CERNET2 Updates

Zhonghui Li
CERNET / Tsinghua University
29 Mar 2018

Outline

- CERNET2 100G Upgrade
- IPv6 Memcache DDoS Attack to CNGI-6IX

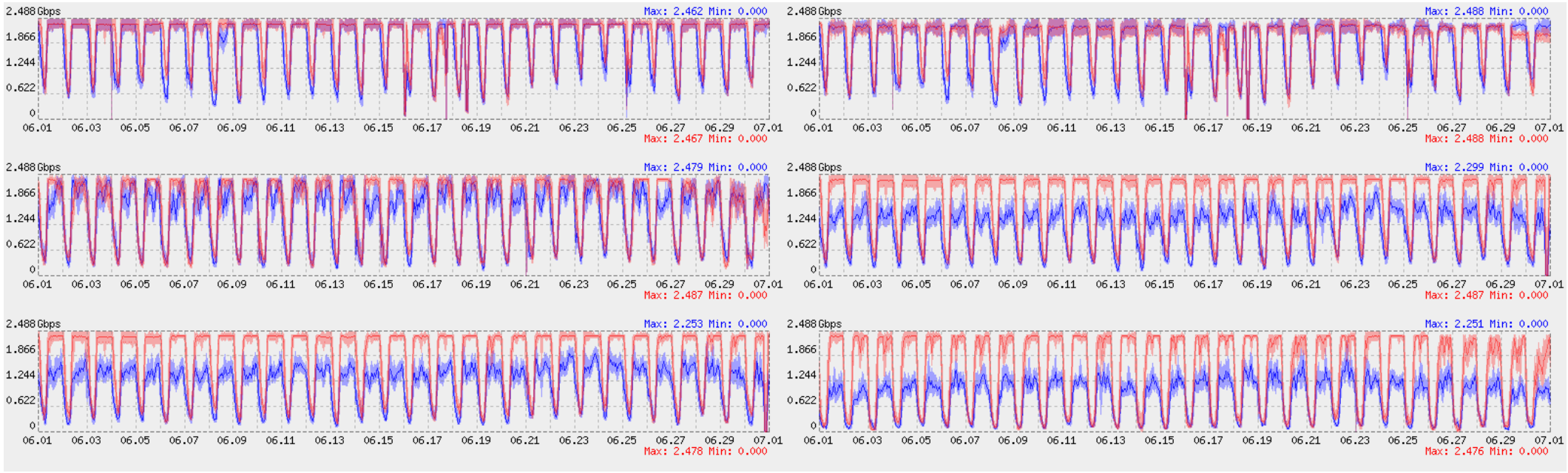
Outline

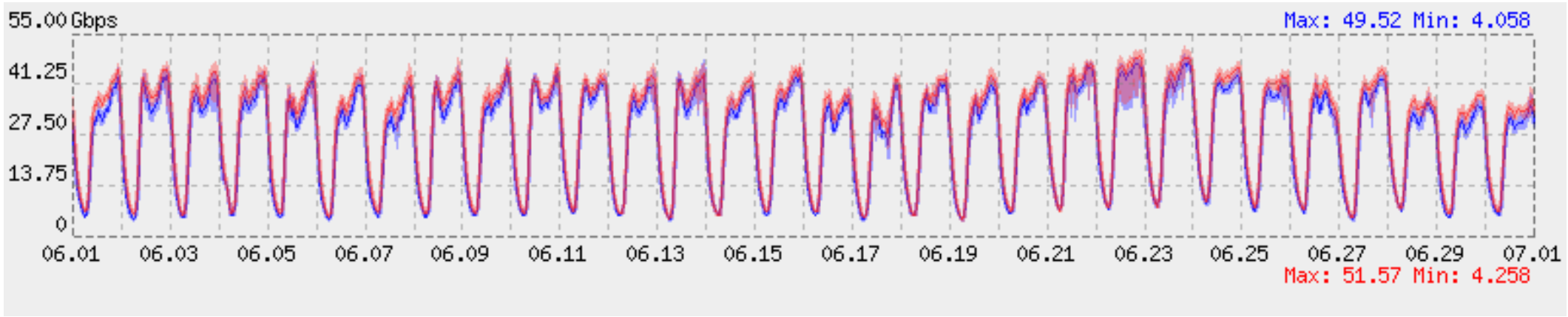
- **CERNET2 100G Upgrade**
- IPv6 Memcache DDoS Attack to CNGI-6IX

CERNET2 Overview

- Native IPv6 national backbone
  - Since 2004
  - 25 PoPs in 20 cities
  - 10G/2.5G backbone link
  - ~600 University, R&E institute
  - 5M users

