CNGI-CERNET2 SAVI Deployment Update

China Education and Research Network (CERNET)

IETF76, Hiroshima

Nov 9, 2009

Outline

- CNGI-CERNE2 SAVI Deployment Goal and Plan
- Vendors' Implementation and Examples
- MIB Design
- Demonstrations
- Conclusions

Brief Introduction

- CNGI is China Next Generation Internet
- CNGI-CERNET2
  - CERNET: was the 2nd Large ISP, 2000+ university campus networks, 20M+ users
  - CERNET2 is the largest IPv6 network
- CNGI-CERNET2 SAVI Deployment
  - 100 universities campus networks nationwide
  - 1 Million users
  - Time frame: 2008-2010
- China Telecom signed collaboration agreement with Tsinghua Univ. on IPv6 collaboration

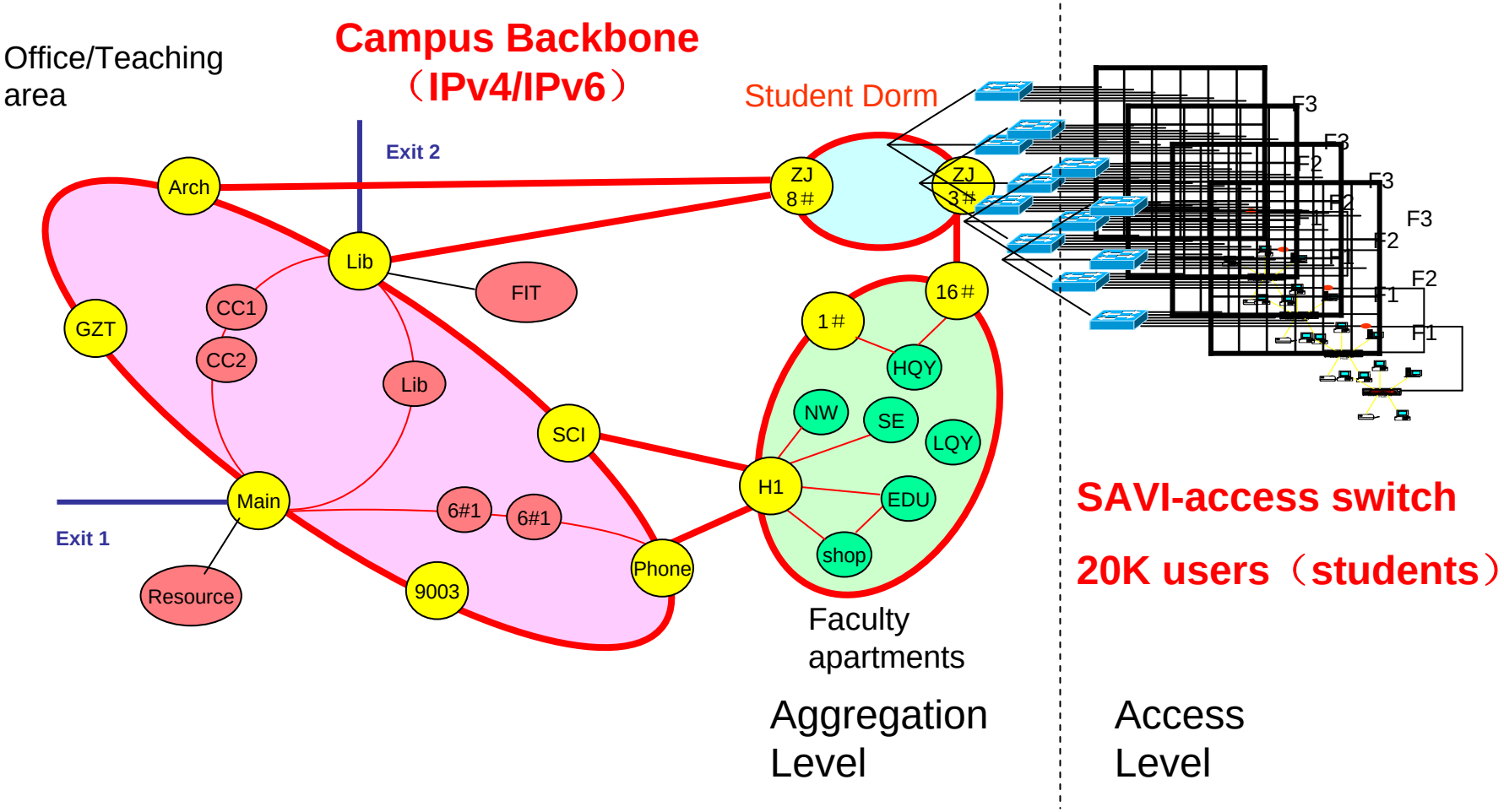
CERNET2 SAVI Deployment Goals

- Strictly Anti-spoofing at host granularity
  - Accurately traceback a host at the switch port. when attack traffic or unwanted traffic happens in SAVI deployed area, we could traceback the precise host by source address of unwanted traffic, then take actions.
  - Accurately bill the traffic usage to the precise host in SAVI deployed area. It's important for a operator to bill by usage not by fixed monthly rate.
  - To get precise measurement data

