SAVI Progress Report in CERNET2

Jianping Wu, Jun Bi, Guang Yao

Tsinghua University/CERNET

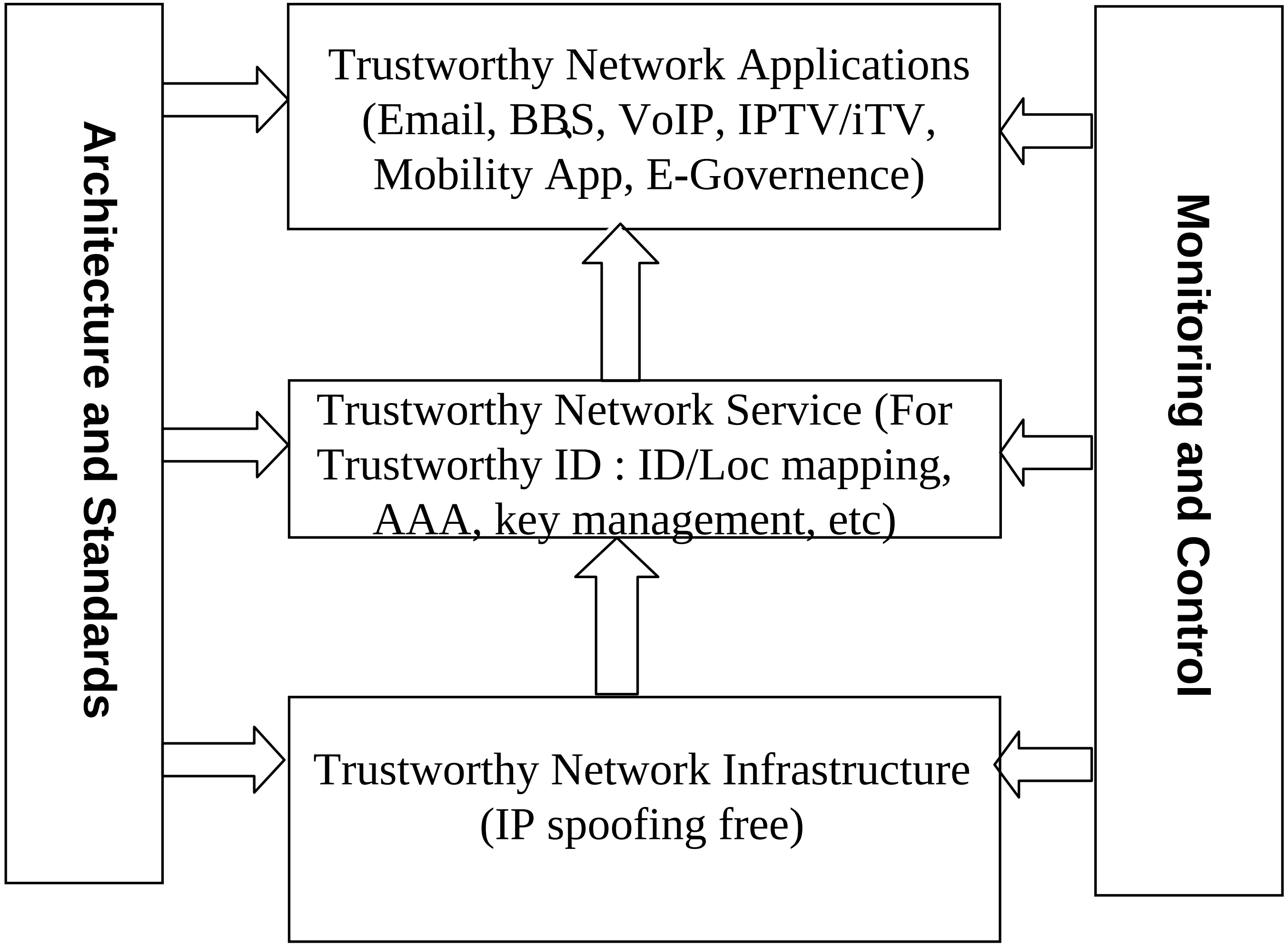
March 23, 2009

Outline

- Background
- Scenarios
- Framework
- Progress report on vendors’ support

Background

Trustworthy Next Generation Internet



Architecture and Standards

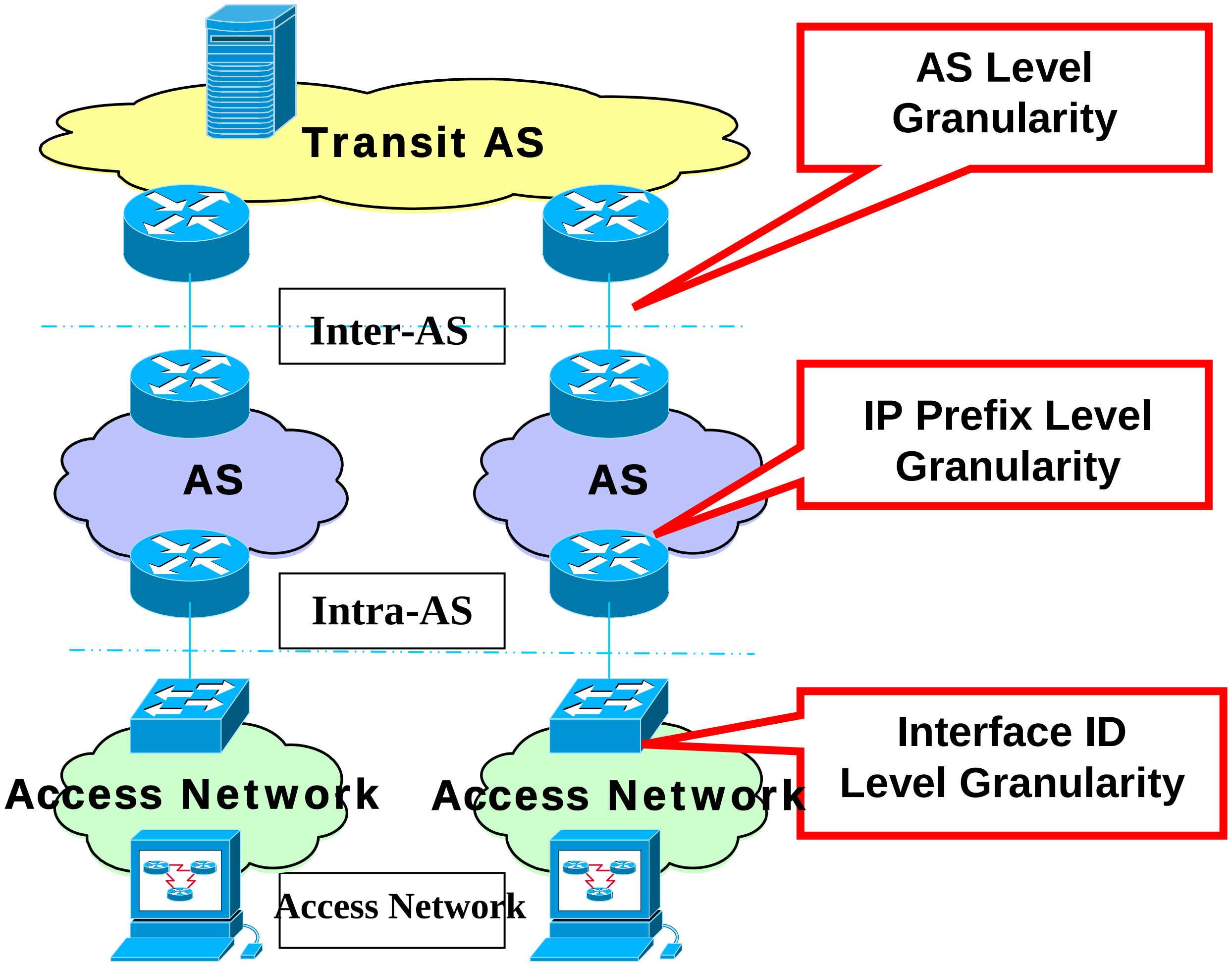
Trustworthy Network Applications (Email, BBS, VoIP, IPTV/iTV, Mobility App, E-Governence)

Trustworthy Network Service (For Trustworthy ID : ID/Loc mapping, AAA, key management, etc)

Trustworthy Network Infrastructure (IP spoofing free)

