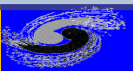
HEPiX Autumn/Fall 2018

IHEP campus network design based on SDN technology

Cui Tao
cuit@ihep.ac.cn
Institute of High Energy and Physical, CAS

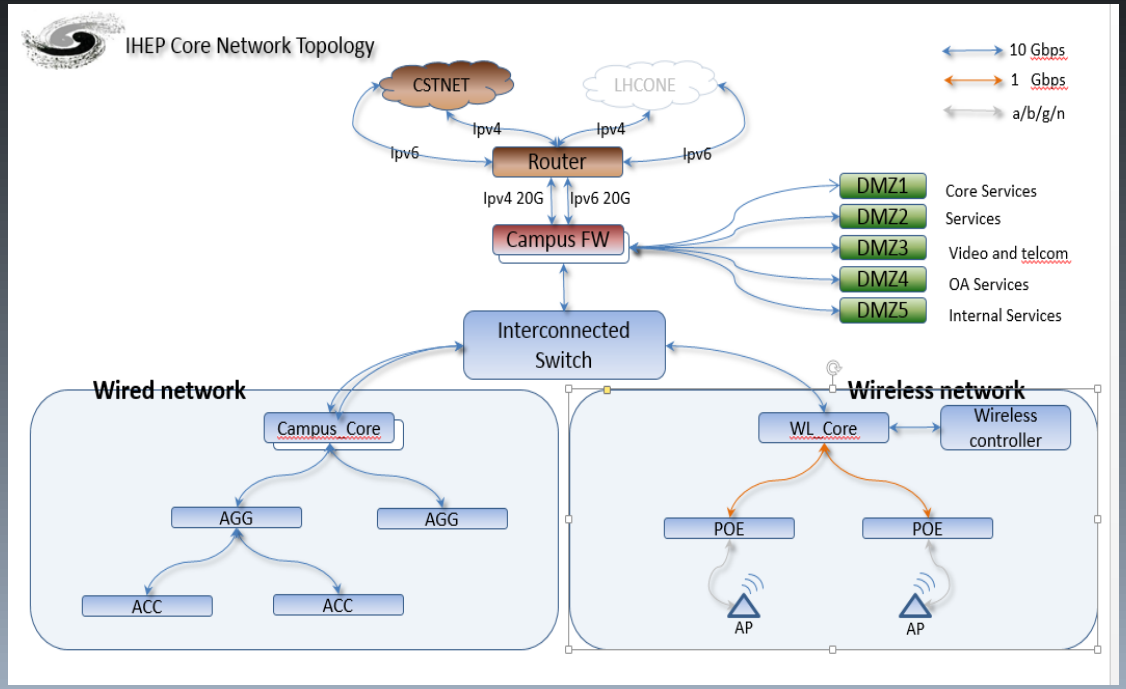


outline

- IHEP campus network today
- New design based on SDN architecture
  - Access control solution
  - Network management
- Test-bed and result
- future plan
- Conclusion

