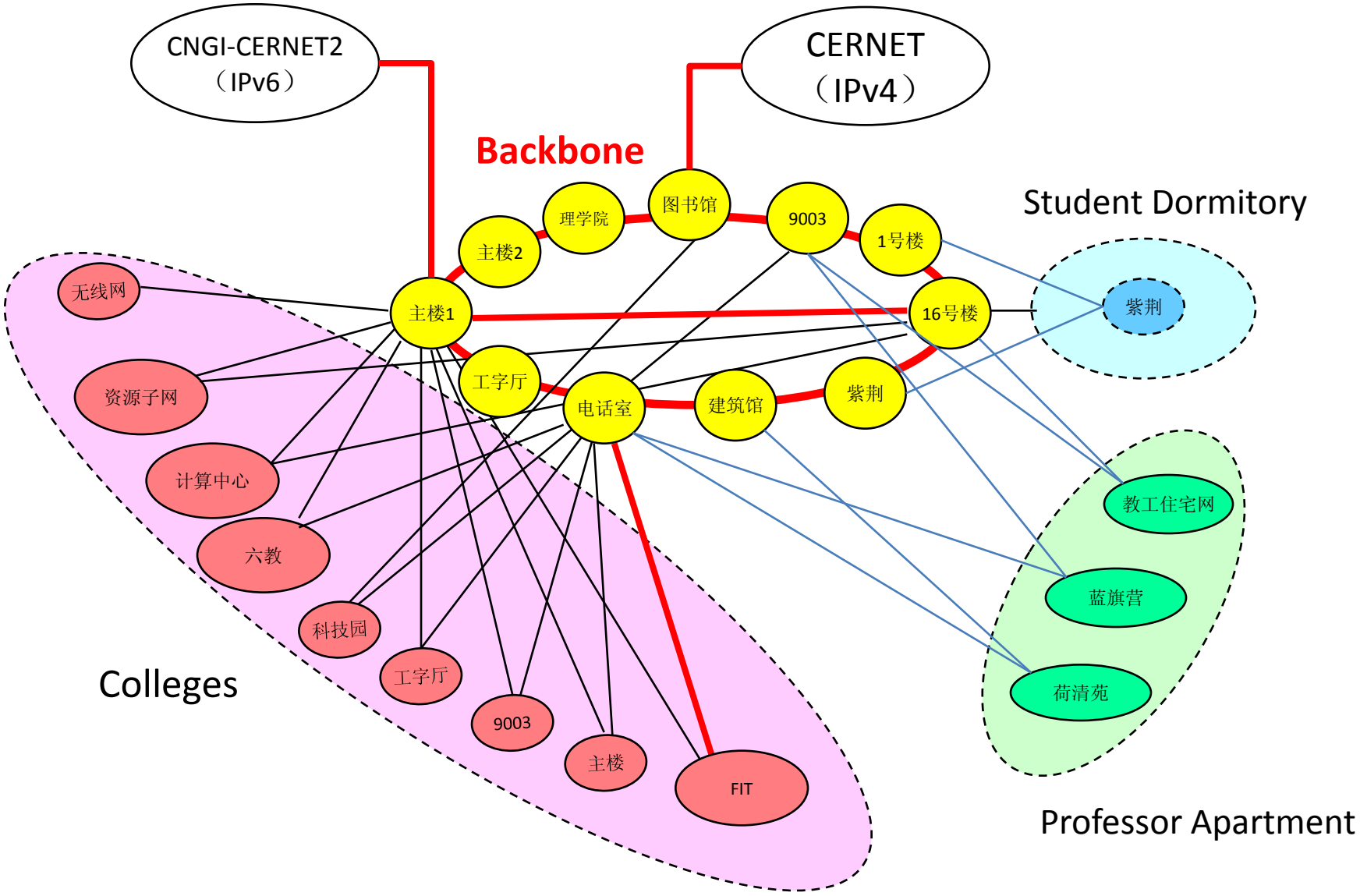
# Operation Notes of IPv6 Network

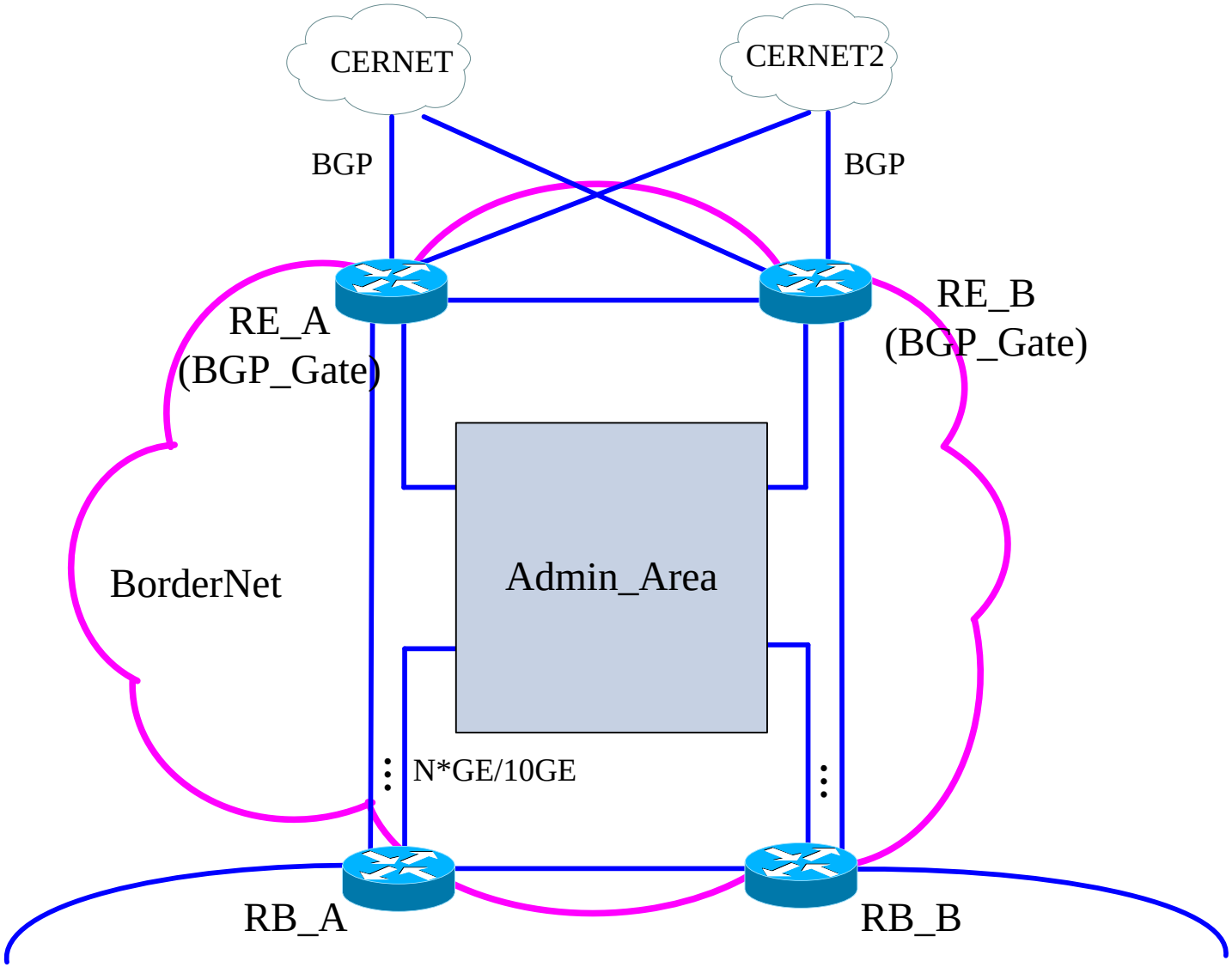
Jilong Wang/Tsinghua University

2010-08

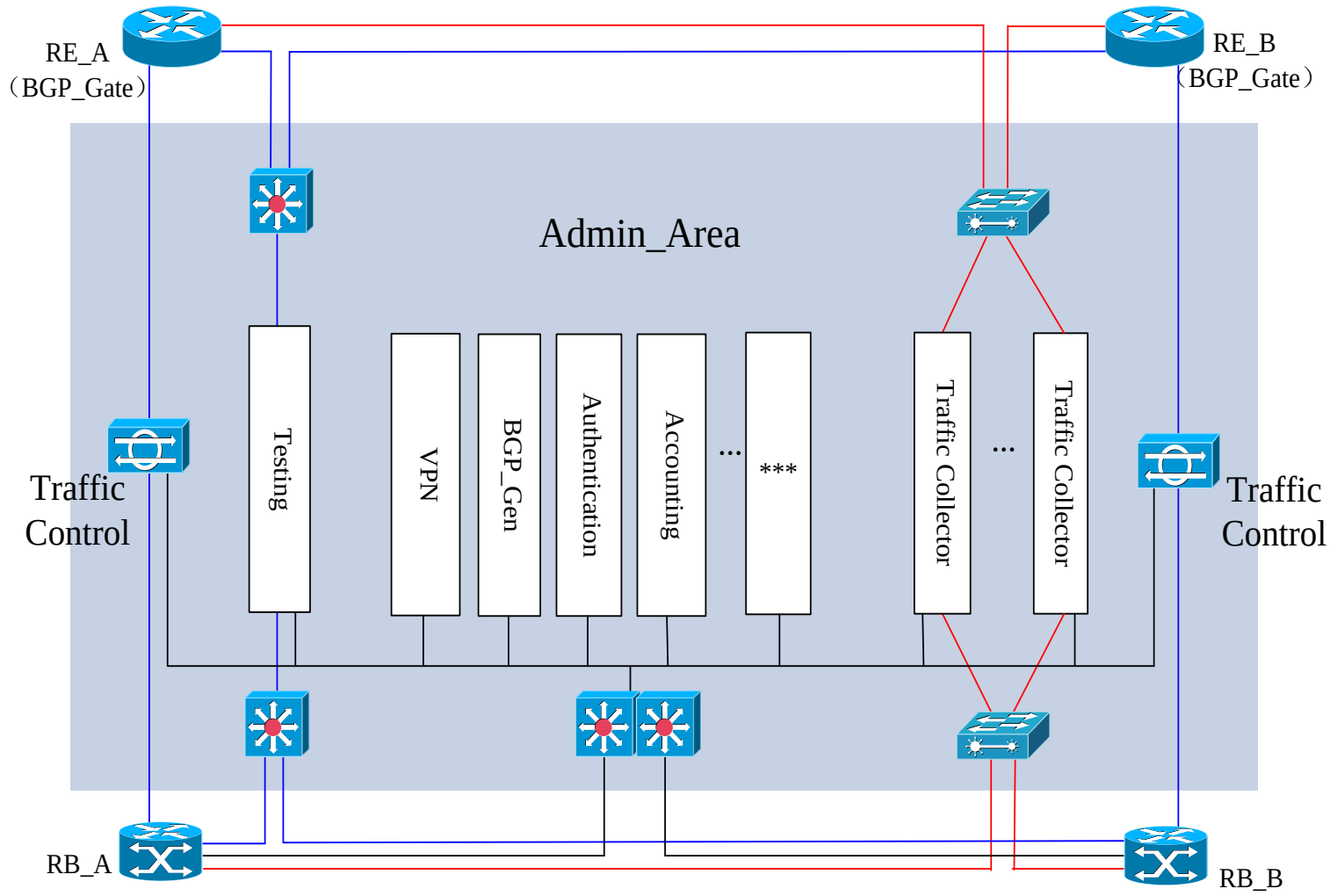
# TUNET


CNGI-CERNET2
（IPv6）
CERNET
（IPv4）
Backbone
理学院
图书馆
9003
1号楼
主楼2
主楼1
16号楼
工字厅
电话室
建筑馆
紫荆
Student Dormitory
紫荆
无线网
资源子网
计算中心
六教
科技园
工字厅
9003
主楼
FIT
Colleges
教工住宅网
蓝旗营
荷清苑
Professor Apartment

