NAT64 Operational Considerations

draft-chen-v6ops-nat64-cpe-03.txt

IETF 82- Taipei, Nov 2011

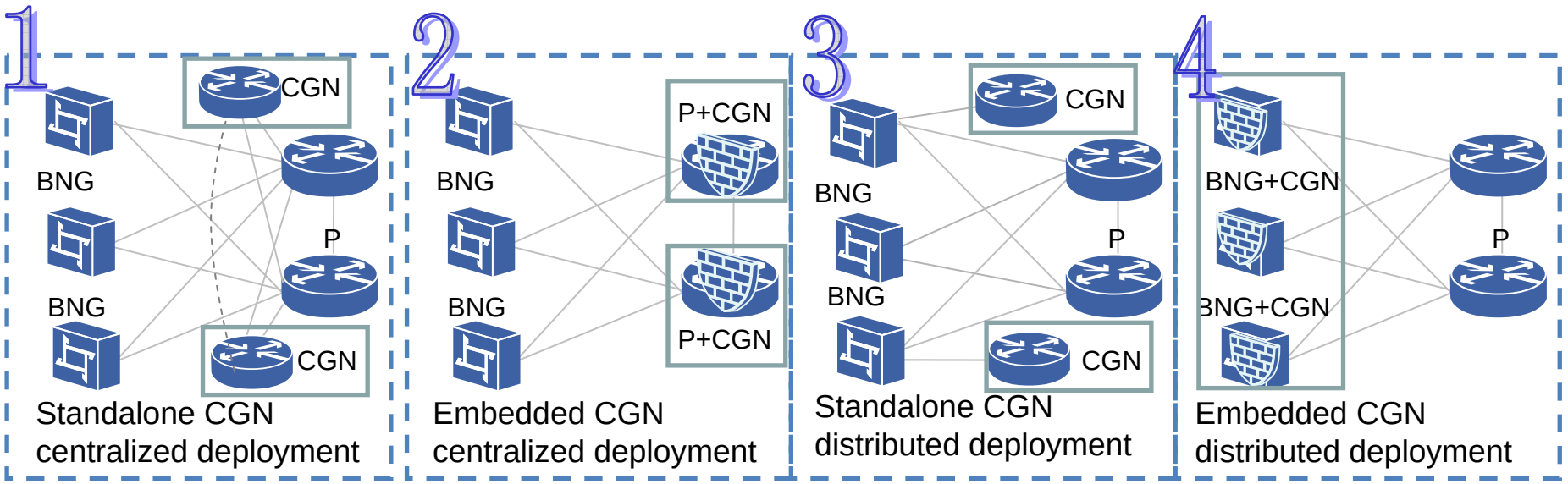
Authors: Gang Chen and Qibo Niu

Presenter: Zhen Cao

Two Parts of NAT64 Operational Consideration

- According to RFC6144:
- IPv6 Network to IPv4 Internet == NAT64-CGN
- IPv6 Internet to IPv4 Network == NAT64-CE