Monitoring and Control

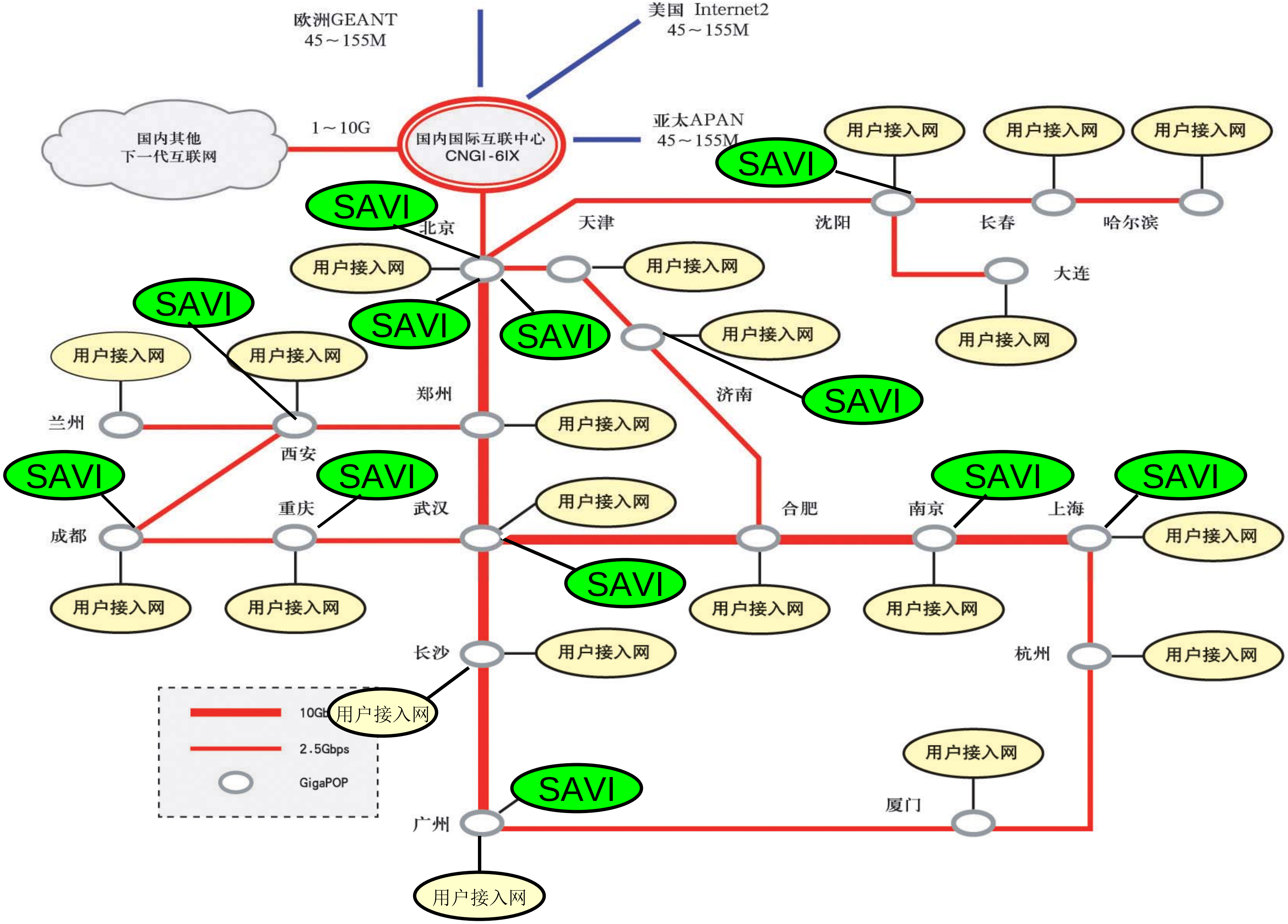
SAVA Architecture in CNGI-CERNET2



Goals and Approach

- Deployment Scale
  - CERNET2 backbone: Inter-AS anti-spoofing
  - 25 Regions (ASes): Intra-AS anti-spoofing
  - 100 Campus networks: Access Network anti-spoofing
  - ~1K-~10K SAVI Sub-networks
  - 1 Million users without IP spoofing
  - 1 Million / 20 ports = ~50K Ethernet SAVI-Switches deployment
- Funding
  - Project funding
  - Part of Government's New Deal
  - Matching funds from 100 Universities
- Time frame: 2008-2010
- Starting from SAVI

Source Address Validation Deployment in CERNET2



Goals and Approach

- Currently 7 vendors participated or being involved (tested in Feb. 2009. to purchase soon):
  - 8 catalog of devices (2 core, 3 aggregation, 3 access)
  - Huawei
  - ZTE
  - H3C (3Com)
  - Bitway
  - Digital China
  - Ruijie
  - GalaxyWind
- 2 Vendors are interested
  - Cisco (6509 informally participated part of test in Feb.)
  - Juniper

Scenarios at SAVI level

Scenarios

SCENARIOS	ANCHORS	DESCRIPTION
Secure MAC Address	MAC Address	Only in Ethernet.
Exclusive Switch Port	Switch Port	Only in Wired network.
Secure Layer2 Associations	Layer2 Associations	Often in Wireless network.
Cable Modem Network	Combination of MAC and Customer Relationship	In Cable Modem network
Classical DSL network	ATM Virtual Channel, or PPPoE or L2TP Session ID.	Classical DSL network
Tunneling Technology	Some Property of Tunnel Tech	IP/IP tunnel, MPLS LSP, or similar tunneling technology
Other Scenarios	Cryptographic Information	No other anchor is available.

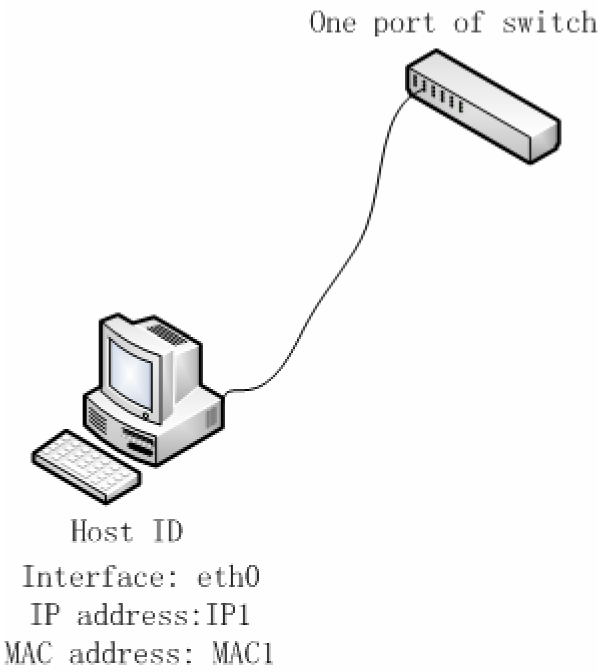
Scenarios

- Three Most Significant Scenarios , by available binding anchor (entity that unspoofable and exclusive for the host)

SCENARIOS	ANCHORS	DESCRIPTION
Exclusive Switch Port	**Switch Port**	**In switch based wired network.**
Secure MAC Address	**MAC Address**	**In Wired/Wireless Ethernet that enabling secure L2 association**
No Popper lower layer Anchor	**Cryptographic Information in data packets**	**No other anchors are available.**

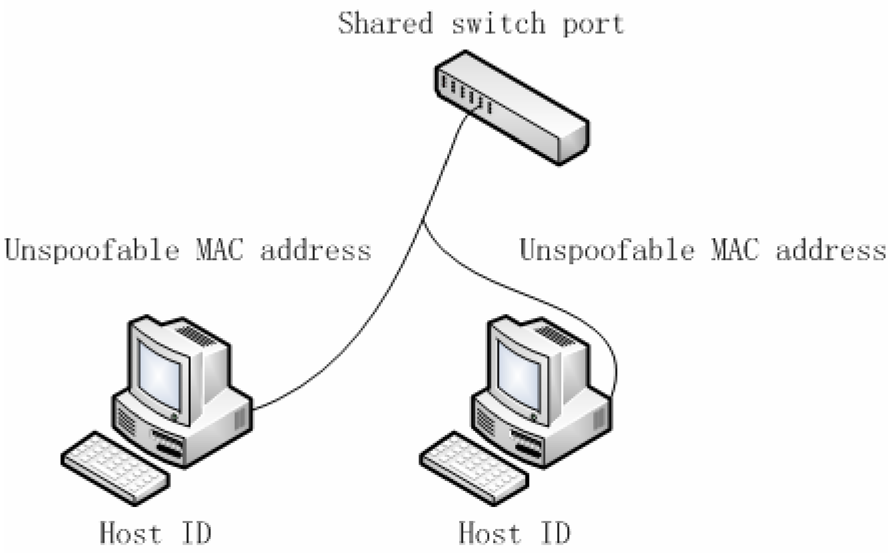
Scenarios

- Exclusive Switch Port
  - Bind IP address with Switch Port



Scenarios

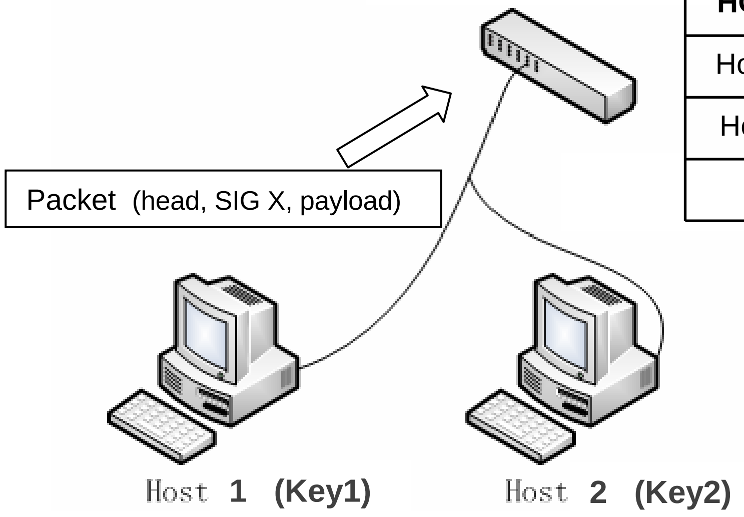
- Secure MAC Address (802.ae/af,802.11i)
  - Bind IP address with MAC address



