

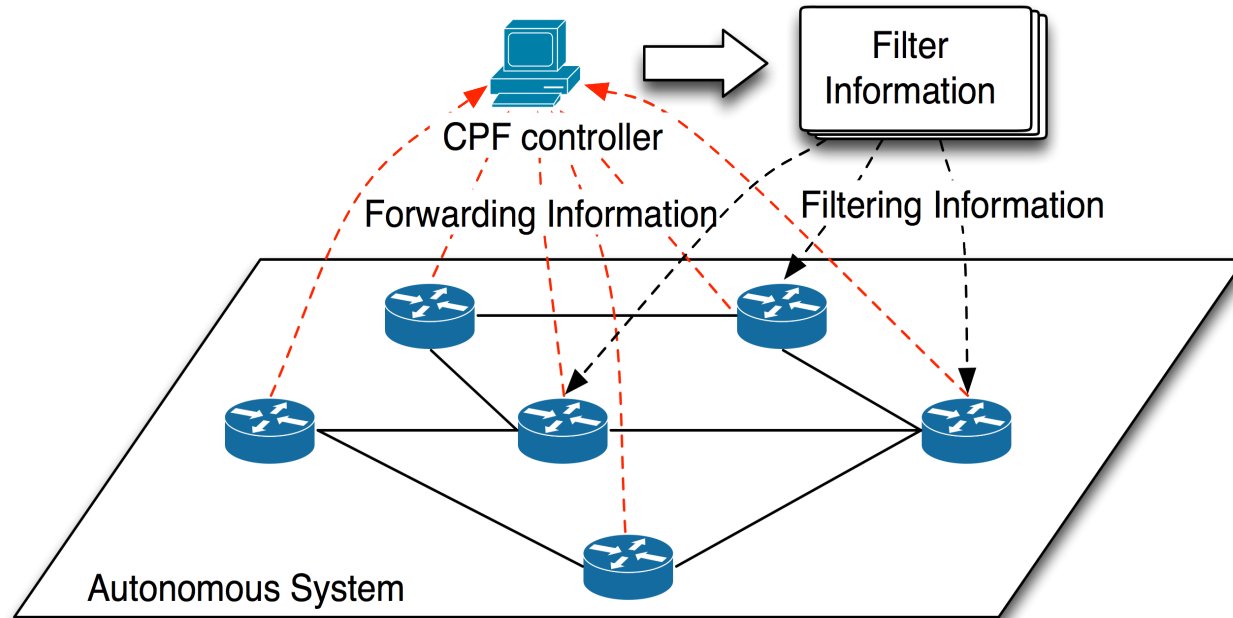


OpenFlow Extension for Intra-AS Source Address Validation

Tao Feng
Tsinghua University, China
CANS 2011

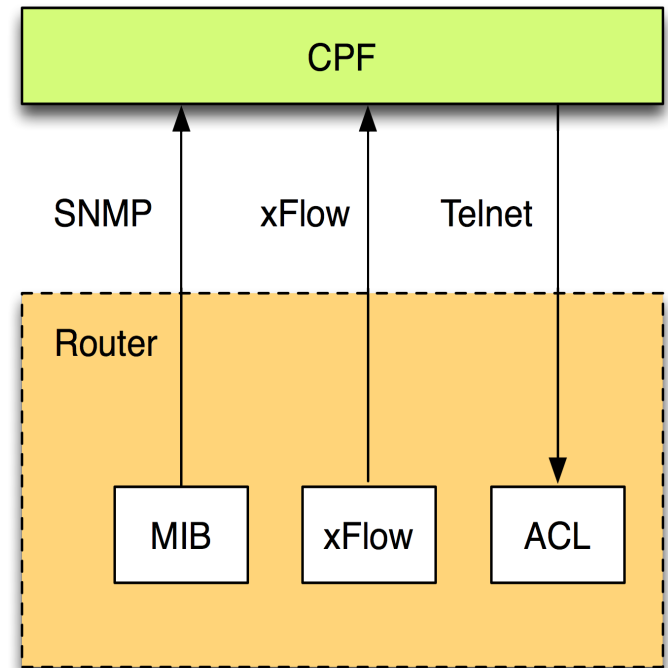
CPF: A Solution of Intra-AS Source Address Validation

- A central control model.
- A Calculated Path Forwarding (CPF) controller collects the forwarding information of every router in an AS, and calculates all possible forwarding paths for every source address, and then issues filter rules (the result of the calculation)
- Routers verify the source address of packets.