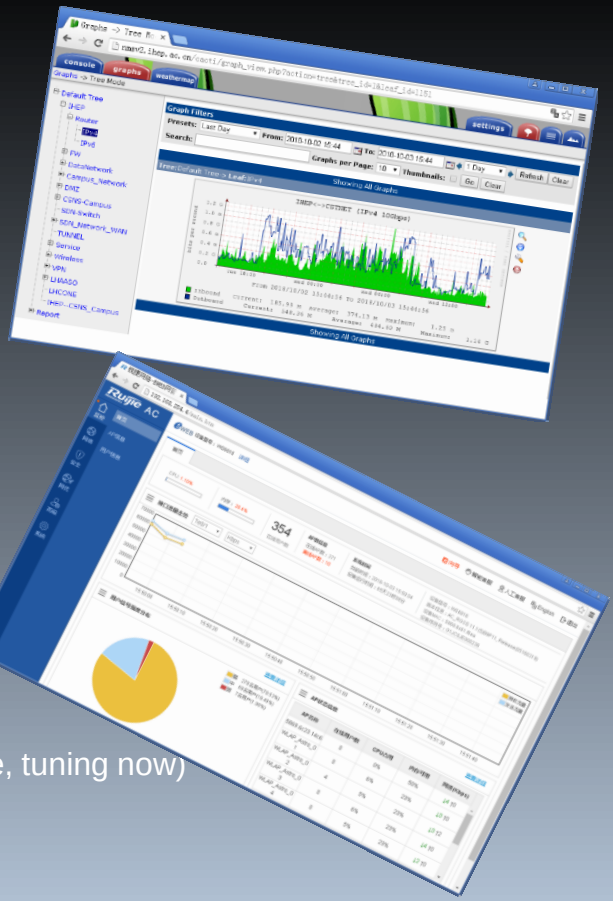
IHEP campus network today

- 25 building
- 2K users
- Facilities 2011
  - Wired Core 2
  - Wireless Core 1
  - L3 switch 45
  - L2 switch 180
  - AC 2
  - POE 45
  - Aps 342
- Network topology
  - Independent wired and wireless network routed by interconnected switch
  - IPv4/6 supported
  - Static routing



IHEP campus network technology

- DNS cluster 5
- DHCP(IPv4/IPv6)
  - Static IP address allocation for ipv4
  - Dynamic address allocation for ipv6
- Access control
  - http://Network.ihep.ac.cn
  - Wired : DHCP snooping bonding based on Mac address, IP address on a switch port
  - Wireless: Based on AC and 802.1X + Radius
- Monitoring
  - Cacti / Zabbix
  - Packet analyzer service based on SPAN (Switched Port Analyzer) and Optical splitter
  - Probe server system to matric the network delay and accessible (not online, tuning now)
  - Log collection system
  - Wireless map / controller monitoring web service



The problems and requirements

- Problems
  - Network equipment update
    - 80% equipment 7 years
    - Potential equipment failure risk
  - New technology needed
  - IP address allocation unified

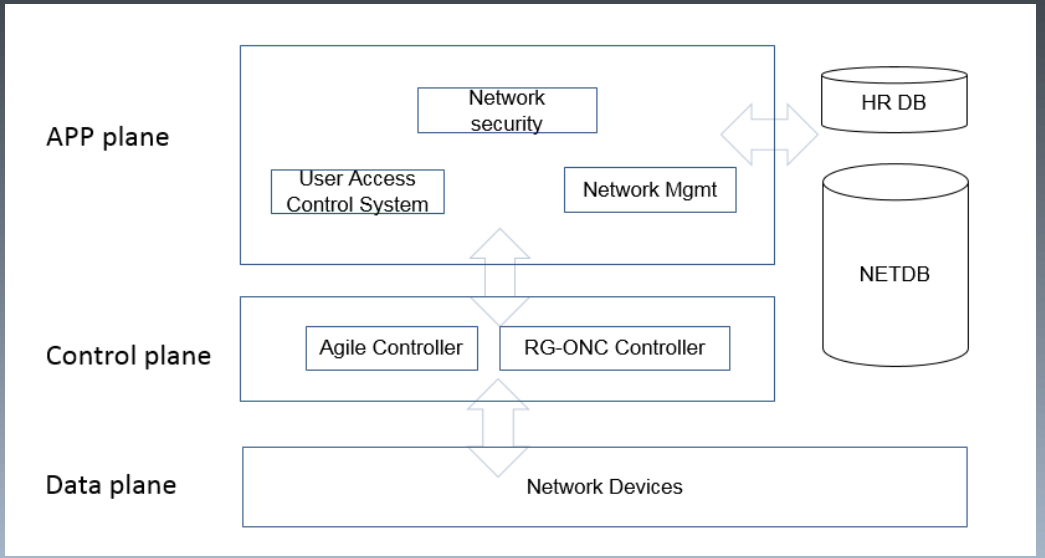
- Requirements
  - New architecture based on SDN conception
  - Network components update
  - More automatic network management means and network monitoring data Integration
  - Unified and automatic IP address allocation solution

outline

- IHEP campus network architecture introduction
- New design based on SDN architecture
  - Access control solution
  - Network management
- Test-bed and result
- future plan
- Conclusion