Scenarios

- No Available Lower Layer Anchors
  - Bind IP address with Cryptographic Information in data packets

HOST CHANGE



Key Table

HOST	KEY	SIG
Host 1	Key1	X
Host2	Key2	Y
…	…	…

Scenarios

- Special Cases
  - Multiple IP addresses (Multi-IP)
    - Multiple IP addresses on one interface
  - Multiple MAC Addresses (Multi-MAC)
    - Multiple MAC addresses on one interface
  - Multiple Interfaces (Multi-IF)
    - Multiple interfaces on one host to the same link
  - Lower Layer Mobility (LLM)
    - Change to another Port of the Same Switch
    - Change to another Switch

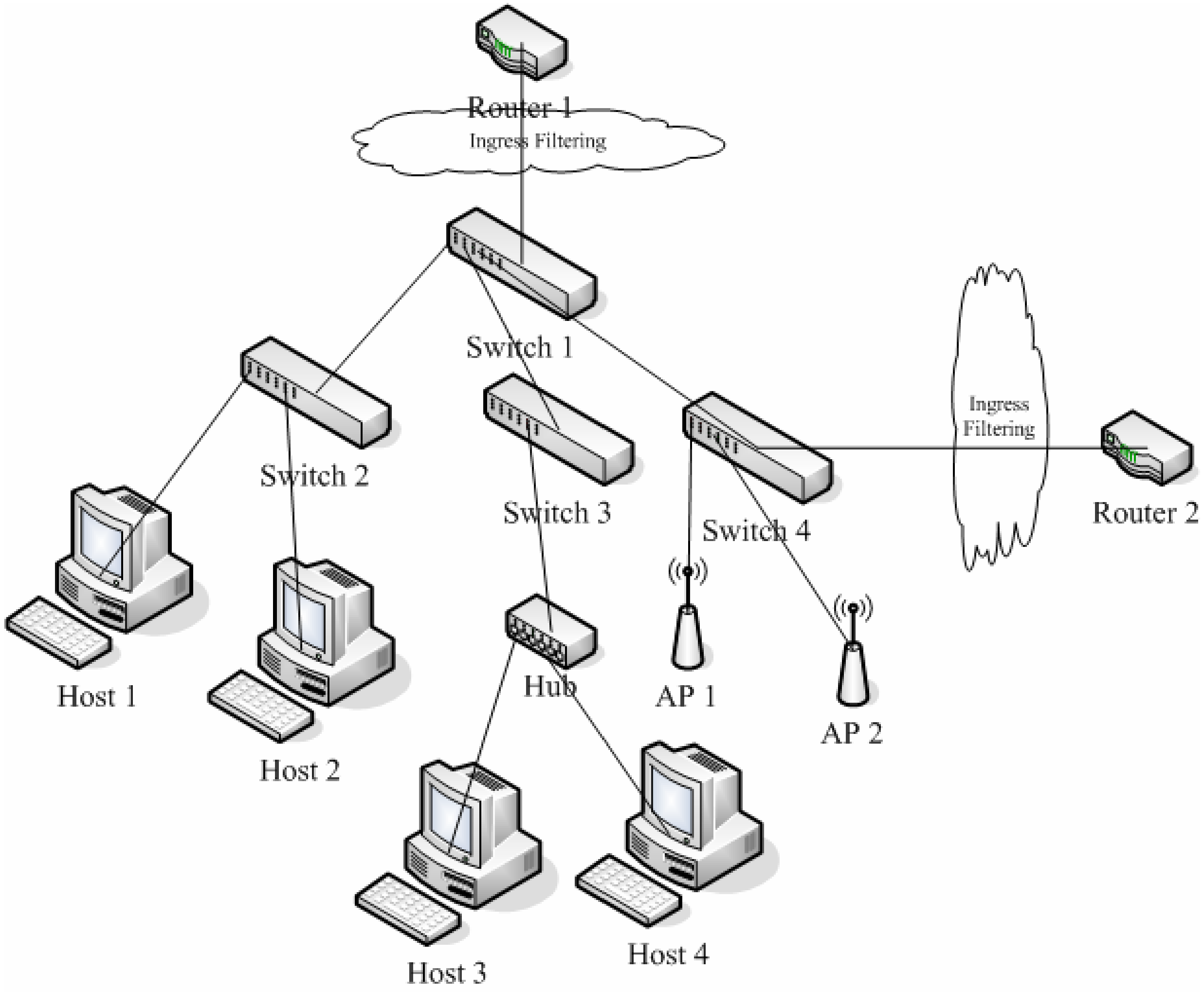


Figure 1 Typical SAVI access network

Framework at SAVI level

Content

- Choosing right binding anchors
- How to set up the initial binding
- How to handle the special cases (re-binding)

Binding Anchors

- Switched Network
  - Binding with exclusive port for the host
- Secure MAC
  - Binding with secure L2 association (802.11ae/af, 802.11i)
- No popper lower layer binding anchor
  - Binding with Cryptographic Information (Host changes)
  - CSA (presented in IETF 72 at Dublin)
  - SAVAH (another version of CSA, presented in HIP RG by A. Gurtov)
  - Some degree of “host-change”

Initial Binding

- Address Assignment Mechanism (AAM)
  - Stateless
  - DHCP
  - Manual
  - SeND/CGA
- During the Address Assigning Process
  - Spoofing happens when host uses the IP address that is not assigned to it by the AAM or hasn’t experienced a successful DAD procedure.
  - How can SAVI device know the assigned address?
    - Snoop the Address Assigning Process
      - SAVI-CPS

Handling Special Cases

- Special Cases
  - Multi-IP, Multi-MAC: add binding entries
  - Multi-IF
  - Lower Layer Mobility (LLM): *Preserve the original IP address?*
    - **NO (such as stateless case)**: Setup a new binding. Remove the old one.
    - **YES**: **(static address)**
- How to handle the special cases of Multi-IF and LLM of static address
  - Tentative IP address test
  - SeND (by unique CGA identifier)
  - HIP (by unique HIP identifier)

Progress report on vendors' support

Progress report on vendors’ support

- Source address validation related testing in Feb.
  - Processing of IPv6 option header with lightweight signature (tag)
  - IPv4 uRPF
  - IPv6 uRPF
  - IPv4 ACL
  - IPv6 ACL
  - Binding IP address with port
  - Binding IP address with MAC
  - NDP snooping
  - ARP snooping
  - DHCPv4 snooping
  - DHCPv6 snooping
  - 802.1x snooping