CPF in Current Network Architecture

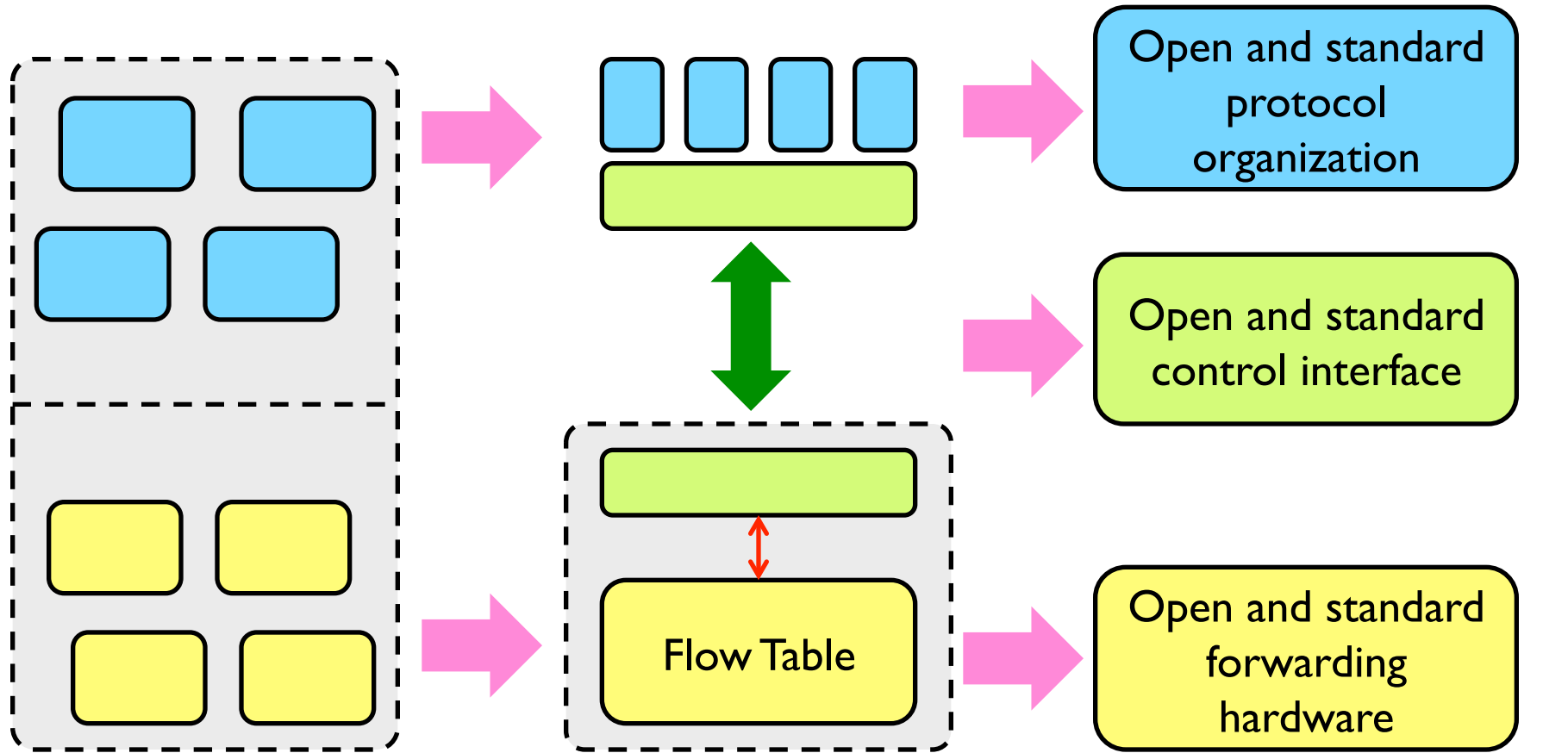
- **SNMP**
 - To poll forwarding information, interface information and subnet information from MIB for generating a global forwarding path.
- **xFlow**
 - To sample packets through xFlow (NetFlow/sFlow) for validating source address of sampling packets.
- **Telnet**
 - To issue the filter rules to network devices.



Limitations of CPF in Current Architecture

- **False positive filter rules**
 - Caused by asymmetric routing, changing spoofing packets and dynamic topology of AS
 - The filtering rules should not be changeless and fixed in the boxes and could be updated as soon as possible to avoid false positive.
- **Complex implementation caused by multi-protocol interfaces**
 - SNMP/xFlow protocols are implemented by different vendors.
 - No echo information in remote Telnet

