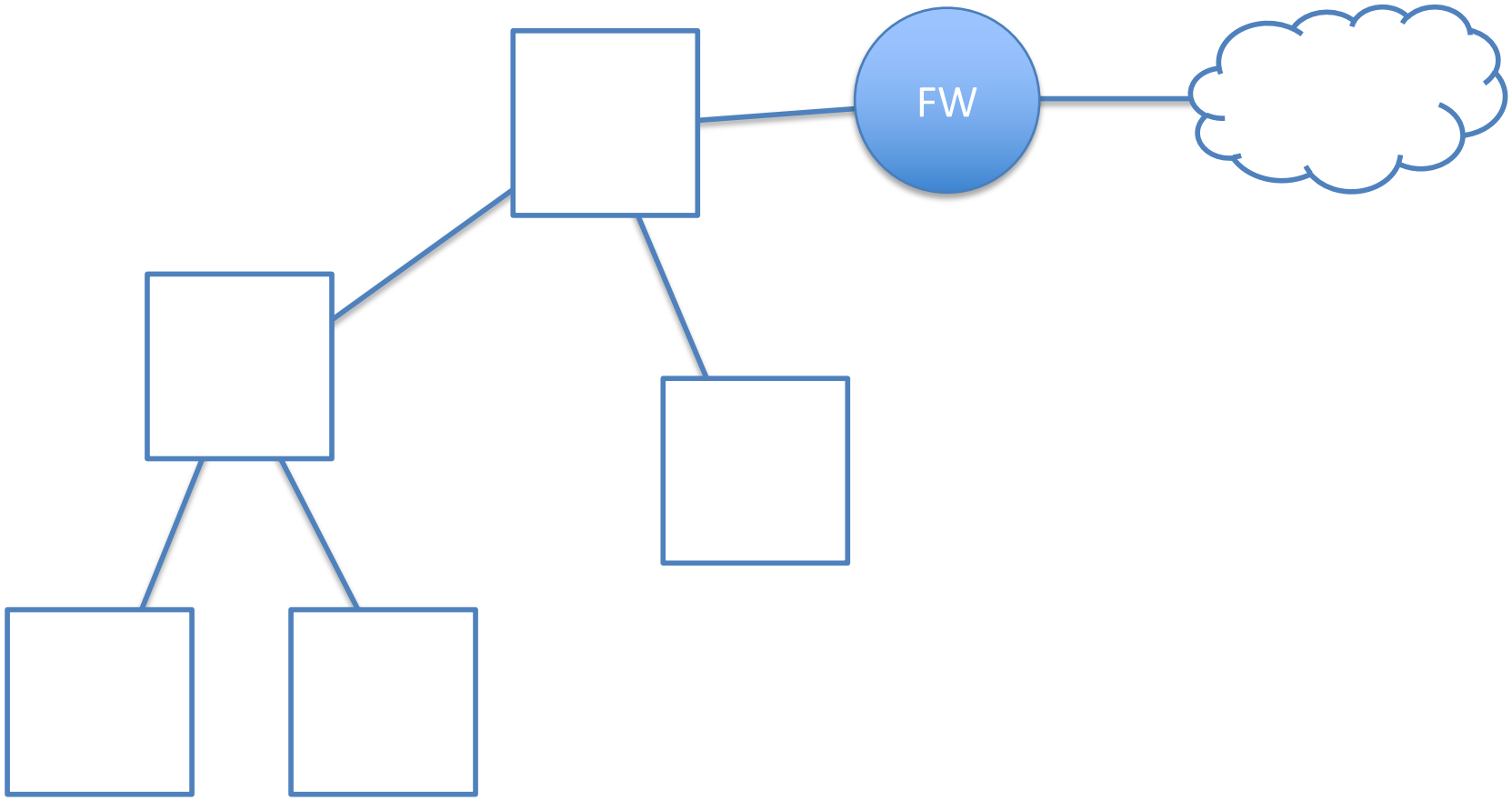
SAFE: Software-defined Authentication FramEwork

