DNS Architecture Evolution and Security O&M Practice

第二届中国域名发展大会

刘紫千
中国电信集团

第二届中国域名发展大会
北京，2017-01-10

CT IP Network Size

- From customer perspective (by Oct 2016)
  - Mobile User (4G) : 2.14 (1.13) hundreds of millions
  - Broadband User(FTTH): 1.29 (0.98) hundreds of millions

- From network capacity perspective (by Nov 2016)
  - Domestic 85Tbps
  - International gateway XXXX Gbps
  - Inter-connection with other Carriers
    - Domestic 2.7Tbps
    - Foreign 6.2Tbps

第二届中国域名发展大会

云堤 SECURITY

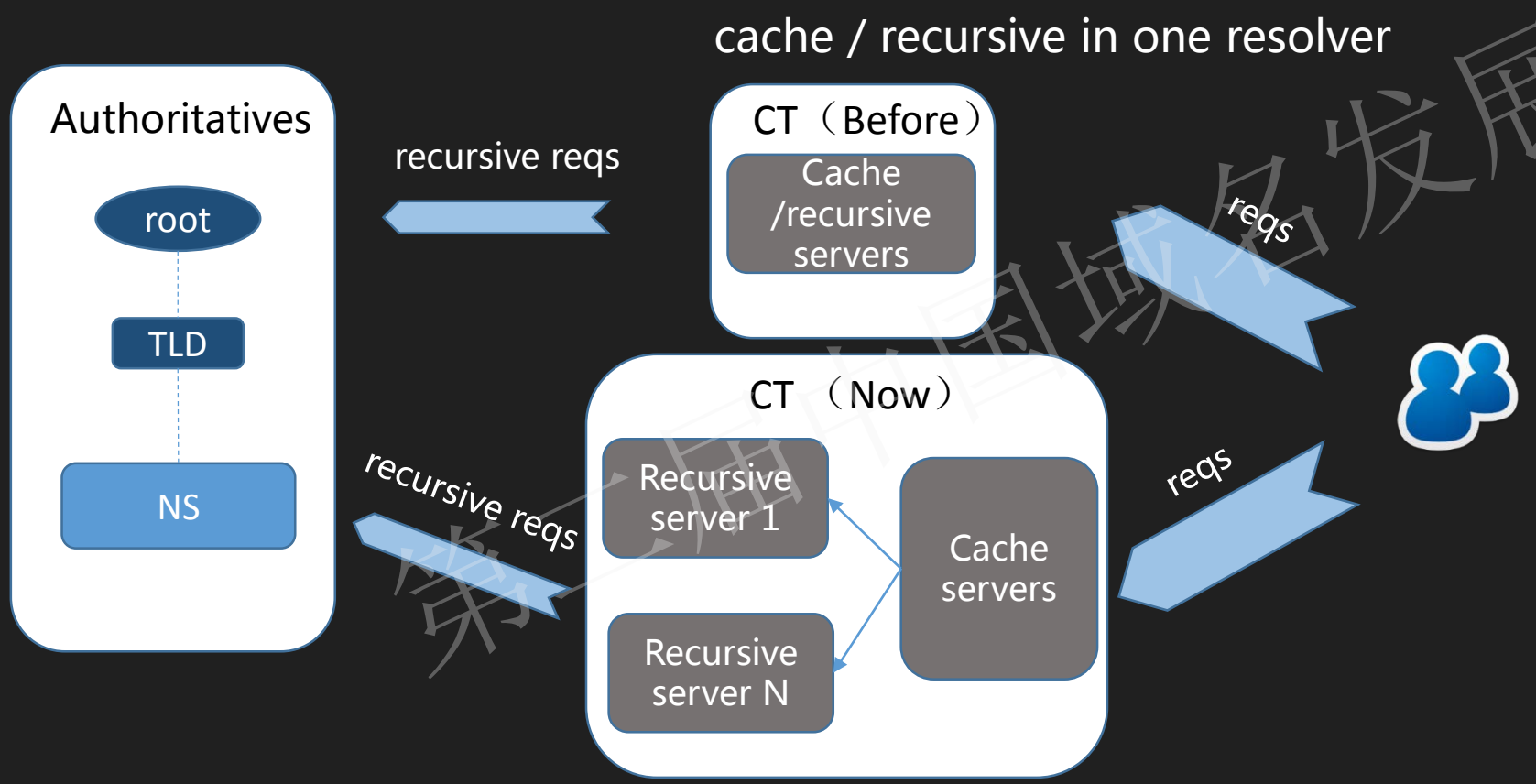
CT DNS Scale

- Nodes
  - Province-based : X+ main clusters, X+ service IP addrs.
  - Total: XX+ clusters XXX+ service IP addrs.
  - Evolving …
- Traffic
  - Peak rate: 1.3 millions QPS
  - Peak traffic: request 7.2 Gbps，response 13.4 Gbps