Our Thoughts on OpenFlow



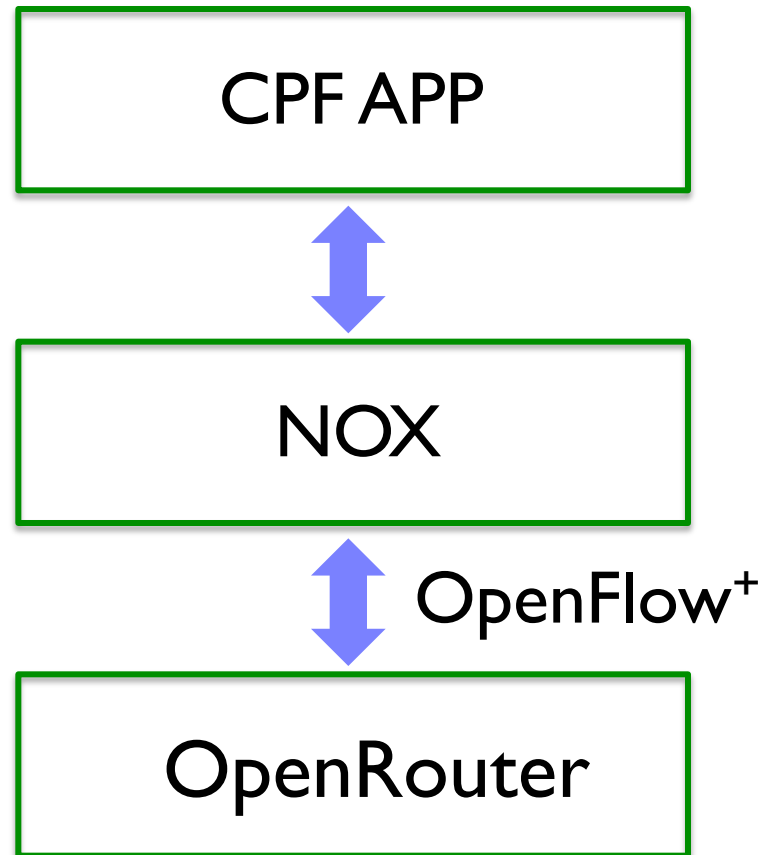
↔ Hardware to OpenFlow

[- - -] Device [Yellow] Hardware [Green] OpenFlow Protocol [Blue] Control Protocol

Considerations on CPF with OpenFlow

- Architecture Consideration
 - Central control architecture of OpenFlow and CPF
- Protocol Consideration
 - Using OpenFlow protocol to unify three protocols (SNMP, xFlow and Telnet).
- Control Consideration
 - Flexible and customized control functions on controller through OpenFlow protocol.

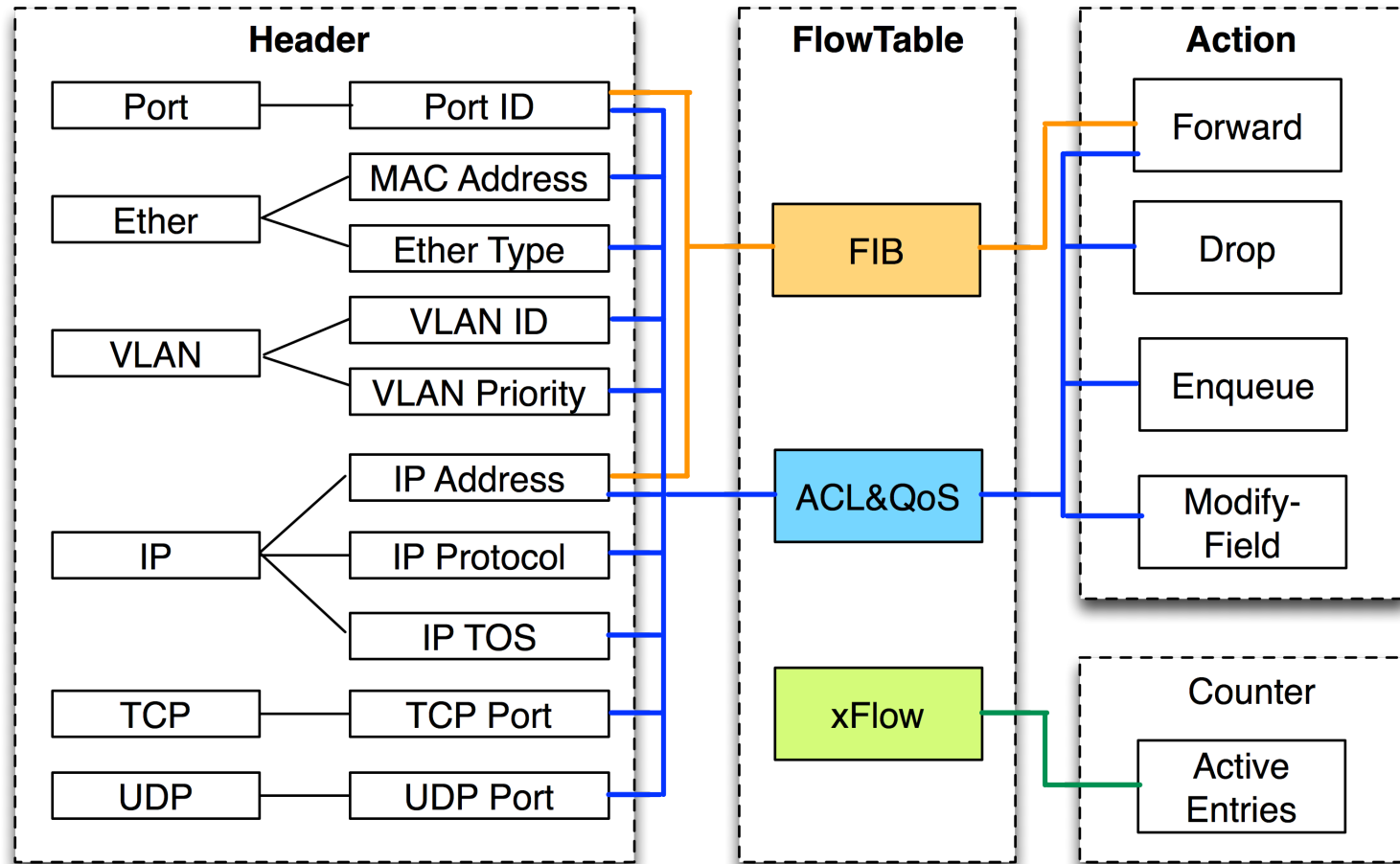
Architecture of CPF based on OpenFlow Extension