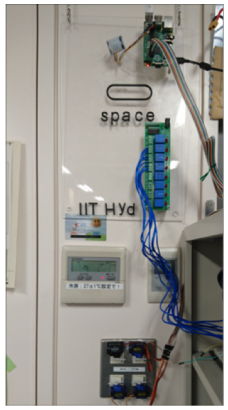
Aditya V Kamath, Sudarshan S, **Kotaro Kataoka**,
Nishant Vijayvergiya, G. Bhargav Reddy, Samrat Phatale
(Indian Institute of Technology Hyderabad)

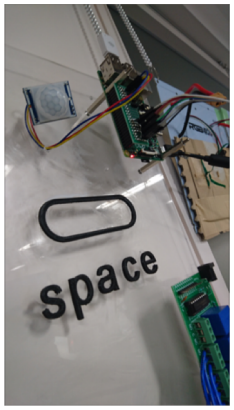
Where is the Firewall?

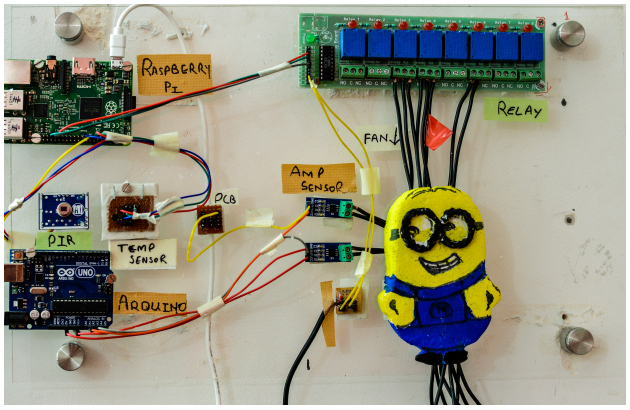


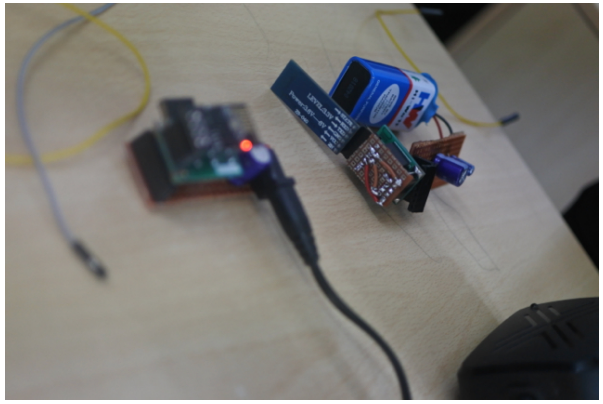
Introduction

- Variety of untrusted devices
  - Internet of Things (IoT), Bring Your Own Device (BYOD) and ~~**Gaming Console**~~
  - Devices without enough capability to undergo the demanded authentication procedure









Legacy Approaches

- Untrusted VLAN
  - Only 12 bits (apprx. 4000 VLANs)
  - Multiple devices may join the same untrusted VLAN (can do something bad together)
- 802.1x
  - All switches must have Authenticator function to communicate with RADIUS servers
  - What happens if devices do not support 802.1x authentication ex) PEAP/EAP-MSCHAP?

