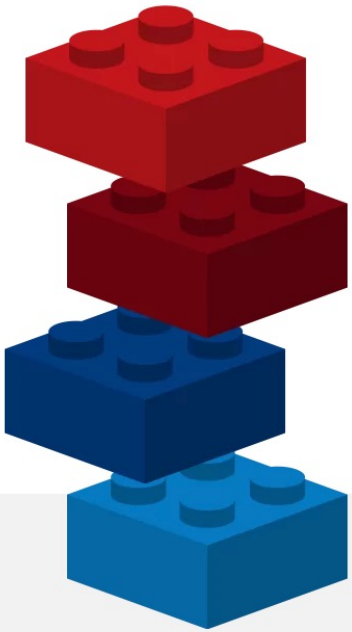
Software Defined Network
SDN

Ch 1

Introduction to SDN & Open Flow



Software-Defined Networking (SDN) Definition

What is SDN? The physical separation of the network control plane from the forwarding plane, and where a control plane controls several devices.

- Software-Defined Networking (SDN) is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications

EVOLUTION OF NETWORK PROVISIONING: 1996-2013

big switch networks

1996

```
Router> enable
Router# configure terminal
Router(config)# enable secret cisco
Router(config)# ip route 0.0.0.0 0.0.0.0 20.2.2.3
Router(config)# interface ethernet0
Router(config-if)# ip address 10.1.1.1 255.0.0.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface serial0
Router(config-if)# ip address 20.2.2.2 255.0.0.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# network 20.0.0.0
Router(config-router)# exit
Router(config)# exit
Router# copy running-config startup-config
Router# disable
Router>
```

Terminal Protocol: **Telnet**

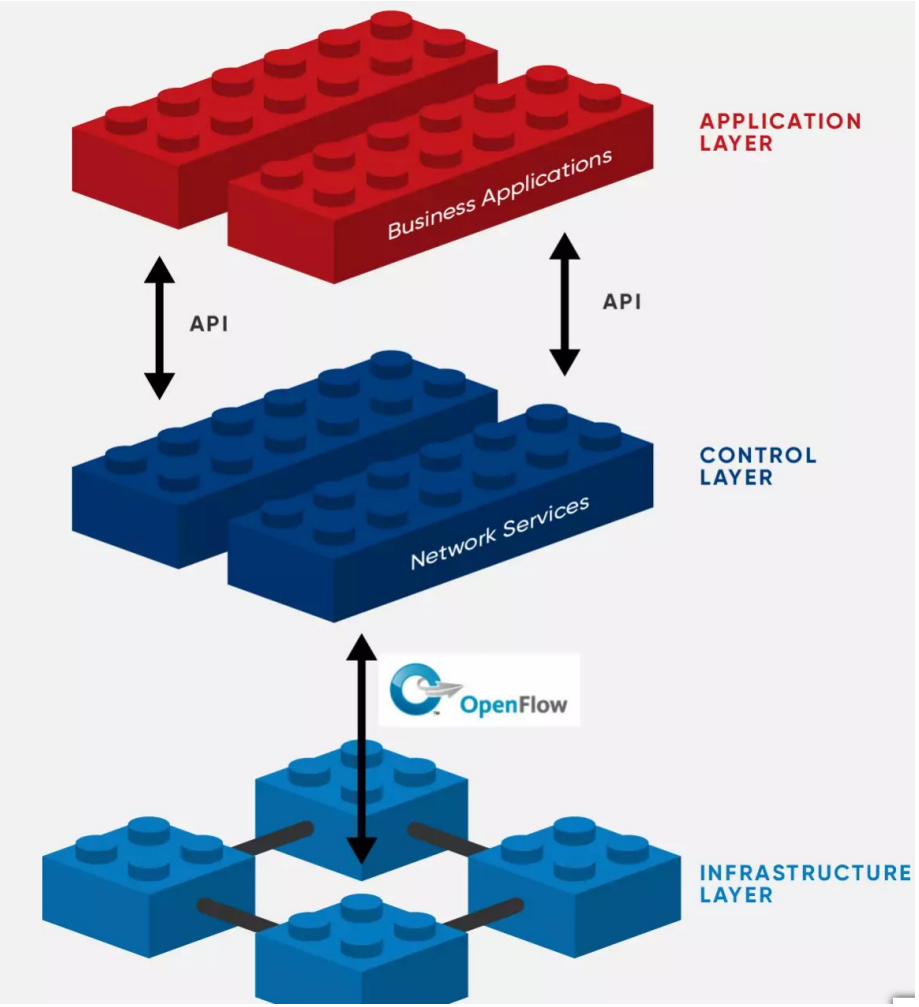
2013

```
Router> enable
Router# configure terminal
Router(config)# enable secret cisco
Router(config)# ip route 0.0.0.0 0.0.0.0 20.2.2.3
Router(config)# interface ethernet0
Router(config-if)# ip address 10.1.1.1 255.0.0.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface serial0
Router(config-if)# ip address 20.2.2.2 255.0.0.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# network 20.0.0.0
Router(config-router)# exit
Router(config)# exit
Router# copy running-config startup-config
Router# disable
Router>
```