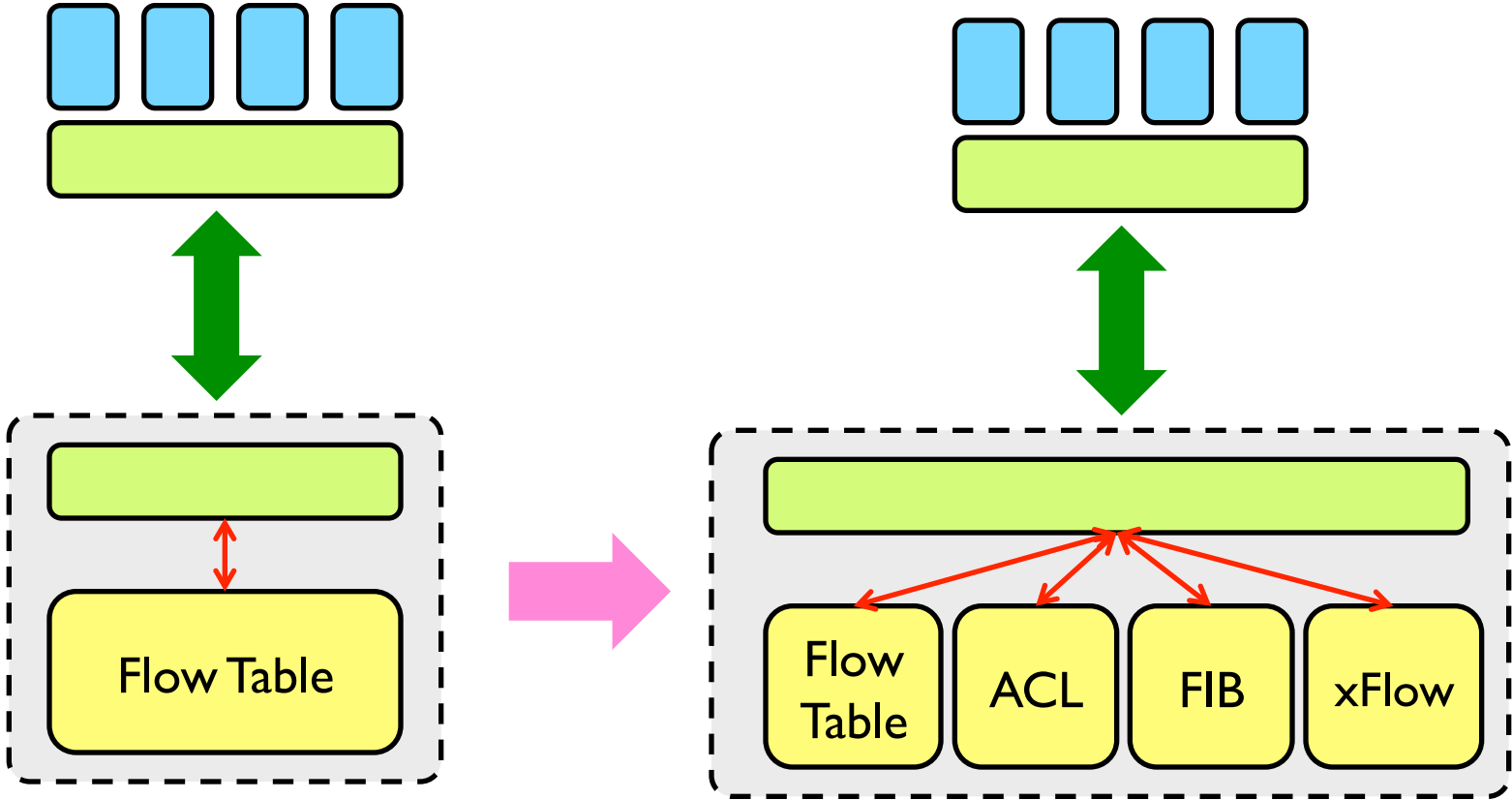
Extension I: Standard Hardware Extension

- More standard hardware not only FlowTable in a network device can be open
 - Only FlowTable hardware is not enough
 - Cost of TCAM is very sensitive to manufactory.
- ACL, FIB and xflow can be regarded as a type or subset of FlowTable.