CERNET2 Backbone Traffic



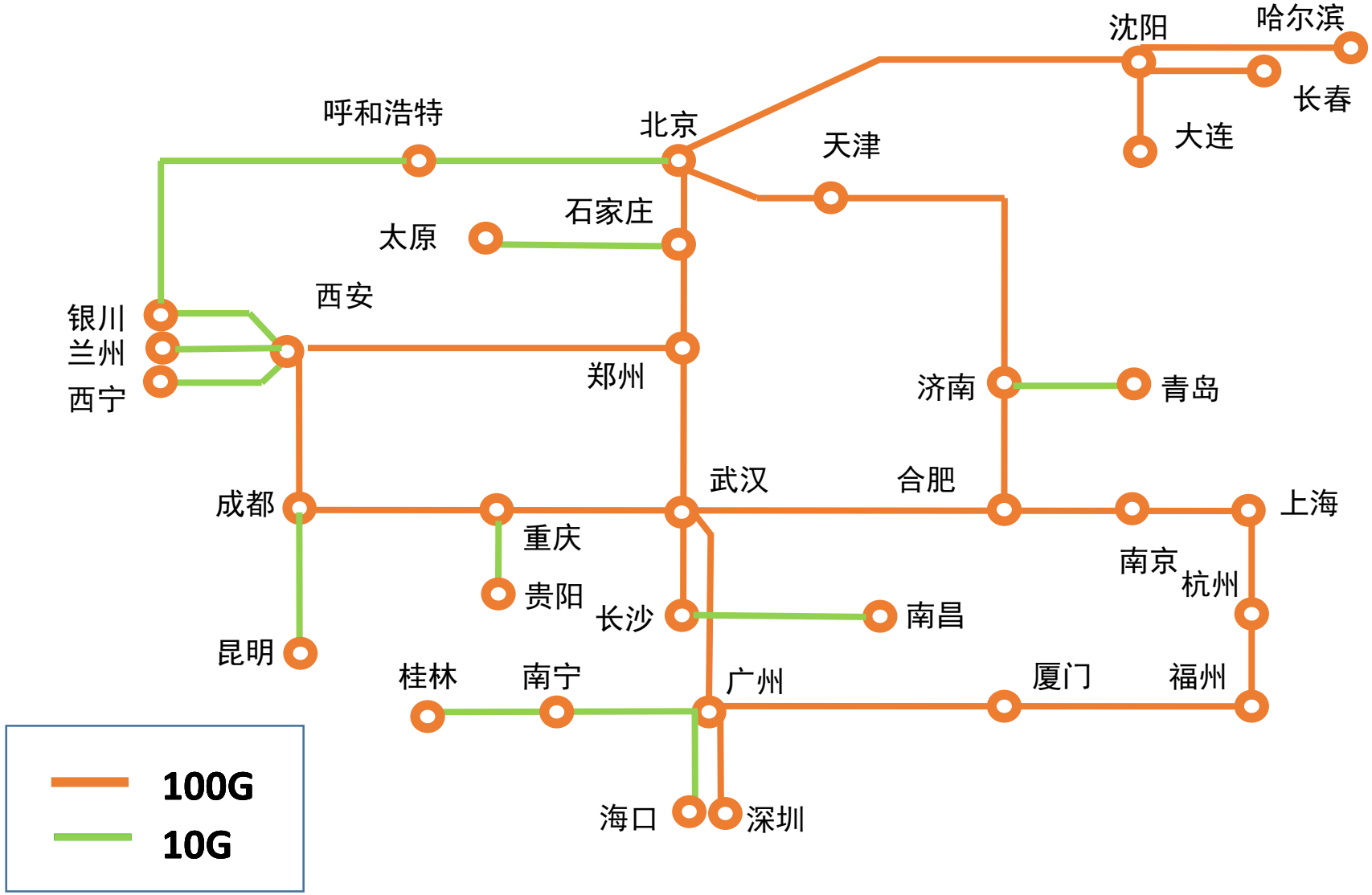


100G Upgrade Plan of CERNET2 Backbone

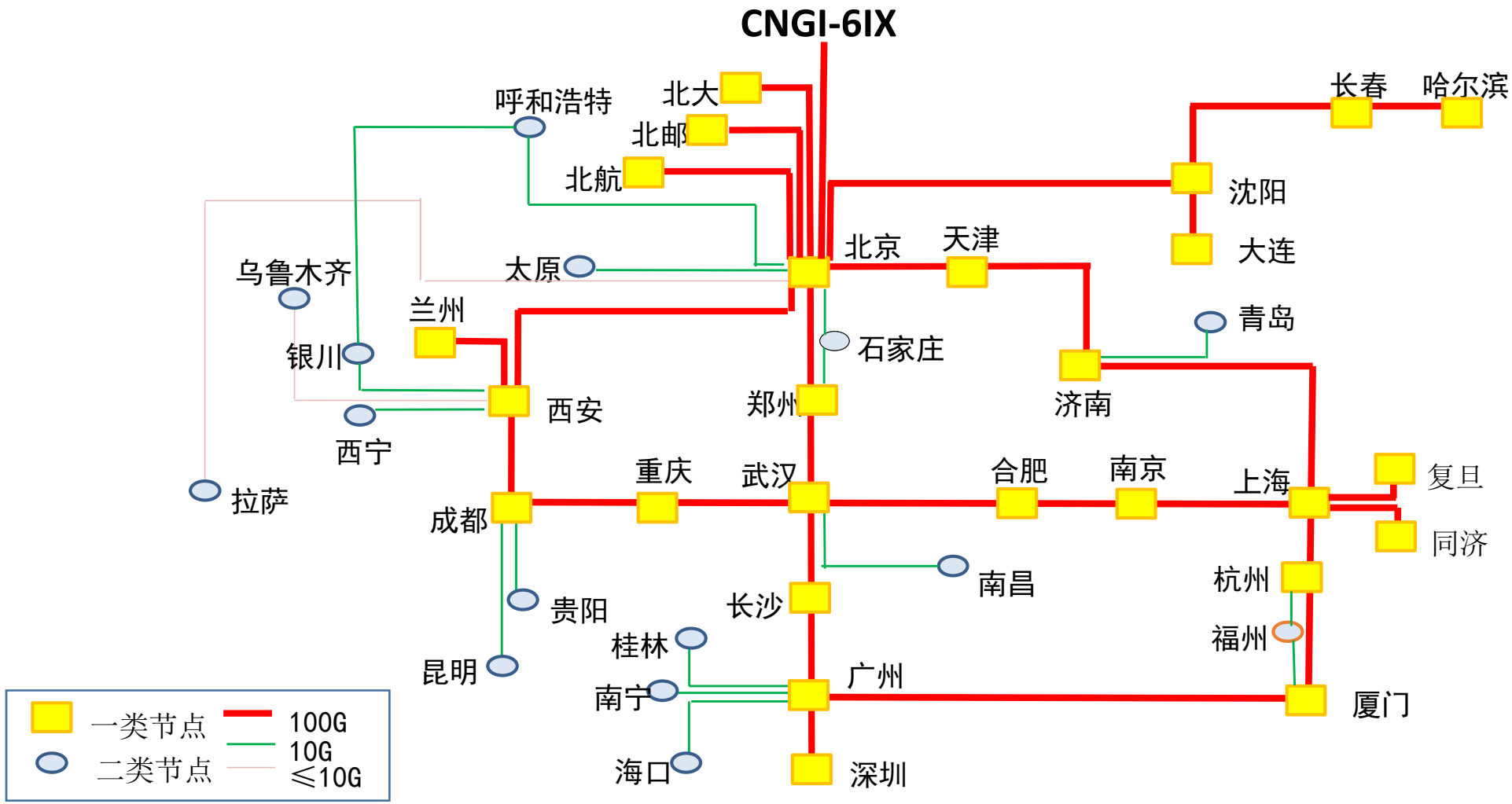
- Objective

	Before upgrade	After upgrade
Protocol	Pure IPv6	Pure IPv6
PoP	25	41
Province/city	20	31
Backbone link	10G/2.5G	100G/10G
Total bandwidth	127.5G	2950G
IPv6 user	5M	≥ 10M
Role	Experimental	Productive