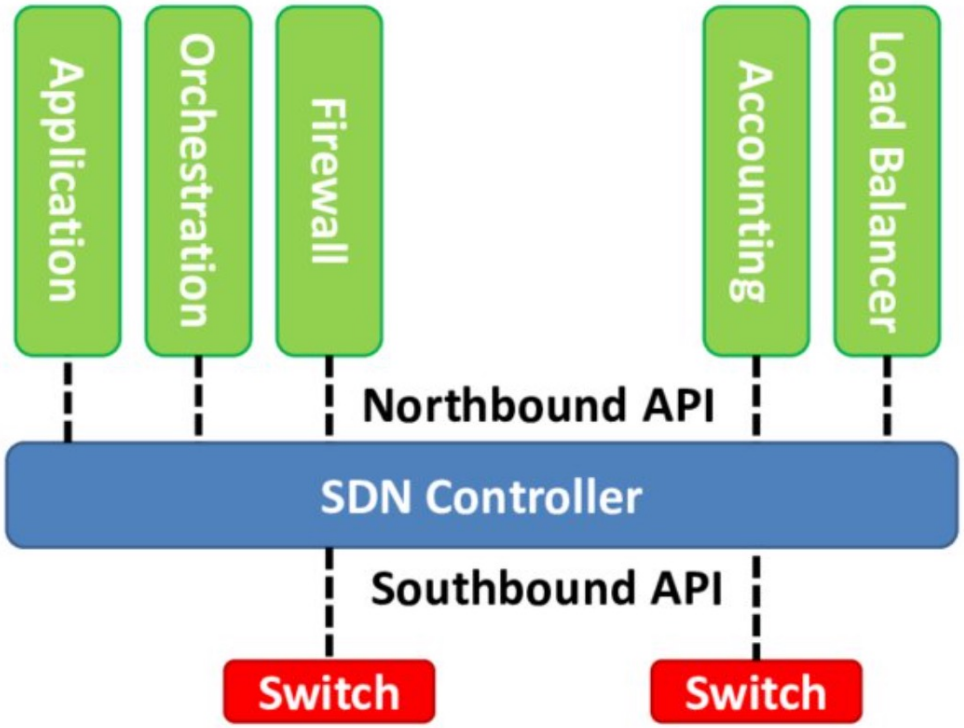
Terminal Protocol: **SSH**

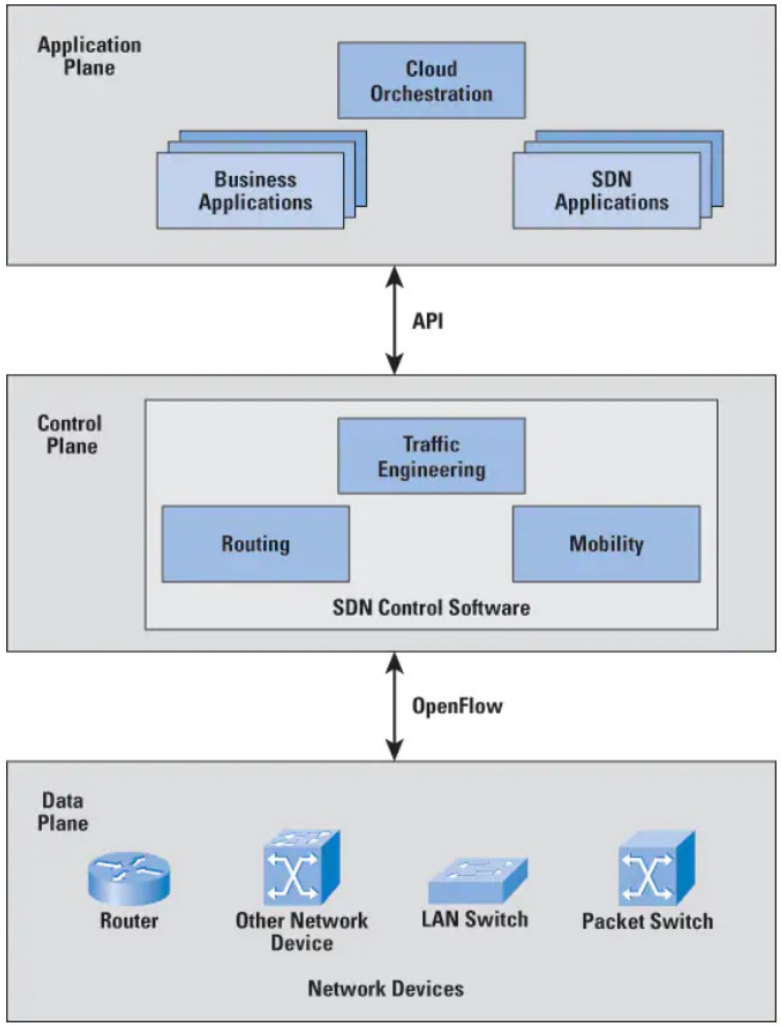
SDN Architecture

- DIRECTLY PROGRAMMABLE
- AGILE
- CENTRALLY MANAGED
- PROGRAMMATICALLY CONFIGURED
- OPEN STANDARDS-BASED AND VENDOR-NEUTRAL



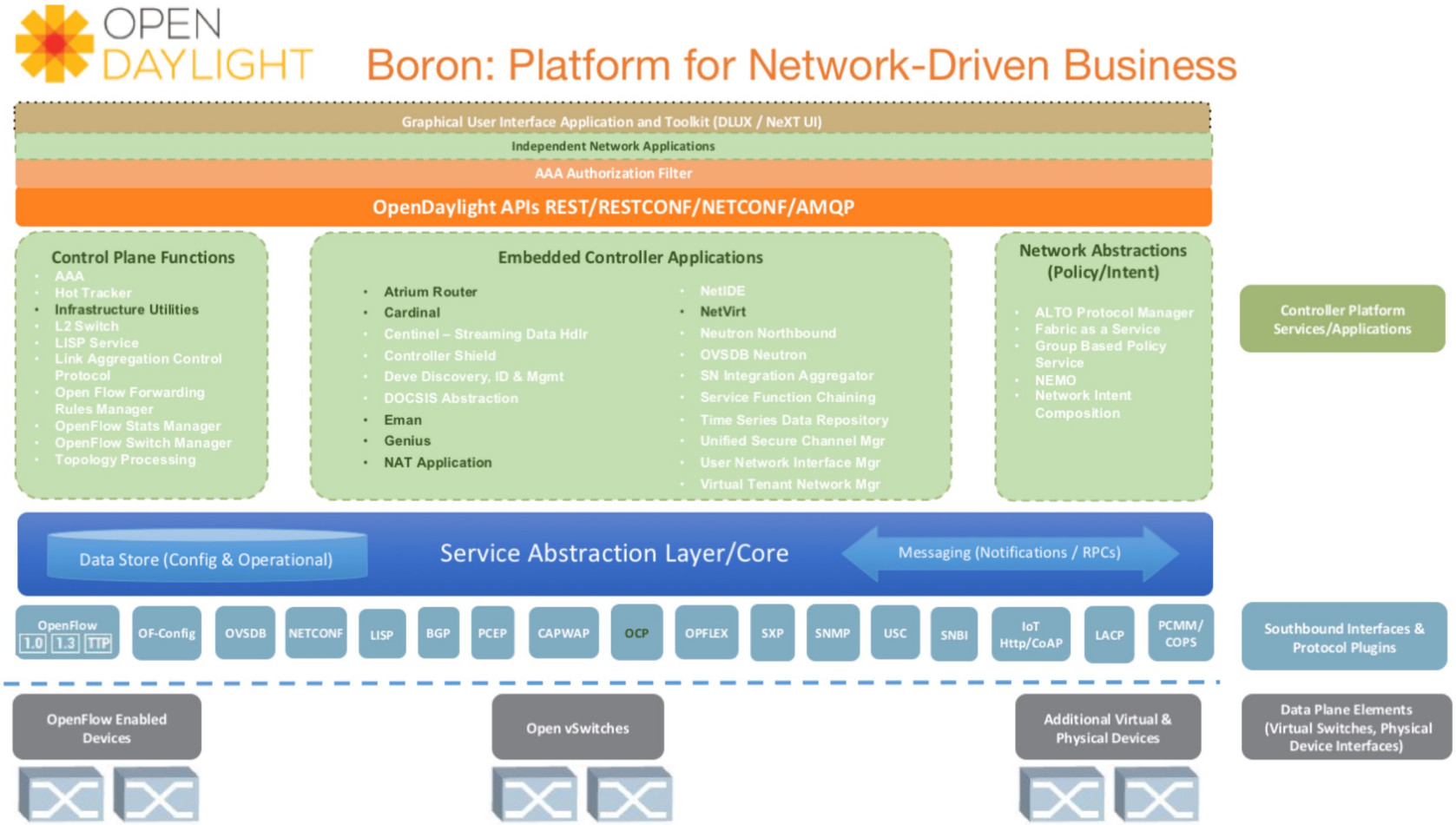
SDN Architecture



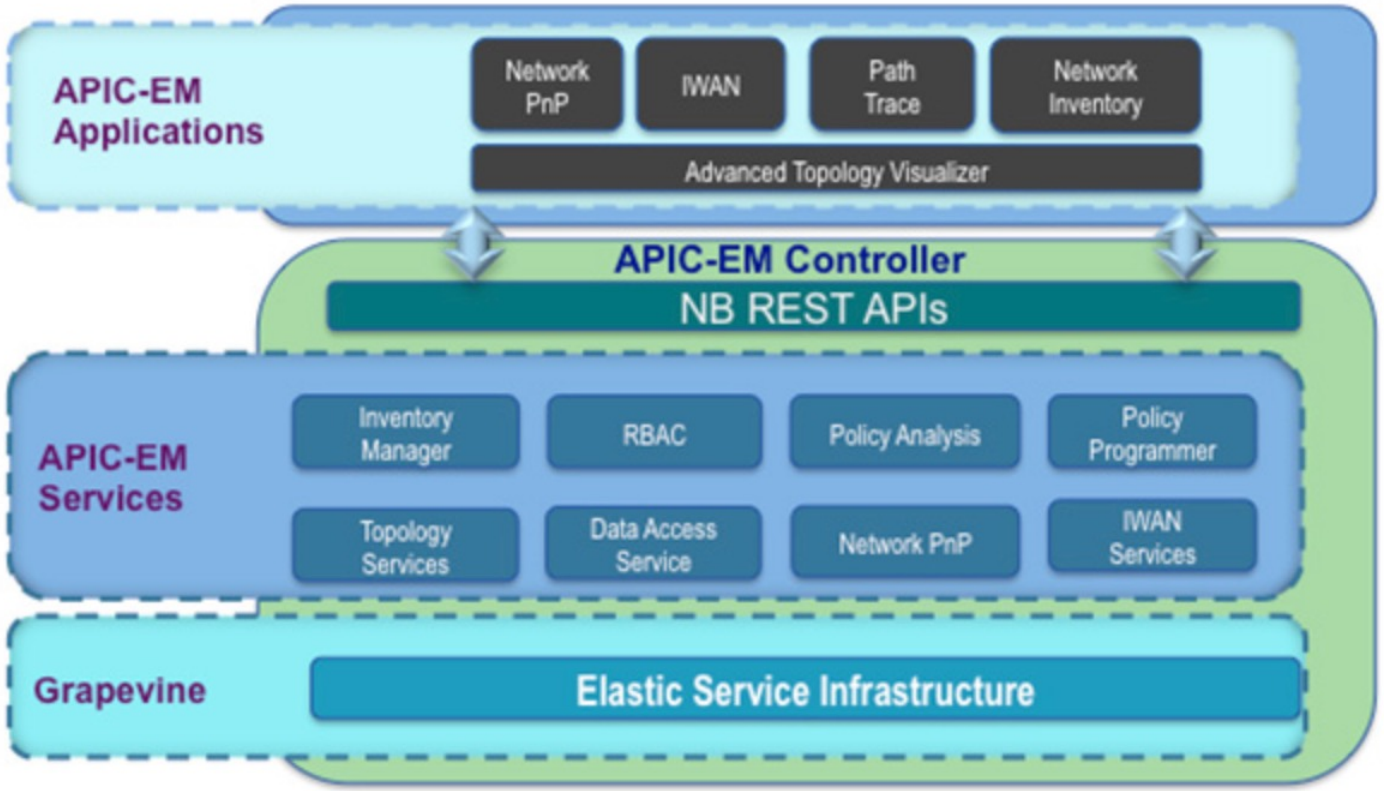


Open Daylight (NorthBound and SouthBound)