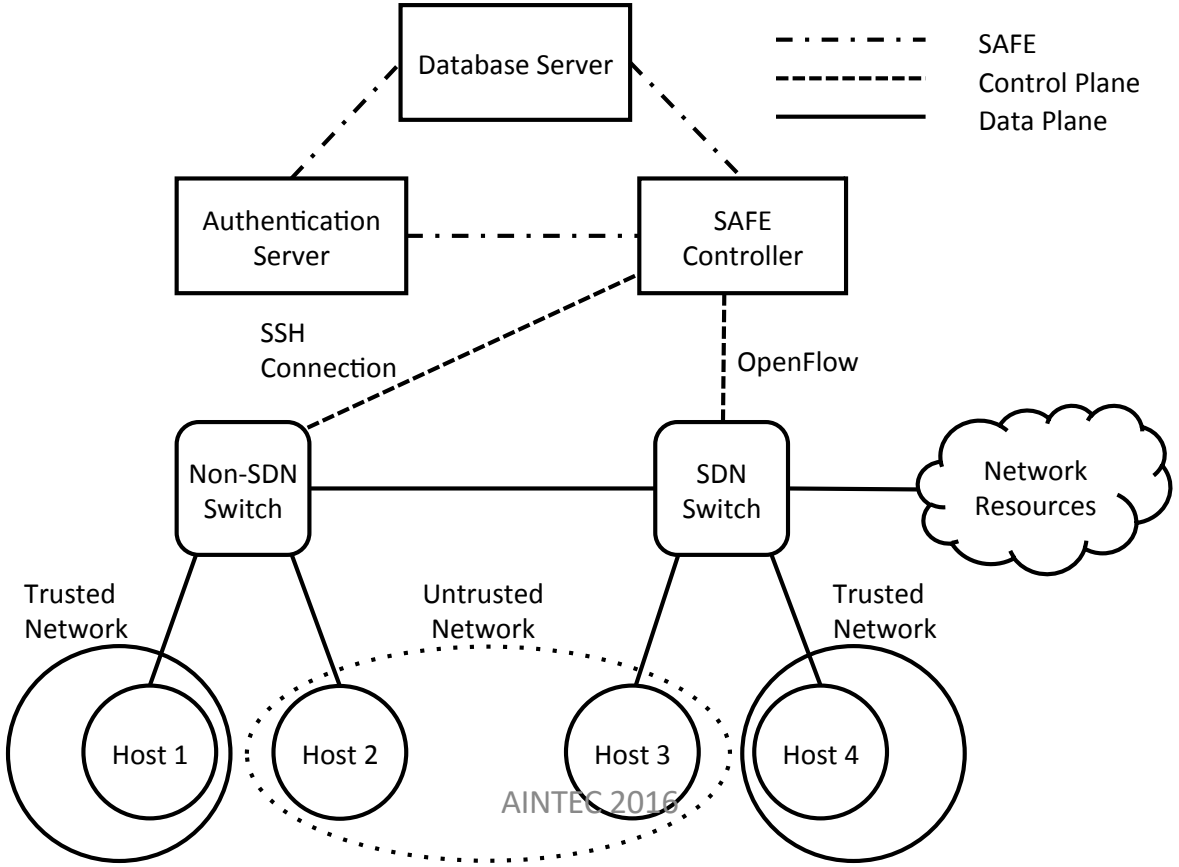
Q: How to trust constrained devices and let them join the network?

- A: Separating the process of Authentication and Access Control (Authorization)
  - Safely trusting devices some how
  - Letting devices connected

- Keeping devices isolated with each other before they get authenticated

SAFE: Software-defined Authentication FramEwork

- Provides the freedom of modes of authentication
- Creating Trusted Network and Untrusted Network
- Isolating a device based on Mac-based Network Slicing

