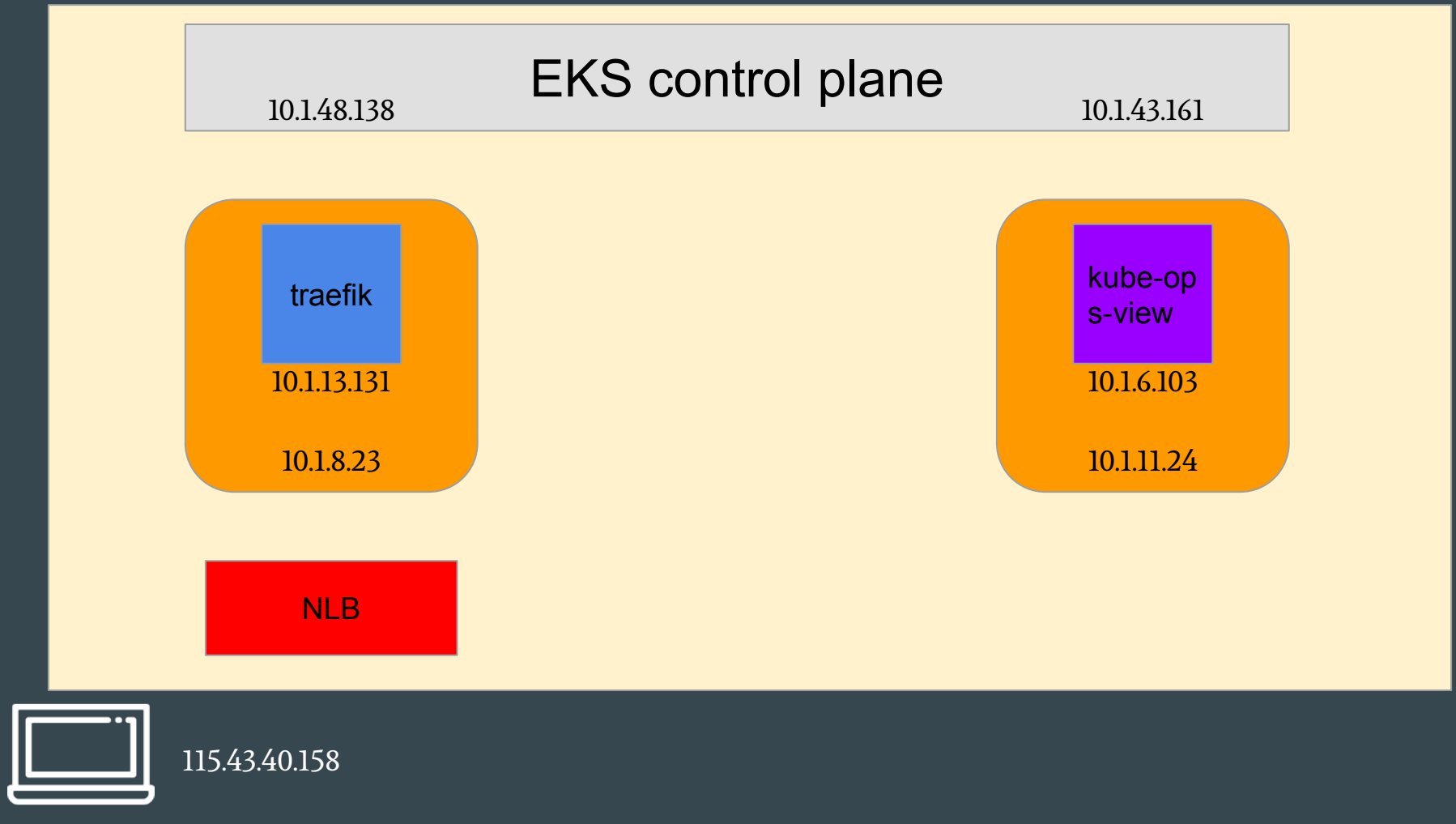
- A powerful GUI network protocol analyzer
- Over 251000 fields in 3000 protocols can filters
- Open source with rich community support
- SharkFest'20 at 10/12 ~ 10/16
- Many of tutorial resources

How to analyze network traffic?