Architecture Diagram



Cisco (NorthBound and SouthBound)



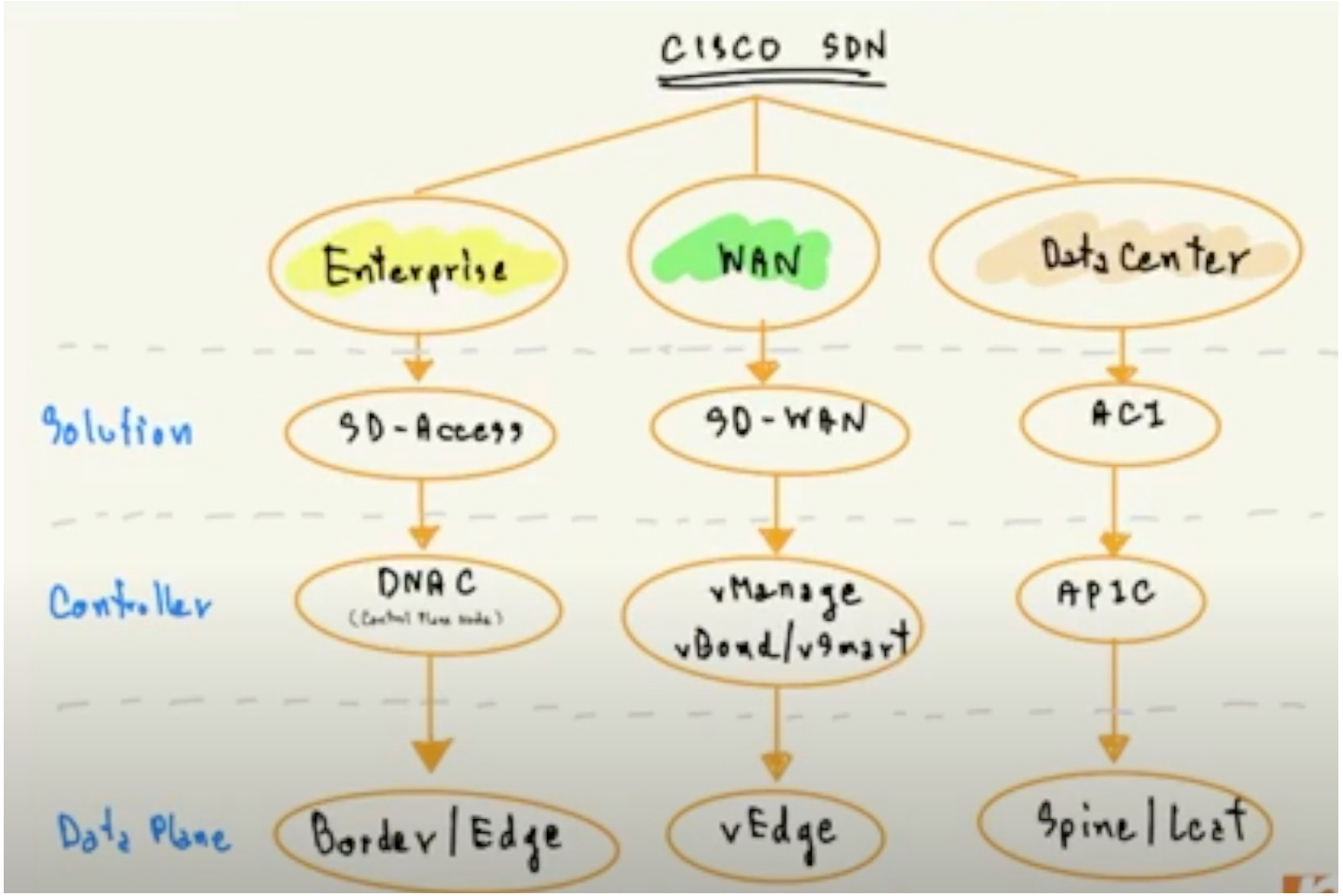
Cisco APIC-EM Northbound Interface

- All capabilities of the controller are exposed through the northbound API. It provides a policy-based abstraction, allowing you to focus on the outcome you want to achieve (for example, "POS traffic is business relevant") rather than focusing on the mechanism that implements that outcome (QoS Policy Map, QoS Class Maps, ACL etc). The Cisco APIC-EM API is REST-based; thus, you can discover and control your network using HTTPS protocol and HTTPS verbs (for example, GET, POST, PUT, and DELETE) with JSON syntax. Cisco APIC-EM features the following key customer applications
- High level application : Python to program

Southbound Interfaces

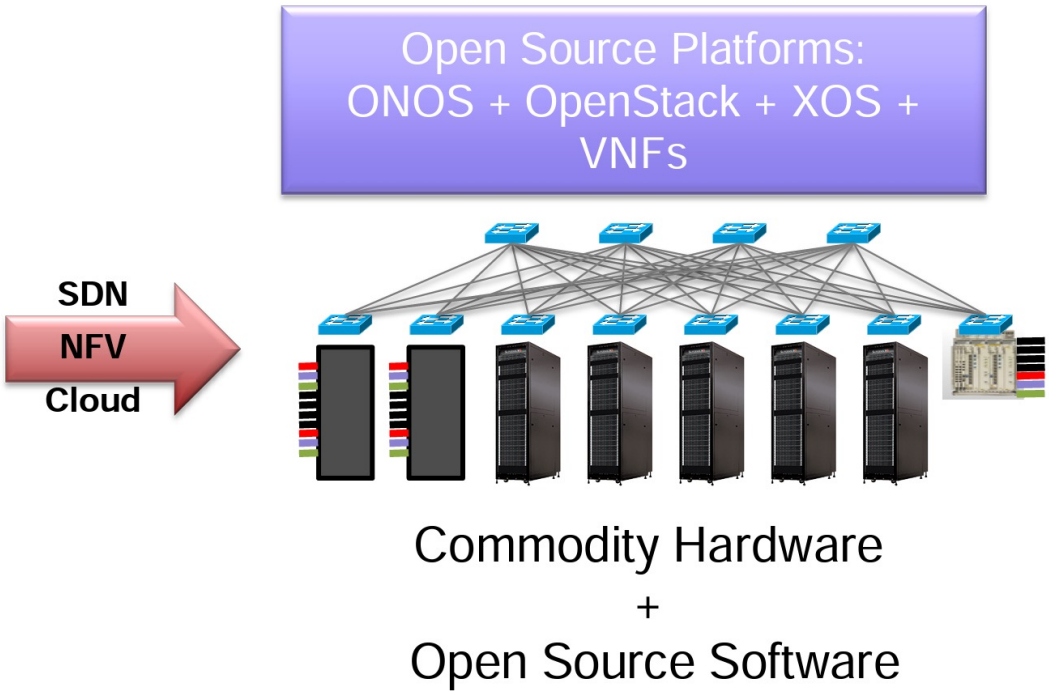
- APIC-EM abstracts the southbound protocols via a rich northbound REST API. Currently supported protocols include CLI/SNMP and in the future will include NETCONF/YANG, but protocol details are hidden from the API consumer. As a user of the controller, you need not concern yourself with the specific protocols that implement your network intent.