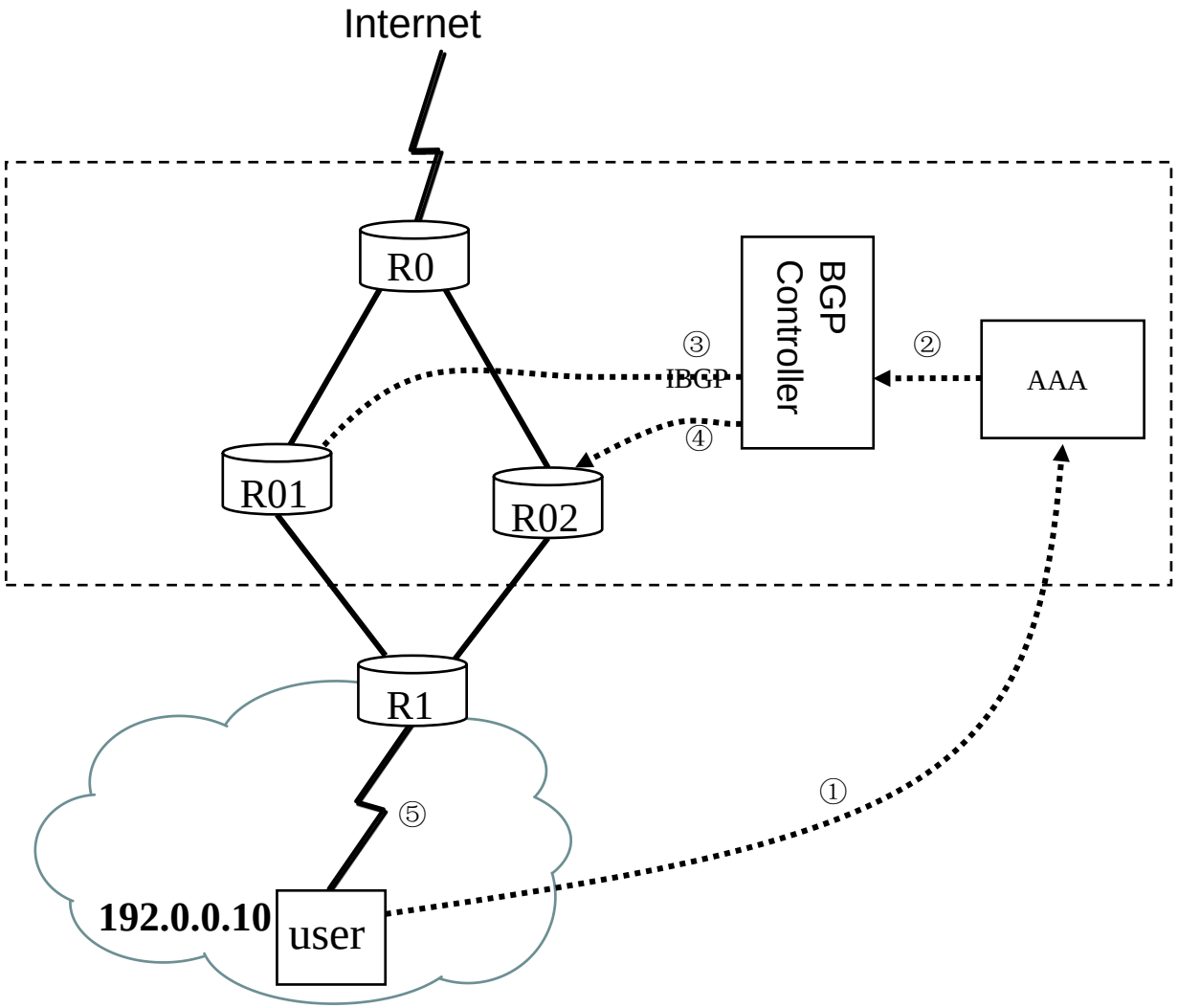
# Border Network



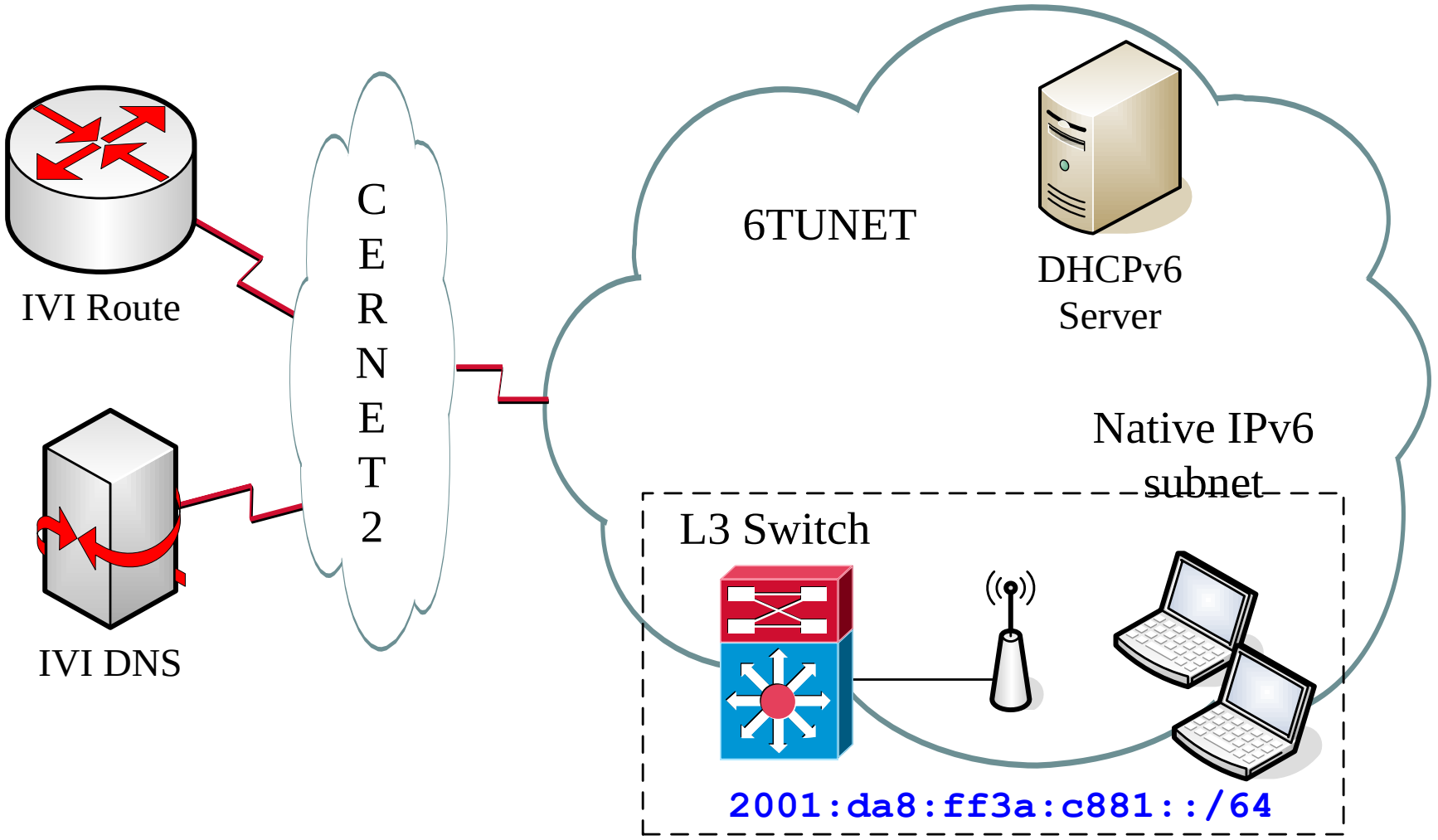
# Admin_Area


RE_A
（BGP_Gate）
RE_B
（BGP_Gate）
Admin_Area
Testing
VPN
BGP_Gen
Authentication
Accounting
...
***
Traffic Collector
...
Traffic Collector
Traffic
Control
Traffic
Control
RB_A
RB_B

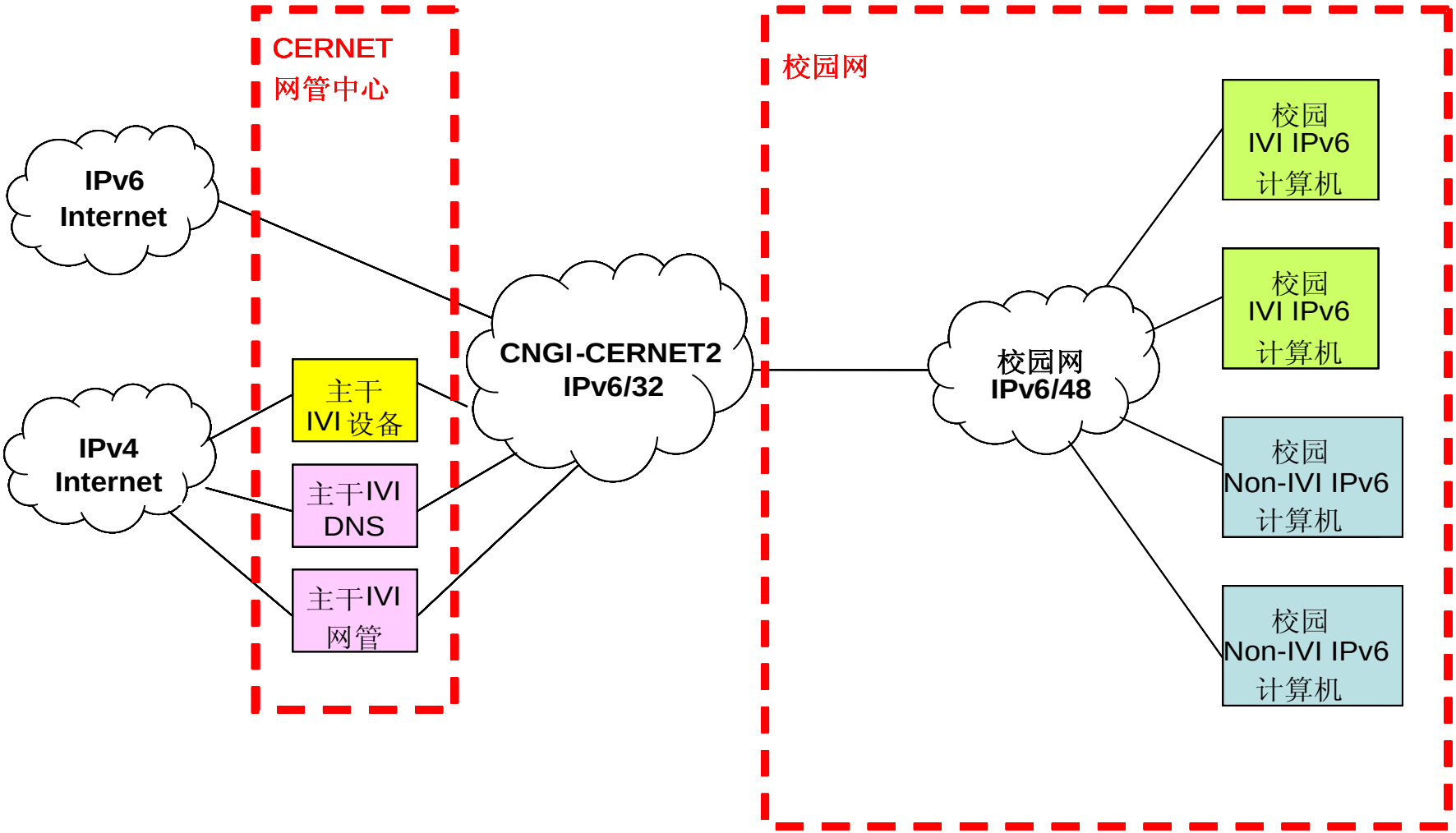