Progress report on vendors’ support

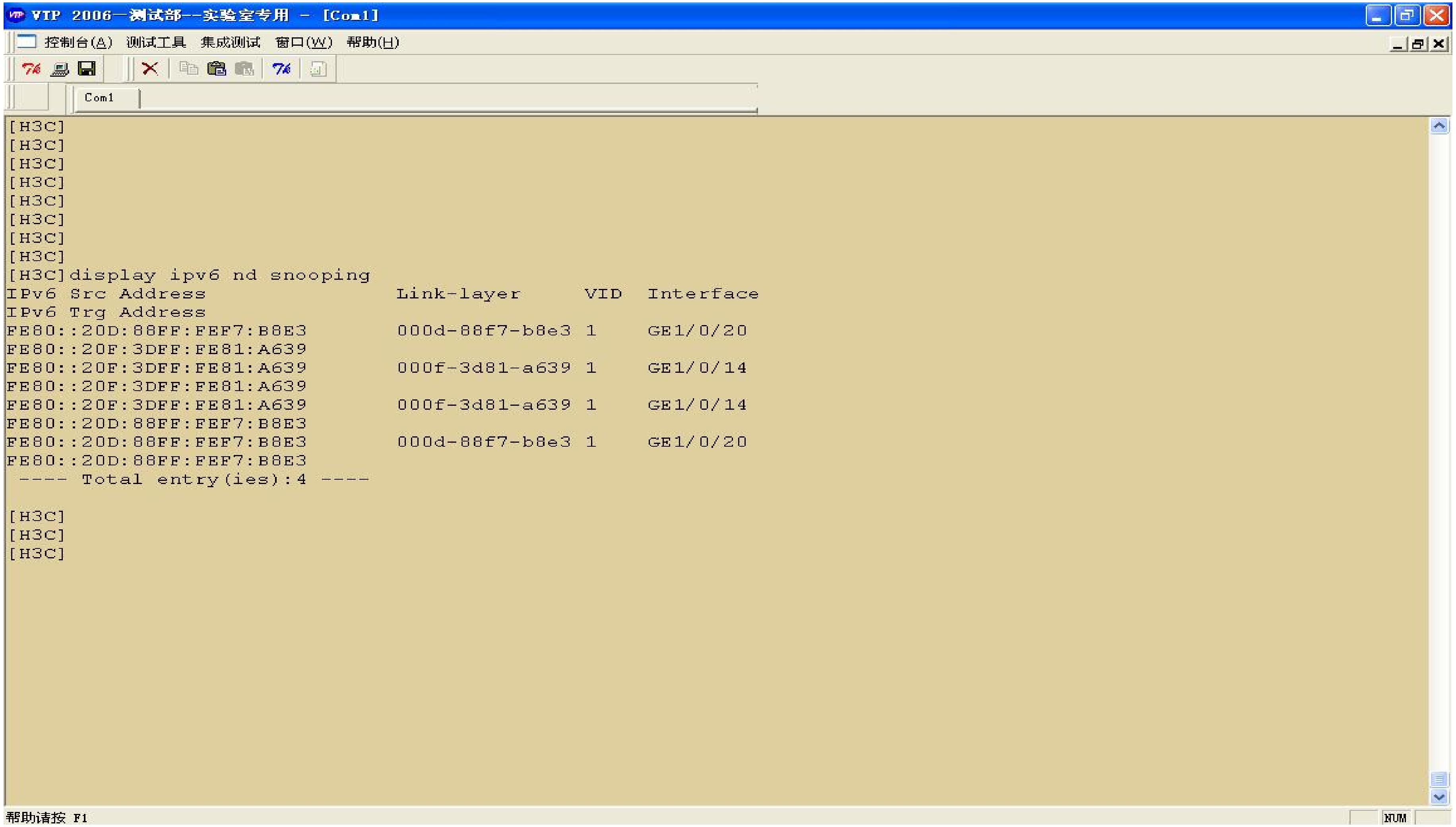
- 7 Vendors fully tested in Feb. 2009
  - 2 catalog of Core devices (10G/GE interfaces)
  - 3 catalog of Aggregation devices (10G uplink, GE interfaces)
  - 3 catalog of Access devices (GE/100M interfaces, 1U standalone box)
  - ~300USD per SAVI-enabled 2.5 Layer switch (IPv4/IPv6 L3-awared L2 switch, with 24x100M ports+2 GE uplinks)

Testing results

- Processing of IPv6 option header and lightweight signature (tag)
  - All vendors support and some vendor could reach line rate
- All vendors support with line rate:
  - IPv4 uRPF, IPv6 uRPF
  - IPv4 ACL, IPv6 ACL
  - Binding IP/port, IP/MAC
- All vendors support snooping, half of them even establish binding table for filtering (see example)
  - NDP snooping, ARP snooping
  - DHCPv4 snooping, DHCPv6 snooping
  - 802.1x snooping

NP snooping and binding table

- H3C (3Com) console

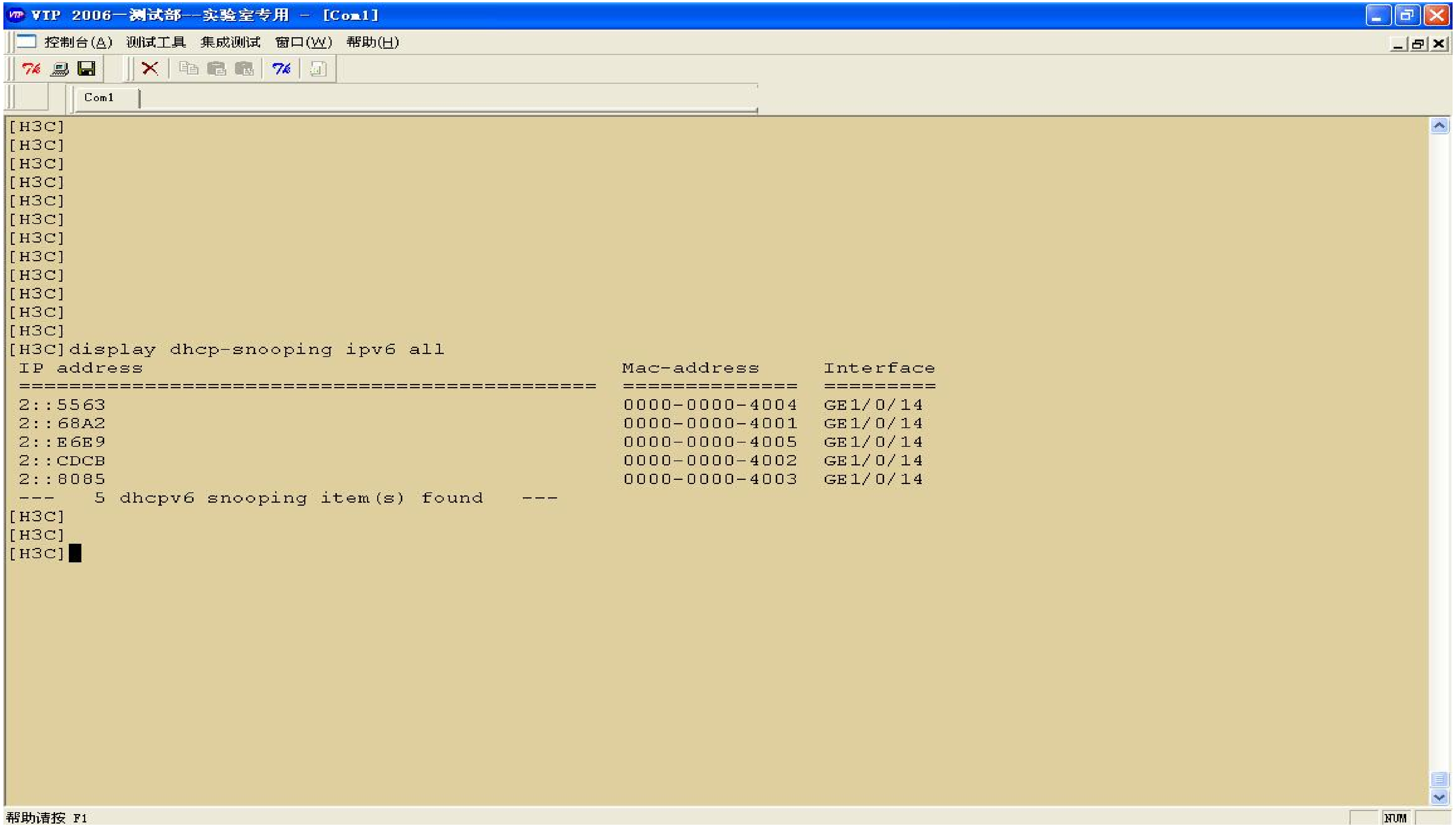

VTP 2006—测试部--实验室专用 - [Com1]
控制台(A) 测试工具 集成测试 窗口(W) 帮助(H)
Com1
帮助请按 F1
NUM

```
[H3C]
[H3C]
[H3C]
[H3C]
[H3C]
[H3C]
[H3C]
[H3C]
[H3C]display ipv6 nd snooping
IPv6 Src Address               Link-layer     VID  Interface
IPv6 Trg Address
FE80::20D:88FF:FEF7:B8E3       000d-88f7-b8e3 1    GE1/0/20
FE80::20F:3DFF:FE81:A639
FE80::20F:3DFF:FE81:A639       000f-3d81-a639 1    GE1/0/14
FE80::20F:3DFF:FE81:A639
FE80::20F:3DFF:FE81:A639       000f-3d81-a639 1    GE1/0/14
FE80::20D:88FF:FEF7:B8E3
FE80::20D:88FF:FEF7:B8E3       000d-88f7-b8e3 1    GE1/0/20
FE80::20D:88FF:FEF7:B8E3
 ---- Total entry(ies):4 ----

[H3C]
[H3C]
[H3C]
```

DHCPv6 snooping and binding table

- H3C (3Com) console


VIP 2006—测试部—实验室专用 – [Com1]
控制台(A) 测试工具 集成测试 窗口(W) 帮助(H)
Com1
帮助请按 F1
NUM

```
[H3C]
[H3C]
[H3C]
[H3C]
[H3C]
[H3C]
[H3C]
[H3C]
[H3C]
[H3C]
[H3C]
[H3C]
[H3C]display dhcp-snooping ipv6 all
 IP address                                      Mac-address     Interface
 ==============================================  ==============  =========
 2::5563                                         0000-0000-4004  GE1/0/14
 2::68A2                                         0000-0000-4001  GE1/0/14
 2::E6E9                                         0000-0000-4005  GE1/0/14
 2::CDCB                                         0000-0000-4002  GE1/0/14
 2::8085                                         0000-0000-4003  GE1/0/14
 ---   5 dhcpv6 snooping item(s) found   ---
[H3C]
[H3C]
[H3C]
```

Progress report on vendors’ support

- 8:30am-1:30am
- 8 Days

Vendors feedback

- Vendors like these features. To enhance the network security is a selling port to other customers.
- Some vendors are tracking SAVI mailing-list.
- Some vendors followed other vendors to quickly deliver the control plan snooping (not complex to implement, seems taking 1 week)
- 20 Million users/thousands campus networks in CERNET. It’s hard to upgrade all switches to SAVI devices in a short term, so still need Intra-AS and Inter-AS anti-spoofing solutions to protect none-SAVI zone.