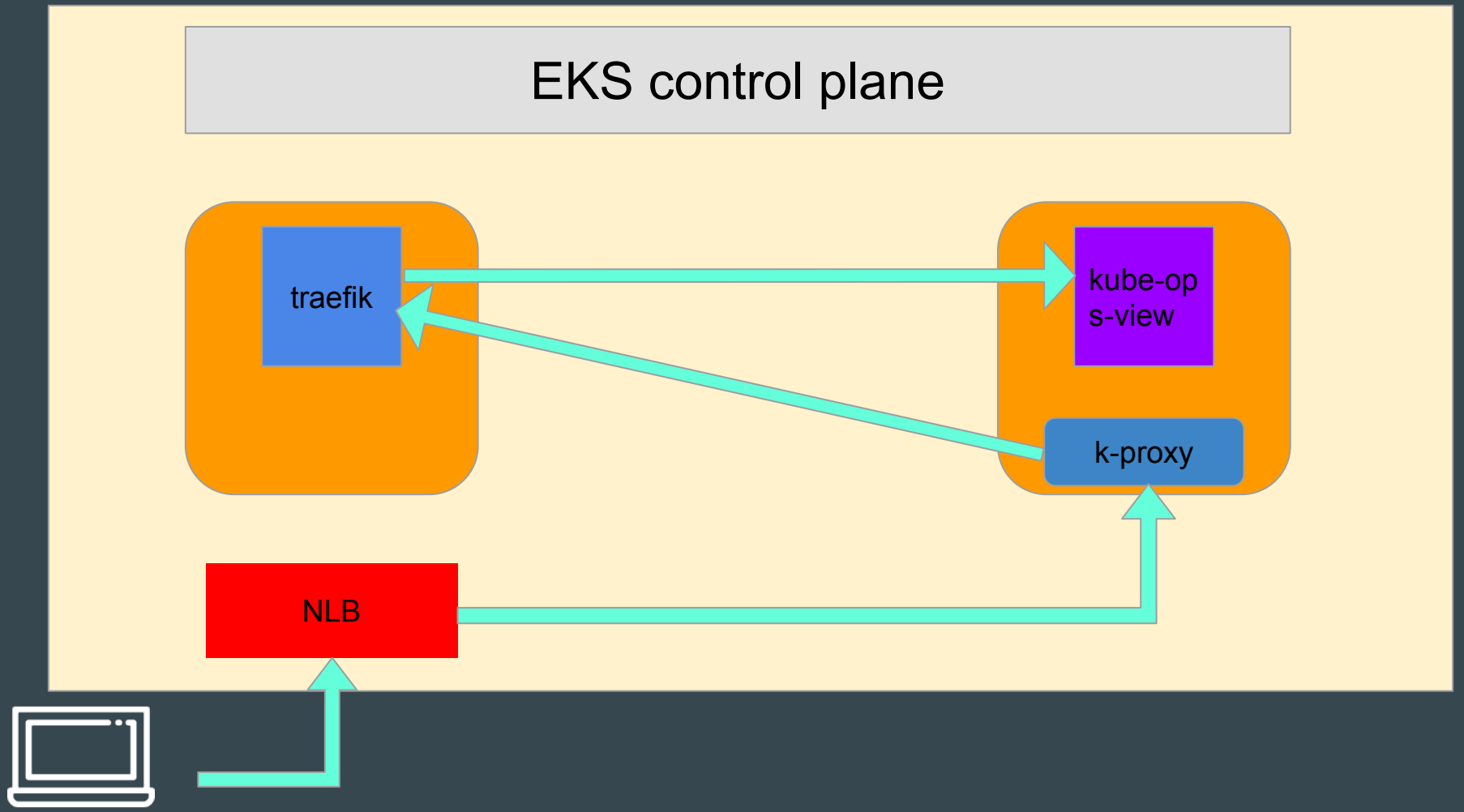
- Start with client-side
- Capture server and client traffic
- Focus on time
- The different environment with different filter
- Keep your eye on the ball
- (resource)