SAVI switches installation:100 Univ. campus net (red dot)

Example: Tsinghua Univ. campus network is being deployed (the number of switches, hosts are real）

subnets	switches	port	hosts	users
114	1018	23414	22644	20280



Vendors’ Implementation and Examples

SAVI switch test for 100 campus networks

Vendors' implementation

- Currently 6 vendors implemented SAVI-CPS in their Ethernet Switches
  - H3C (3Com): S5500EI, S5500SI, S5120EI、E126A, E152, E328, E352
  - ZTE: ZXR10 8900,5900,3900A
  - Digital China: DCRS-5950,3950
  - Ruijie: RG-S8600,S5750,S5760,S2900,S2600
  - Bitway: BitStream 7000, 6000, 3000
  - Centec: E600 and E300
- Cisco, Huawei are also collaborating with CERNET for implementation
- IPv6 Forum- "IPv6 ready logo" test for SAVI (BII)

SAVI-CPS Switch Examples

H3C S5500 switch

Digital china S3950 switches

Console Example

```
[H3C]dis ip check source ipv6
Total entries found: 4
MAC            IP                          VLAN Port                 Type
001d-09b6-a763 2001::7D1B:A5AE:44DE:FCB1 2    GigabitEthernet1/0/3   ND-SNP
001d-09b6-a763 FE80::B47E:A4DD:166D:89E0 2    GigabitEthernet1/0/3   ND-SNP
001d-09b6-a763 2001::B47E:A4DD:166D:89E0 2    GigabitEthernet1/0/3   ND-SNP
001d-09b6-a763 2001::1004                2    GigabitEthernet1/0/3   DHCPv6-SNP
```