# BGP Gateway


Internet
R0
BGP Controller
③
IBGP
②
AAA
④
R01
R02
R1
⑤
①
192.0.0.10
user

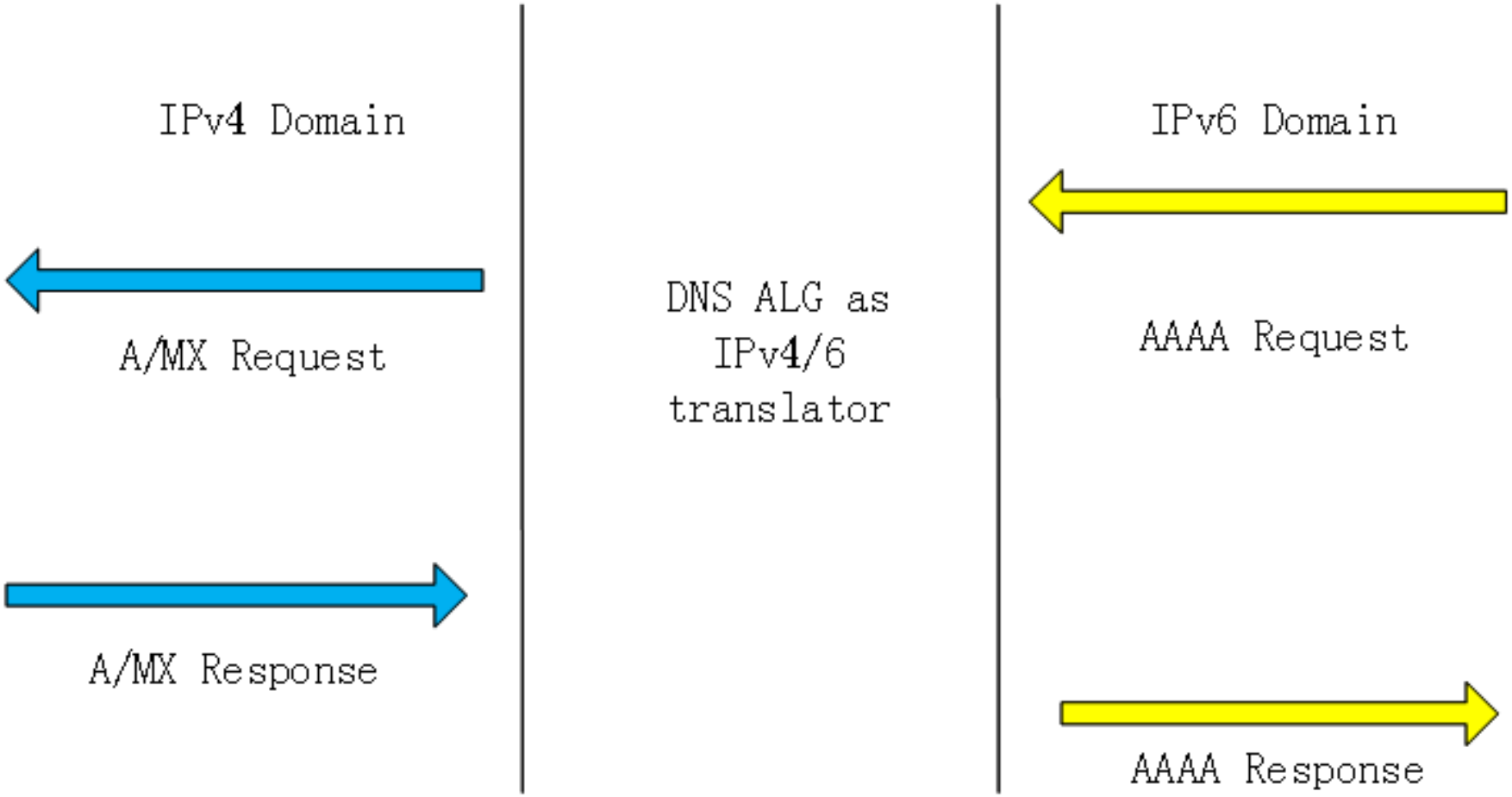
# A Pure IPv6 Network



# IVI


CERNET
网管中心
IPv6
Internet
IPv4
Internet
主干
IVI 设备
主干IVI
DNS
主干IVI
网管
CNGI-CERNET2
IPv6/32
校园网
校园网
IPv6/48
校园
IVI IPv6
计算机
校园
IVI IPv6
计算机
校园
Non-IVI IPv6
计算机
校园
Non-IVI IPv6
计算机