Lab

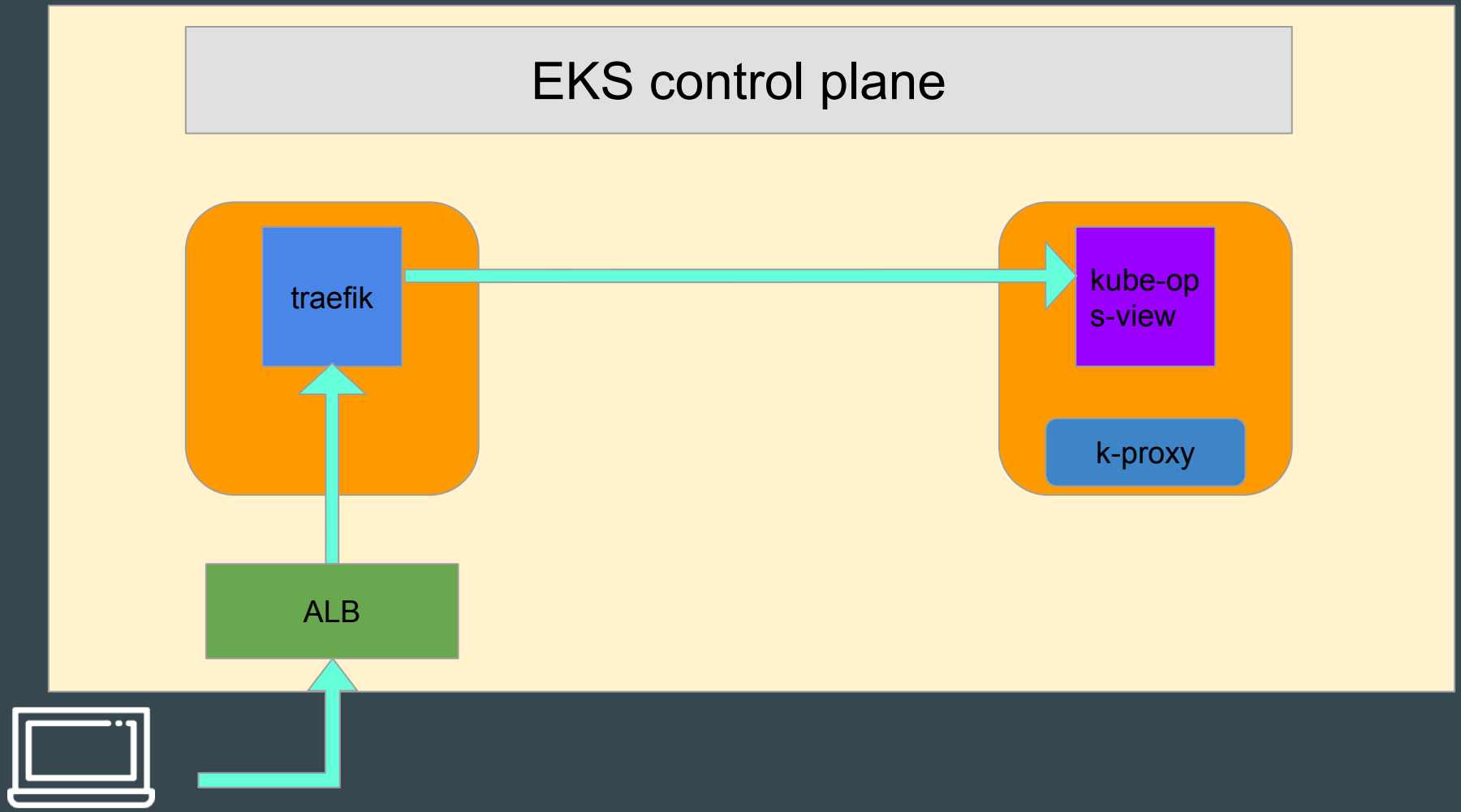

EKS control plane
traefik
kube-op
s-view
NLB


EKS control plane
10.1.48.138
10.1.43.161
traefik
10.1.13.131
10.1.8.23
kube-op
s-view
10.1.6.103
10.1.11.24
NLB
115.43.40.158

- what is 169.254.169.254
- Dynamic Configuration of IPv4 Link-Local Addresses
- EKS architectural overview
- Elastic network interfaces


EKS control plane
traefik
kube-op
s-view
k-proxy
NLB

- Application Load Balancer target type


EKS control plane
traefik
kube-op
s-view
k-proxy
ALB

Reference

- What is a DNS PTR record?
- 鳥哥 DNS 正反解
- tcpdump relate project
- Wireshark CLI tools & scripting
- tcpdump group github
- Top 10 Wireshark Filters
- Wireshark Display Filter Reference
- Wireshark distribution command line

- what is 169.254.169.254
- Dynamic Configuration of IPv4 Link-Local Addresses
- EKS architectural overview
- Elastic network interfaces
- Network Load Balancer Support in Kubernetes 1.9
- Application Load Balancer target type