第二届中国域名安展大会

云堤 SECURITY

DNS Architecture Evolution - Inner



Lesson

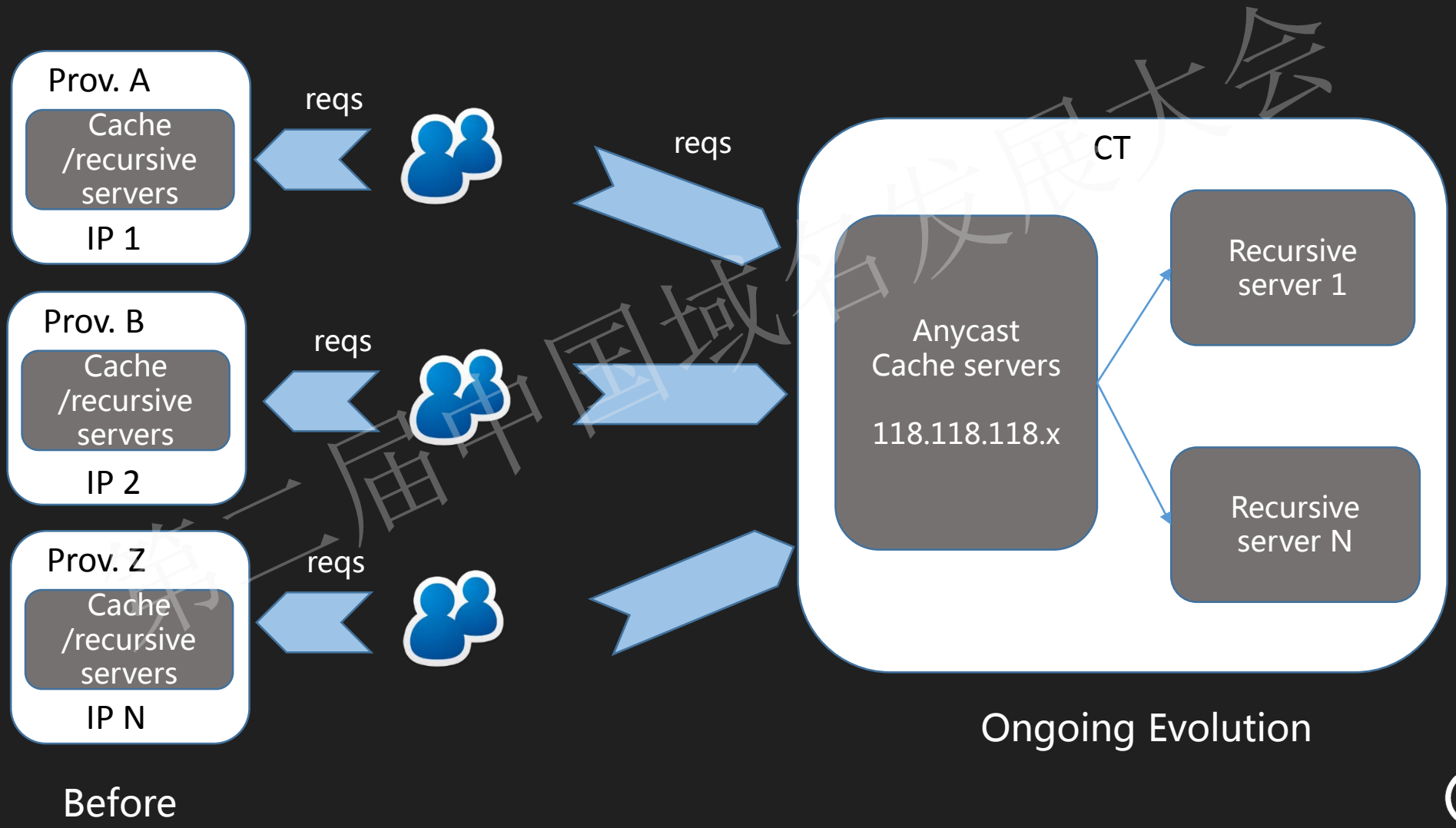
- 519 accident in 2009

Different roles

- High capacity in cache
- CDN-friendly recursives
- No 4-layer LB but OSPF anycast in between