# IVI DNS


IPv4 Domain
A/MX Request
A/MX Response
DNS ALG as
IPv4/6
translator
IPv6 Domain
AAAA Request
AAAA Response

# Plug&play pure IPv6 based on IVI

- DHCPv6 Server (ISC DHCP4.1.1-P1)

```
subnet6 2001:da8:ff3a:c881::/64 {
    range6 2001:da8:ff3a:c881:200:: 2001:da8:ff3a:c881:200::;
    range6 2001:da8:ff3a:c881:300:: 2001:da8:ff3a:c881:300::;
    ... ...
    range6 2001:da8:ff3a:c881:fe00:: 2001:da8:ff3a:c881:fe00::;
    option dhcp6.name-servers 2001:250:aaa0:100:1::2;
    option dhcp6.domain-search "v6.tsinghua.edu.cn";
    }
```

# Plug&play pure IPv6 based on IVI

- Router (Cisco 7609， maybe different by IOS version)

  interface Vlan30

  no ip address

  ipv6 address 2001:DA8:FF3A:C881:100::/64

  ipv6 enable

  ipv6 nd prefix default 2592000 604800 no-autoconfig

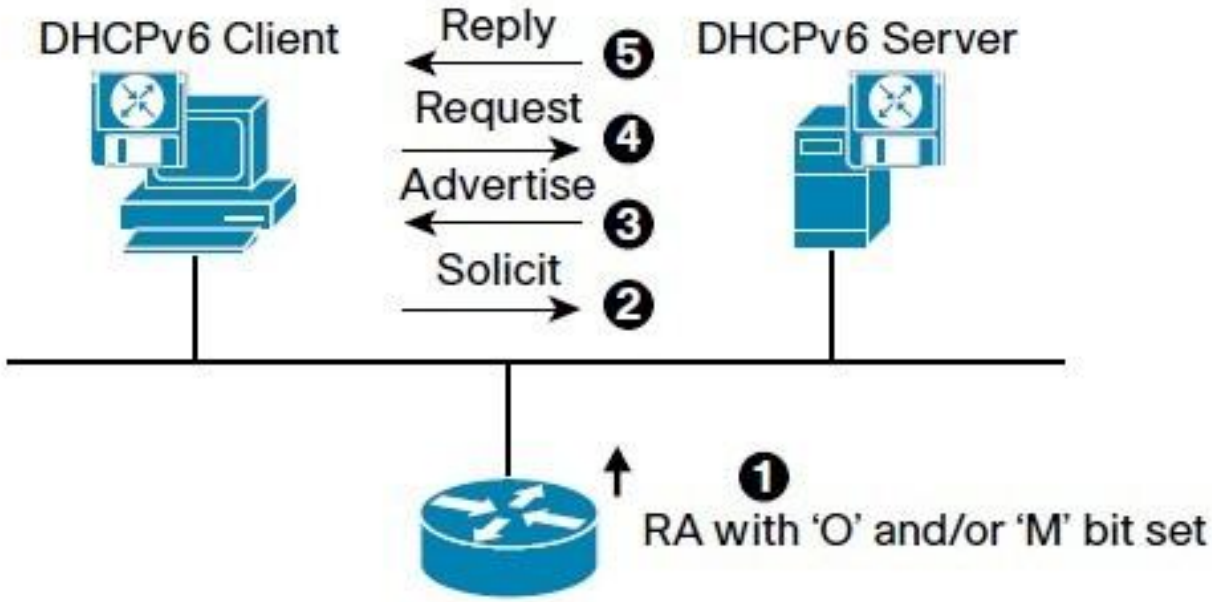
  ipv6 nd managed-config-flag

  ipv6 nd other-config-flag

  ipv6 nd ra suppress

  ipv6 dhcp relay destination 2402:F000:1:901::9:8

# RFC 3315 DHCP for IPv6




•'O' bit—When this bit is set, the client can use DHCPv6 to retrieve Other configuration parameters (ie: DNS addresses)

• 'M' bit—When this bit is set, the client may use DHCPv6 to retrieve a Managed IPv6 address from a DHCPv6 server

# Plug&play pure IPv6 based on IVI

- Client
  - Win7
    - Get DHCP IVI6 address by default
  - Windows XP
    - Dibbler 0.7.3
    - Configuration file:

```
iface “wireless interface" {
 ia
 option dns-server
 option domain }
```

# Plug&play pure IPv6 based on IVI

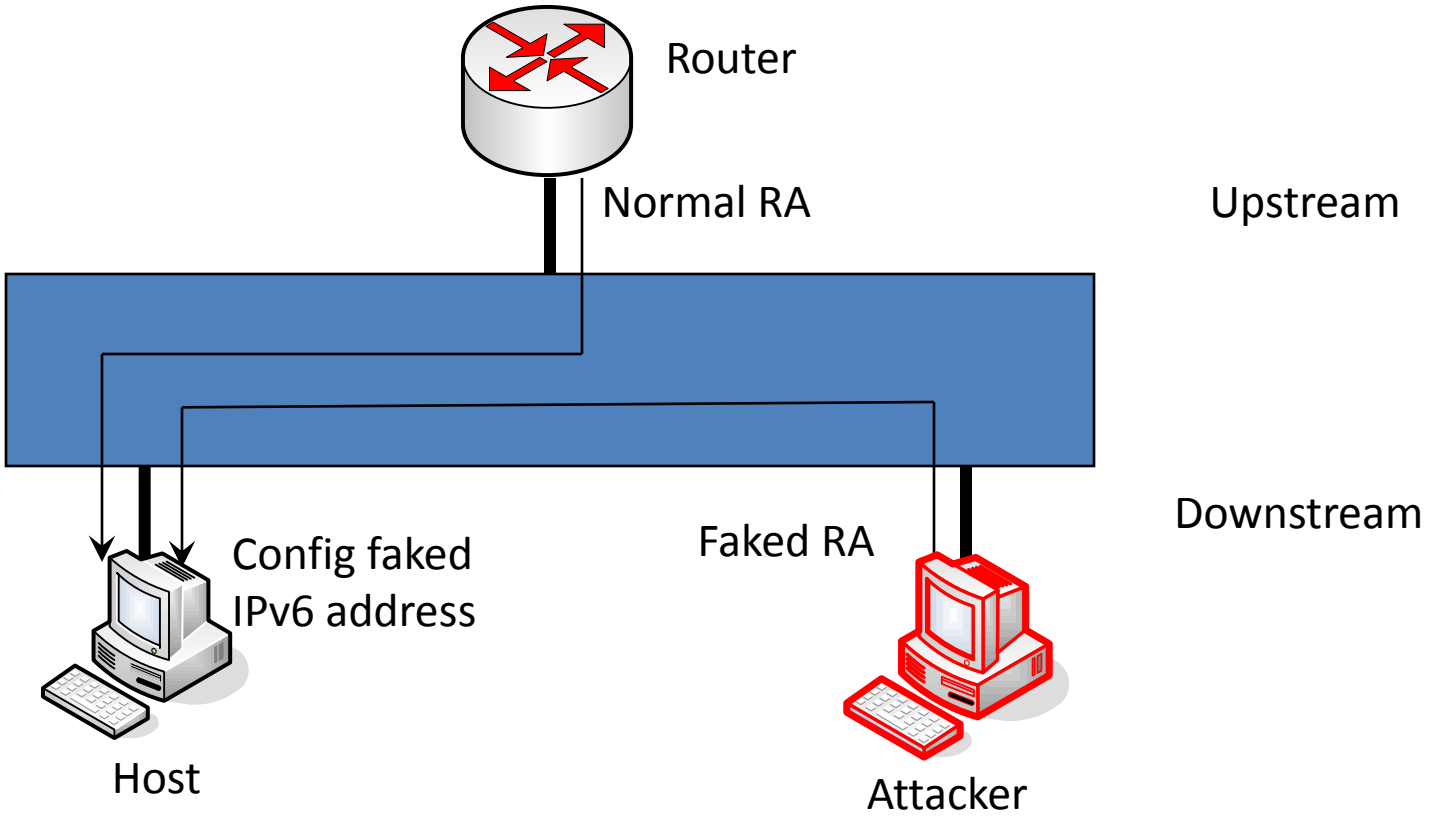
- Win7


- Windows XP

# IPv6 RA Spoofing Attack

- RA:
  - Router Advertisement in IPv6
  - Used for address autoconfiguration by hosts
- RA spoofing attack:
  - Faked RA from downstream ports of a switch
  - Host:
    - Address autoconfiguration according to faked RA
    - This Address cannot be used to access the Internet

