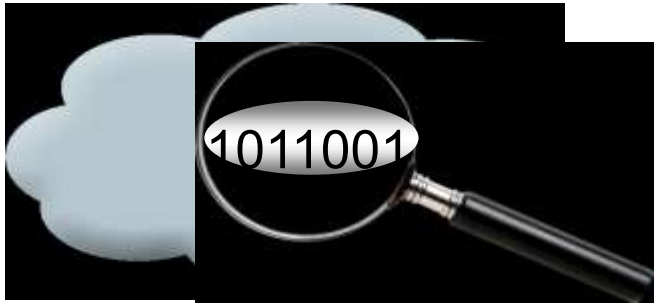
G ˝Ḥ DDoS

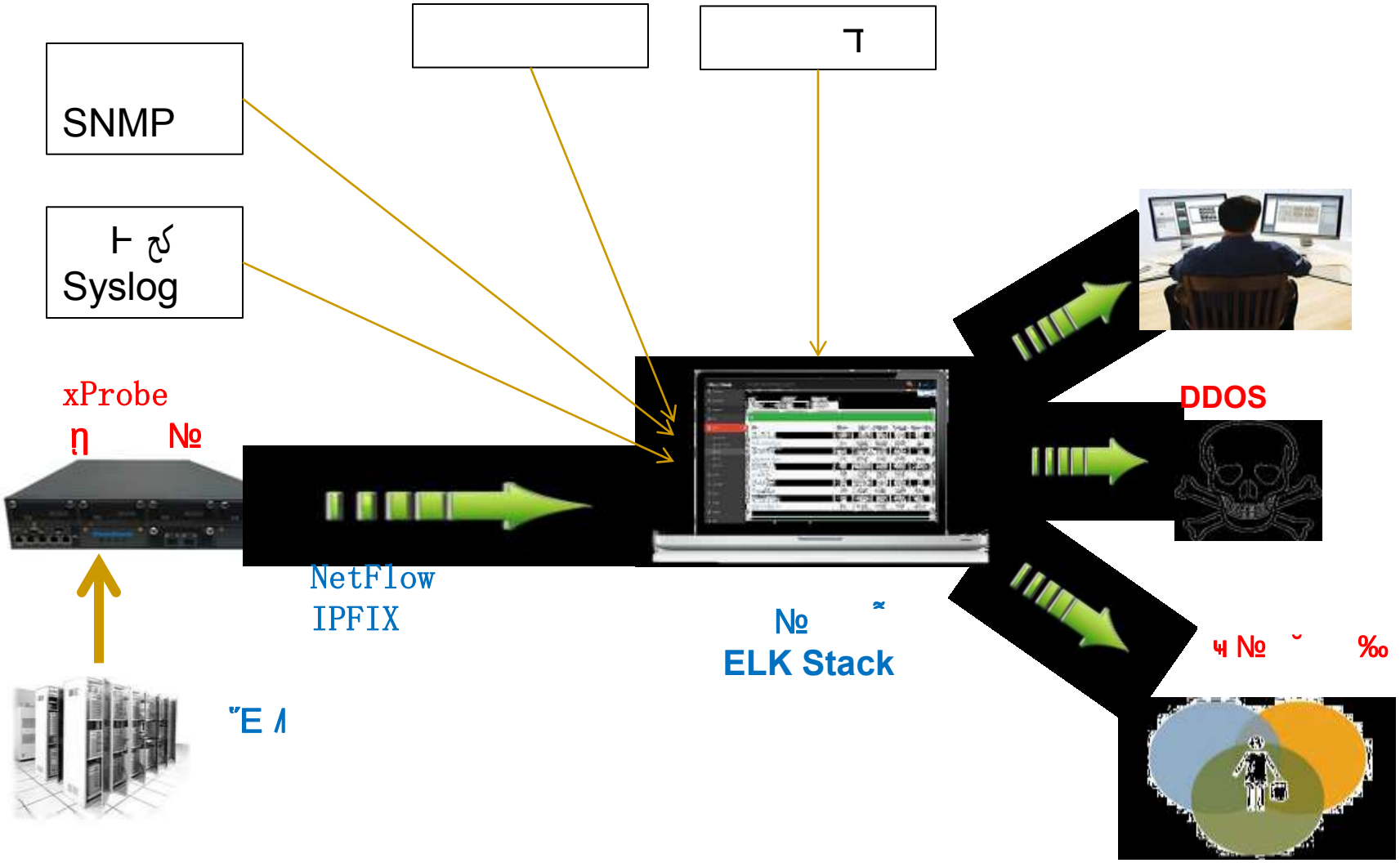