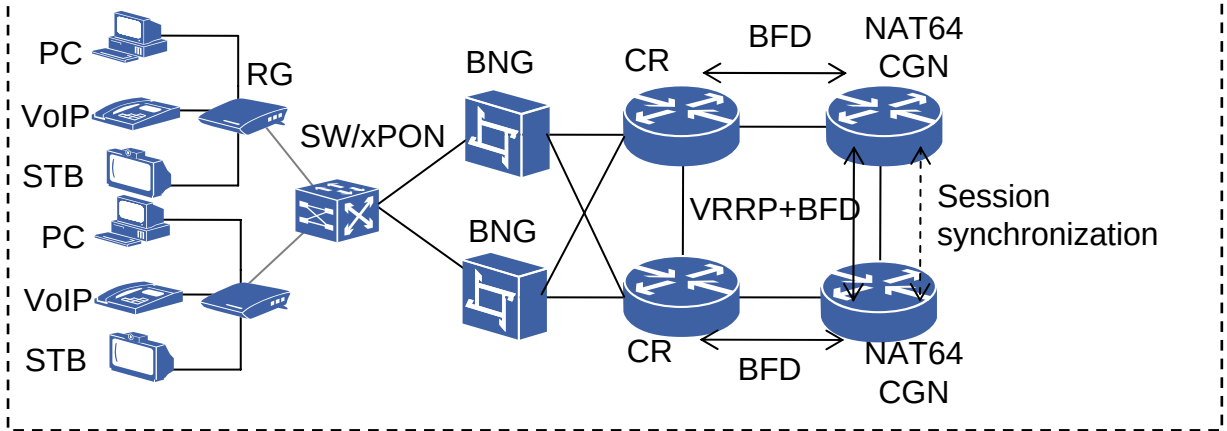
NAT64-CGN: Consideration on Networking



- Implementation mode: Standalone CGN and Embedded CGN
  - Standalone CGN: Dedicated devices achieve NAT64 CGN;
  - Embedded CGN: The existing devices integrate NAT64 CGN, for example, BNG, Router platform or PDSN/GGSN
- CGN location: Centralized deployment and distributed deployment
  - Centralized deployment: NAT64 CGN is deployed at high layer, for example, Core layer of MAN network;
  - Distributed deployment: NAT64 CGN is deployed at low layer, for example, BRAS/SR of MAN network;
- There are four combinations as shown at above figure
- Operators should choose CGN mode based on many factors, such as user scale, NAT64-CGN maturity, investment, migration risk and so on.

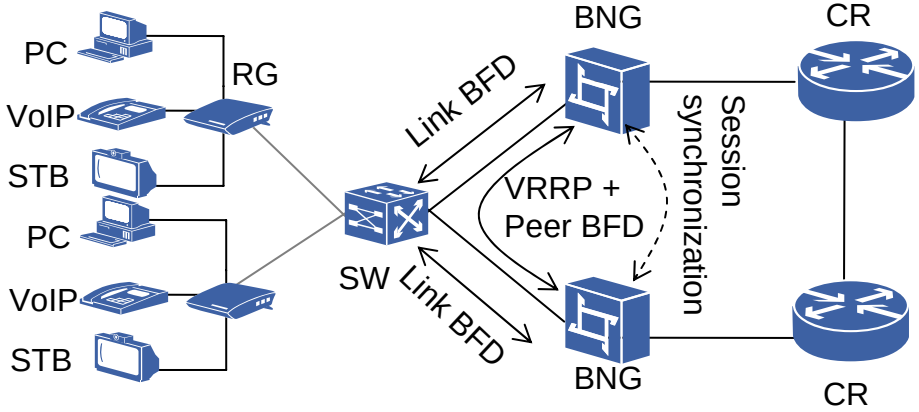
NAT64-CGN: Consideration on Reliability

High Reliability for Standalone NAT64-CGN



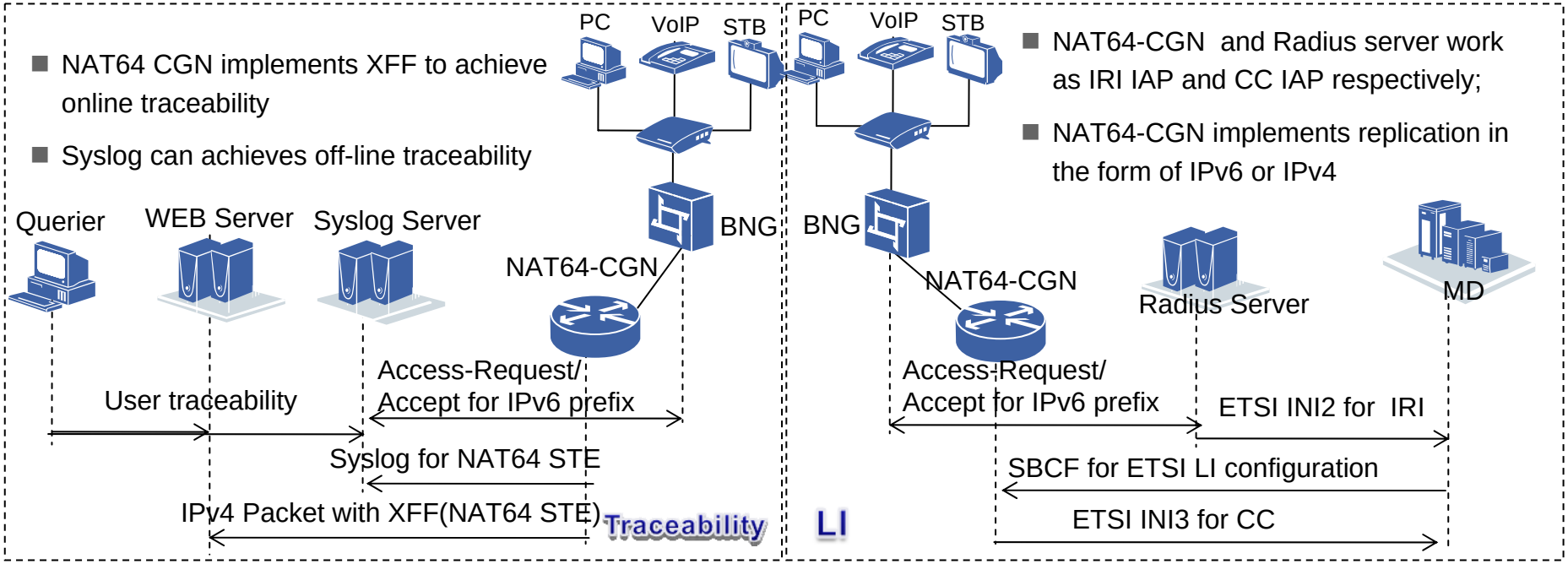
- VRRP + BFD achieve fast fault detection and master/Slave switchover
- Session synchronization protocol achieves NAT64 BIB (Binding Information Base) and STE (Session table Entry) synchronization between Master and Backup NAT64 CGN