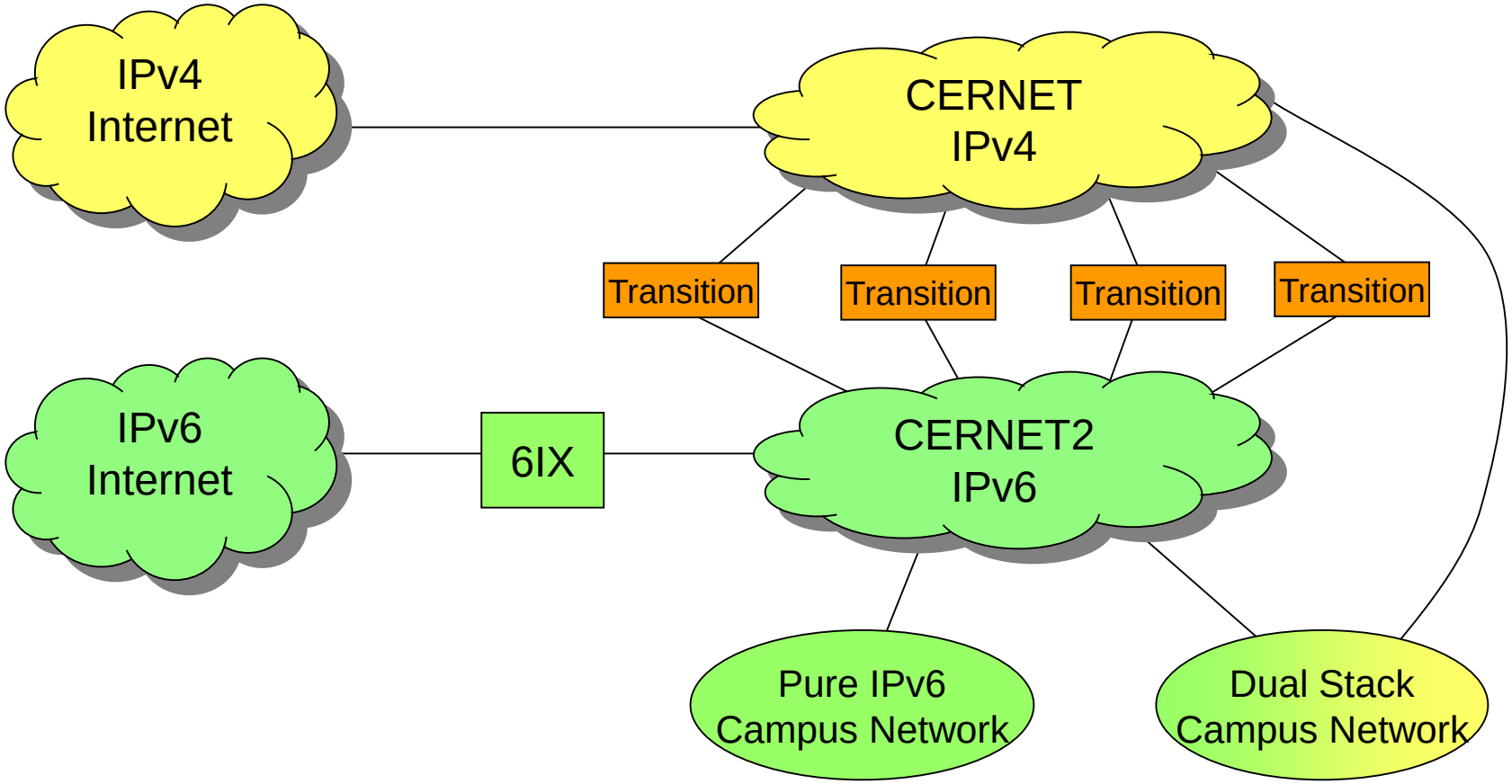
DWDM Optical Transmission Network



New Backbone Topology

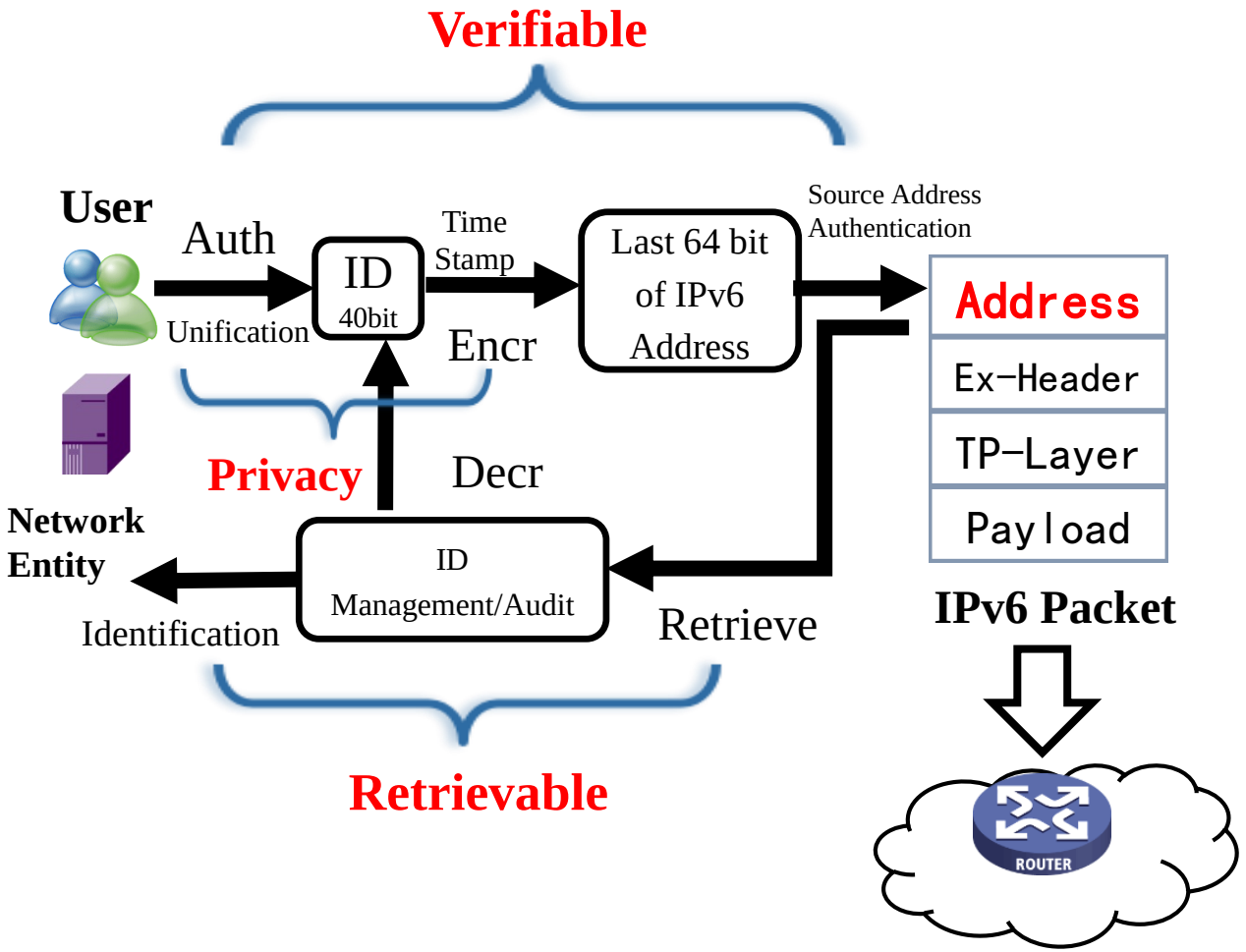


IVI Deployment (IPv6 Transition)



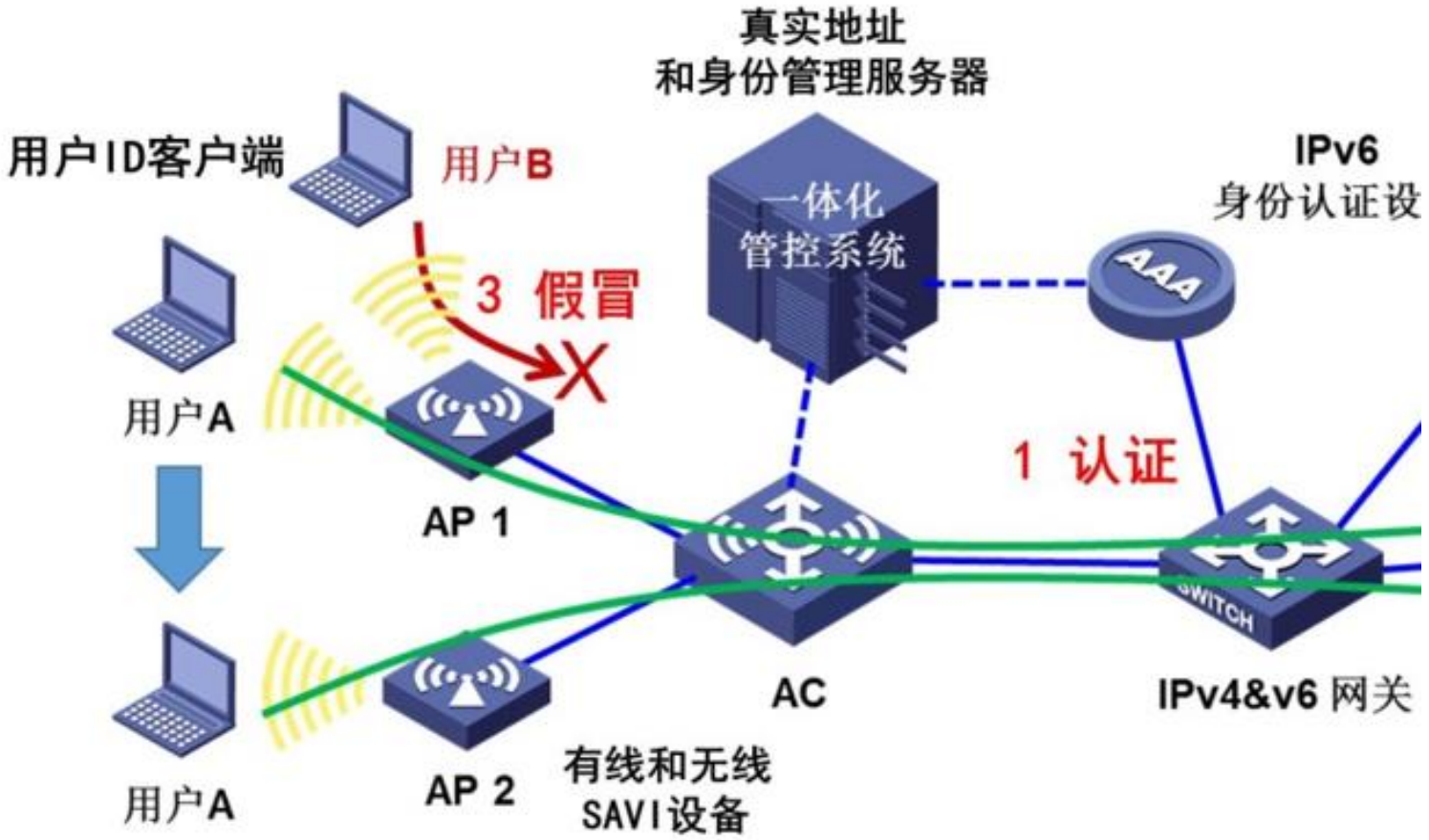
SAVI Deployment (IPv6 Cyber Security)