Extension I: Standard Hardware Extension



Extension 1: Standard Hardware Extension



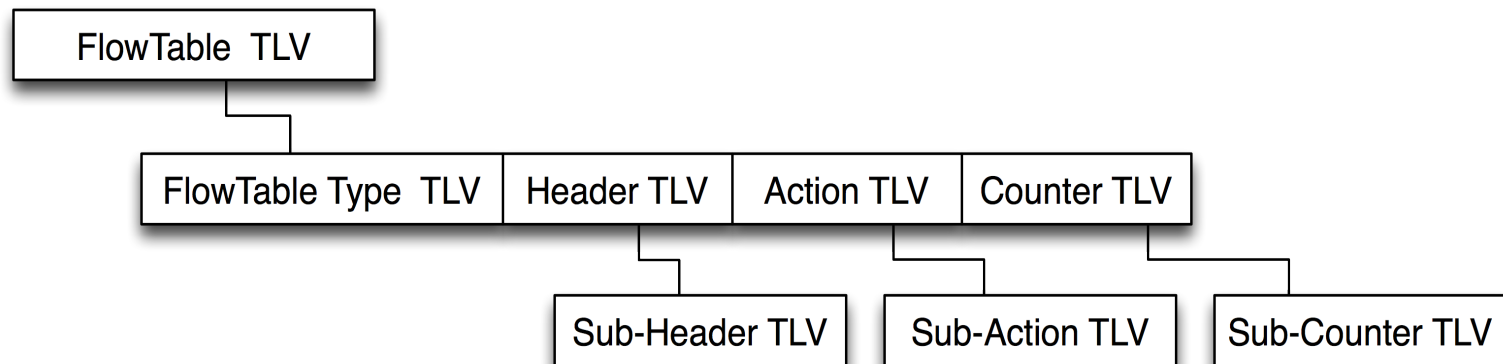
↔ Hardware to OpenFlow

[- - -] Device [Yellow] Hardware [Green] OpenFlow Protocol [Blue] Control Protocol

Extension I: Standard Hardware Extension

- FlowTable Type Extension

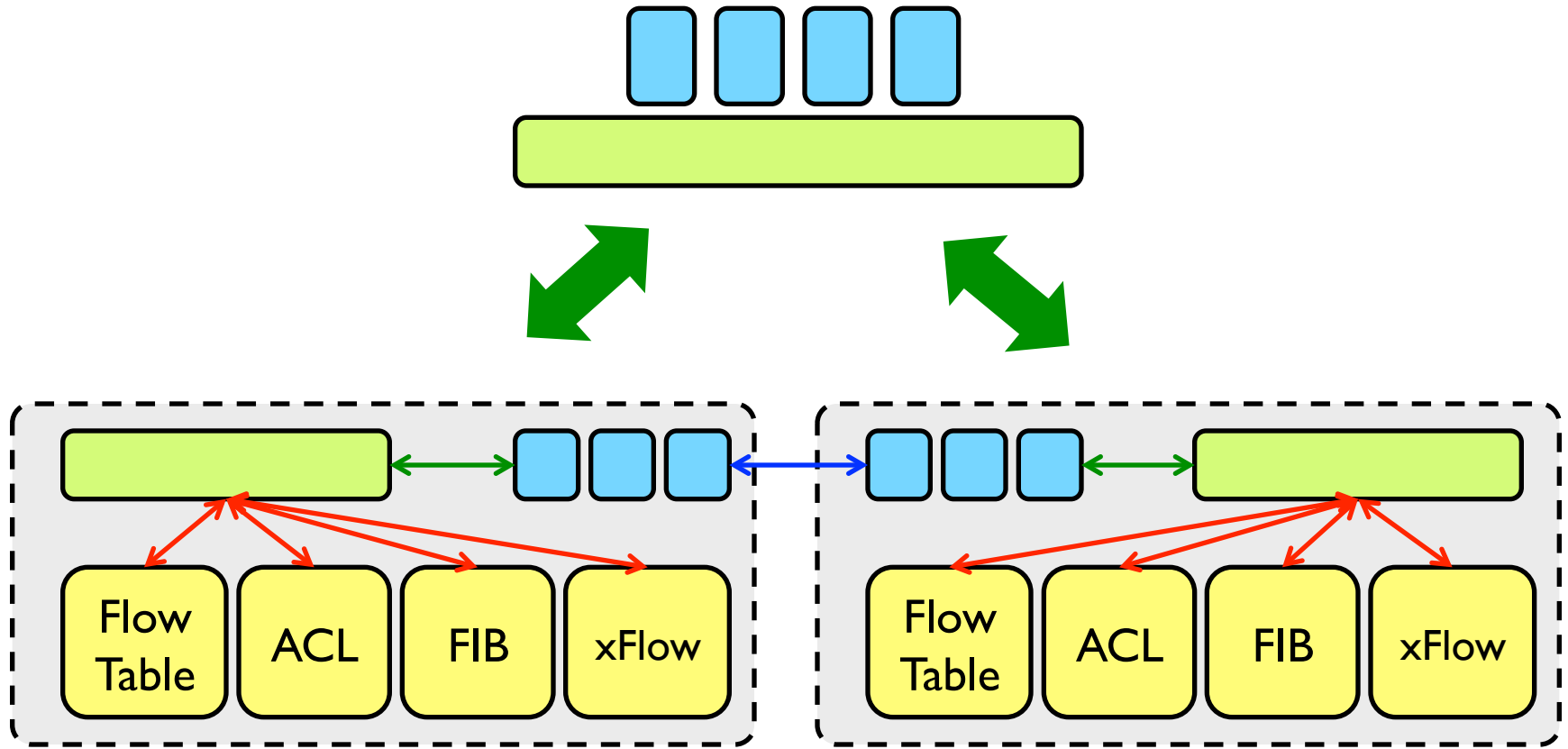
- Different values of “Type” field in TLVs identify different types of FlowTable.
- Any type of FlowTable can contain sub-TLVs: Header sub-TLV, Action sub-TLV and Counter sub-TLV(optional).
- In different types of FlowTable, the specific content of these three sub-TLVs may be different.