№ ˜ Ḭ DDoS

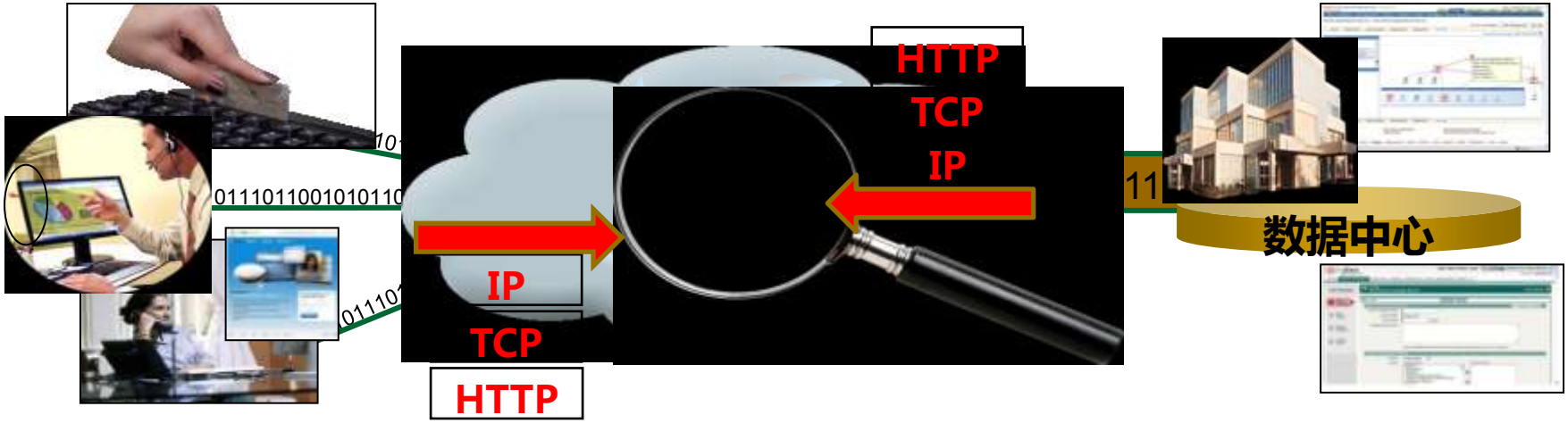
ชัน ห (CEO)