High Reliability for Embedded NAT64-CGN



- Link BFD and VRRP + Peer BFD achieve fast fault detection and master/Slave switchover
- Session synchronization protocol achieves NAT64 BIB, STE, subscribers session, QoS and accurate binding information (NAS address and Port) synchronization between Master and Backup BNG

NAT64-CGN: Consideration on Security

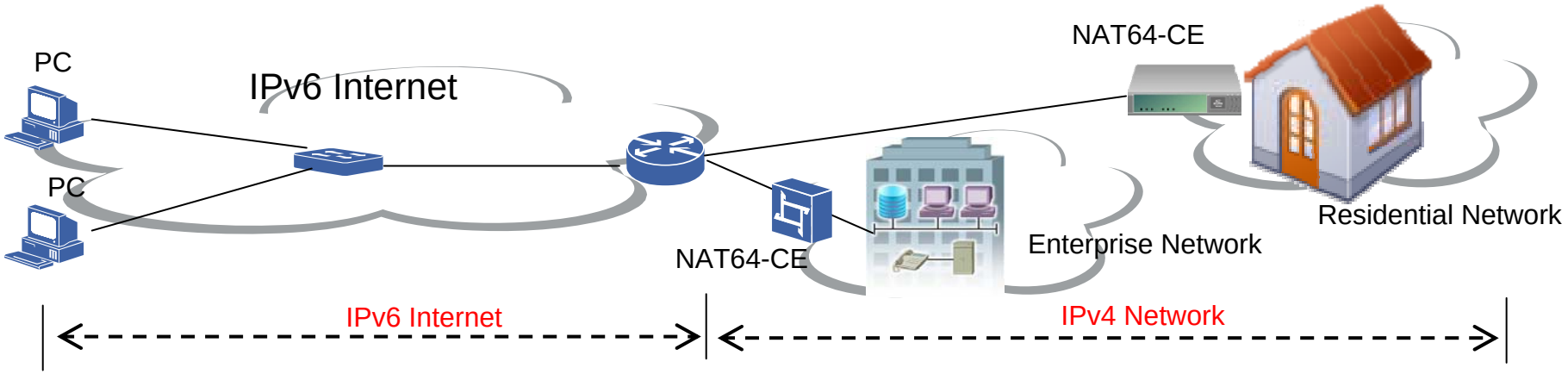


- Security requirements include legal mandatory requirements and device requirement in scenario of NAT64
- Legal mandatory security: User traceability and Lawful interception, there is no standard to implement NAT64-CGN traceability and Lawful interception. We suggest XFF and syslog to achieve traceability, ETSI LI (to be extended) to lawful interception;
- Devices security: RFC 6146 provides TCP-tracking, Endpoint- dependent filtering mechanisms to protect CGN form DDOS, we also suggest Blacklist, uRPF and other mechanisms to ensure devices security

NAT64-CGN: Optimization

- Service Richness: FTP-ALG, SIP-ALG, RSTP-ALG, H.323-ALG, SCCP-ALG, PPTP-ALG and so on;
- User policy: NAT64 CGN can assign different sizes of port ranges for different subscribers and implement different QoS policy, and embedded NAT64-CGN (BRAS + CGN) should cooperate user profile of BRAS and CGN profile to implement different user policies;
- P2P service: NAT64-CGN integrates with PCP server, and assign IPv4 address/Port to PCP client through PCP MAP/PEER mode;