- Source Address Validation Improvement



SAVI Deployment (IPv6 Cyber Security)

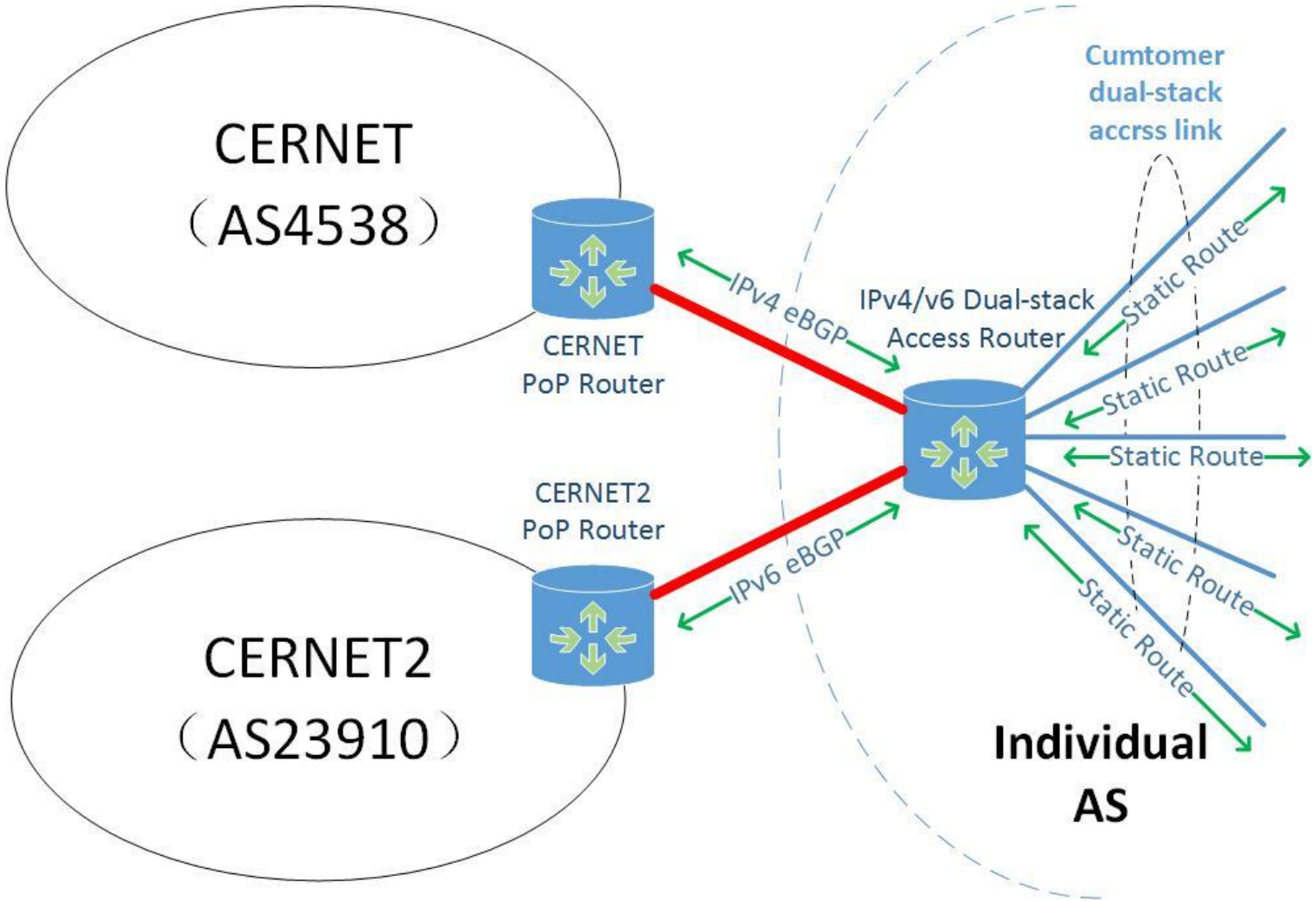
- Deployment in CERNET2 campus network



Technical consideration on customer network's connection to CERNET and CERNET2

- Consideration
  - Separated IPv4 & IPv6 backbone
    - CERNET (AS4538): Pure IPv4 (after the 100G upgrade of CERNET2)
    - CERNET2 (AS23910): Pure IPv6
  - Most of customer networks prefer single connection to CERNET & CERNET2 PoP (same location)
  - Difference in routing design between CERNET and CERNET2
    - CERNET: PoP router and access router in same domain (AS4538)
    - CERNET2: PoP router and access router in different domain
      - All PoP routers belong to AS23910
      - Access router in each node has its own AS number (AS24348- AS24372)
        - Experimental role of CERNET2

Option 1 (Dual-stack Access Router)