# IPv6 RA Spoofing Attack



# The Weakness of RA Spoofing

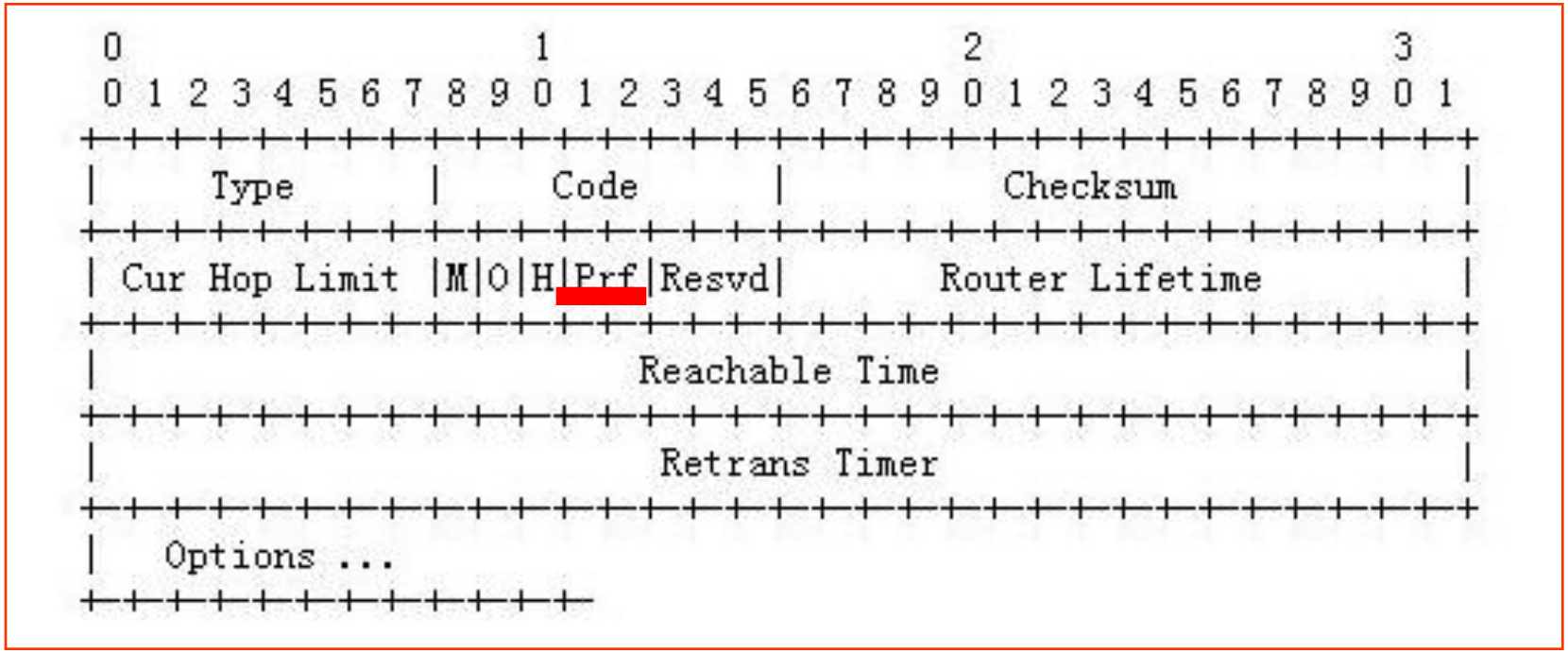
- Router may send RA packet from time to time, thus attacker have to send spoofing RA packet at regular intervals

| N | Time | MAC Source | MAC Destination | Frame | Protocol |
|---|---|---|---|---|---|
| 1 | 08:25:03.171 | 00:23:89:11:C5:00 | 33:33:00:00:00:01 | IPv6 | ICMPV6->Router Advertisement |
| 6 | 08:26:28.984 | 00:23:89:11:C5:00 | 33:33:00:00:00:01 | IPv6 | ICMPV6->Router Advertisement |
| 4 | 08:26:41.281 | 00:23:89:11:C5:00 | 33:33:00:00:00:01 | IPv6 | ICMPV6->Router Advertisement |
| 6 | 08:26:45.062 | 00:23:89:11:C5:00 | 33:33:00:00:00:01 | IPv6 | ICMPV6->Router Advertisement |
| 12 | 08:27:48.343 | 00:23:89:11:C5:00 | 33:33:00:00:00:01 | IPv6 | ICMPV6->Router Advertisement |
| 20 | 08:28:32.796 | 00:23:89:11:C5:00 | 33:33:00:00:00:01 | IPv6 | ICMPV6->Router Advertisement |
| 26 | 08:28:53.468 | 00:23:89:11:C5:00 | 33:33:00:00:00:01 | IPv6 | ICMPV6->Router Advertisement |
| 27 | 08:28:56.859 | 00:23:89:11:C5:00 | 33:33:00:00:00:01 | IPv6 | ICMPV6->Router Advertisement |
| 28 | 08:29:00.234 | 00:23:89:11:C5:00 | 33:33:00:00:00:01 | IPv6 | ICMPV6->Router Advertisement |
| 30 | 08:29:03.515 | 00:23:89:11:C5:00 | 33:33:00:00:00:01 | IPv6 | ICMPV6->Router Advertisement |
| 11 | 08:29:31.265 | 00:23:89:11:C5:00 | 33:33:00:00:00:01 | IPv6 | ICMPV6->Router Advertisement |
| 13 | 08:29:35.250 | 00:23:89:11:C5:00 | 33:33:00:00:00:01 | IPv6 | ICMPV6->Router Advertisement |
| 14 | 08:29:38.937 | 00:23:89:11:C5:00 | 33:33:00:00:00:01 | IPv6 | ICMPV6->Router Advertisement |
| 15 | 08:29:42.218 | 00:23:89:11:C5:00 | 33:33:00:00:00:01 | IPv6 | ICMPV6->Router Advertisement |