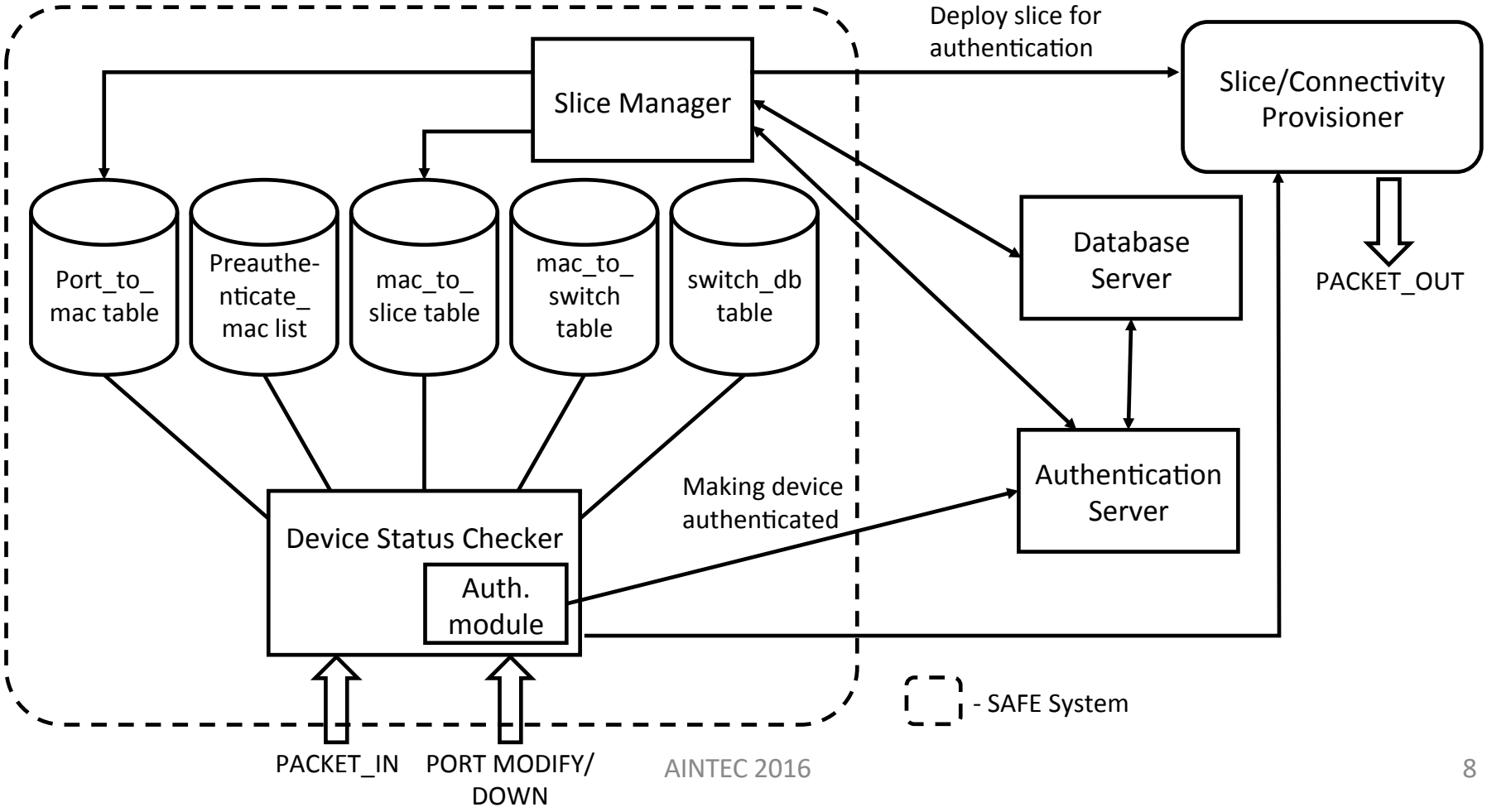


Isolating Unauthenticated Hosts

- Creating a network slice using MAC address and the connected port on SDN switch
  - PORT_UP / DOWN / MODIFY messages of OpenFlow
- Isolation to a device
  - Can communicate with only Authentication Server to get authenticated
  - Can communicate with nobody until Authentication Server sends the SDN controller to grant the access