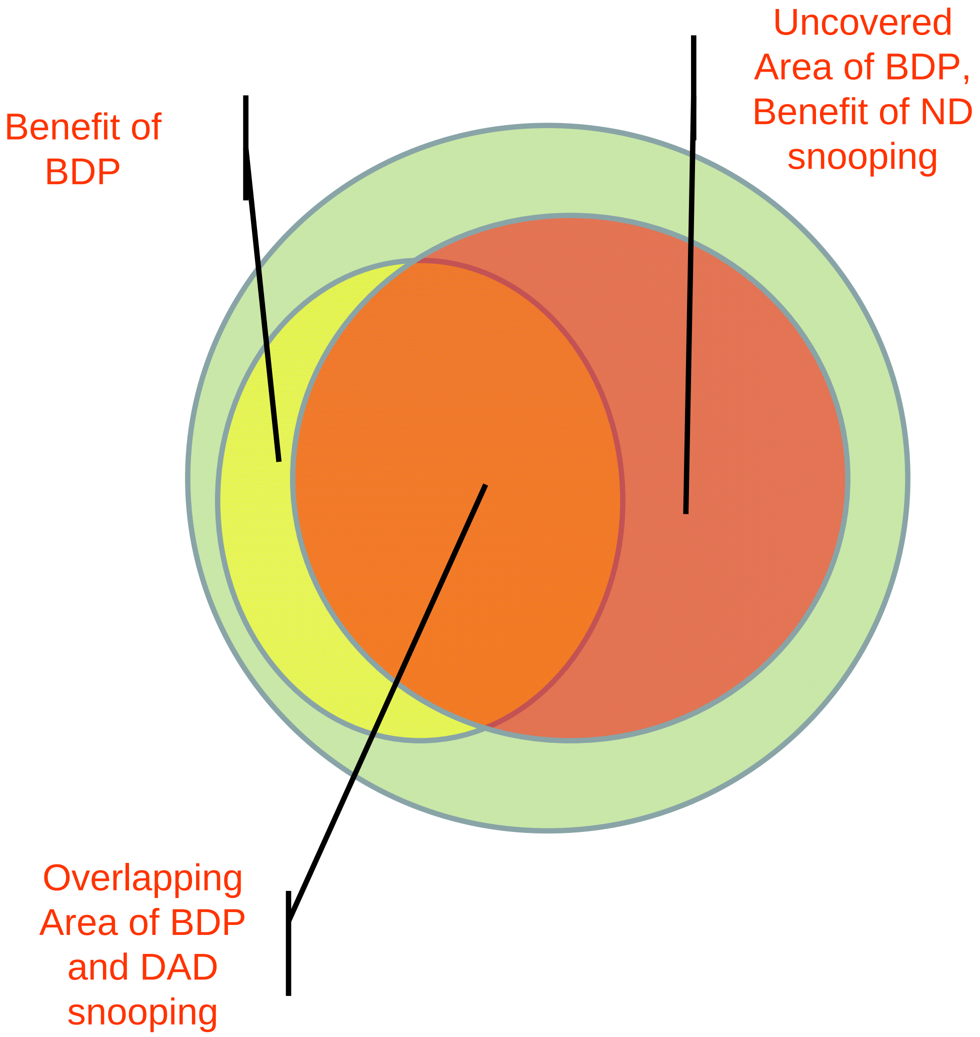
Analysis on binding distribution protocol

Jun Bi

Analysis on binding distribution protocol

- Why distributing bindings?
  - If a SAVI device wants to set up an initial binding for an address, it must firstly decide whether this address has been “assigned to another node” in the subnetwork.
  - BDP tells the device whether this address has been “bound on other SAVI devices”.
  - DAD verifies the device whether this address is “being used by another node” in the subnetwork
  - “address assigned to another node” ,“address bound on other SAVI devices”, and “address being used by another node” have different meanings.

Analysis on binding distribution protocol



Benefit of BDP

Uncovered Area of BDP, Benefit of ND snooping

Overlapping Area of BDP and DAD snooping

🟩 • Assigned Address

🟨 • Bound Address

🟥 • Being Used Address

Address bound but not being used:

- Some protected static address (could be manually set ?)
- Sleeping host (addr renew?)
- Temporarily disconnected host ?

Address being used but not bound:

- Hosts attached to non-SAVI device (SAVI-device and non-SAVI device In the same subnetwork).

Analysis on binding distribution protocol

- Benefits of BDP
  - The yellow part
- Limitations of BDP
  - For overlapping area (orange part), BDP is equal to DAD snooping
  - For uncovered area (red part), DAD snooping is still needed.

Analysis on binding distribution protocol

- How should a perfect BDP look like?
  - Once a binding is established or removed on a SAVI device, any other SAVI devices have the ability to get known this event immediately through the BDP.
  - Once a binding event is synchonized by BDP, the corresponding binding must be truly established or removed.

Analysis on binding distribution protocol

- Difficulties of designing a good BDP
  - Synchronization in real-time
    - Push or pull?
    - Push: handling the conflict, scalability, etc…
    - Pull: Not real time
  - Source authentication and event verification
- Currently, didn’t see a BDP yet
- If there is a BDP, we would provide more analysis

Thank You!
Q & A

A proposed solution SAVI-CPS

Jun Bi

SAVI-CPS

- CPS (Control Plan/Packet Snooping): Initial binding based on control packet snooping at the SAVI-switch

    v.s. FCFS+BDP

- Discuss: Handle special cases (when re-binding is necessary)

Control Packet Snooping

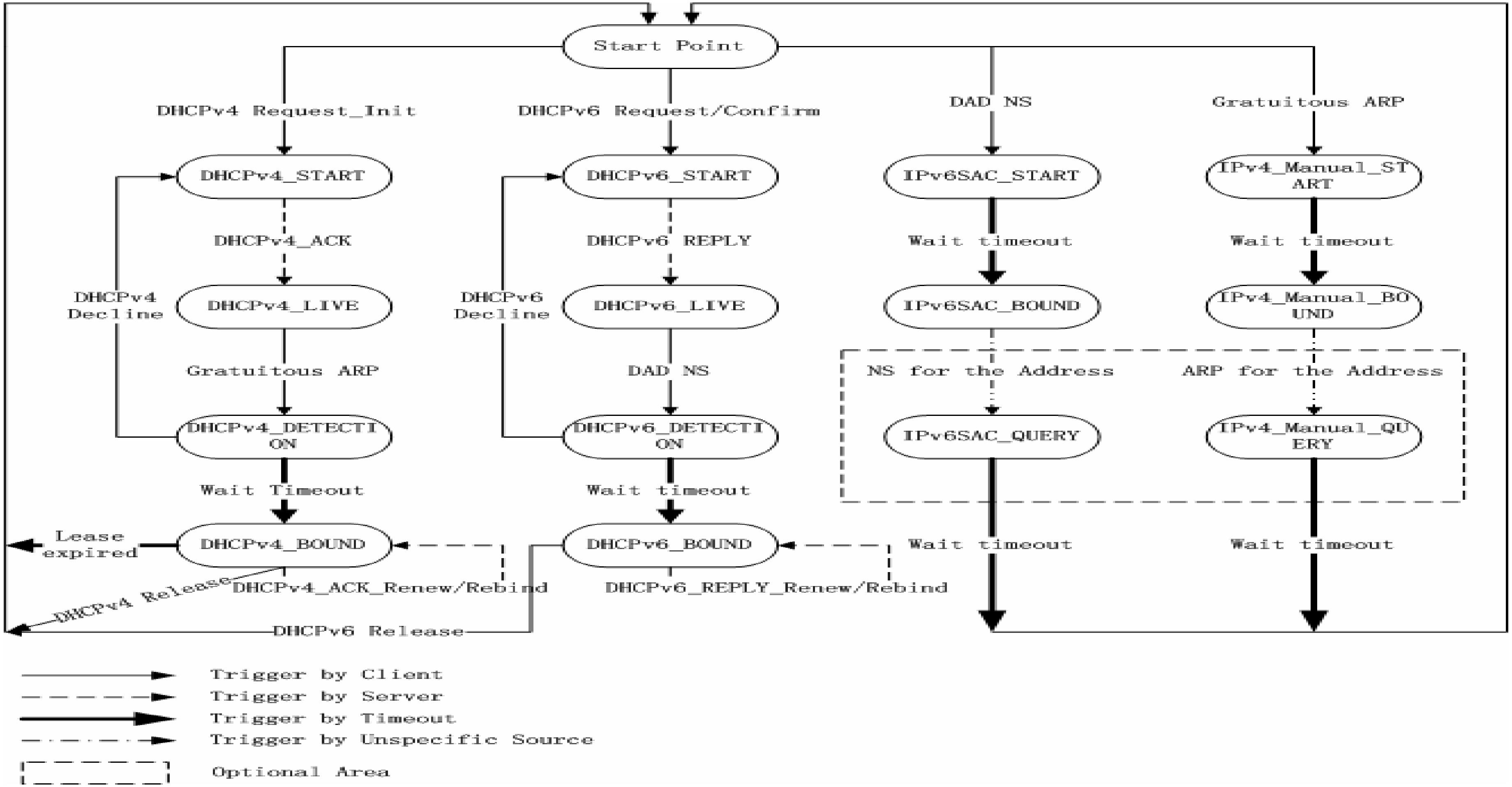
- Benefits
  - Support the existing address assignment standards
  - Don’t need to design a real-time BDP
  - Initial binding based on only control packets not data packets (important advice from some vendors)