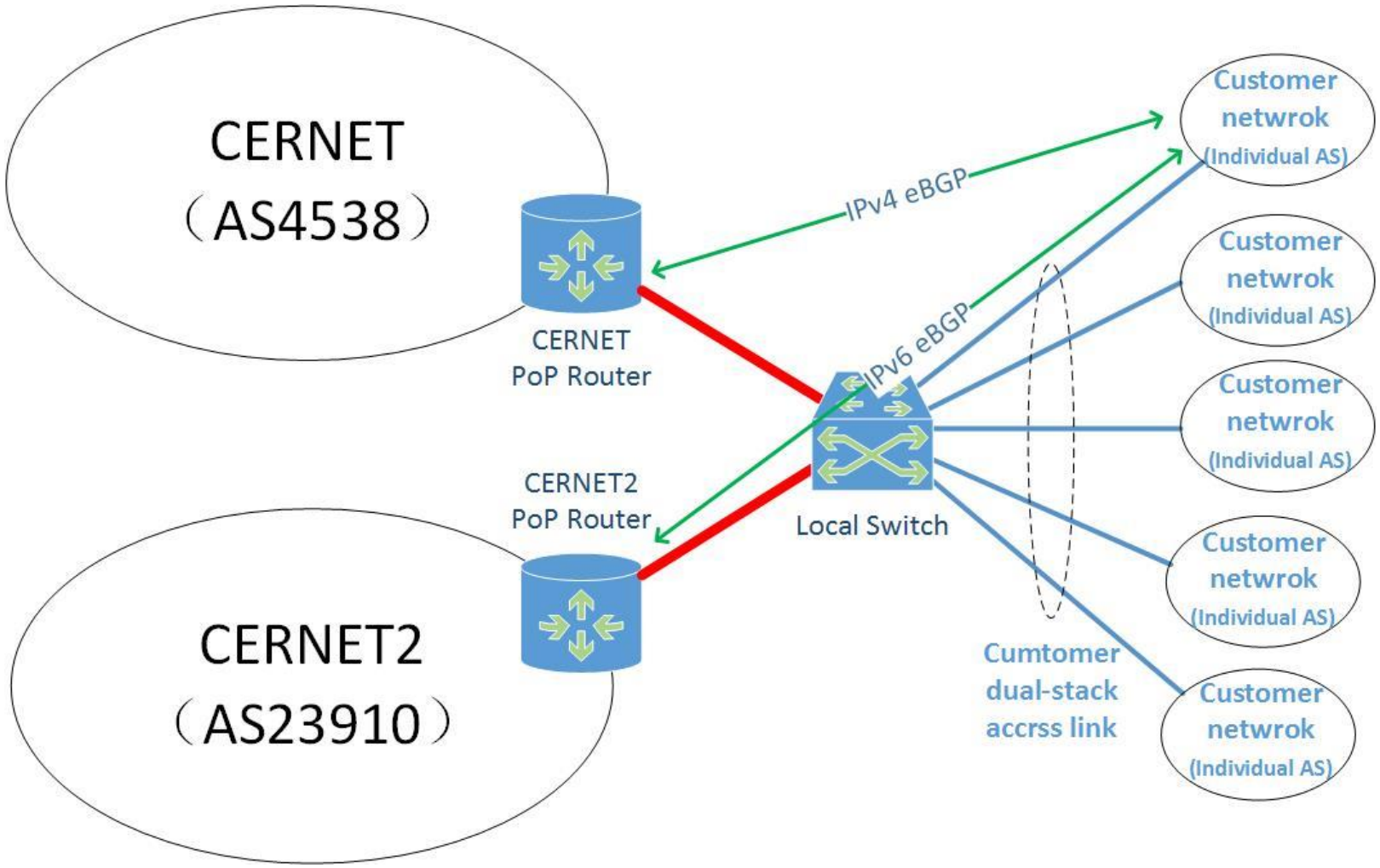
Pro:

- Easy to implement (only IPv4/v6 static route is needed), and IPv4 & IPv6 access is transparent to customer networks
- Hierarchical & Robust (L3 access via access router)
- Easy for monitoring and management (via L3 access router)

Con:

- Higher CAP-EX (access router)
- Routing complexity (individual AS for each node)
- Less flexible (routing, multi-homing)

Option 2 (Local Exchange Point)



Pro:

- Lower CAP-EX (local switch)
- Simplicity (L2 connection)
- More flexible (routing, multi-homing, private peering)

Con:

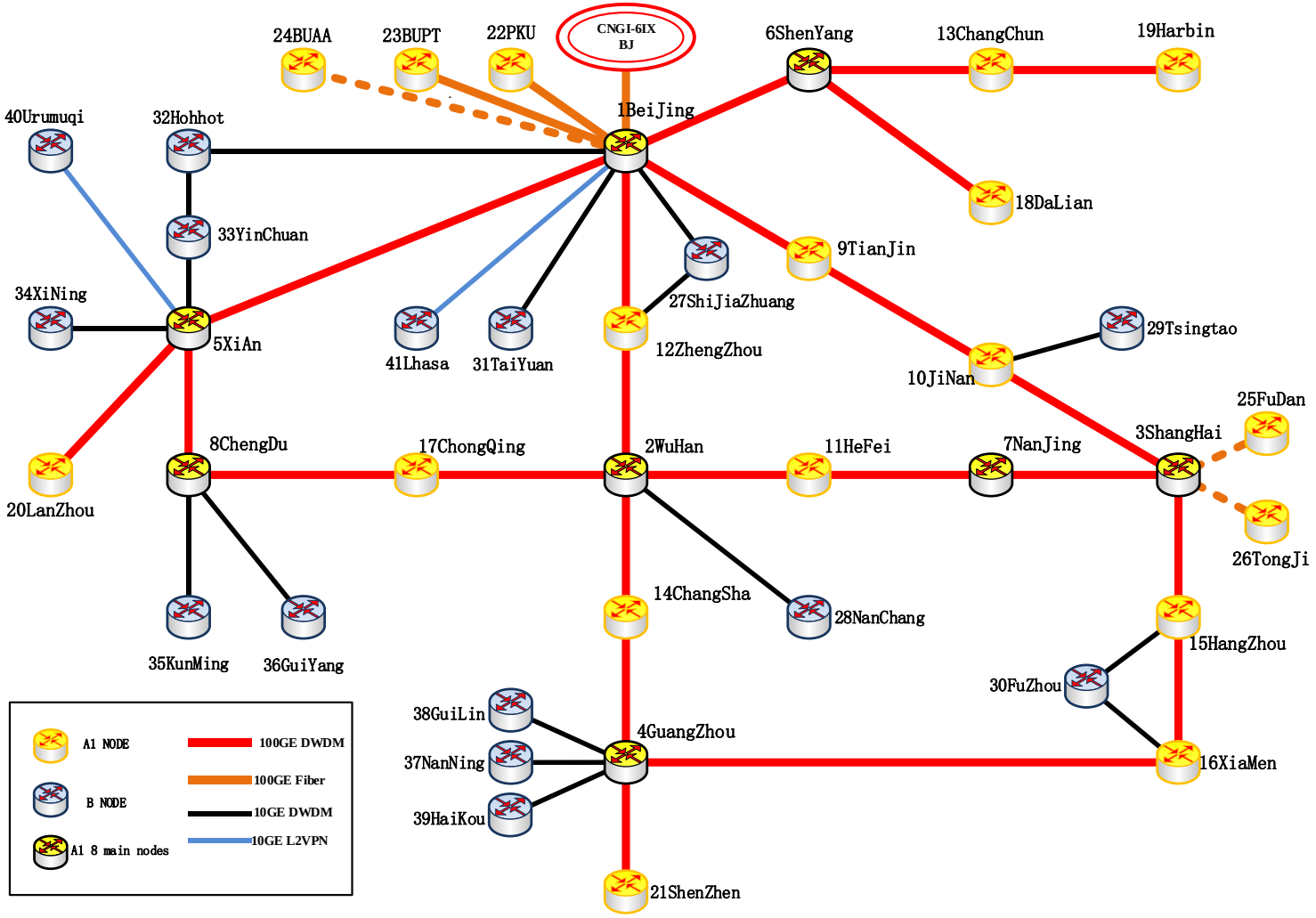
- Complicate implementation (both for NOC and customer networks), and IPv4 & IPv6 access is not transparent to customer networks
- Nonhierarchical & Vulnerable (L2 access)
- Difficult to monitor, manage and control (Less function on L2 switch)

Our choice

- Based on current situation for most of CERNET & CERNET2 customer networks, we choose Option 1 (Dual-stack Access Router) as preferred implementation scheme for CERNET2 Upgrade Project
  - To simplify the operation of CERNET2, the individual AS number for edge/access router in each PoP might be withdrawn gradually
- Option 2 might be considered for some nodes in the future, when
  - The customer network border routers become more powerful (full/part routing table, security, QoS etc.)
  - Most of customer networks in the node have their own AS numbers
  - Most of customer networks are more familiar with BGP
  - Increasing demand on multi-homing from customer networks
  - Increasing demand on private peering among customer networks

Progress of 100G Upgrade

- Delivery and activation of 41 PoP core routers (Huawei NE40e X8A)
  - Done
- 100G x 28
  - Almost done except for 3 intra-city links
    - Beijing (THU) – BUAA
    - Shanghai (SJTU) – Fudan Univ.
    - Shanghai (SJTU) – Tongji Univ.
- 10G x 16
  - Done



Next Step

- Complete the implementation of new pure IPv6 backbone of CERNET2
  - Implemented and running in parallel with current CERNET2 IPv6 backbone
- Migrate customer traffic to new 100G CERNET2 backbone
  - Migrate CERNET2 edge/access routers to the new backbone
- Tendering for new CERNET2 edge/access router for each PoP
  - 100G/10G uplink to core router
  - 100G capable for particular customer, e.g. National Supercomputing Centers
  - Sufficient 10G/1G ports for CERNET/CERNET2 customer access link
- New tech & service under consideration and evaluation
  - SRv6
  - EVPN
  - DDoS mitigation
  - etc.