Extension 2: Control Model Extension

- Centralized control model
 - Strong: control efficiency with a global view
 - Weak: scalability and robust.
- Distributed control model
 - Strong: scalability, computing resources efficiency.
 - Weak: computing non-conformance in case of slow convergence
- A coexisting collaborative model of distributed control and centralized control is needed in networking and exchanging information with each other

Extension 2: Control Model Extension



↔ Hardware to OpenFlow ↔ Protocol to OpenFlow ↔ Protocol to Protocol

[- - -] Device [Yellow Box] Hardware [Green Box] OpenFlow Protocol [Blue Box] Control Protocol

Extension 2: Control Model Extension



- Rules to resolve control conflicts:
 - Introduce an arbitration module to execute the optimal selection for both controls from the inside and outside.
 - Use fixed priority levels to choose the optimal control.
 - Both of the control operations will coexist.

Extension 3: OpenFlow Message Extension

- Data reorganized by TLV
 - To support more types of information exchange between the control plane and the data plane
 - To support the easy extension of the length of network information in OpenFlow protocol

Extension 3: OpenFlow Message Extension

- TLV format can:
 - Efficiently organize OpenFlow data with variable length
 - Conveniently implement the extension for the length and type of OpenFlow data
- In TLV format, each piece of data is organized by the triple of (Type, Length, Value)
- TLV can be used or arranged recursively

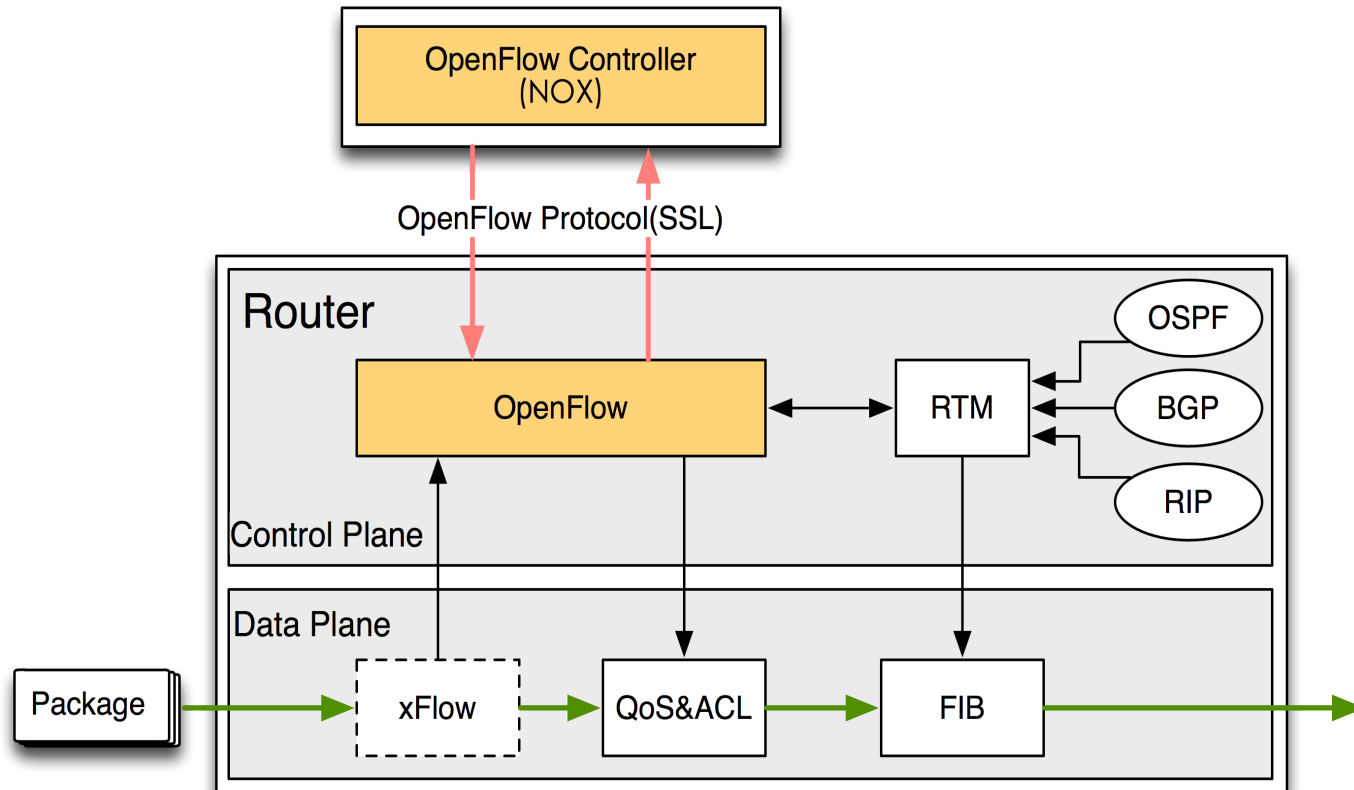
| | | |
|----------------------------|------------------------------|------------------------------------|
| TLV Type (Fixed length) | TLV Length (Fixed length) | TLV Value ("TLV Length" length) |
|----------------------------|------------------------------|------------------------------------|