Control Packet Snooping

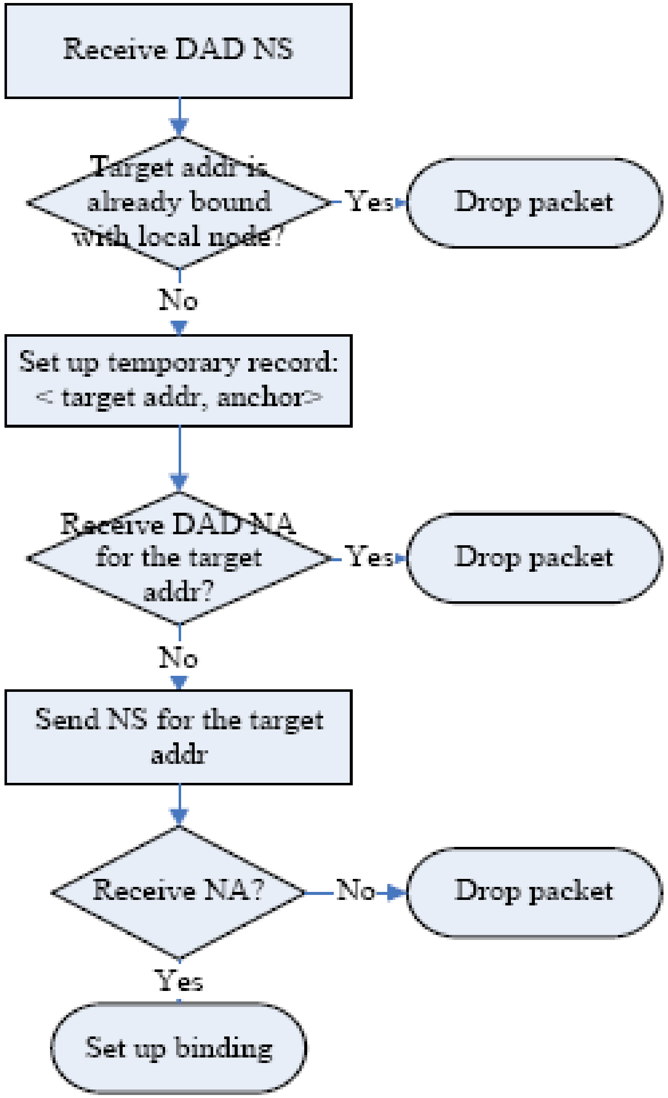
- Which protocols to snoop?
  - DHCP
    - DHCPv4
    - DHCPv6
  - Duplicate Address Detection
  - Gratuitous ARP
- Handle static address
  - Manually bind static address with anchor

Control Packet Snooping

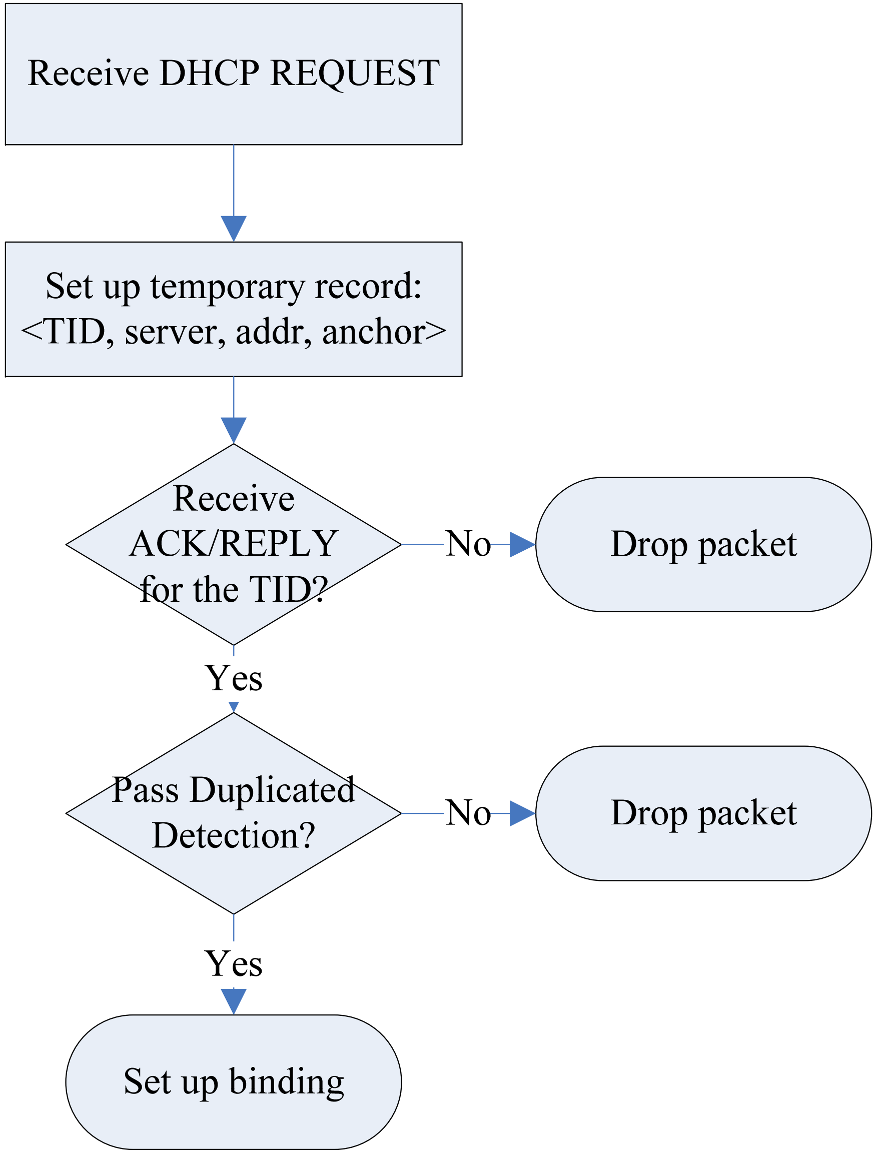
- SAVI Device State Transition Diagram



Example: ND snooping


Receive DAD NS
Target addr is already bound with local node?
Yes
Drop packet
No
Set up temporary record: < target addr, anchor>
Receive DAD NA for the target addr?
Yes
Drop packet
No
Send NS for the target addr
Receive NA?
No
Drop packet
Yes
Set up binding

DHCPv4/v6 snooping



Receive DHCP REQUEST

Set up temporary record:
<TID, server, addr, anchor>

Receive ACK/REPLY for the TID?

No

Drop packet

Yes

Pass Duplicated Detection?