ประเภทของ SDN ที่ใช้งาน



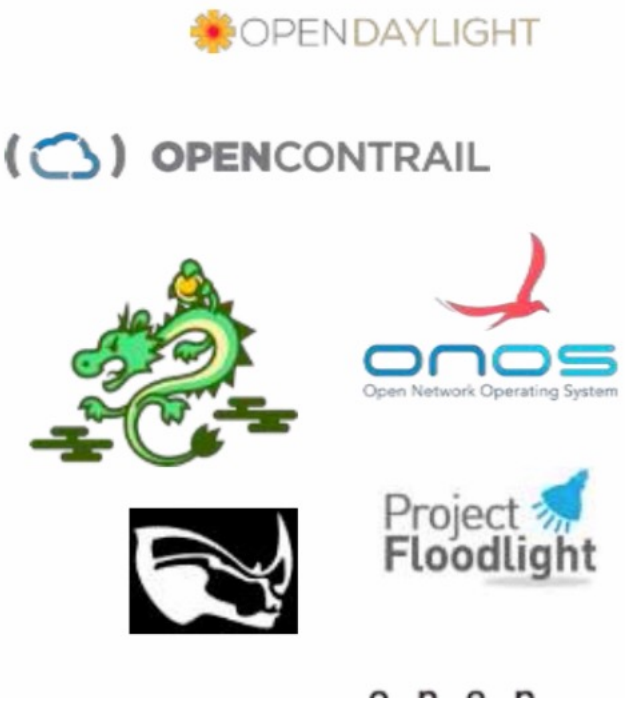
CORD: Central Office Re-architected as a Datacenter

CORD = SDN x NFV x Cloud



Controller Landscape

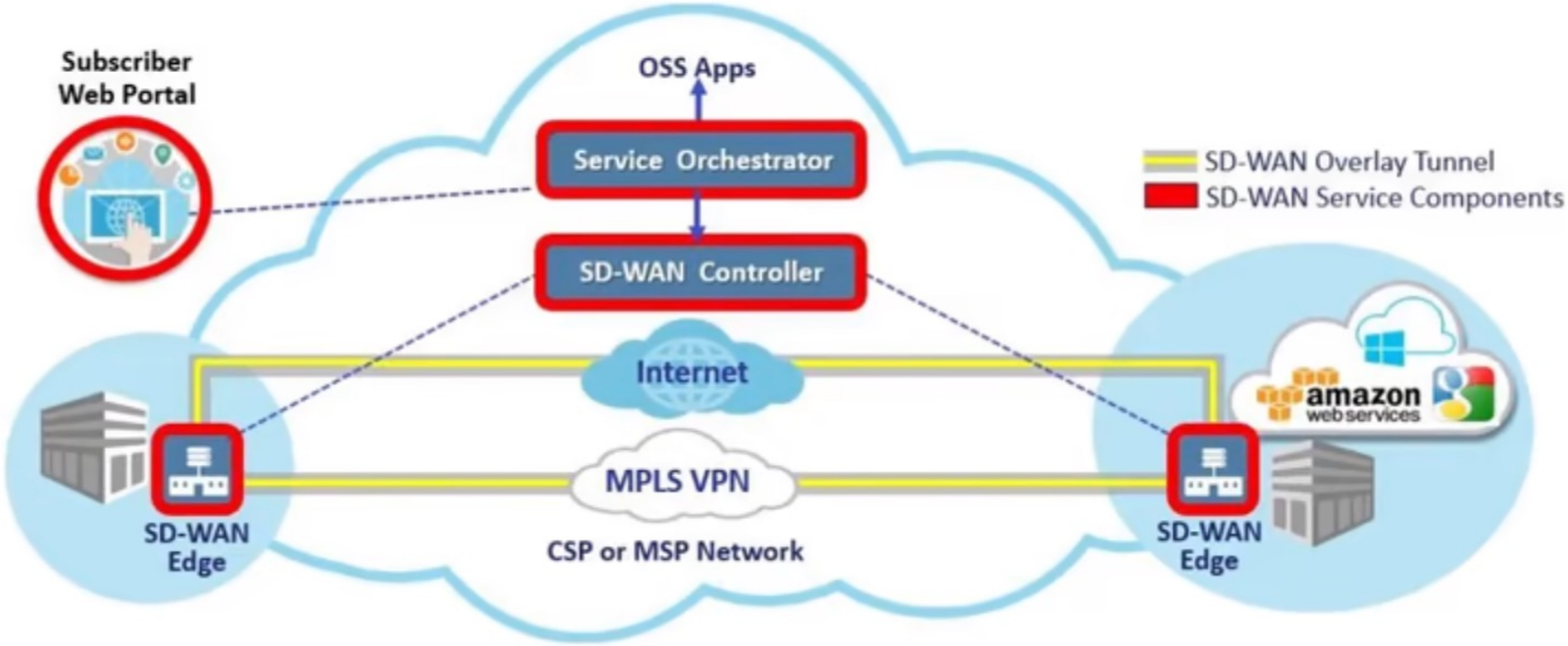
Active	Not Active (Apparently)
Floodlight	Beacon
LOOM	FlowER
OpenContrail*	NOX/POX
OpenDaylight*	NodeFlow
OpenMUL	
ONOS*	
Ryu*	
Trema	