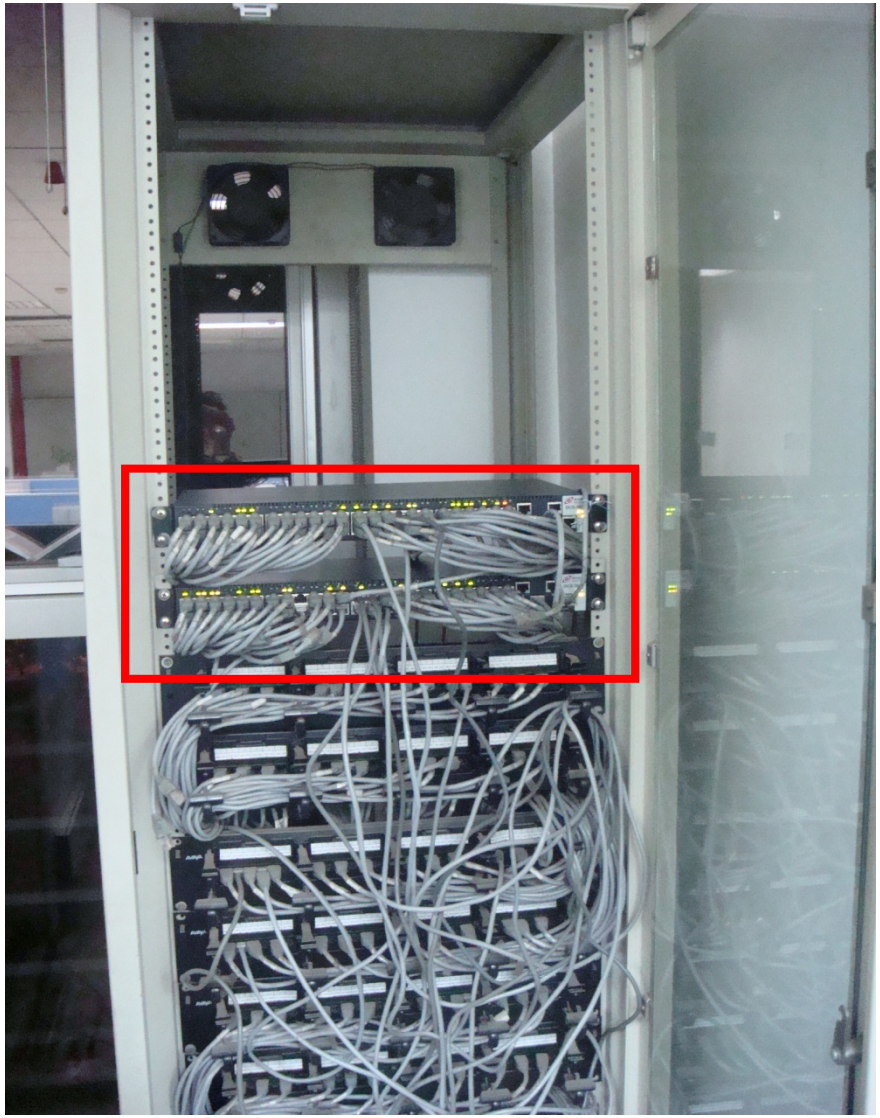
Binding State Table of *H3C S5500*

Entry:

Source IP | Source MAC | Vlan ID | Type(DHCP or ND)

Real Deployment

- FIT Building of Tsinghua University
- IPv4/v6 Dual Stack
- *Digital China* *S3950* Switches



Real Deployment

- IPv6 usage in Tsinghua FIT Building: IPv6 VoD, IPv6 Web, IPv6 transition, and IPv6 experiments(Testbed)
- The SAVI Switch
  - Bind IPv6 address, MAC address, Port, VlanID and the State
  - Discard packets from hosts with source not bound (SAVI-host port only)
  - The new SAVI switch runs well, and no **complaint** from users yet (the control packet loss at link never happens)

Real Deployment

Command Line Design

- **Config** and **Display**
- Config command (*H3C*)：

1)start dhcp snooping ：

[H3C]ipv6 dhcp snooping enable

2)start nd snooping and nd detection in vlan:

[H3C]vlan 2

[H3C-vlan2]ipv6 nd detection enable

[H3C-vlan2]ipv6 nd snooping enable

Command Line Design

3) Start address validation on specific port：

[H3C-GigabitEthernet1/0/1]ip check source ipv6 ip-address mac-address

4）Manually binding on port :

[H3C-GigabitEthernet1/0/1]user-bind ipv6 ip-address 2001::9

Command Line Design

- **Display** command(*H3C*)
  - display dhcp snooping

    [h3c]display ipv6 dhcp snooping user-binding dynamic
  - display nd snooping

    [h3c]display ipv6 nd snooping
  - display filtering table

    [h3c]display ip check source ipv6

Current SAVI-CPS Deployment in CERNET2

- SAVI-CPS switches is being installed
  - H3C (3Com): 10000+ switches in 79 universities
  - Ruijie: 9000+ switches in 91 universities
  - Digital China: 2000+ switches in 26 universities
  - ZTE: 200+ switches in 16 universities
  - Bitway and Centec: in Tsinghua testbed
- To install more in next steps

SAVI MIB Design

MIB Design

- The CERNET Network Center is designing a Network management system for SAVI
  - To manage, configure, and display SAVI functions/infomation using MIB
  - Worked with the vendors to make a draft design

MIB Draft Design: MUST

- Set:
  - Enable or disable DHCP Snooping and ND Snooping.
  - Enable or disable the address validation on port.
  - Binding limitation at a port
- Get:
  - DHCP Snooping or ND Snooping function are enabled or not
  - Binding State Table/Filter Table entries
  - Address validation is enabled or not (in data plane).

MIB Draft Design: Optional

- Get
  - Number of spoofed packets discard per port
  - Number of unspoofed packets forwarded per binding table entry
- Trap message
  - If an port received attack packets exceeding the limit, the switch sends trap message to network management system.
- Reason to be optional
  - Not all hardwares (chips) support it, may be implemented in a higher-end switch

Demonstrations

Video Demonstrations

- We have recorded video for 13 scenarios
  - Prevent attack against DAD procedure
  - Prevent attack against DAD procedure from undeployed area.
  - Prevent RA spoofing attack
  - Prevent DHCP server spoofing
  - Prevent address exhausting attack
  - Binding in SLAAC and DHCP Co-Existing Environment
  - Host changes port
  - Host changes port across switches
  - Topology Changing (Change port)
  - Topology Changing (Change switch)
  - Switch Reboot
  - DHCPv6 Only Environment
  - Duplicated SLAAC Address
  - To download: ftp://ietf:ietf@202.112.49.246

Onsite Demo in IETF75

- 

Conclusions

Conclusions

- SAVI drafts have been implemented by multiple vendors
- Based on current test and deployment, our SAVI solutions are stable
  - No major issues observed
- We will continue the deployment of SAVI solutions in CNGI-CERNET2
  - 100 Campus networks and 1 Million users
  - Build network management system

Thank You!
Q & A