SAFE Controller

- Running on top of SDN controller



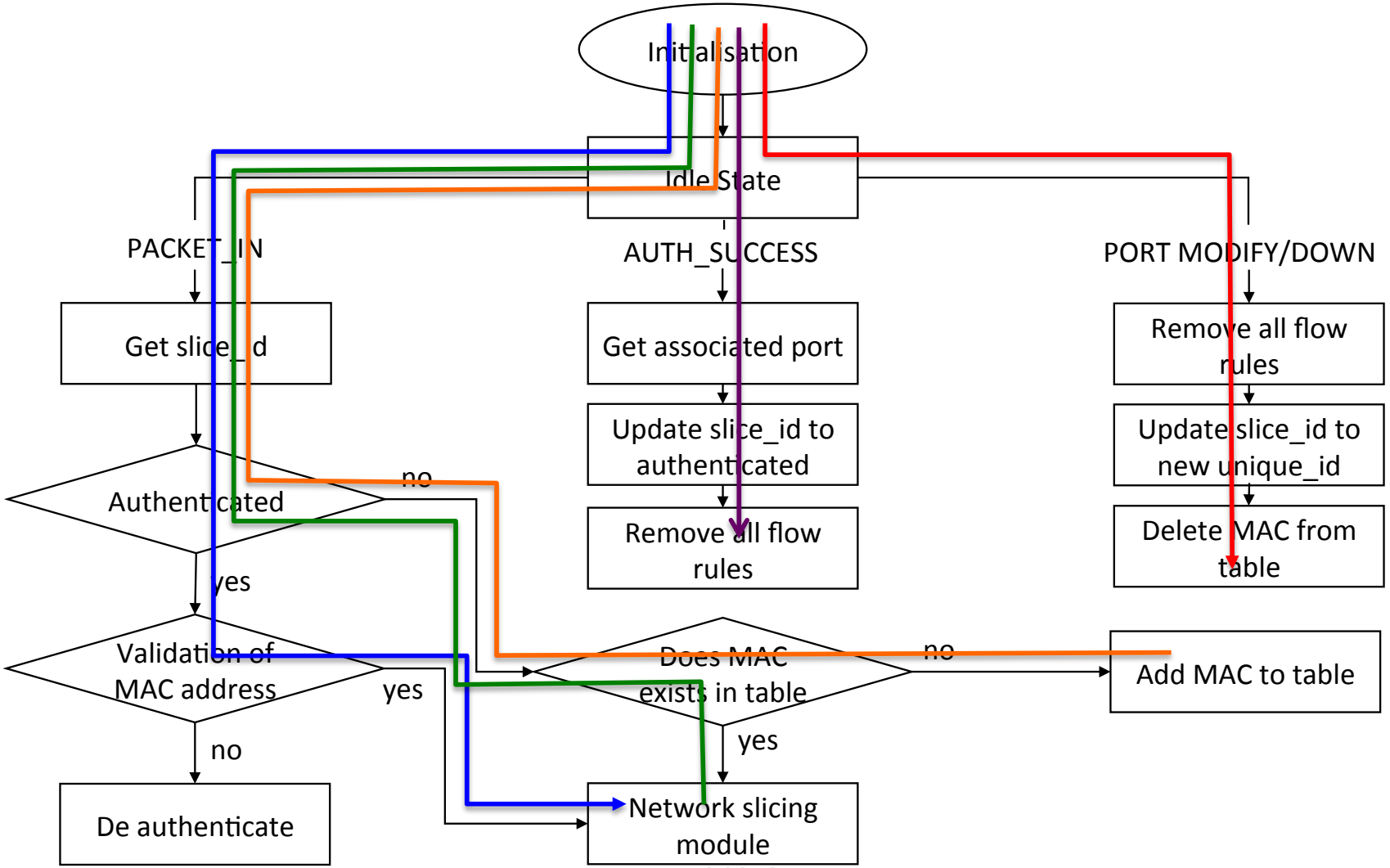
Role of Authentication Server

- SOMEHOW authenticate a device
  - Direct Authentication: An unauthenticated device communicates with the authentication server on the trunkated network slice
  - Indirect Authentication: Checking the list of trusted MAC address and find the matching entry
- Send a go-sign to SAFE controller to authorize the device to communicate in the network