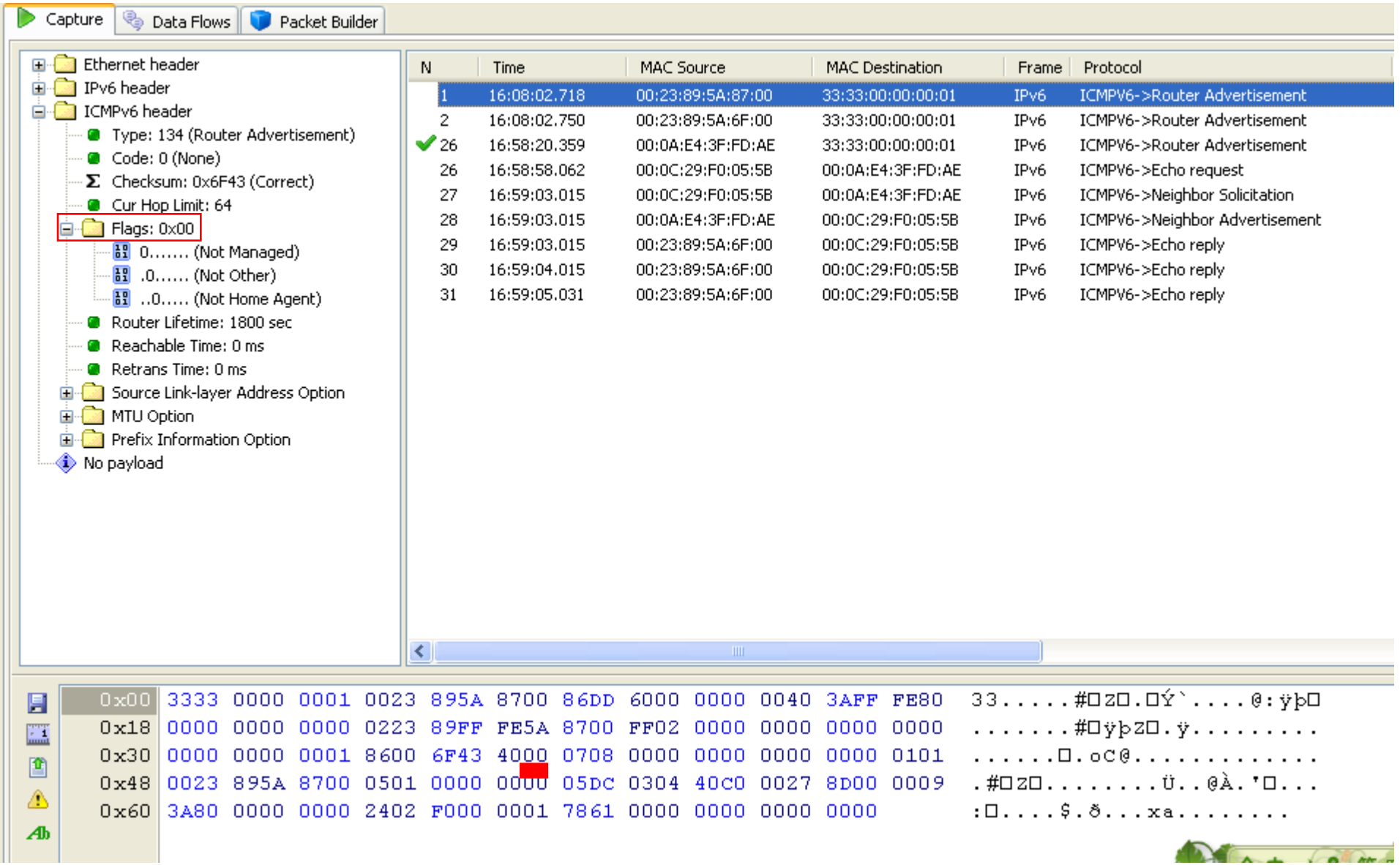
# Router Preferences

RFC4191

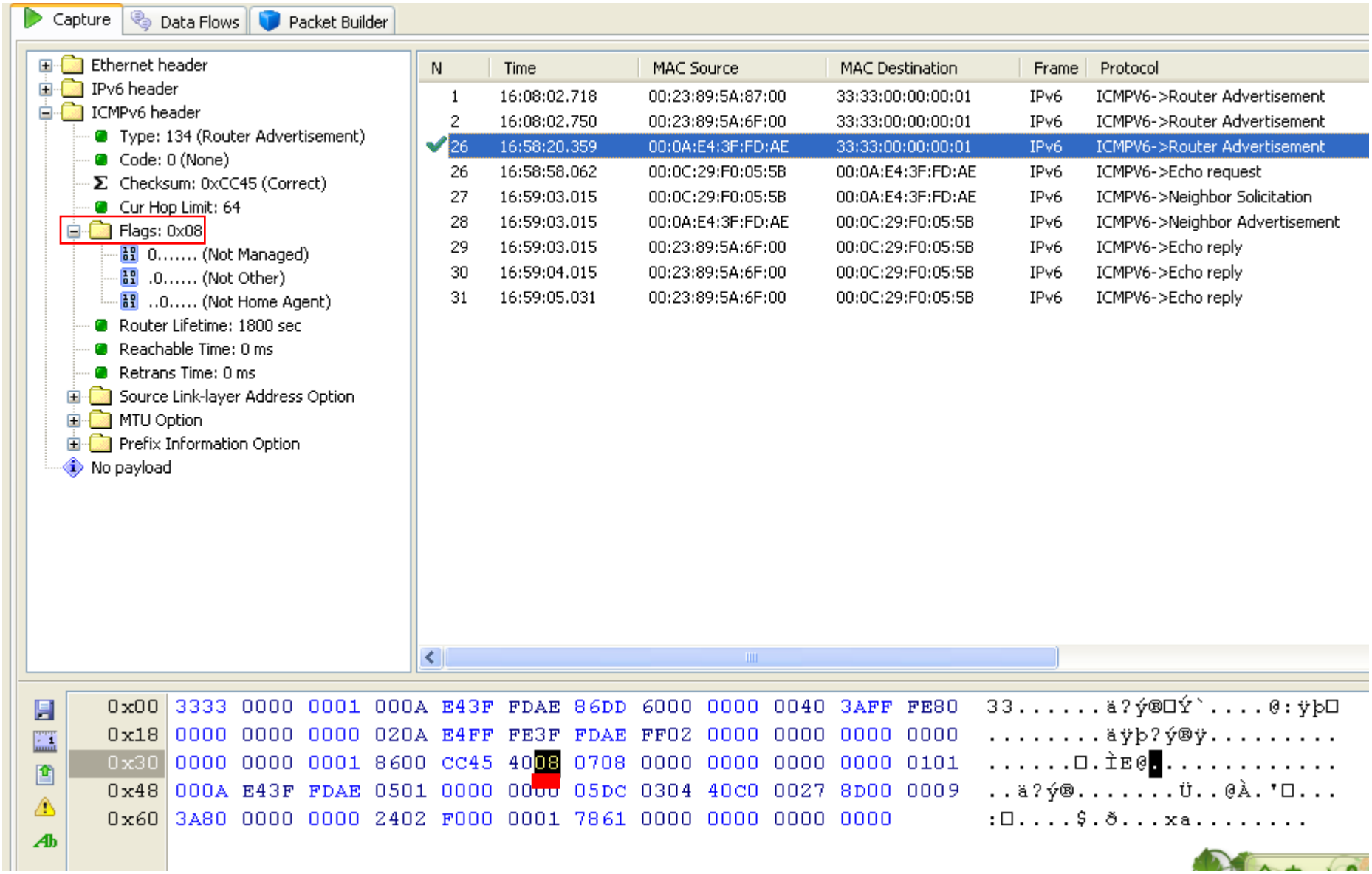
| | |
|---|---|
| 01 | High |
| 00 | Medium (default) |
| 11 | Low |
| 10 | Reserved - MUST NOT be sent |



# RA packet sent by router： RP bit is 00， Medium (default)



# Spoofing RA packet： RP is 01， high



By spoofing RA, we inject a route on target host

```
C:\Documents and Settings\Administrator>ipv6 rt
::/0 -> 6/fe80::20a:e4ff:fe3f:fdae pref 16 life 29m57s (autoconf)
2001:da8:200:900e::/64 -> 2 pref 1if+8=9 life 29d23h59m24s (autoconf)
::/0 -> 2/fe80::5efe:59.66.4.50 pref 1if+256=257 life 29m24s (autoconf)
::/0 -> 6/fe80::223:89ff:fe5a:8700 pref 256 life 29m20s (autoconf)
2402:f000:1:7861::/64 -> 6 pref 8 life 29d23h59m57s (autoconf)
::/0 -> 6/fe80::223:89ff:fe5a:6f00 pref 256 life 29m20s (autoconf)
```