Benefits of OpenFlow⁺



- More openness for network devices.
- More efficient control for the network.
- More flexible organization for data in OpenFlow Protocol.
- More low-cost implementation for OpenFlow device.

OpenFlow⁺-based Router (OpenRouter)

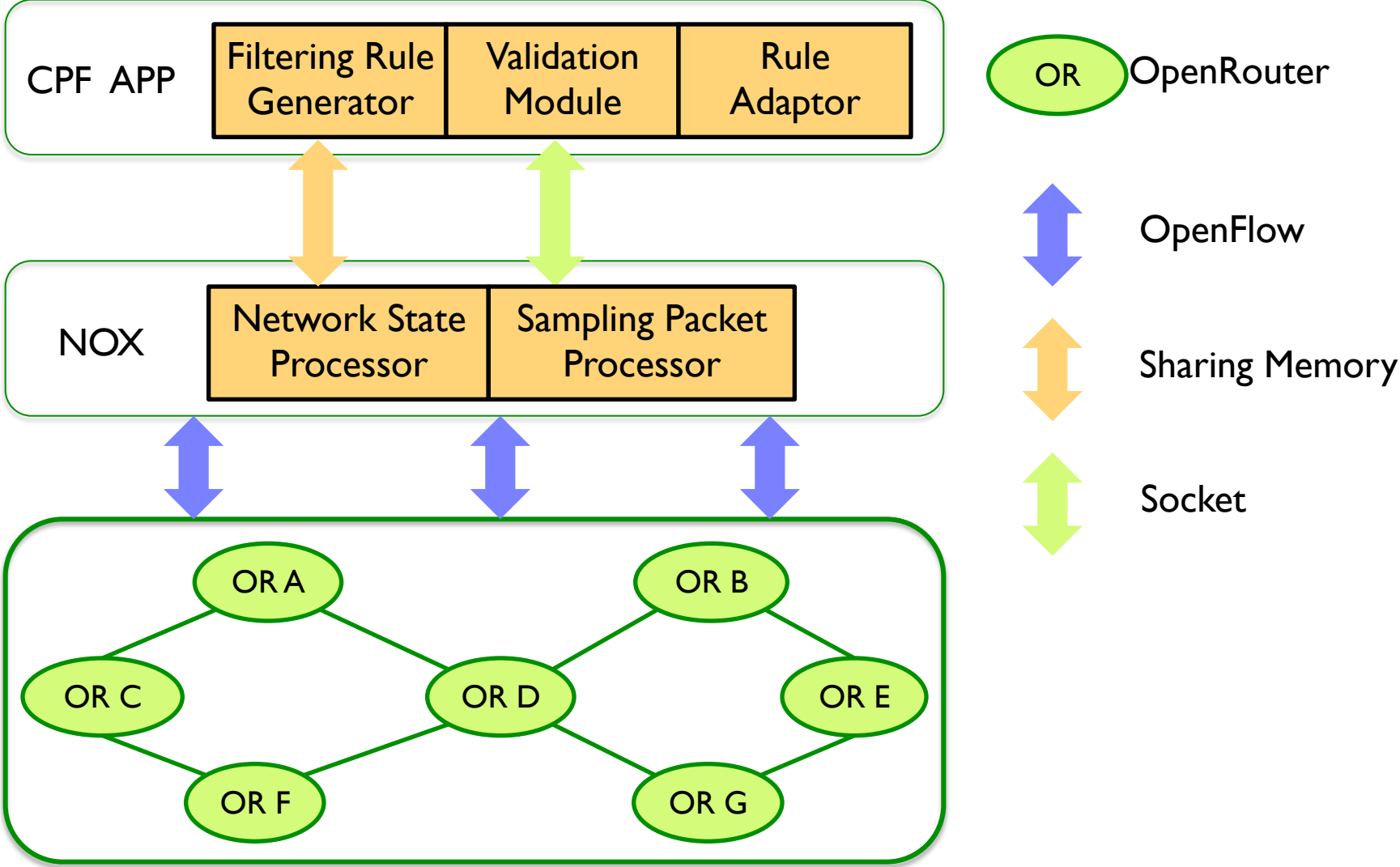


- OpenFlow⁺ in a commercial router
 - DCRS 5980/5950, DigitalChina Company, RouterSwitch

OpenFlow⁺-based Router (OpenRouter)

- The details of OpenRouter:
 - An OpenFlow module is embedded into control software of OpenRouter.
 - OpenFlow protocol is redesigned and reconstructed with TLV.
 - FlowTable is implemented using existing hardware resources (ACL&QoS and FIB).
 - OpenFlow module acts as an interfaces with Routing Table Management (RTM) module and sFlow module.
 - Two asynchronous messages and a synchronous message are added to transmit routing information and sampling packets.