New campus network design based on SND architecture

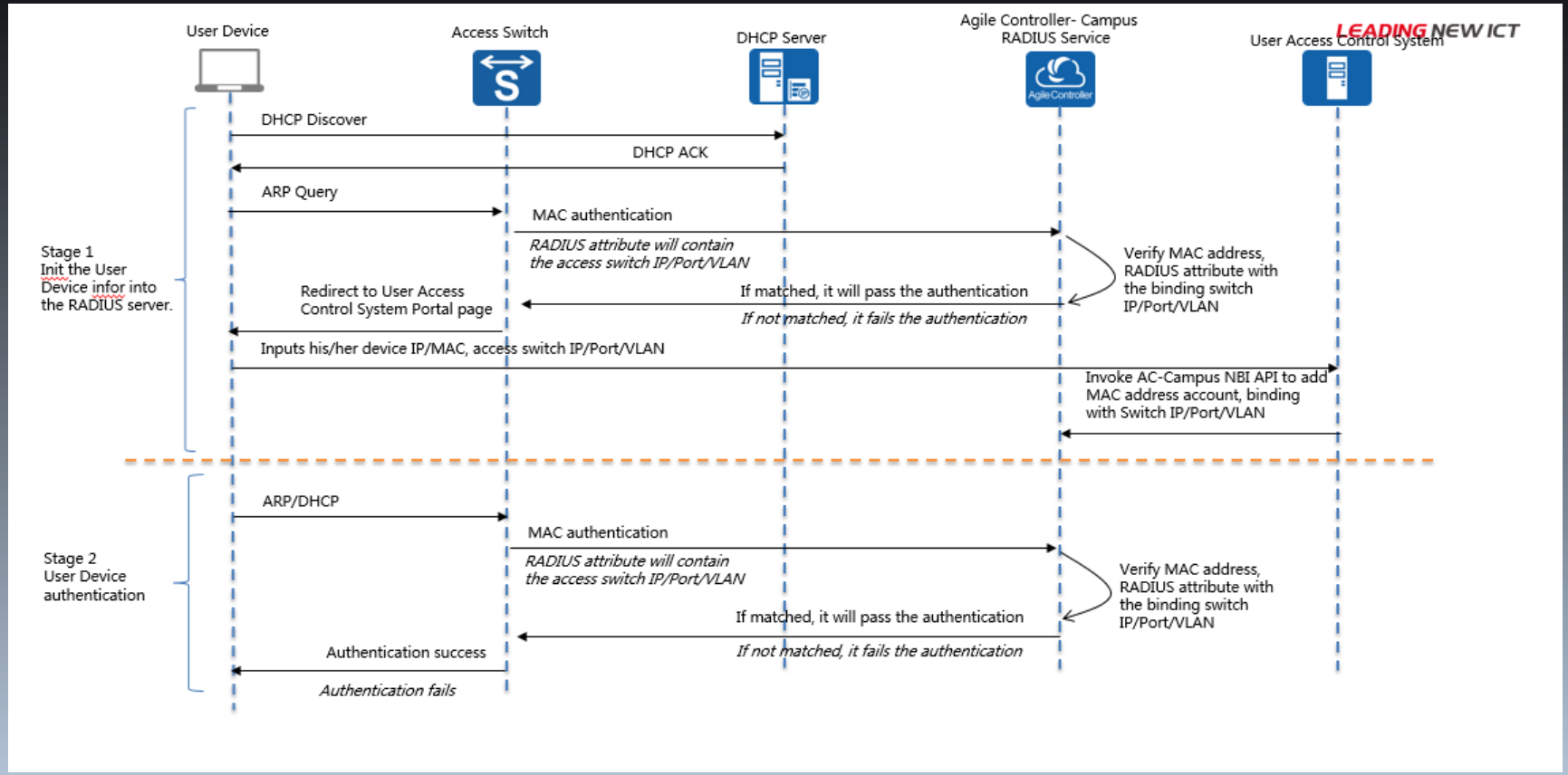
- Open source or company ?
- Two company solution
  - Network topology
    - Hierarchical architecture
    - Standardized interfaces
      rest API / netconf API
    - Data centralized NETDB
      more metadata and time series data
  - Fully DHCP IP address allocation
  - Access control and network mgmt (Step 1)
    - Access control
      - Convenient, self-service, self-management
    - Network control
    - Network monitoring and analysis
  - Network security (Step 2)