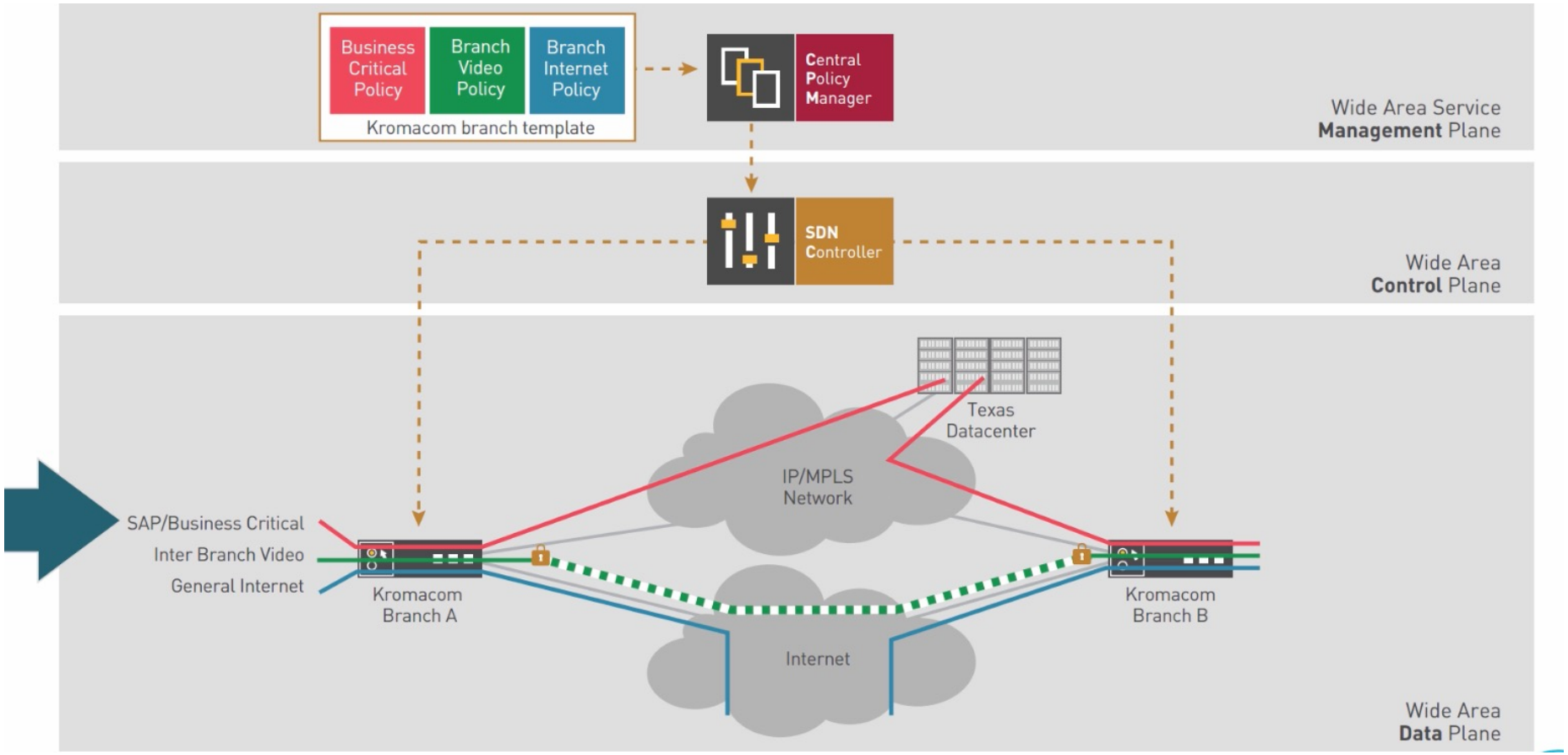


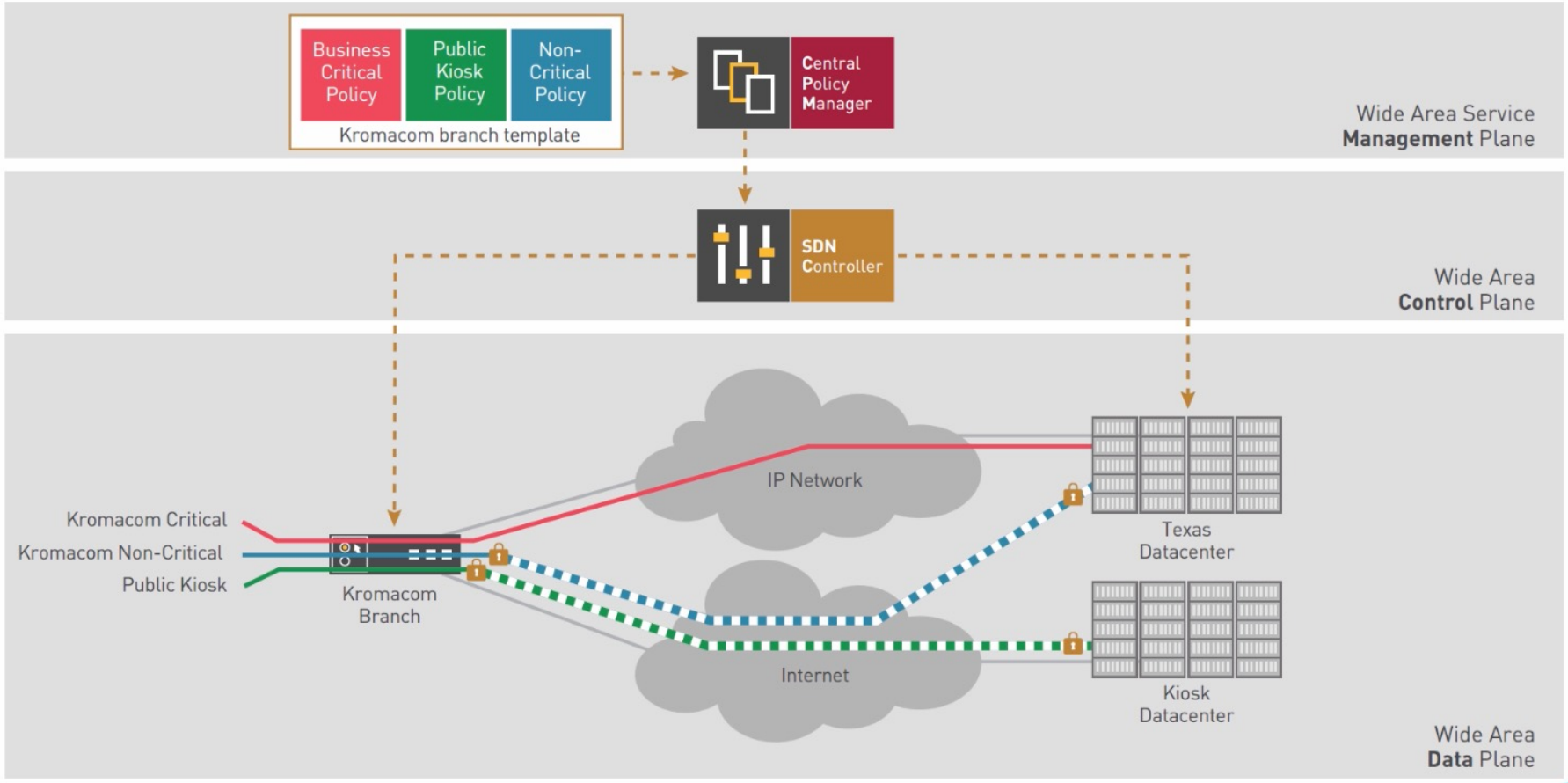
SD-WAN

- An SD-WAN (or SDWAN) can connect several branch locations to a central hub office or cover multiple locations in a large campus such as a university campus. Because it is abstracted from hardware, it is more flexible and available than a standard WAN.