The preference of spoofing route is high. It exist together with the route advertised by router. However, the target host will select high preference route.

```
C:\Documents and Settings\Administrator>ping ipv6.beijing2008.cn

Pinging ipv6.beijing2008.cn [2001:252:0:1::2008:6] with 32 bytes of data:

Request timed out.
Reply from 2001:252:0:1::2008:6: time=1ms
Reply from 2001:252:0:1::2008:6: time<1ms
Reply from 2001:252:0:1::2008:6: time=1ms

Ping statistics for 2001:252:0:1::2008:6:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

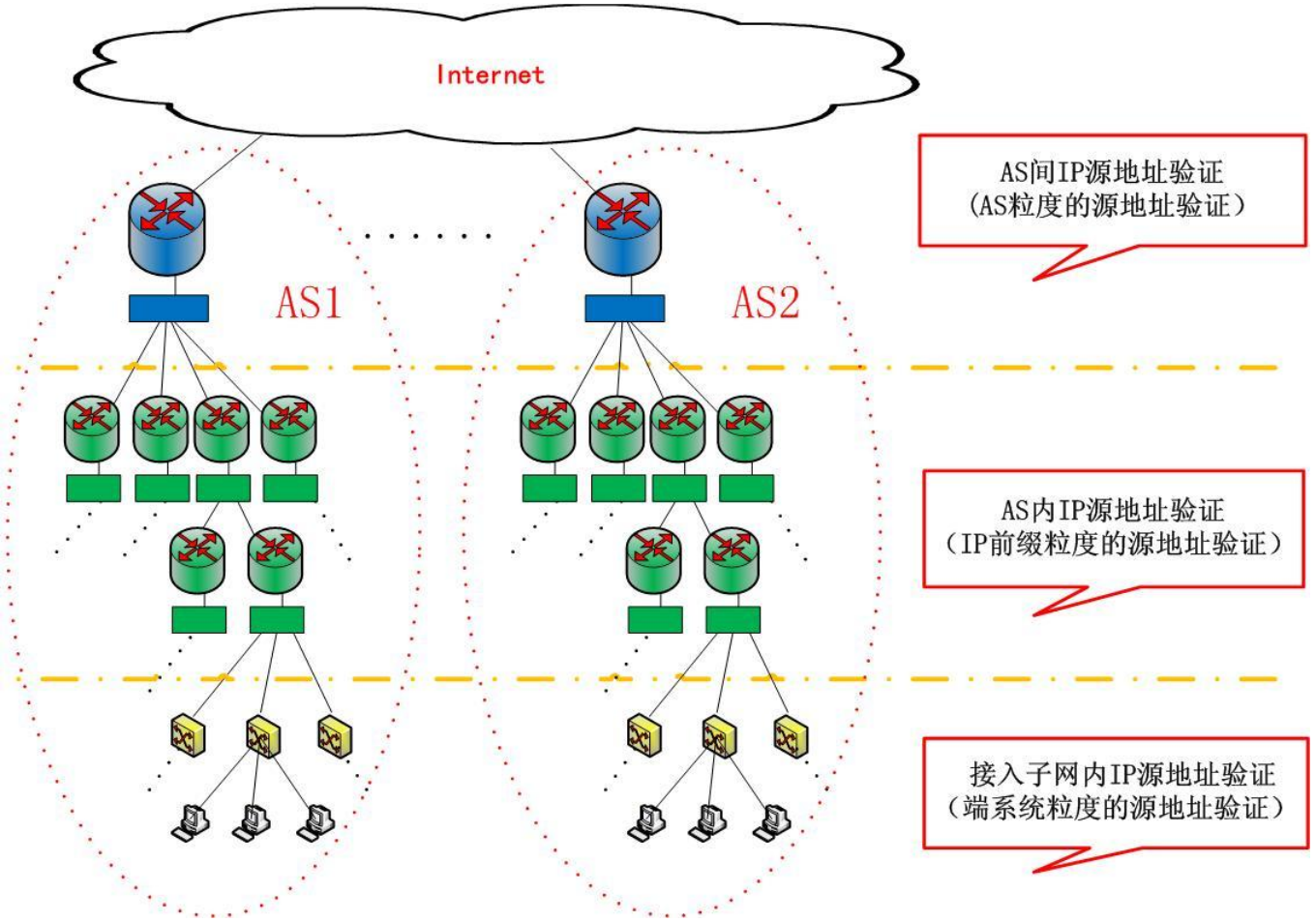
# Notes

- RFC4861（Neighbor Discovery for IP version 6 ) ask router set RP to 00
- But end system like windows support RFC 4191

# Preventing RA Spoofing Attack

- SAVI switch:
  - Source Address Validation Improvements
  - Standardized by IETF SAVI workgroup
- CLI
  - Global mode
    - ipv6 ndp snooping enable
  - Interface mode: SAVI-RA-Trust port
    - ipv6 ra trust
    - RA not received from a SAVI-RA-Trust port MUST be discarded.

# IPv6 SAVI

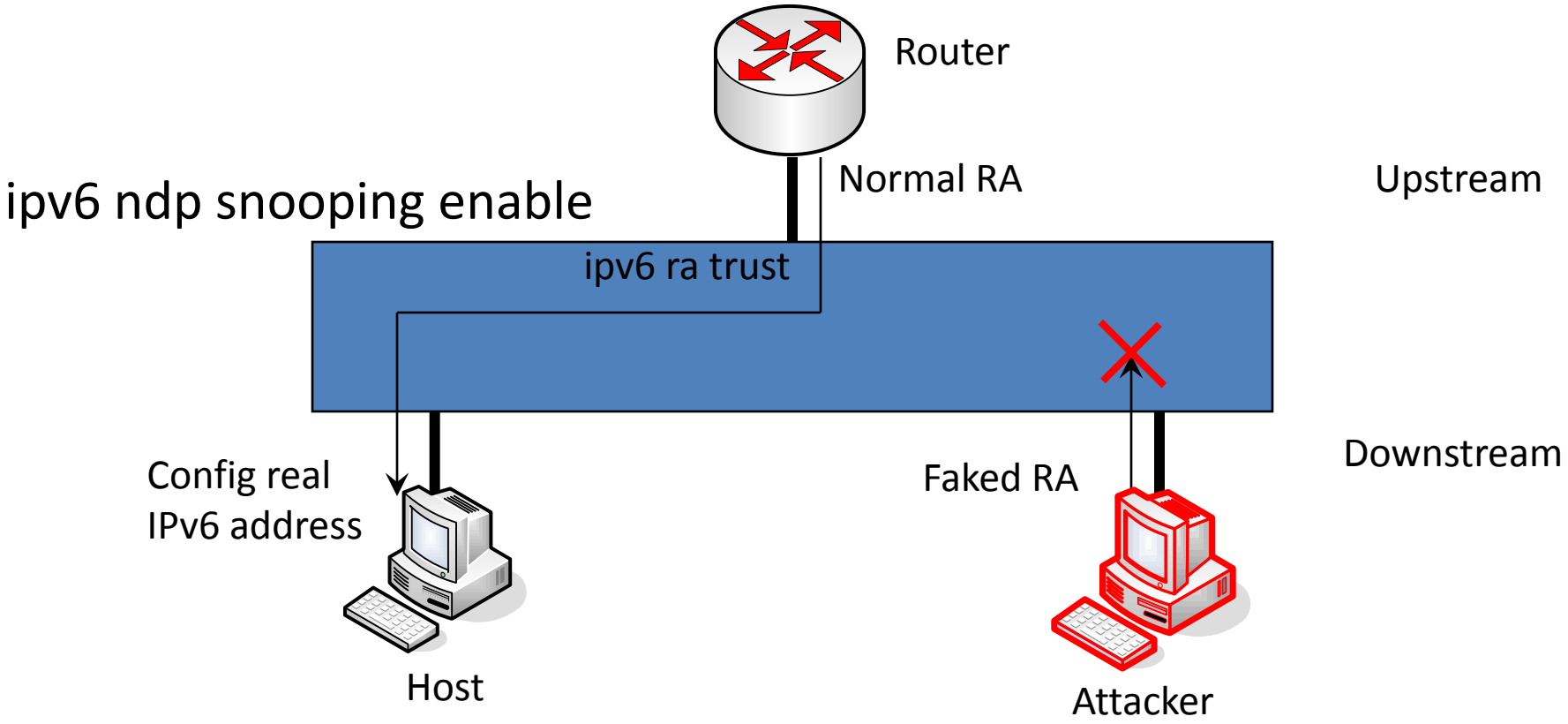



J. Wu, J. Bi, X. Li, G. Ren, K. Xu, RFC 5210 (SAVA)

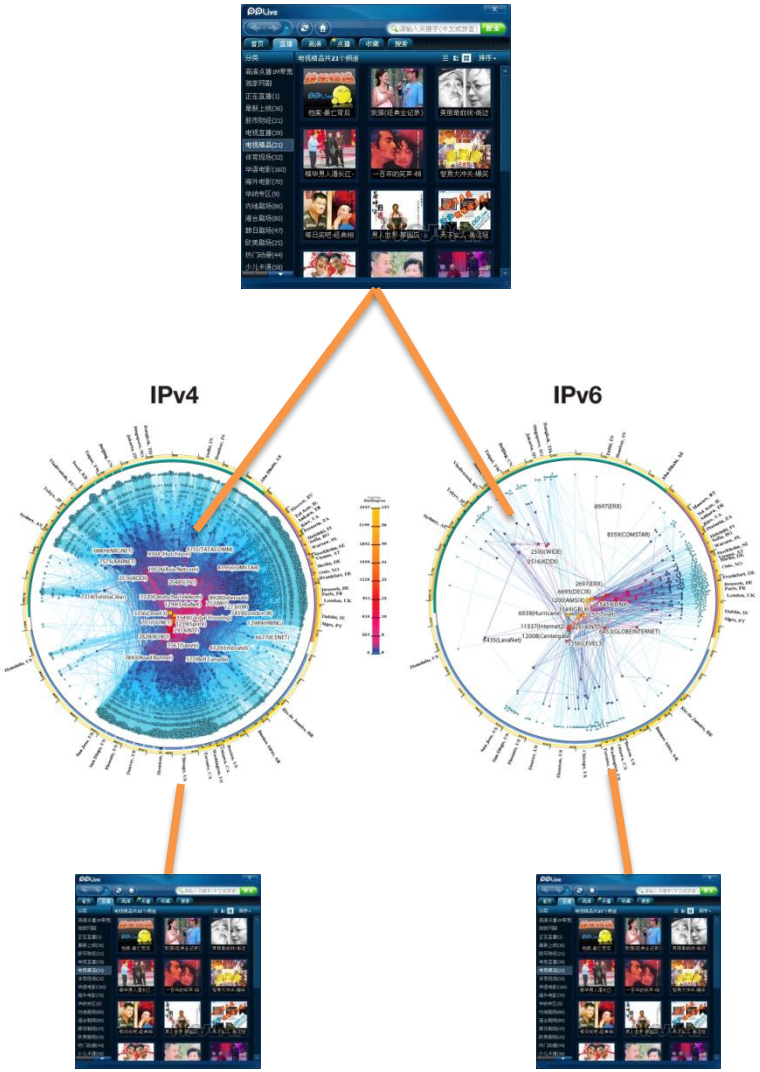
# SAVI: 接入子网源地址验证

- basics：
  - DHCPv6，SLAAC
  - Produce port binding by listening control packet
  - DHCPv6
    - DHCPv6 Request/Reply
    - DHCPv6 Renew/Rebind/Release/Decline
  - SLAAC: StateLess Address AutoConfiguration
    - DAD NS: Neighbor Solicitation
      - Duplicate Address Detection

# Preventing RA Spoofing Attack



# IPv6 Resources

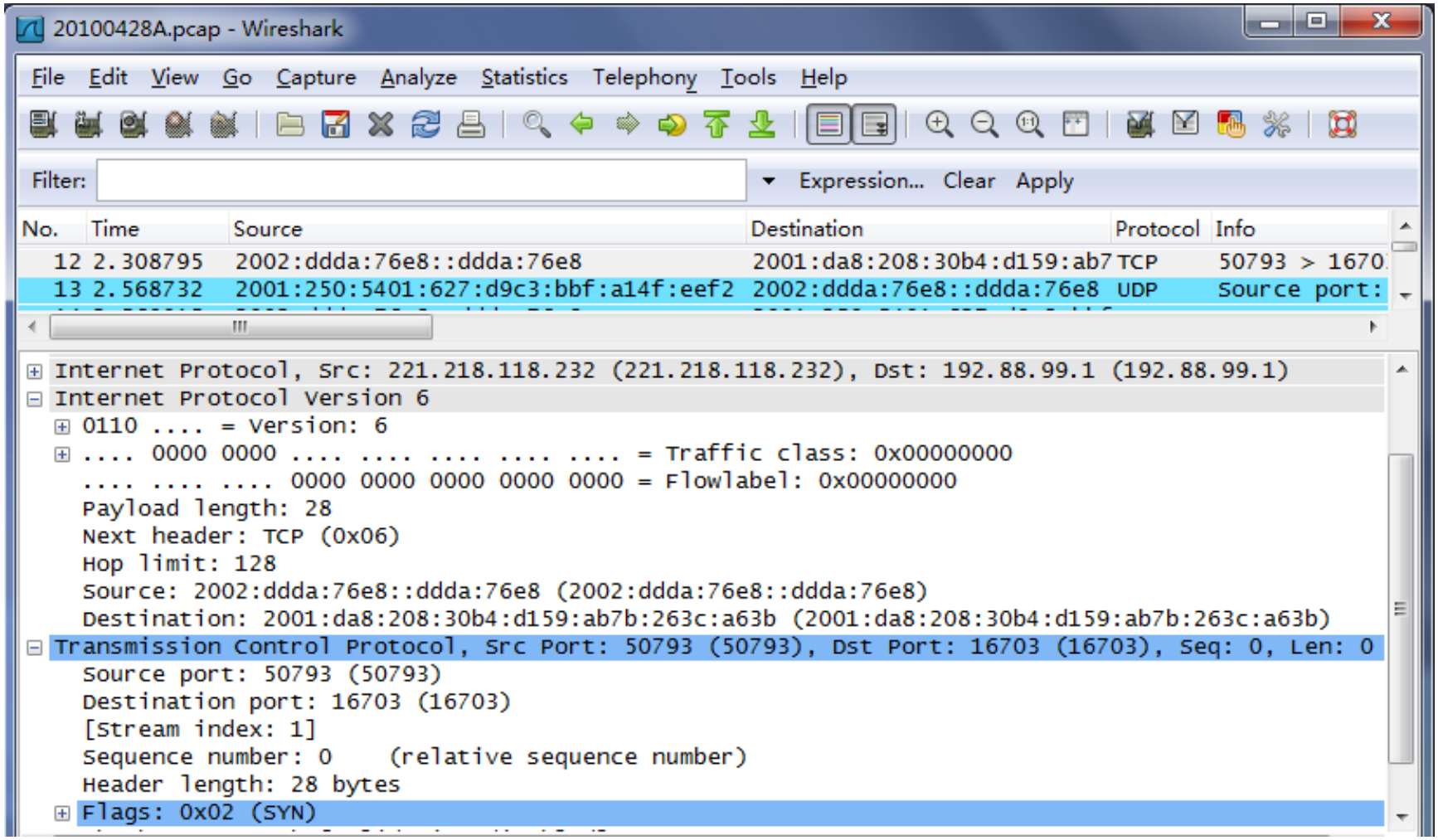



- Dual-Stack Resources：for the convenience of IPv6 users
- Pure IPv6 Resource：attract IPv6 users
- There is risk for dual stack resources！ ！ ！