NAT64-CE Consideration

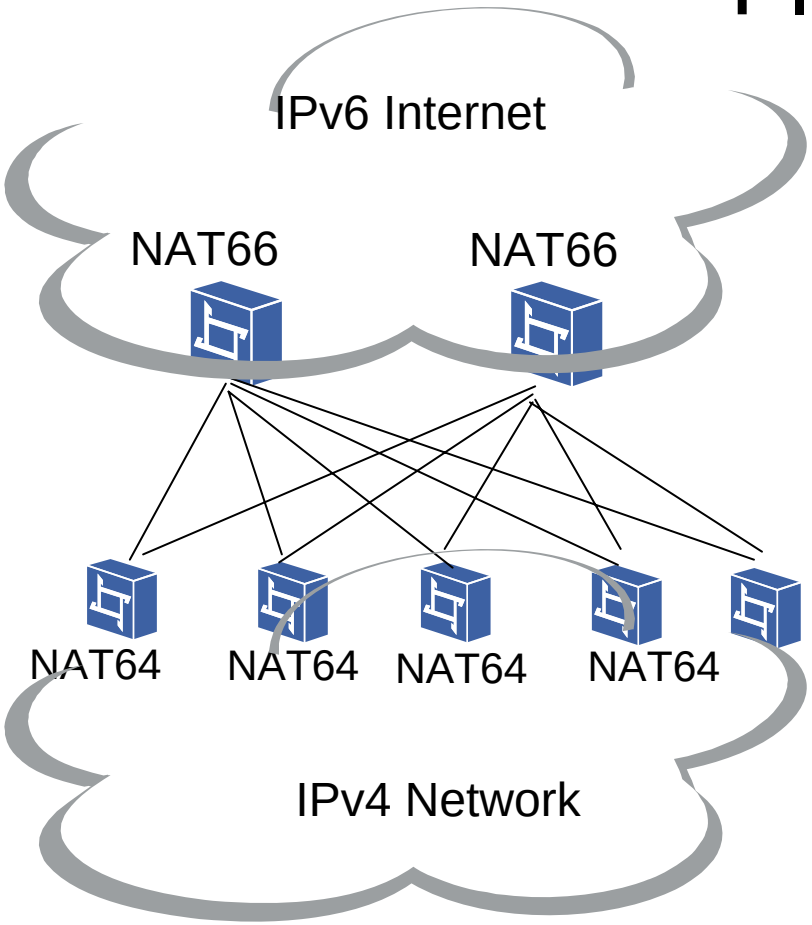


- Location: NAT64 would be subsided to a customer edge, e.g. Enterprise-GW or Residential network (including M2M)
- Networking mode: Centralized vs distributed deployment

NAT64-CE Challenge: address space

- One challenge remains: IPv6 space much bigger than IPv4 space
- When increasingly numerous users in IPv6 Internet access to an IPv4 network, there will be not enough IPv4 address/port serving the mapping
- Distributed NAT64-CE could serve for expanding IPv4 spaces by increasing reuse ratio of IPv4 address

NAT64-CE Challenge: DDoS/SYN Flood



- DDoS will severely degrade web performance
- Use of L3 load balancer
  - 10G line rate DDoS defense, like SYN Flood, using SYN PROXY-COOKIE
  - Load balancing between NAT64 devices
  - NAT66 could be used

A practice at ipv6.baidu.com

NAT64-CE Consideration: Mapping info & User Analysis

- Mapping information on the NAT64-CE is important for who deploy it
  - Not only for logging, but also for user behavior analysis
  - the traceability for accurate advertisement delivering

NAT64-CE: Consideration on Naming

- Using independent sub domain for ipv6 services, other schemes will seriously influence the ipv4 users experience
  - Use ipv6.xxx.com instead of www.xxx.com
- Following the recommendation of RFC6144: there is no need to synthesize AAAA from A records, since static AAAA records can be put in the regular DNS to represent these IPv4-only hosts