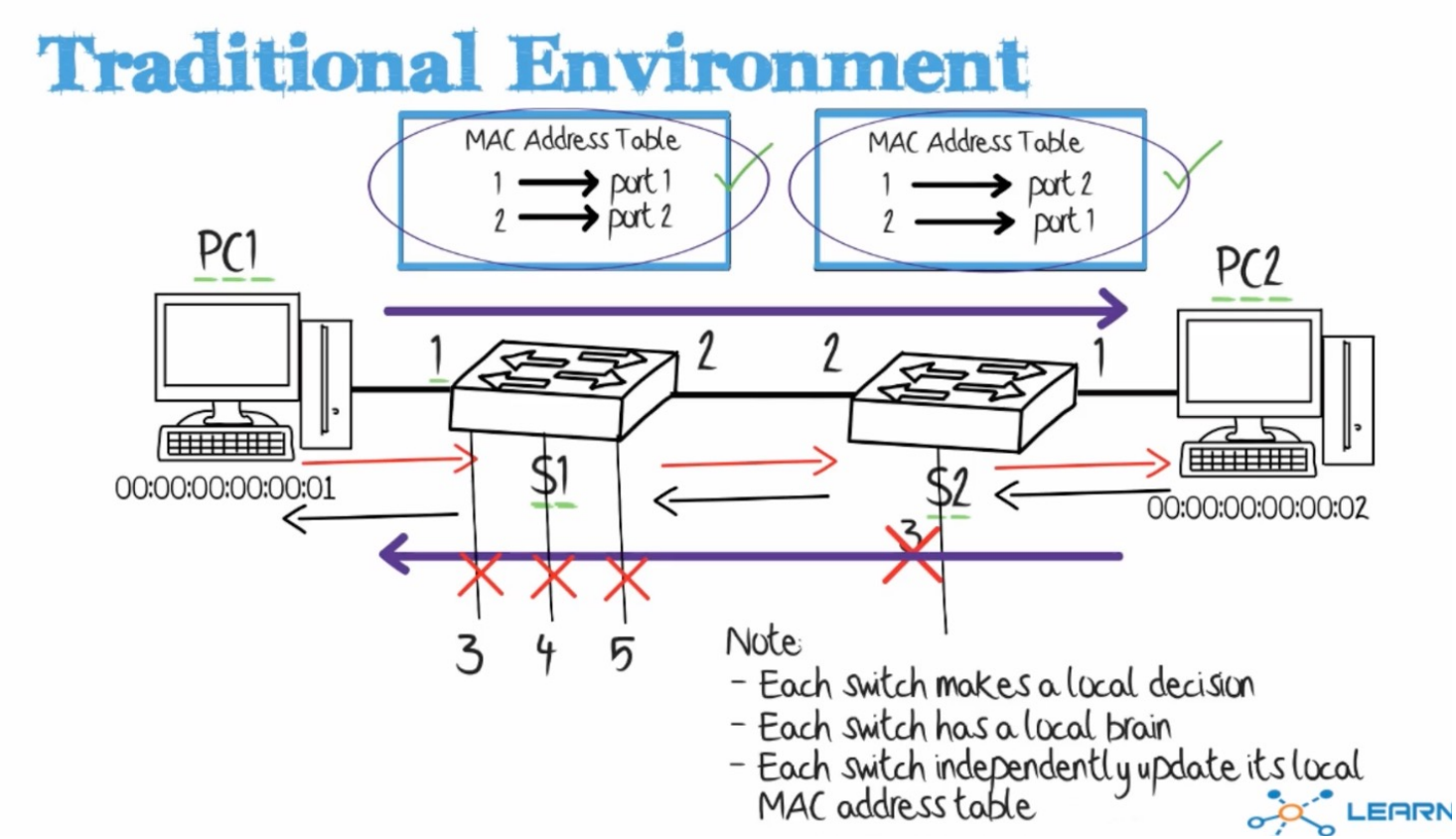
SD-WAN Service Components



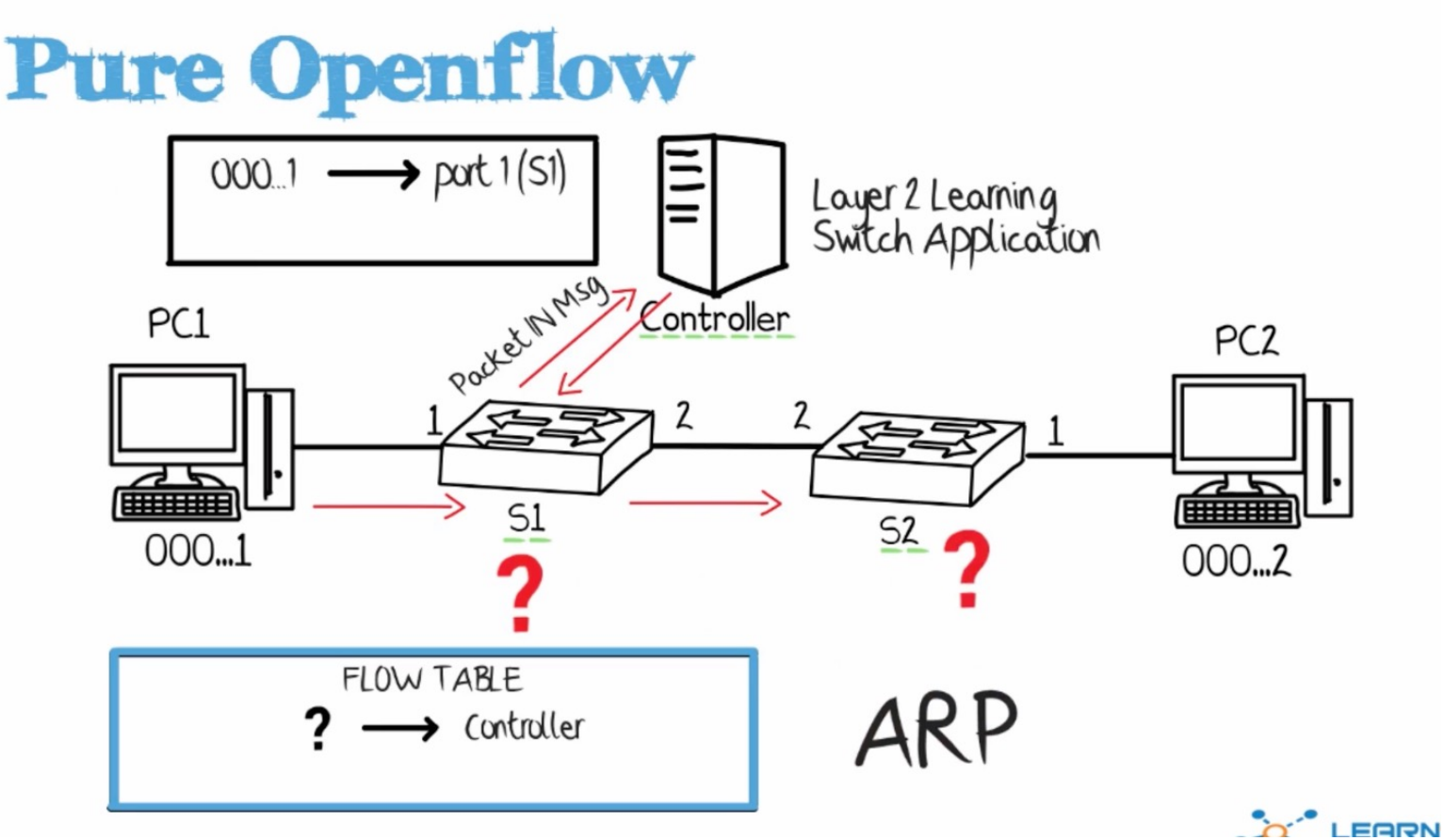

Business Critical Policy
Branch Video Policy
Branch Internet Policy
Kromacom branch template
Central Policy Manager
Wide Area Service Management Plane
SDN Controller
Wide Area Control Plane
Texas Datacenter
IP/MPLS Network
SAP/Business Critical
Inter Branch Video
General Internet
Kromacom Branch A
Kromacom Branch B
Internet
Wide Area Data Plane


Business Critical Policy
Public Kiosk Policy
Non-Critical Policy
Kromacom branch template
Central Policy Manager
Wide Area Service Management Plane
SDN Controller
Wide Area Control Plane
IP Network
Kromacom Critical
Kromacom Non-Critical
Public Kiosk
Kromacom Branch
Texas Datacenter
Internet
Kiosk Datacenter
Wide Area Data Plane