CPF Controller



NOX



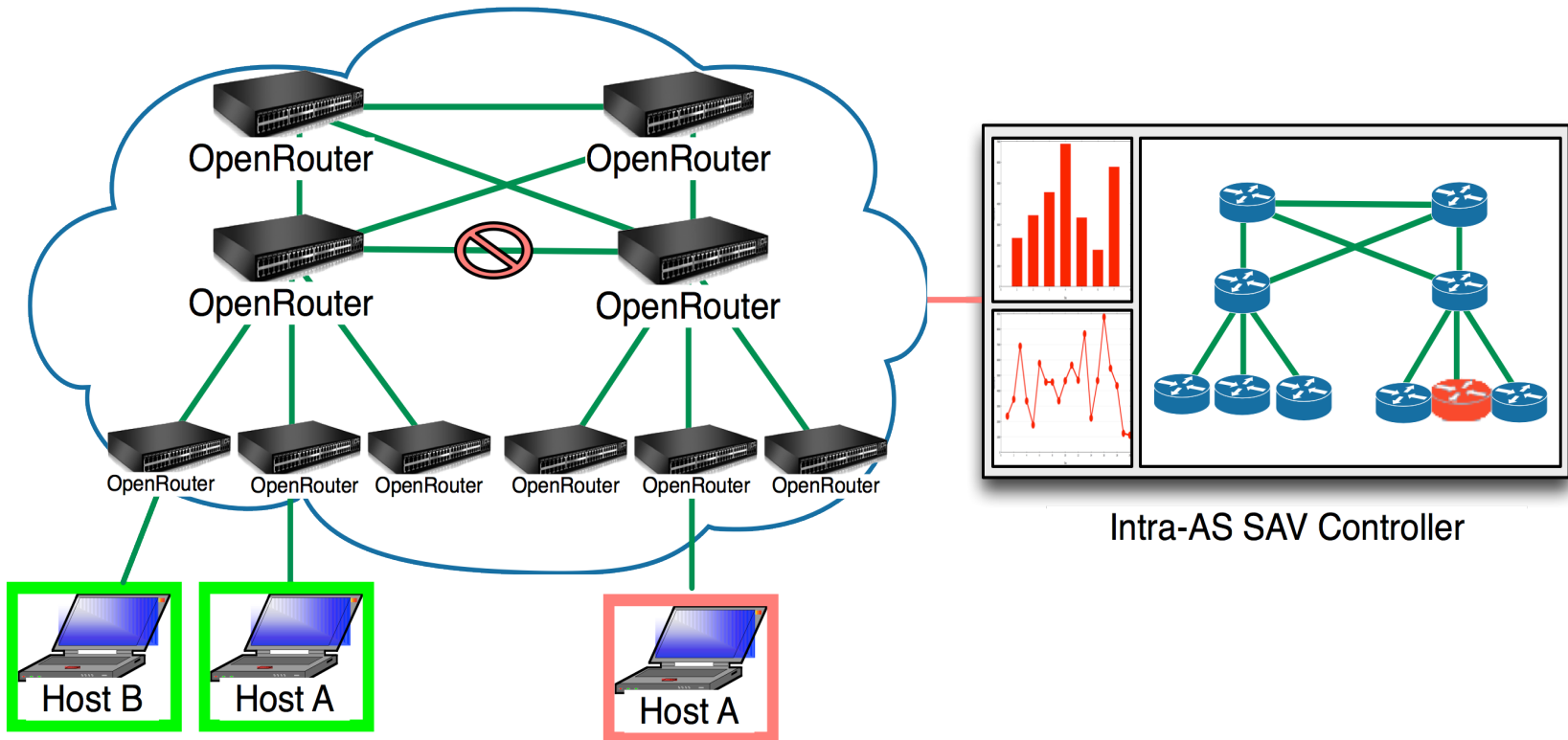
- Network State Processor
 - To receive and resolve network state messages, and announce an event of network state.
- Sampling Packet Processor
 - To receive and resolve sampling packets messages, and announce an event of sampling packets.

CPF APP



- **Filtering Rule Generator**
 - To calculate flow path and re-calculate on flow path change
- **Validation Module**
 - To determine whether a packet is spoofing or not.
- **Rule Adaptor**
 - To configure filtering rules onto OpenRouter through OpenFlow

The Testbed of CPF based on OpenFlow⁺



Future Work on OpenFlow

- FlowTable Extension
 - FlowTable compression: Bloom filter, etc
 - FlowTable quick lookup algorithms: longest prefix matches or some multi-dimensional lookup
- Controller Extension
 - Common functions: network overview
 - Cooperation and interaction of multiple controllers intra-domain and inter-domain: inter-AS source address validation
 - Network primitive: requirement or functional description for network protocol.



Thanks

Tao Feng
Tsinghua University, China
CANS 2011