ห˛ Ɛ ≠ ˋE˜

info@clearclouds-global.com




SNMP
Syslog
xProbe
NetFlow
IPFIX
ELK Stack
DDOS



大数据采集平台：DPI

1－ e ش

2－ e ش

❑

❑

❑

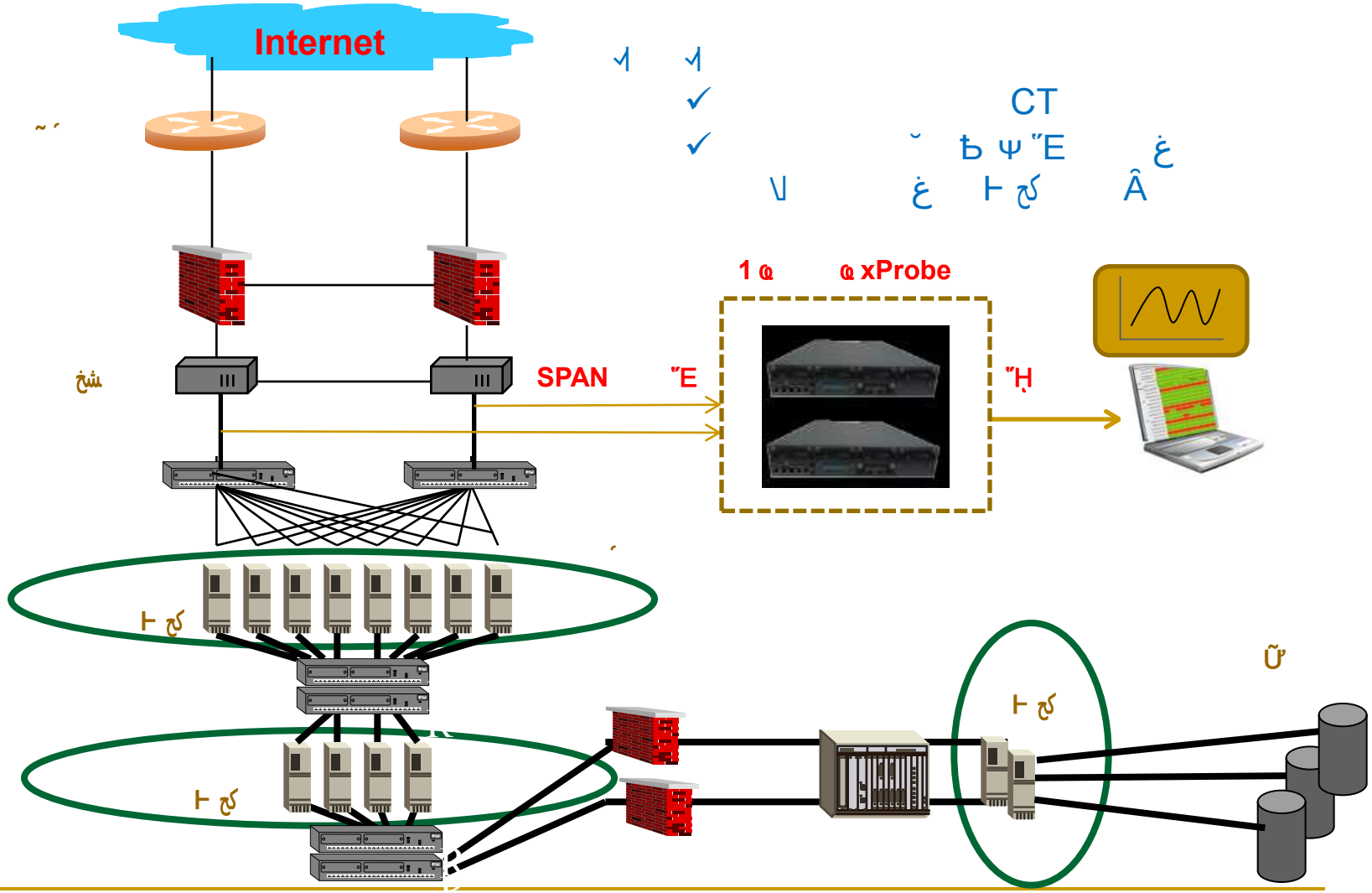
❑

‘E˜ ªª ج’ ৭

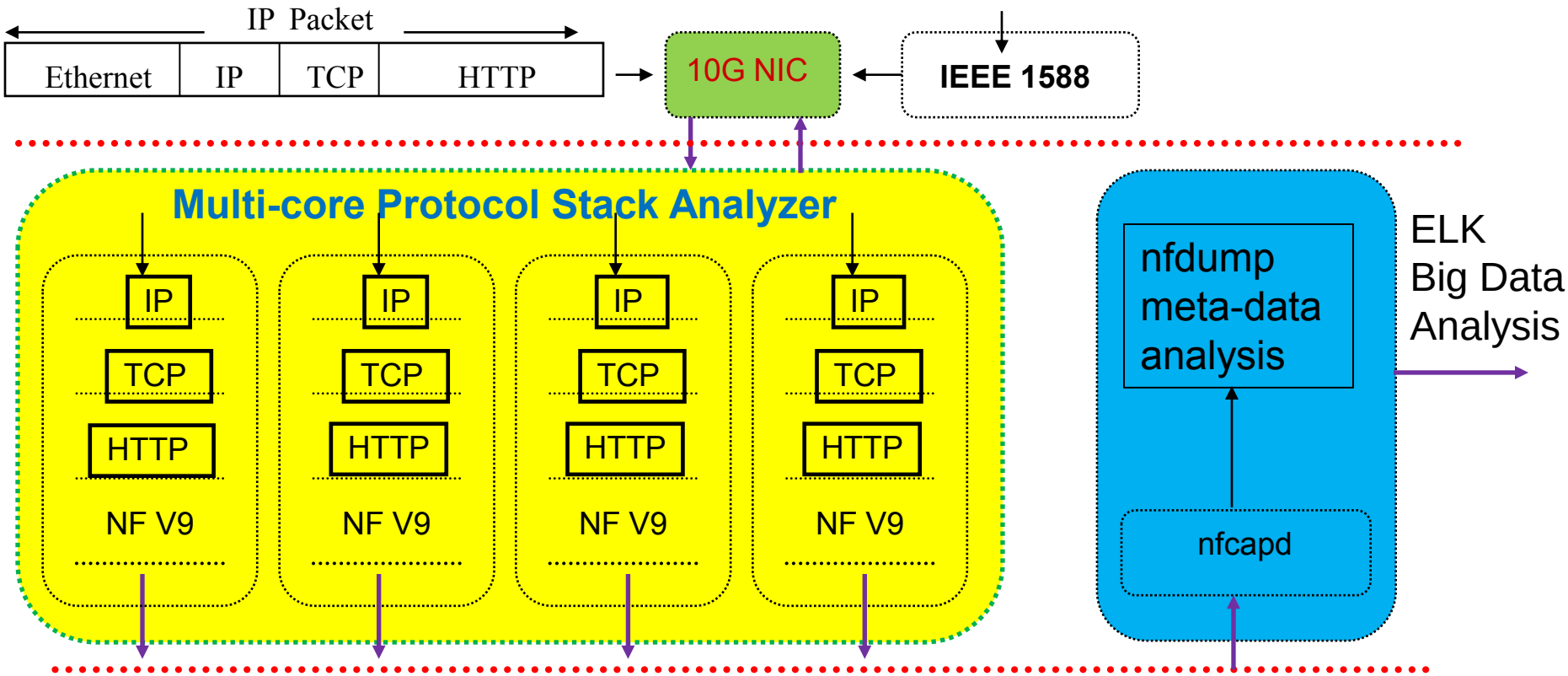
- ;‘,‘ ৸˜ ⊢ ج ã̃
- L

ˋẼ ᪤ ج' ŋ

ĩ ȕ ҉ à 𝒟ρ à ẽ ҹ


Internet
SPAN
xProbe

Parallelizing Network Applications



- Load balance based on Intel NICs
- Lock-free FIFO for core-2-core communication
- Source-2-source transformation for generating parallel C

Metadata: about protocol transactions

- TCP
  - (IP_src, IP_dst, Port_src, Port_dst, Protocol)
  - (SYN, RST, FIN, TIME_OUT)
  - (Server_Latency, Client_Latency)
  - (Gbps, PPS, Ave_Len)
- HTTP
  - (URL, Status_Code, Method, Page_View)
  - (Server_Latency, Client_Latency)
  - (Host, Refer, User-Agent, XFF Cookie)
  - More….

№ ' Netflow vs. Packets

- Flow № ˘ ϰ Ḥ
  ɲ ̋Ḥ =!=

- ´ Ũ ̃ ϩ ε
  10G/100G Mission: impossible

- ɯ ϧ ̃ ̋Ḥ ϖ̄ ϖ
  - ضي №
  -

Metadata: Basic Operations

- [illegible]
  - [illegible] URL (all URLs)
- [illegible]
  - [illegible] URL [illegible] (click rate)
- [illegible]
  - [illegible] URL (topN URLs)
- [illegible]
  - URL [illegible] (latency)

Challenge: Faster and Faster!

- Gathering meta-data faster
- Making aggregation faster
- Pumping metadata into ES faster
- Analyzing data faster
- IP CIDR address aggregation faster

谢谢！