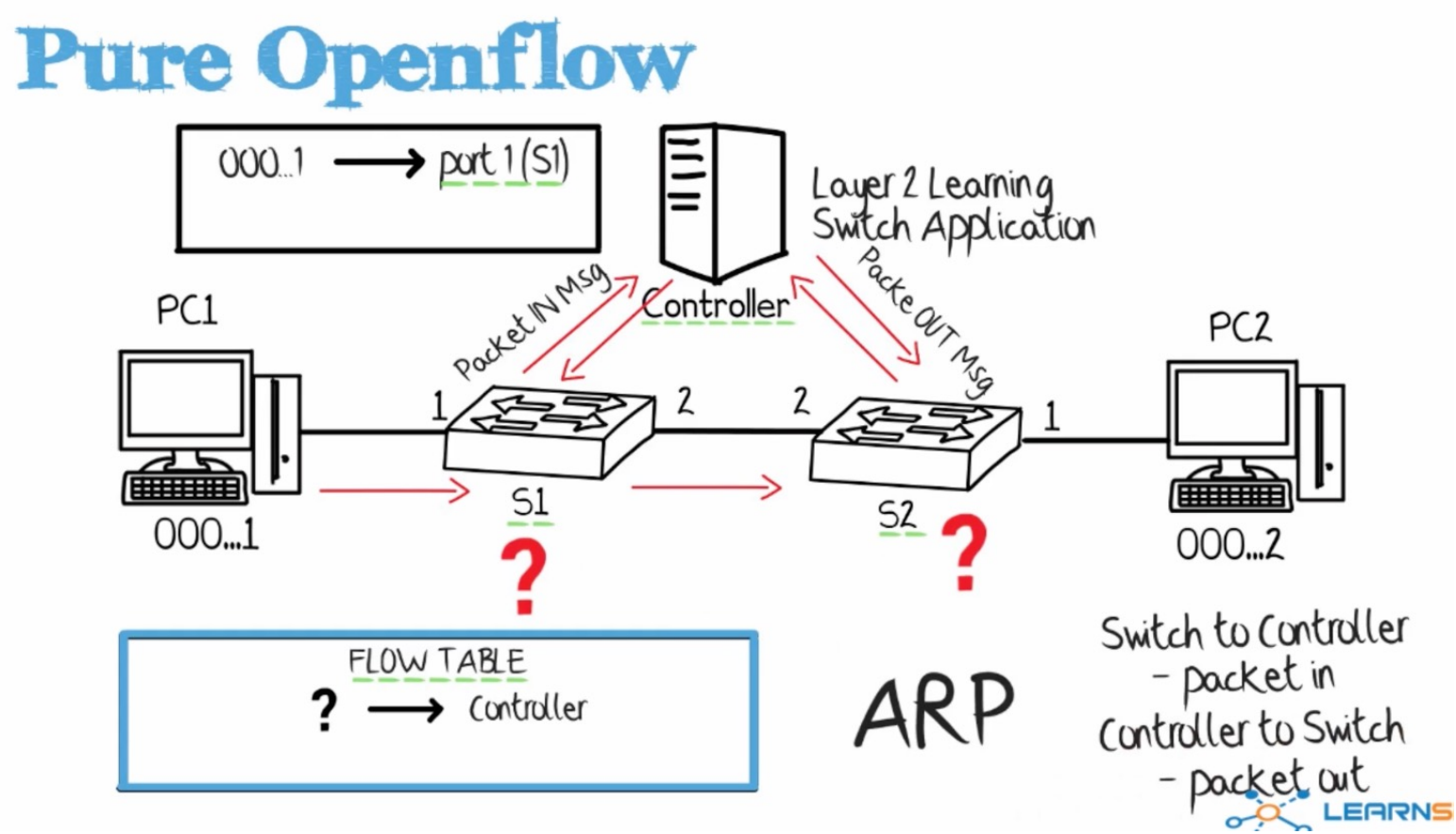
Traditional Forwarding



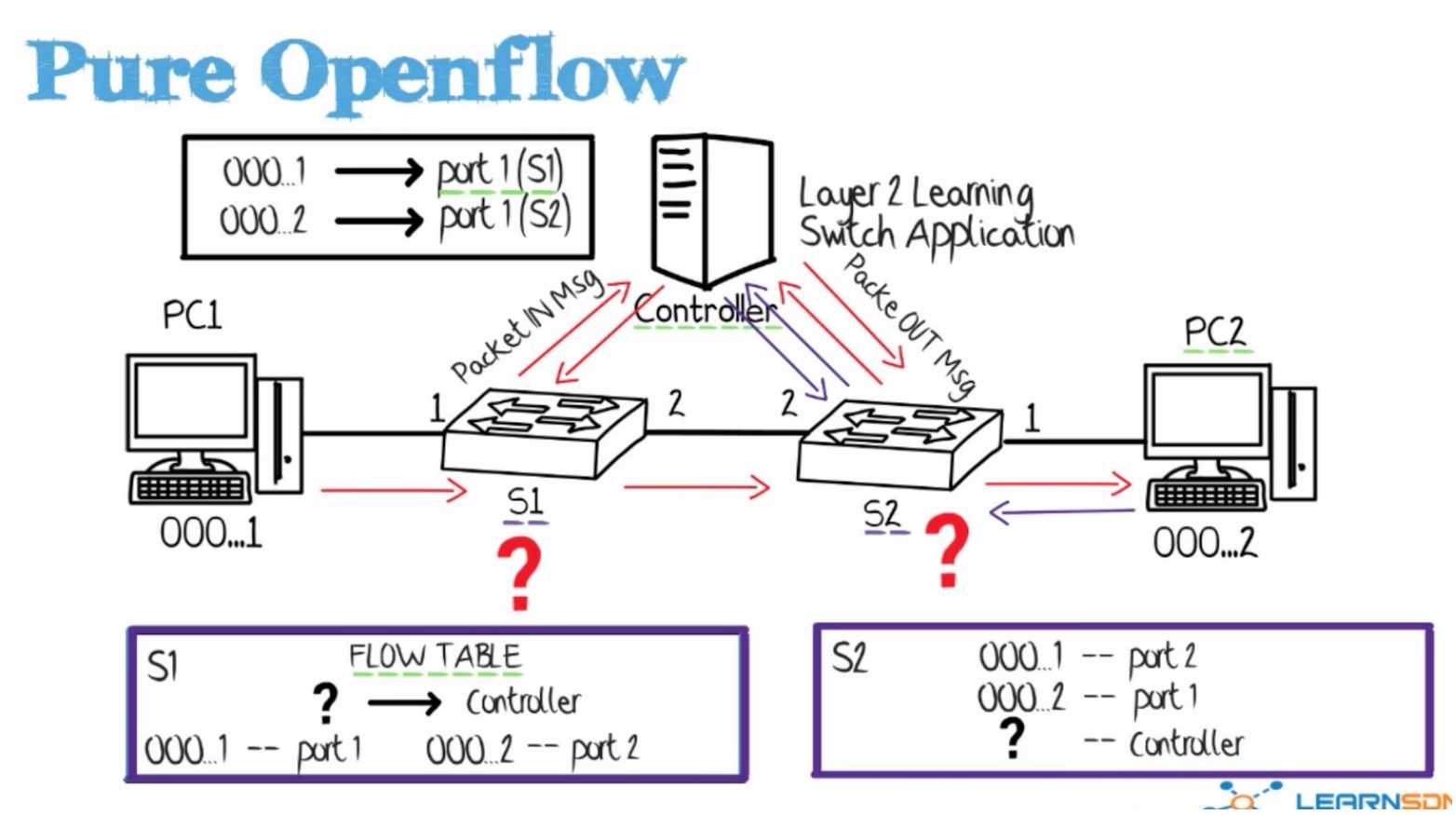
OpenFlow Forwarding



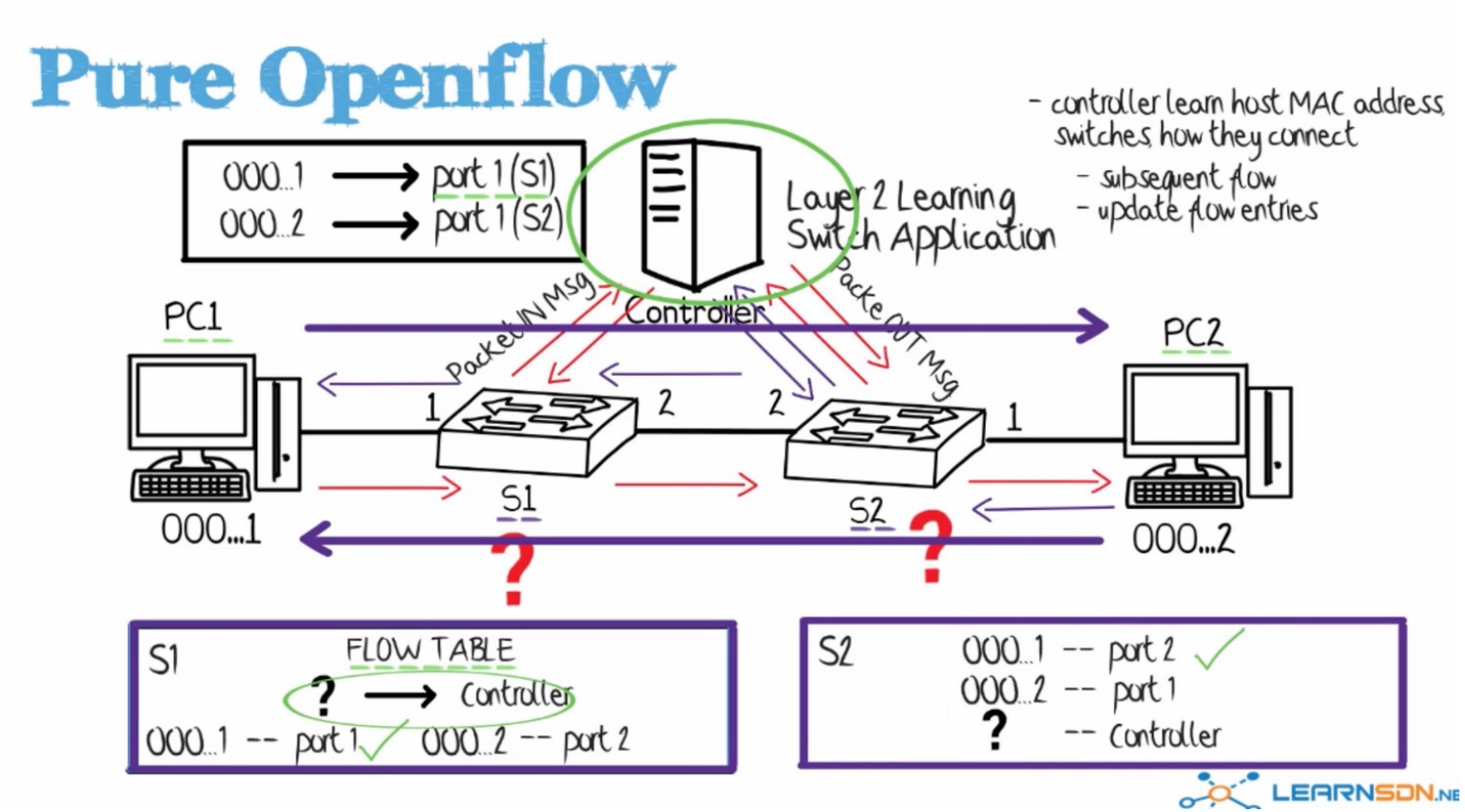
OpenFlow Forwarding



OpenFlow Forwarding



OpenFlow Forwarding



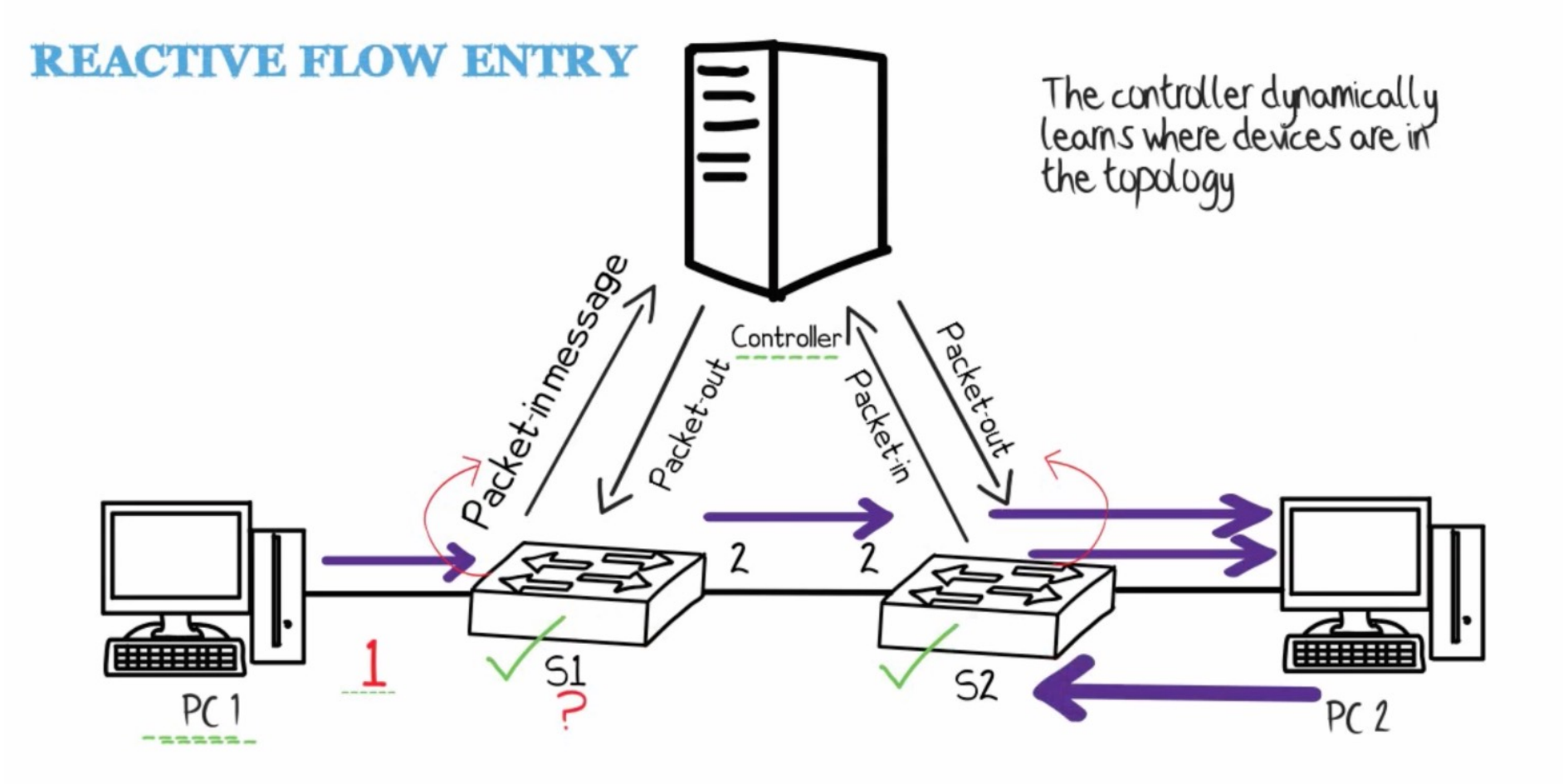