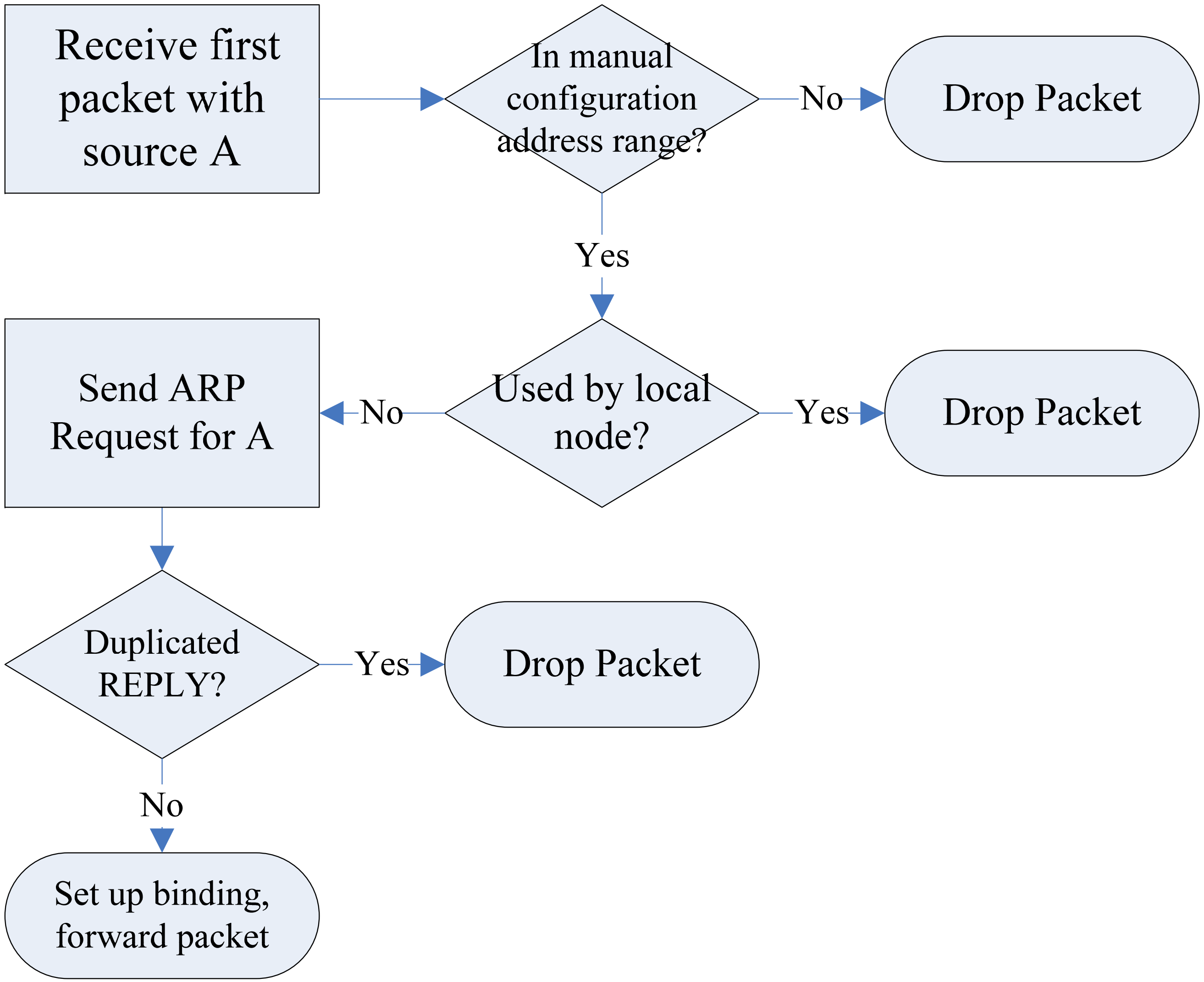
No

Drop packet

Yes

Set up binding

IPv4 binding



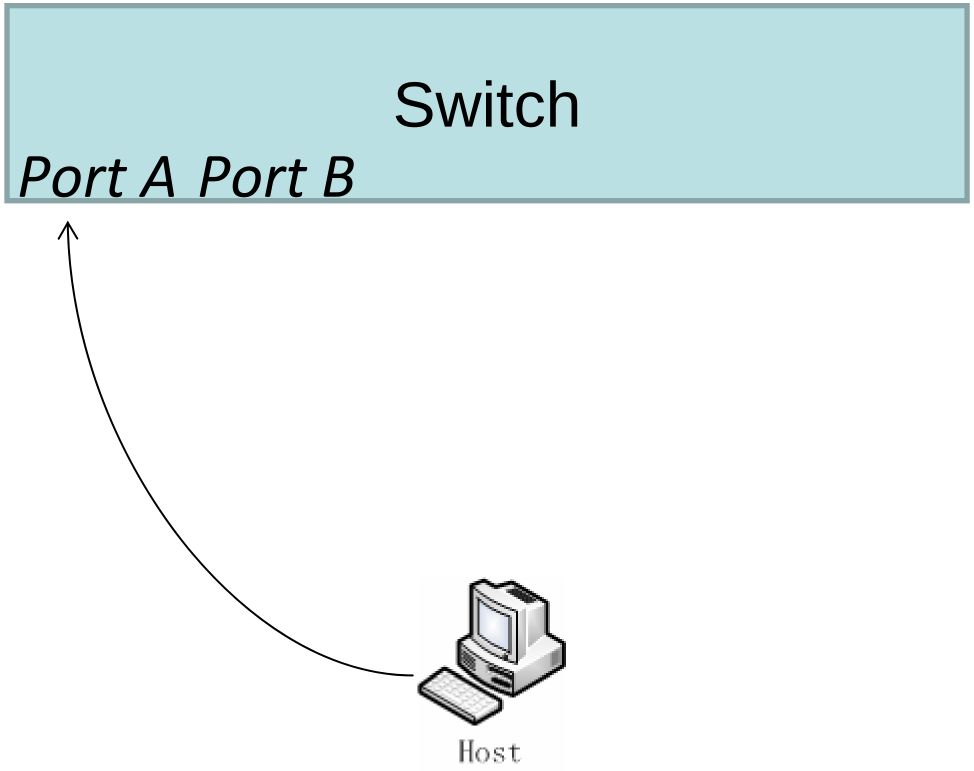
Handle special cases of SAVI

- Two special cases are hard to handle
  - node that move to another port on the same link
    - Static address
    - DHCP/Stateless address will not cause a problem
  - node with multiple interfaces to the same link
- It’s re-binding (a separate question from initial binding)
- It might be handled by many ways
  - SeND, HIP (by using unique id of the host)
  - we also propose a method called “tentative test”

Handle special cases of SAVI

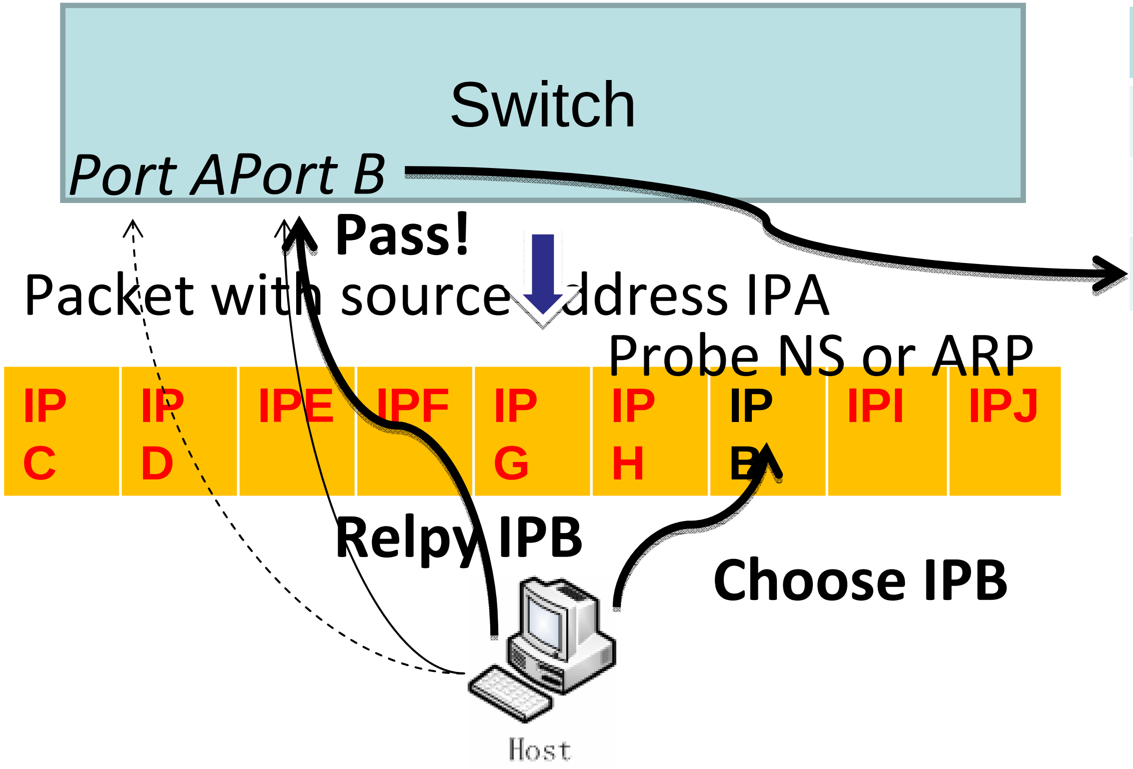
- Tentative test
  - A test to distinguish multiple interfaces to the same LAN and movement of static address from spoofing.
  - Assumption: 2 or more addresses(IPv4 or IPv6) are assigned to an interface of a host
    - Usually works for IPv6
    - Also works for IPV4 if it is a dual-stack node