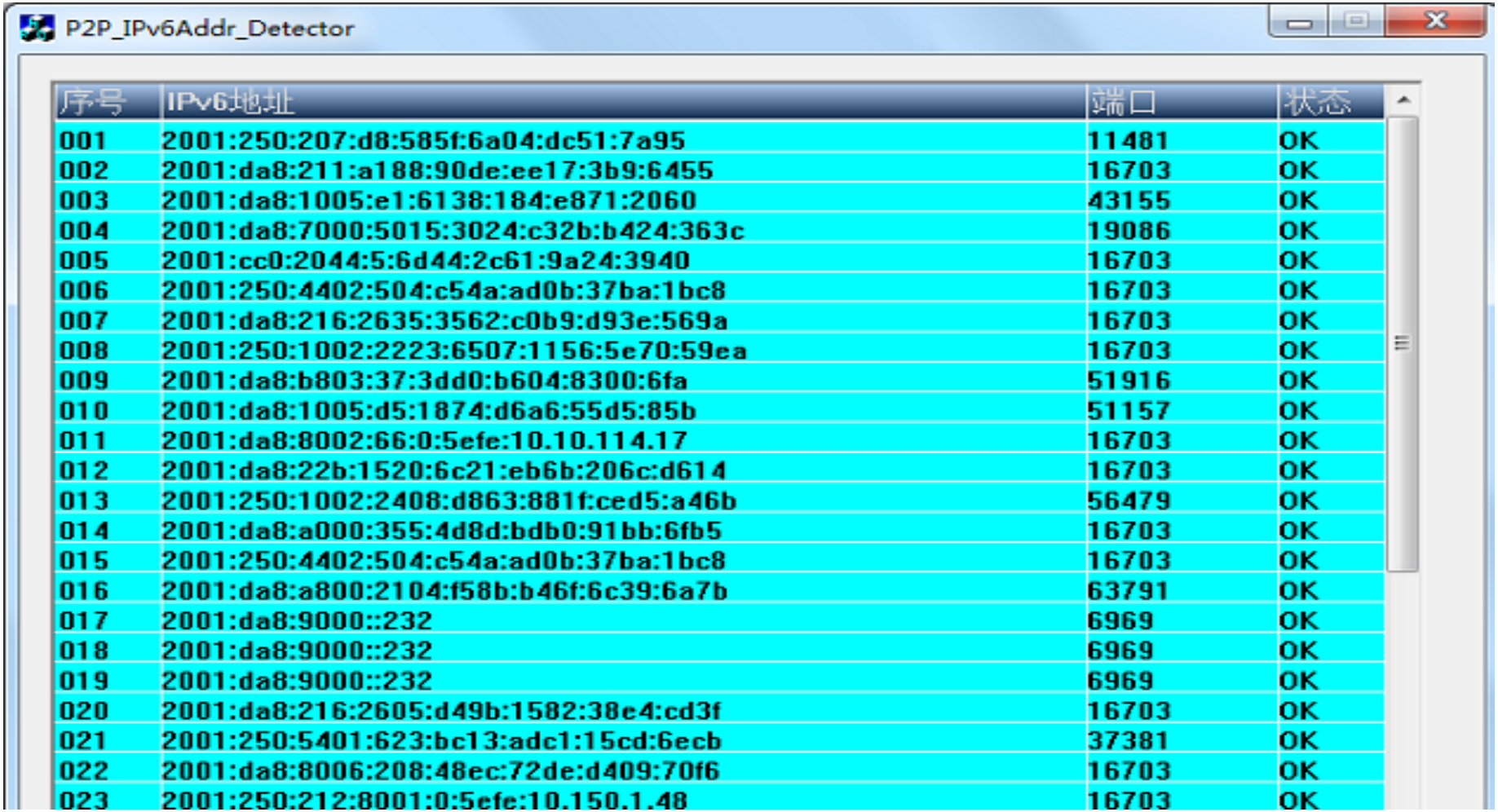
# Scan IPv6 Network

- Scan is always the first step for attacking
- But in IPv6 world, it is hard to scan even a /64 LAN !!!
- We try to scan IPv6 hosts through overlay network like P2P
- We study the problem on uTorrent(www.utorrent.com )

# Monitor Communication



# Retrieve IPv6 host address




| 序号 | IPv6地址 | 端口 | 状态 |
|---|---|---|---|
| 001 | 2001:250:207:d8:585f:6a04:dc51:7a95 | 11481 | OK |
| 002 | 2001:da8:211:a188:90de:ee17:3b9:6455 | 16703 | OK |
| 003 | 2001:da8:1005:e1:6138:184:e871:2060 | 43155 | OK |
| 004 | 2001:da8:7000:5015:3024:c32b:b424:363c | 19086 | OK |
| 005 | 2001:cc0:2044:5:6d44:2c61:9a24:3940 | 16703 | OK |
| 006 | 2001:250:4402:504:c54a:ad0b:37ba:1bc8 | 16703 | OK |
| 007 | 2001:da8:216:2635:3562:c0b9:d93e:569a | 16703 | OK |
| 008 | 2001:250:1002:2223:6507:1156:5e70:59ea | 16703 | OK |
| 009 | 2001:da8:b803:37:3dd0:b604:8300:6fa | 51916 | OK |
| 010 | 2001:da8:1005:d5:1874:d6a6:55d5:85b | 51157 | OK |
| 011 | 2001:da8:8002:66:0:5efe:10.10.114.17 | 16703 | OK |
| 012 | 2001:da8:22b:1520:6c21:eb6b:206c:d614 | 16703 | OK |
| 013 | 2001:250:1002:2408:d863:881f:ced5:a46b | 56479 | OK |
| 014 | 2001:da8:a000:355:4d8d:bdb0:91bb:6fb5 | 16703 | OK |
| 015 | 2001:250:4402:504:c54a:ad0b:37ba:1bc8 | 16703 | OK |
| 016 | 2001:da8:a800:2104:f58b:b46f:6c39:6a7b | 63791 | OK |
| 017 | 2001:da8:9000::232 | 6969 | OK |
| 018 | 2001:da8:9000::232 | 6969 | OK |
| 019 | 2001:da8:9000::232 | 6969 | OK |
| 020 | 2001:da8:216:2605:d49b:1582:38e4:cd3f | 16703 | OK |
| 021 | 2001:250:5401:623:bc13:adc1:15cd:6ecb | 37381 | OK |
| 022 | 2001:da8:8006:208:48ec:72de:d409:70f6 | 16703 | OK |
| 023 | 2001:250:212:8001:0:5efe:10.150.1.48 | 16703 | OK |

Thanks!