Databases and Data Structures

- *switch_db*: DPID mapping to switch objects
  - *dest_mac_to_port*: returns the output port of a given destination MAC address of host.
  - *port_to_slice*: returns the slice id of the given port.
  - *slice_to_ports*: returns a list of ports belonging to the given slice id in that switch.
- *mac_to_slice*
  - A hash table that returns the slice id to which a given MAC address is attached
  - Necessary for packets that come across TRUNK ports
- *preauthenticated_mac*
  - list of all authenticated MAC addresses provided by trusted authentication procedures
  - started outside of controller modules, **enabling support for third party authentication mechanisms outside of the protected network**
- *mac_to_switch*
  - A hash table returns the switch object to which device with a given MAC address is directly connected

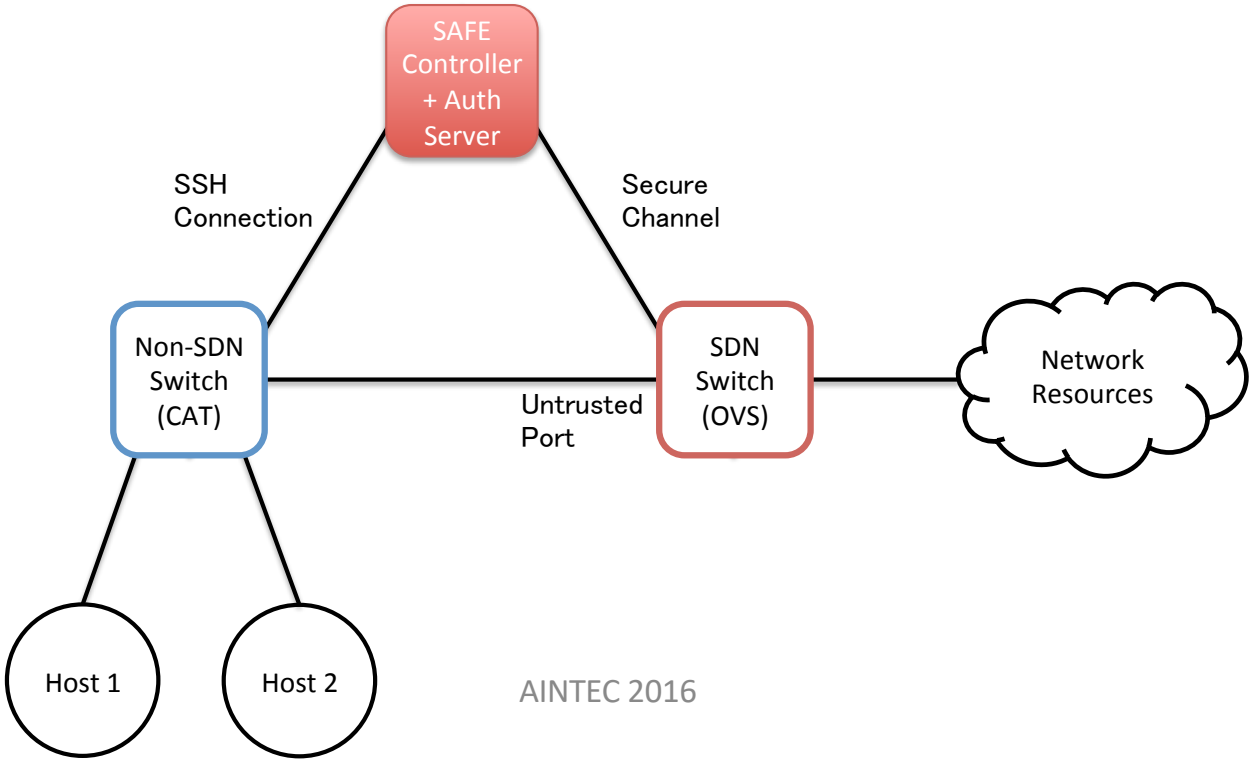
Access Control using SAFE



Interoperability with non-SDN switches

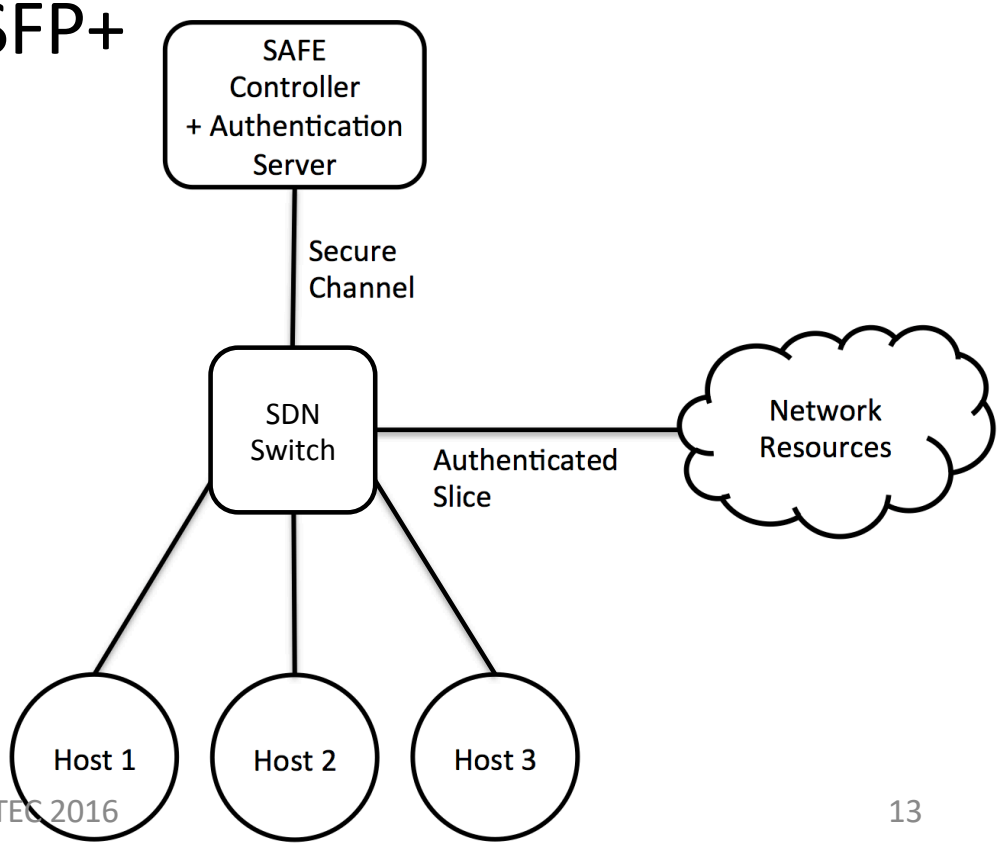
- The ports on OpenFlow switches which connect to non-SDN switches has a special *slice_id* "UNTRUSTED SLICE"
- At least one OpenFlow switch in the network
- The non-SDN switch data structure only contains *mac_to_port* table

- ACL1 -> Authentication -> ACL2
  - ACL1 allows packets only to the MAC address of the authentication server on a specific port
  - ACL2 allows all packets with a given source MAC address to communicate on a specific port



Implementation

- Mininet (Emulation)
- Hardware SDN Switch (Live Testbed)
  - HP 3800-24G-PoE+-2SFP+
- Non-SDN Switch (Interoperability)
  - Cisco Catalyst 2960



Discussions

- Natively Supporting Wi-Fi Clients
- Consistency among Multiple Authenticators
- Drawback of Involving Non-SDN Switches
  - Unwanted handling of L2 broadcast messages
- Alternative Modes of Authentication
- Supporting Various Identifiers and Authentication Modes

Conclusion and Future Work

- Heterogeneity of device capability and unavailability of support of specific authentication modes
- Solution by SAFE
  - Separating authentication and access control in the network
  - Providing the freedom on mode of authentication without compromising on the isolation of untrusted hosts and security of the network resources
  - Easy to deploy because any additional support is not required on the host sid
  - Interoperability with non-SDN switch coexist in a single coverage
- Future work
  - Addressing the point in discussions
  - Extending SAFE to Wi-Fi networks
  - Larger deployment

THANK YOU. Q&A?