Outline

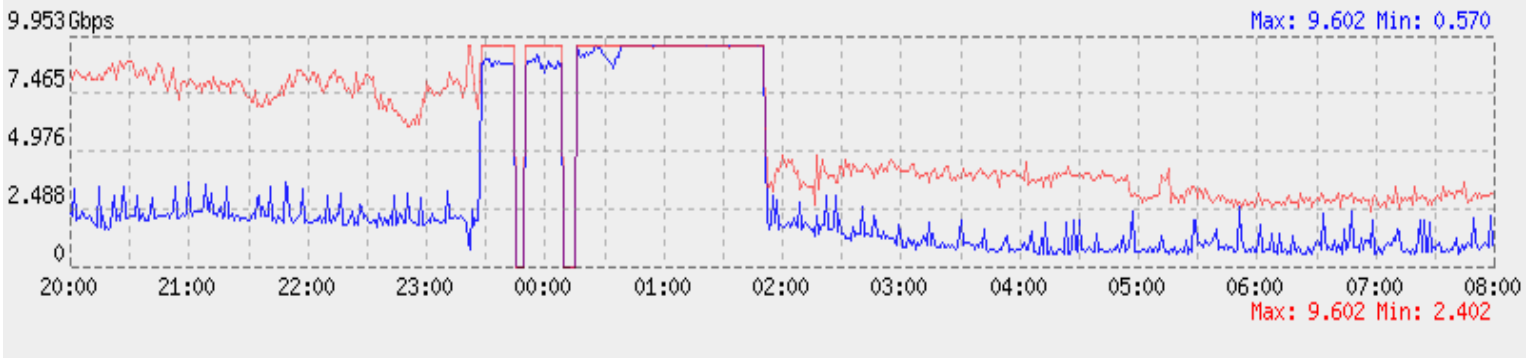
- CERNET2 100G Upgrade
- **IPv6 Memcache DDoS Attack to CNGI-6IX**

IPv6 Memcache DDoS Attack to CNGI-6IX

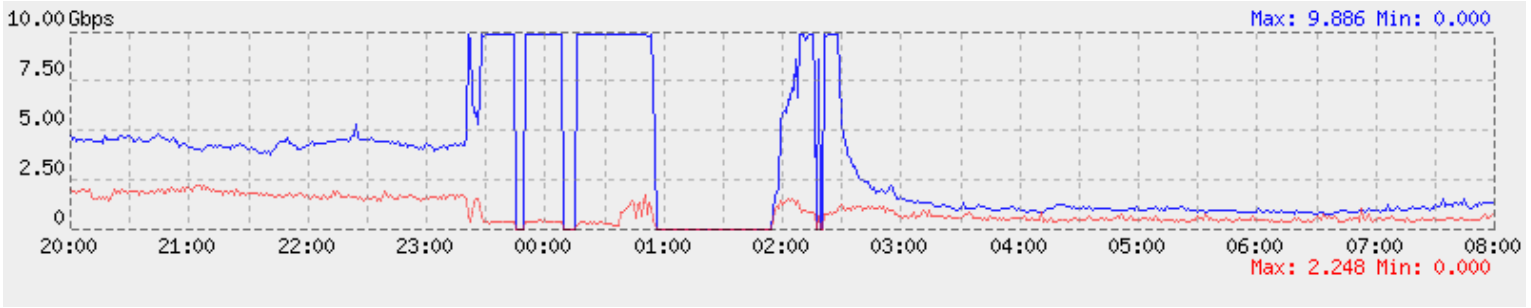
- The first large-scale IPv6 DDoS attack to CERNET/CNGI-6IX infrastructure
- Start time of DDoS attack
  - 23:20 BJT on 1st Mar 2018
- Attack target
  - IPv6 address on CNGI-6IX BJ-LA 10G link
- Source of attack traffic
  - One of IPv6 commodity ISP peering in LA
- Impact
  - Continuous and serious traffic congestion on BJ-LA 10G link

Action taken

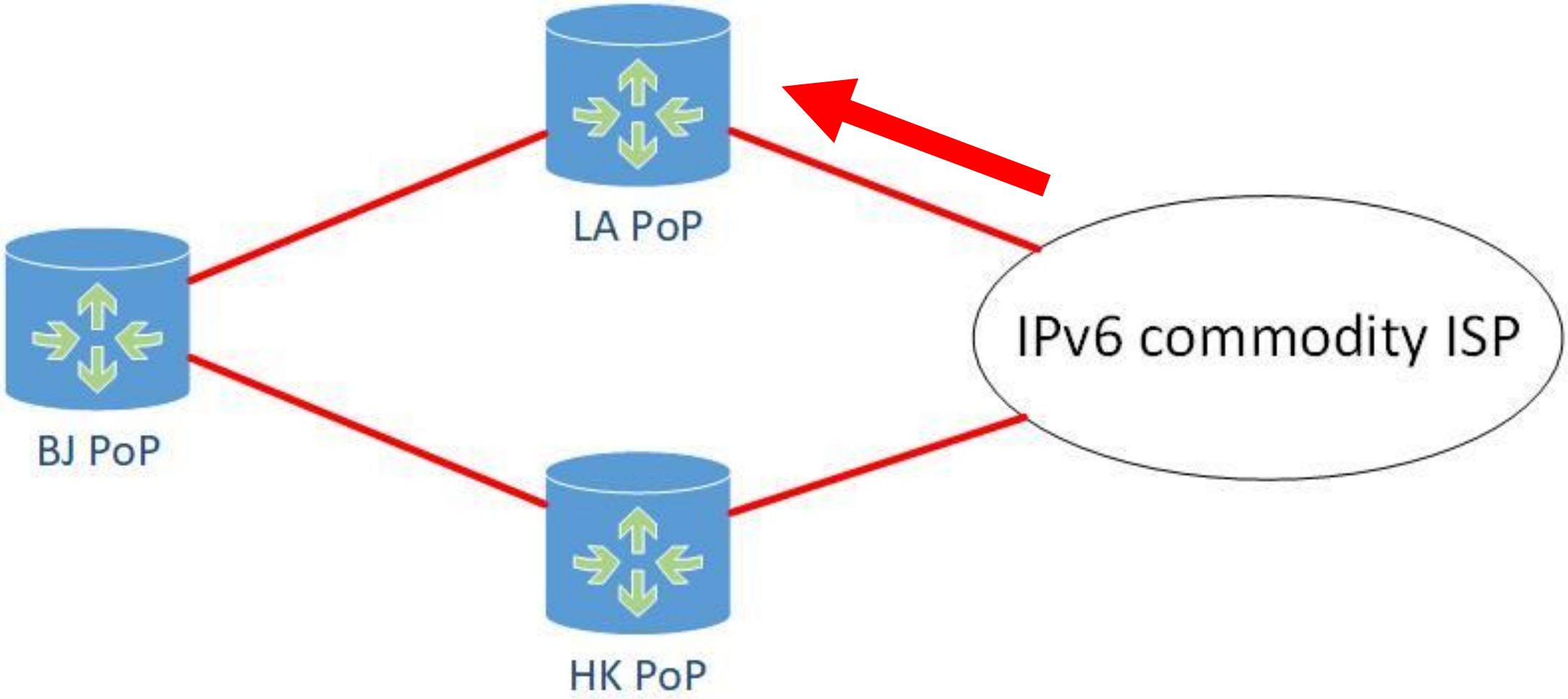
- Applied firewall filter for UDP port 11211 on LA router interface connected with that ISP