Movement of static address



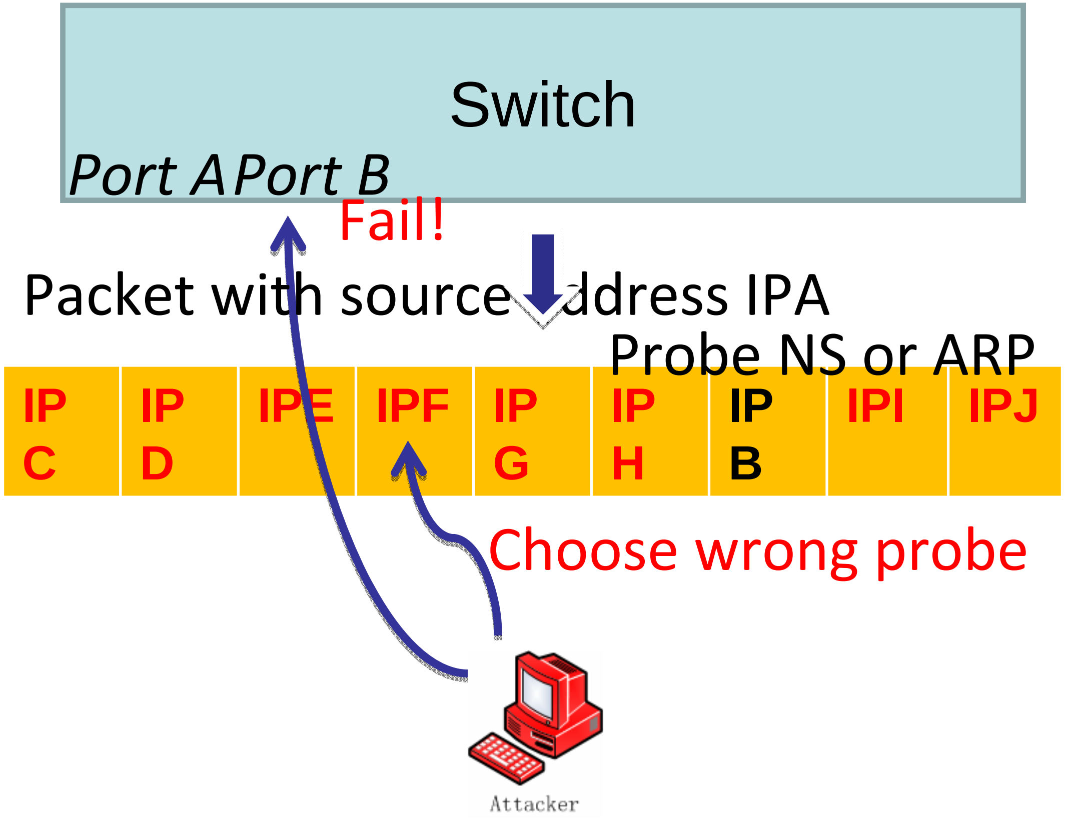
Port-ACL	
Port	Address
A	IPA:Static
A	IPB

Movement of static address



Port-ACL	
Port	Address
A	IPA:Static
A	IPB

Movement of static address



Switch

Port A Port B

Fail!

Packet with source address IPA

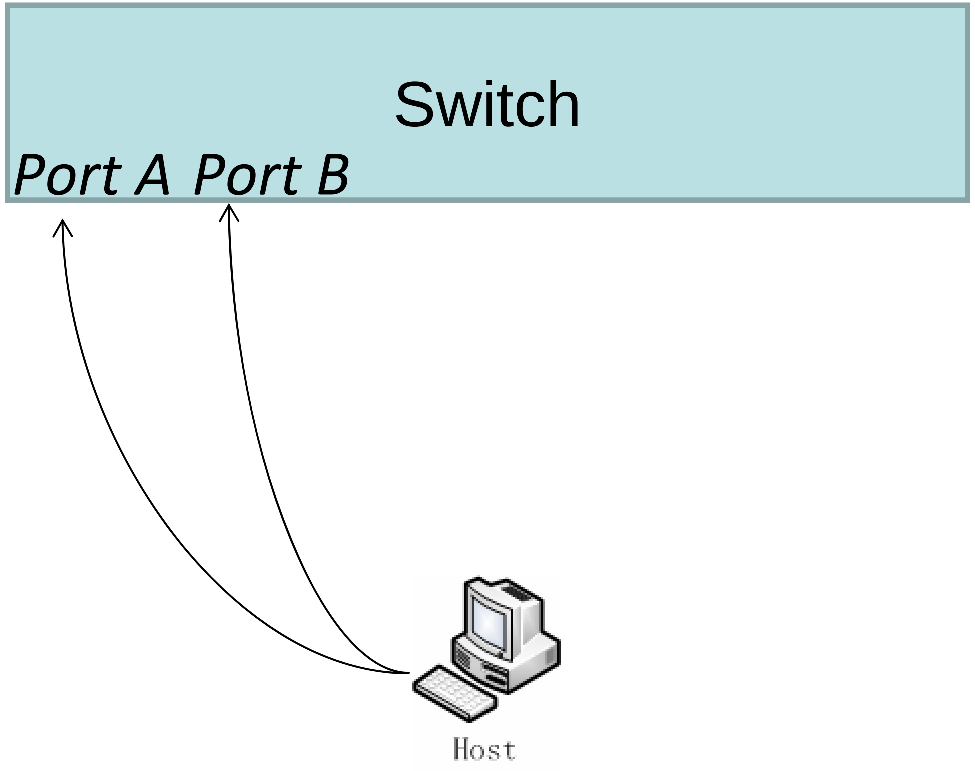
Probe NS or ARP

IP C	IP D	IPE	IPF	IP G	IP H	IP B	IPI	IPJ

Choose wrong probe

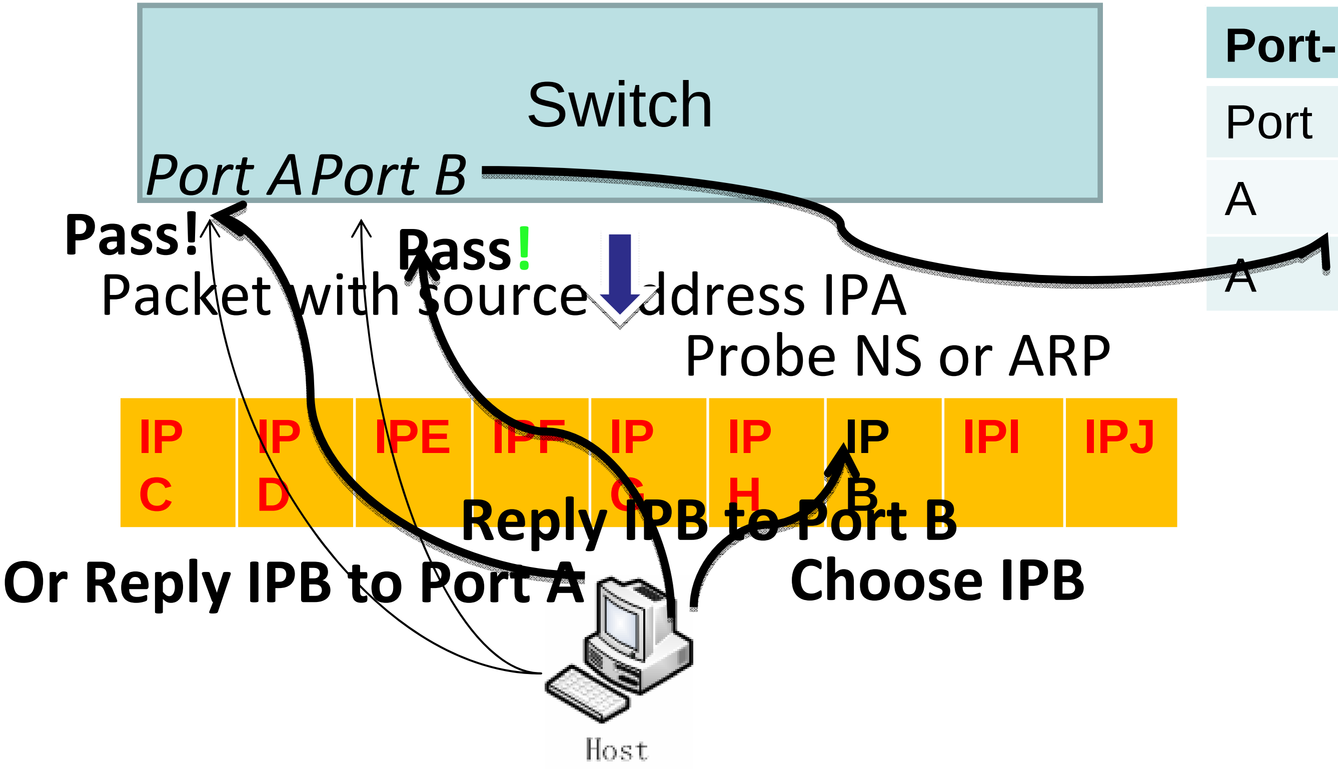
Port-ACL	
Port	Address
A	IPA:Static
A	IPB

Multiple interfaces to the same link



Port-ACL	
Port	Address
A	IPA:Static
A	IPB

Multiple interfaces to the same link



Switch

Port A Port B

Pass!

Pass!

Packet with source address IPA

Probe NS or ARP

IP C

IP D

IPE

IPF

IP G

IP H

IP B

IPI

IPJ

Reply IPB to Port B

Or Reply IPB to Port A

Choose IPB

Port-ACL	
Port	Address
A	IPA:Static
A	IPB

Thank You!

Q & A

Thank You!

Q & A