Current Practices in China Mobile

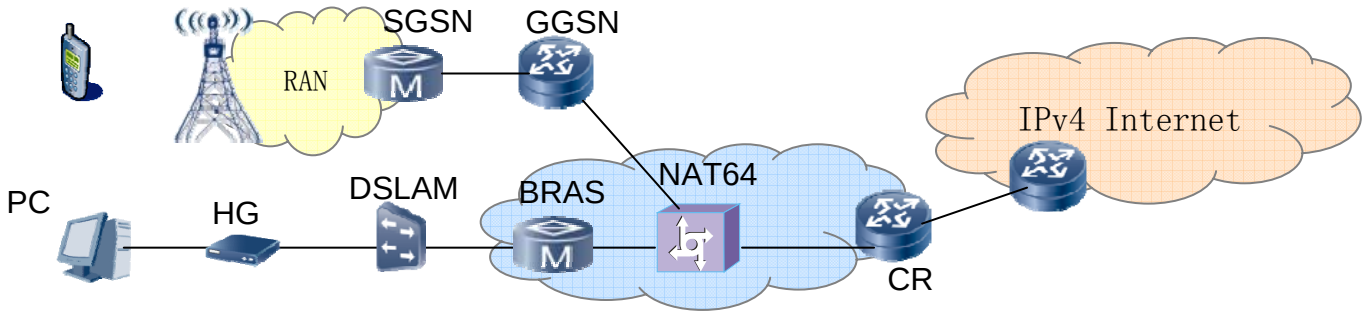
- China Mobile would launch IPv6 trials in one provincial network at 2011 Q4
- The scope of the trials includes 2G/3G Network, fixed broadband network , WLAN and CNGI network
- The objective of trials is to develop at least 5000 IPv6 commercial customers. More details are shown in the below table

Items	Number of users
Fixed Network	2000
WLAN Network	1500
Mobile Network	1500
CNGI Network	500

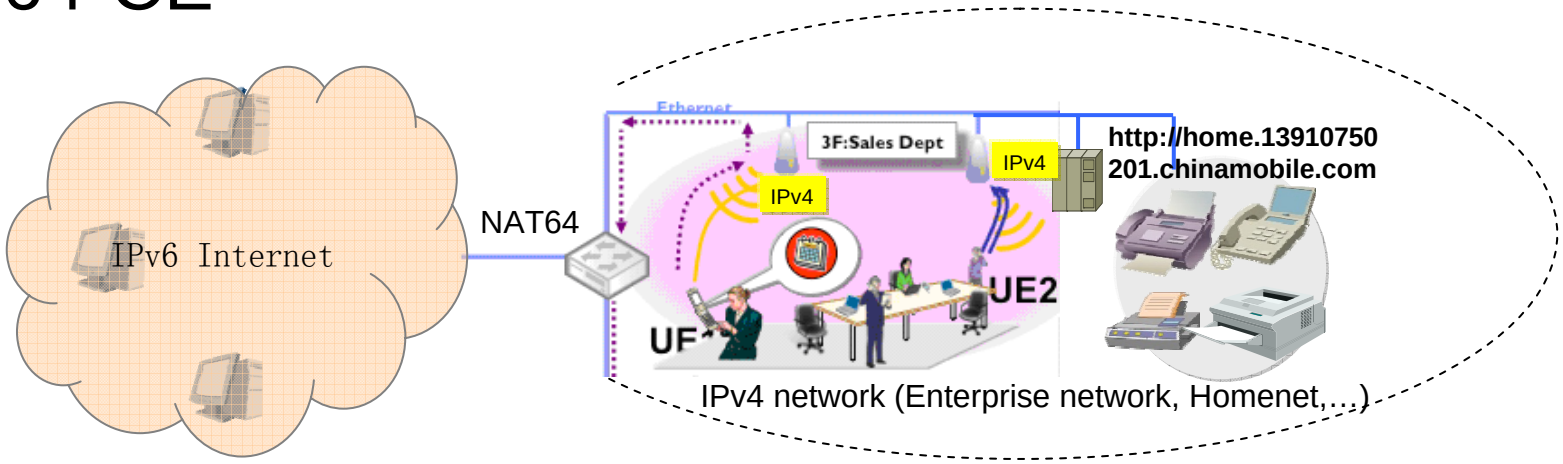
- The test cases are mainly focusing on “Dual-stack+NAT64”
- NAT64-CGN and NAT64-CE use cases would be introduced

NAT64 Deployments

NAT64-CGN



NAT64-CE



Next steps

- The draft have been presented four times. We are looking for adoption
- Future works
  - Add concrete use cases to demonstrate deployment guidance
  - Elaborate justification for different NAT64 environment (NAT64-CGN or NAT64-CE)