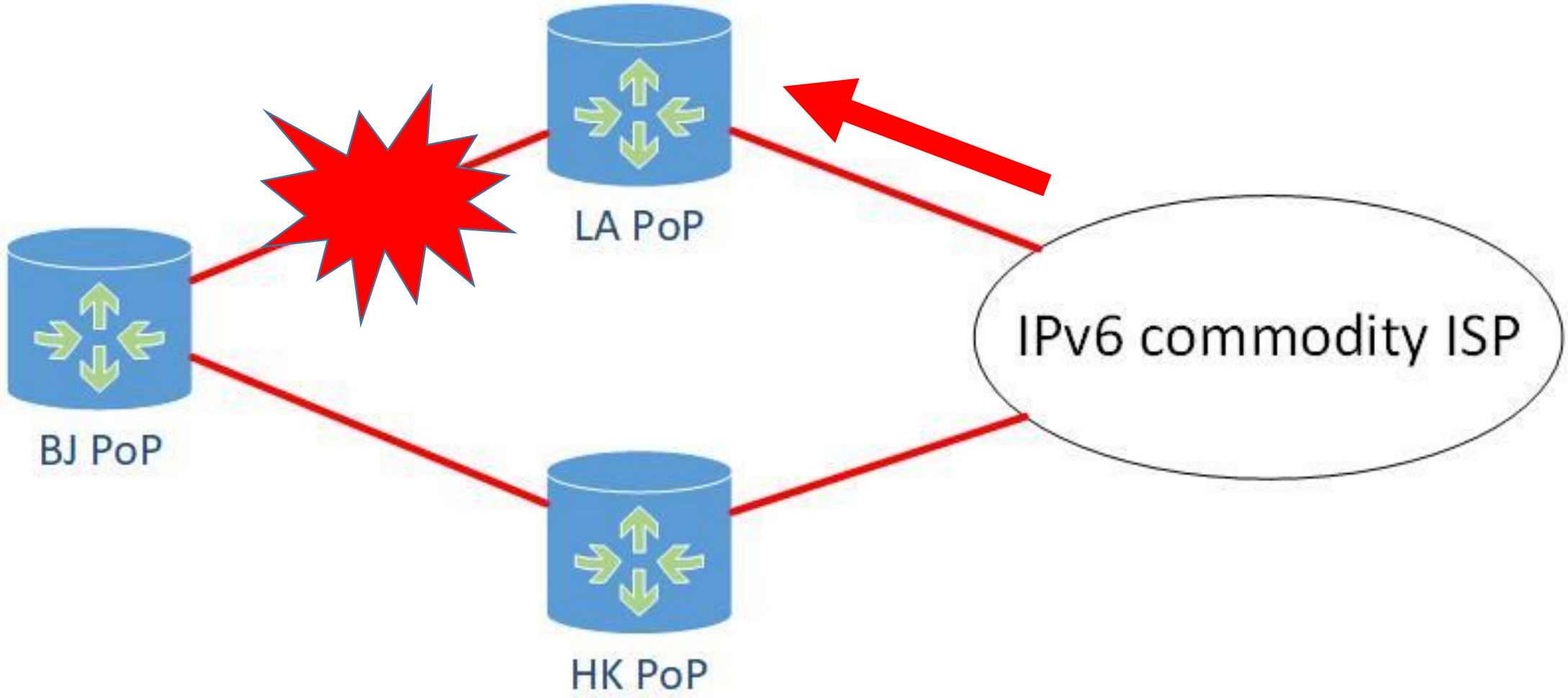
- Requested the ISP to block the DDoS attack traffic inside its backbone



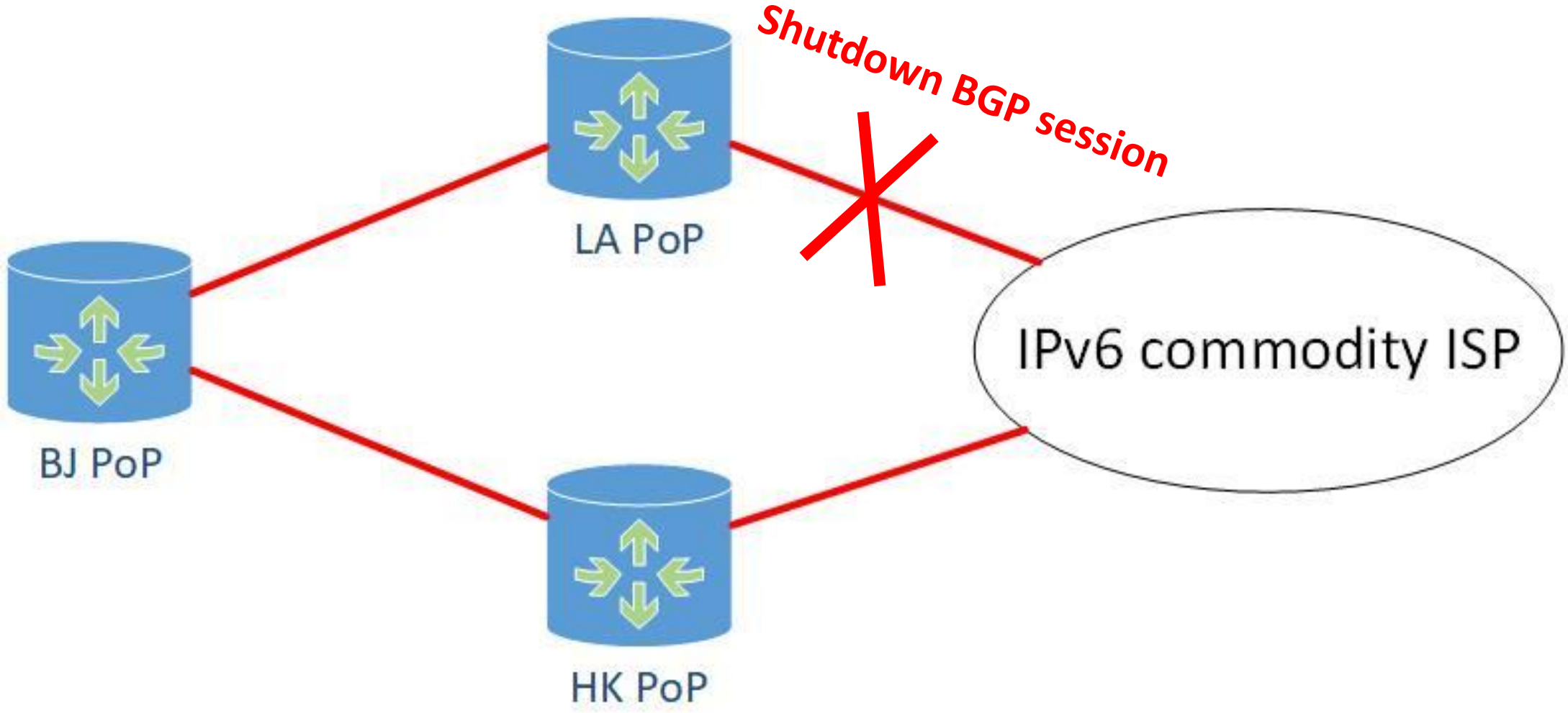
How did the attack traffic go through CNGI-6IX backbone