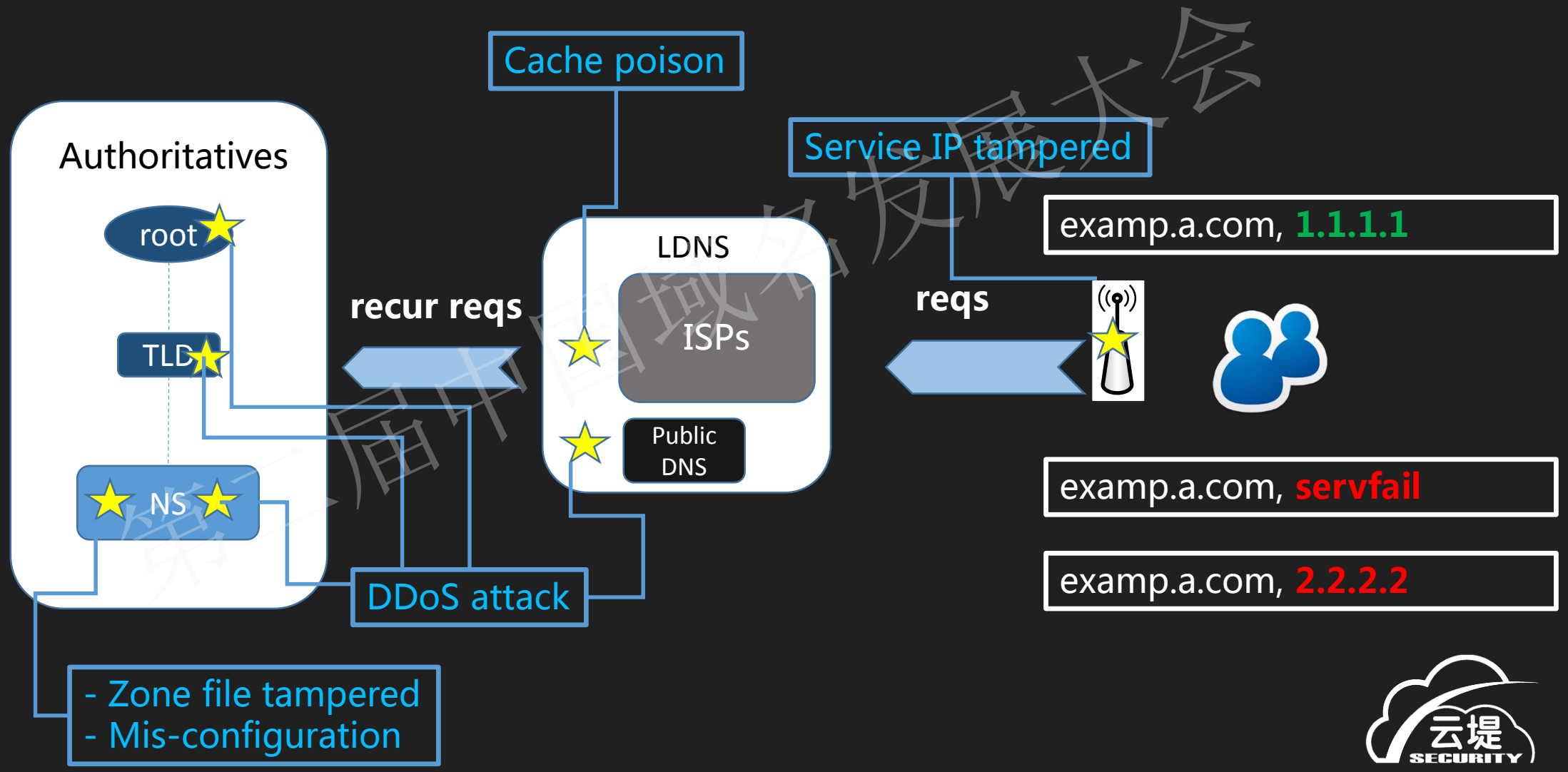
第十届中国域名发展大会

DNS Architecture Evolution - Outter



第一届中国域名发展大会

Threats to the whole DNS ...



Counter Measures

- End user
  - Anti-CSRF，no default login account to the home routers
  - Abandon the DNS-abusing software design
- Upstream network
  - Rate limit at network layer
  - Upstream network ddos mitigation
  - Fully redundant bandwidth
- Cache/Recursive
  - Architecture rebuilt
  - Fully redundant computing resourses
  - Full coverage & heterogeneous surveillance – OSS
  - Cahce flush – through APIs
  - Cahce RR Snap-shot reload -- OSS
  - Recognize the recursive attack and other malicious/abnormal pkt format -- OSS
- Authoritatives
  - BGP anycast
  - Secure the admin account
  - Dedicated tunnel with high-valued recursive IP addrs. → Diff Serv

第二届中国域名发展大会

云堤 SECURITY

中国电信
CHINA TELECOM

Thank You

第二届中国域名发展大会

云堤
SECURITY