Wired network access control solution by HUAWEI

- Reserved DHCP address (IPv4/6)
  - To fix IP address after DHCP process by rest API
- User self-registration
  - Register online device info comparing and reviewing
  - Register offline just reviewing
- Agile Controller
  - radius control on the side of access switch
  - 4-keys to be compared on the side of controller
    - Device mac address
    - Device IP address
    - Switch IP address which device linked
    - Switch port index which device linked
  - Multiple points register

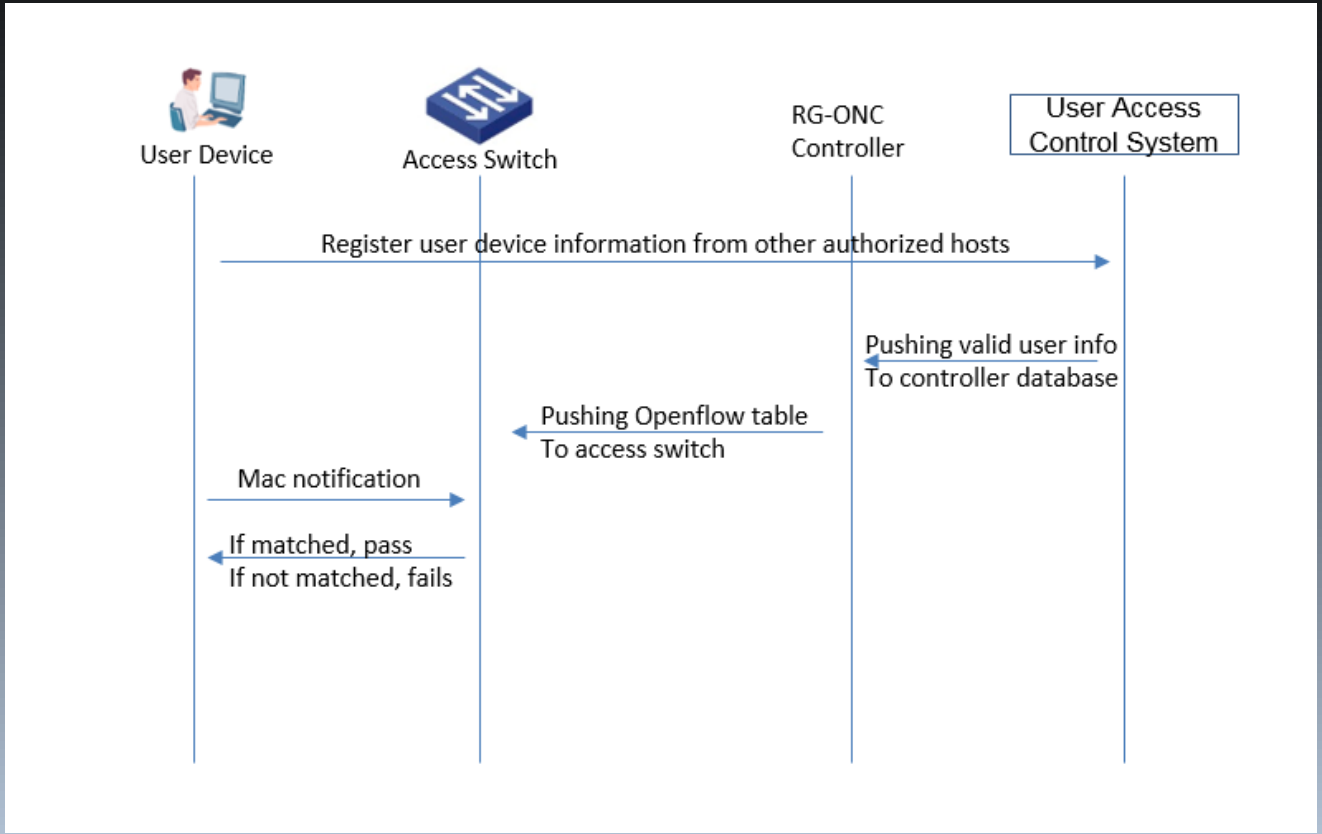
Wired network access control solution by HUAWEI