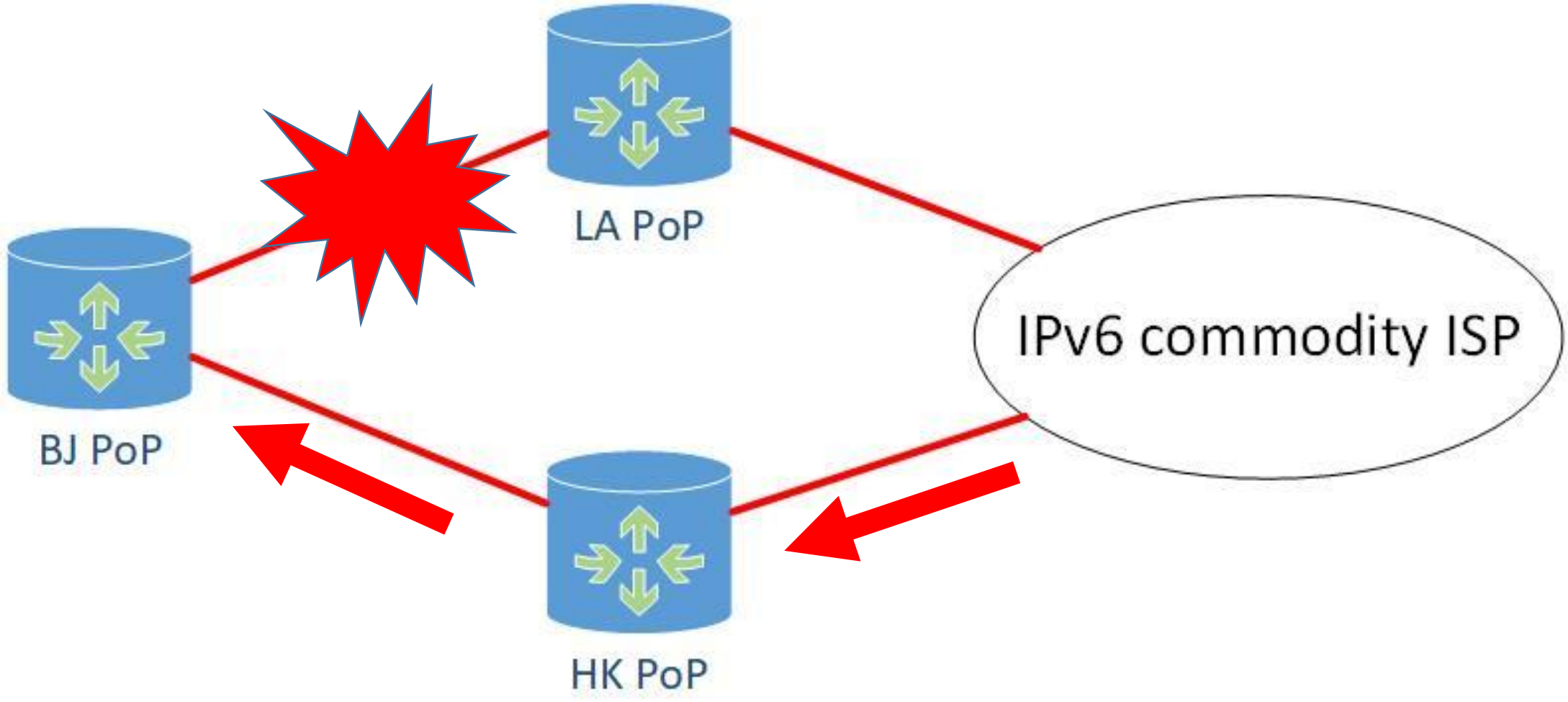
How did the attack traffic go through CNGI-6IX backbone



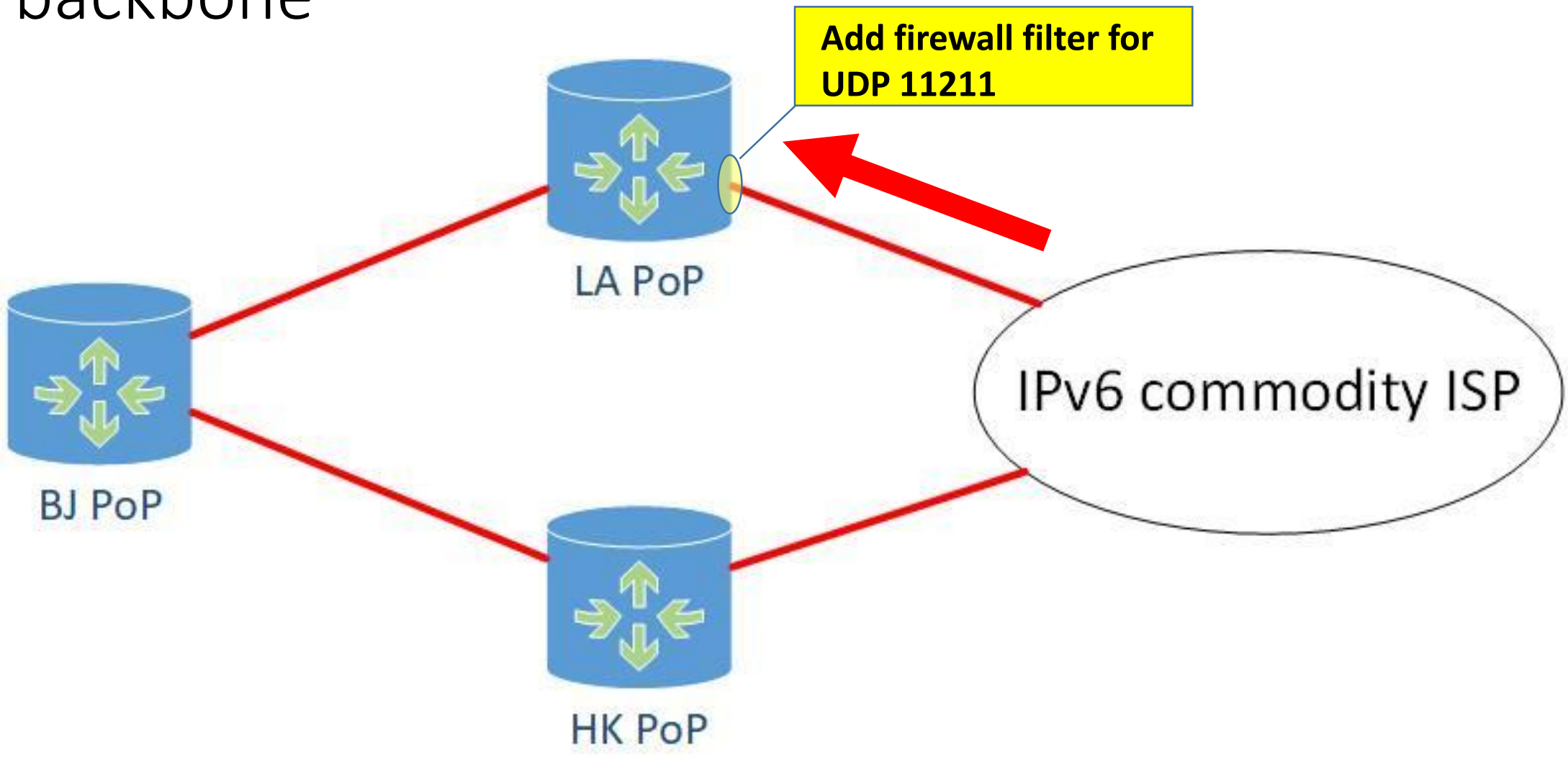
How did the attack traffic go through CNGI-6IX backbone



How did the attack traffic go through CNGI-6IX backbone



How did the attack traffic go through CNGI-6IX backbone



Lessons and thinking

- Necessity of online real-time IPv6 flow analysis system with abnormal traffic detection and alerting
- IPv6 DDoS mitigation measures
  - Traffic scrubbing: high cost and not work for this case
    - Attack target is infrastructure not customer network
  - BGP Flowspec: cooperation from external peer
- Is it the time for us to pay more attention to IPv6 network security?

Thanks!