Wired network access control solution by Ruijie

- Based on Openflow 1.3
  - Openflow tables to control user access or not
- static address allocation
- User self-registration from authorized hosts
- RG-ONC Controller
  - Openflow table control on the access switch side
  - 4-keys to be compared on the access switch side
    - Device mac address
    - Device IP address
    - Switch IP address which device linked
    - Switch port index which device linked
  - No multiple points register supported

Wired network access control solution by Ruijie



Wireless network access control solution by Ruijie

- Dynamic address allocation
- Centralized control mode
  - Two AC controller and about 340APs
- User self-registration by portal
- Ruijie wireless controller + remote radius
  - 802.1X authentication

Network management

- Network information collection
  - Get info by traditional way such SNMP, Rsyslog and Linux script(Telnet)
    - Network delay test
    - Network traffic statistics
  - Get info from controller by API
    - Online user devices information
    - Online arp table, mac table and port list

- Network control
  - Black/white list by Controller to stop a device or free authentication

outline

- IHEP campus network architecture introduction
- New design based on SDN technology architecture
  - Access control solution
  - Network management
- Test-bed and result
- future plan
- Conclusion

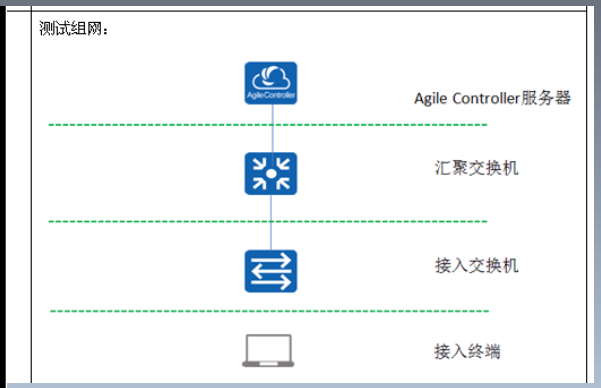
The test-bed and result

- Two solutions
  - HUAWEI , Ruijie
  - Test-bed has been built since Aug 2018
  - Agile Controller + HUAWEI S7703, S6720-32C-SI, S5720-28X-LI
  - RG-ONC + Ruijie N18010, S6220, S5760
- The verification of main functions have been completed
  - Access control
  - Black/white list
- 16 Rest API required
  - 43.75% supported
  - Limited query capacity

```
[S5720-28X-LI]display access-user  user-id 17

Basic:
  User ID                     : 17
  User name                   : GNS
  Domain-name                 : default
  User MAC                    : 34e6-d70b-65d3
  User IP address             : 192.168.10.246
  User vpn-instance           : -
  User IPv6 address           : -
  User access Interface       : GigabitEthernet0/0/21
  User vlan event             : Success
  QinQVlan/UserVlan           : 0/10
  User vlan source            : user request
  User access time            : 2000/04/05 07:39:12
  User accounting session ID  : S5720-2000210000000100c****0000011
  Option82 information        : -
  User access type            : WEB
  Terminal Device Type        : Data Terminal
  Web-server IP address       : 192.89.13.231

AAA:
  User authentication type    : WEB authentication
  Current authentication method   : RADIUS
  Current authorization method    : -
  Current accounting method       : RADIUS
```



API developing

- Access control and authentication
  - to add, delete or modify valid user information
  - Querying authentication rules by Mac
- Network management
  - User equipment black/white list
- Network information query and statistics
  - User access log query
  - Un-normal network traffic query
  - Arp and mac tables query
  - …

outline

- Campus network architecture introduction
- New design based on SDN architecture
  - Access control solution
  - Network management
- Test-bed and result
- future plan
- Conclusion

The future plan

- To replace old network equipment
  - 2018 50%
  - 2019 50%
- To complete campus network based on SDN architecture in the next 6 month
- To update and integrate network monitoring and control capacity

outline

- Campus network architecture introduction
- New design based on SDN architecture
  - Access control solution
  - Network management
- Test-bed and result
- future plan
- Conclusion

The conclusion

- SDN architecture helps us more clear descripting our campus network topology.
- SDN control plane provides control means like black list and make things possible for automatic network maintain or management
- More intelligent monitoring systems are needed for the new architecture because controller can’t provide more detail about network status

Thanks !