PROACTIVE FLOW ENTRY
vs
REACTIVE FLOW ENTRY

DOES EVERY FIRST PAKCET HAVE TO GO TO THE CONTROLLER?

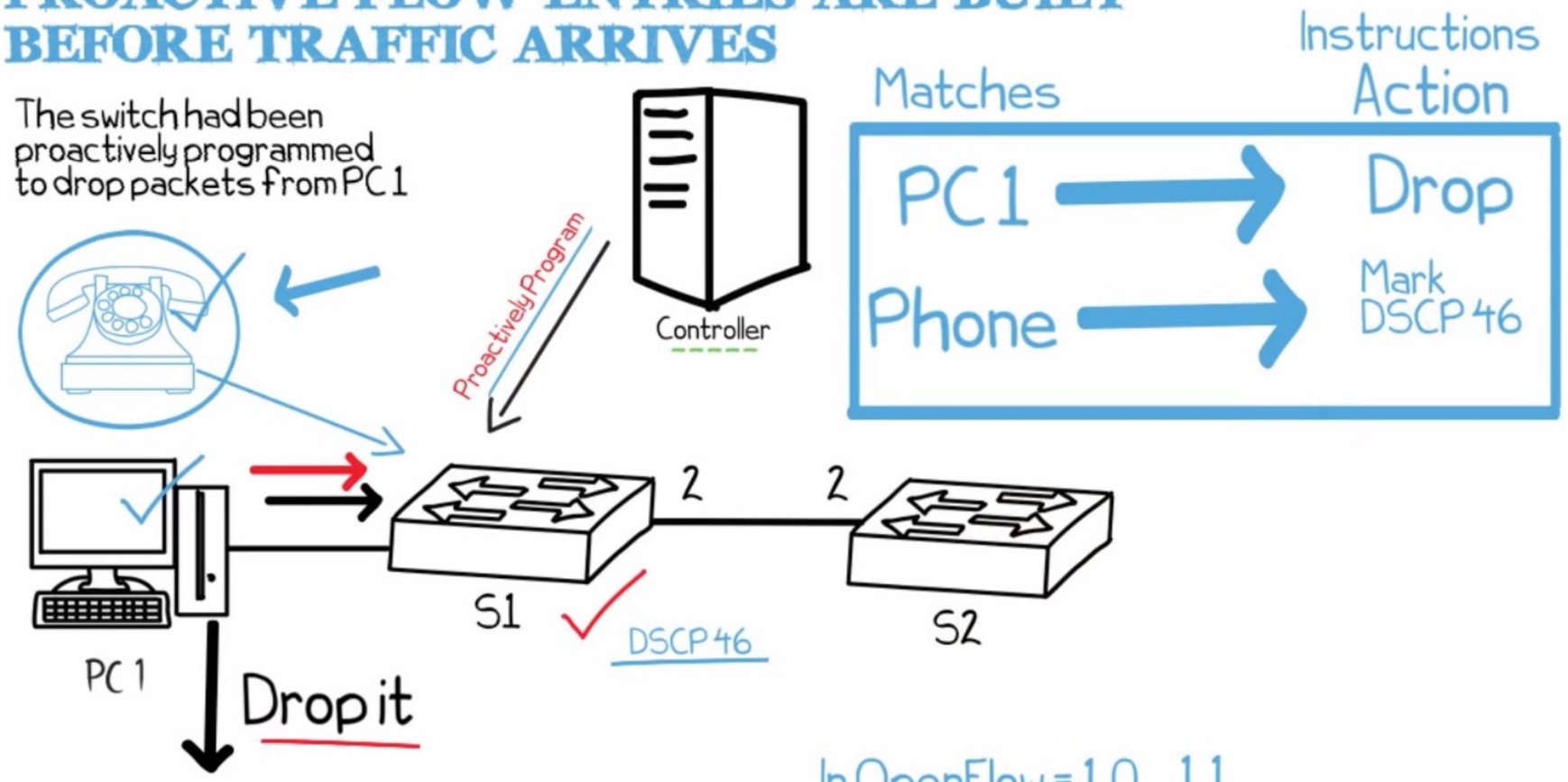
HOW FAR AWAY CAN THE CONTROLLER BE FROM THE SWITCHES?

DOES THE CONTROLLER HAVE TO BE IN THE SAME SWITCH?

CAN IT BE IN THE SAME LOCAL AREA NETWORK?

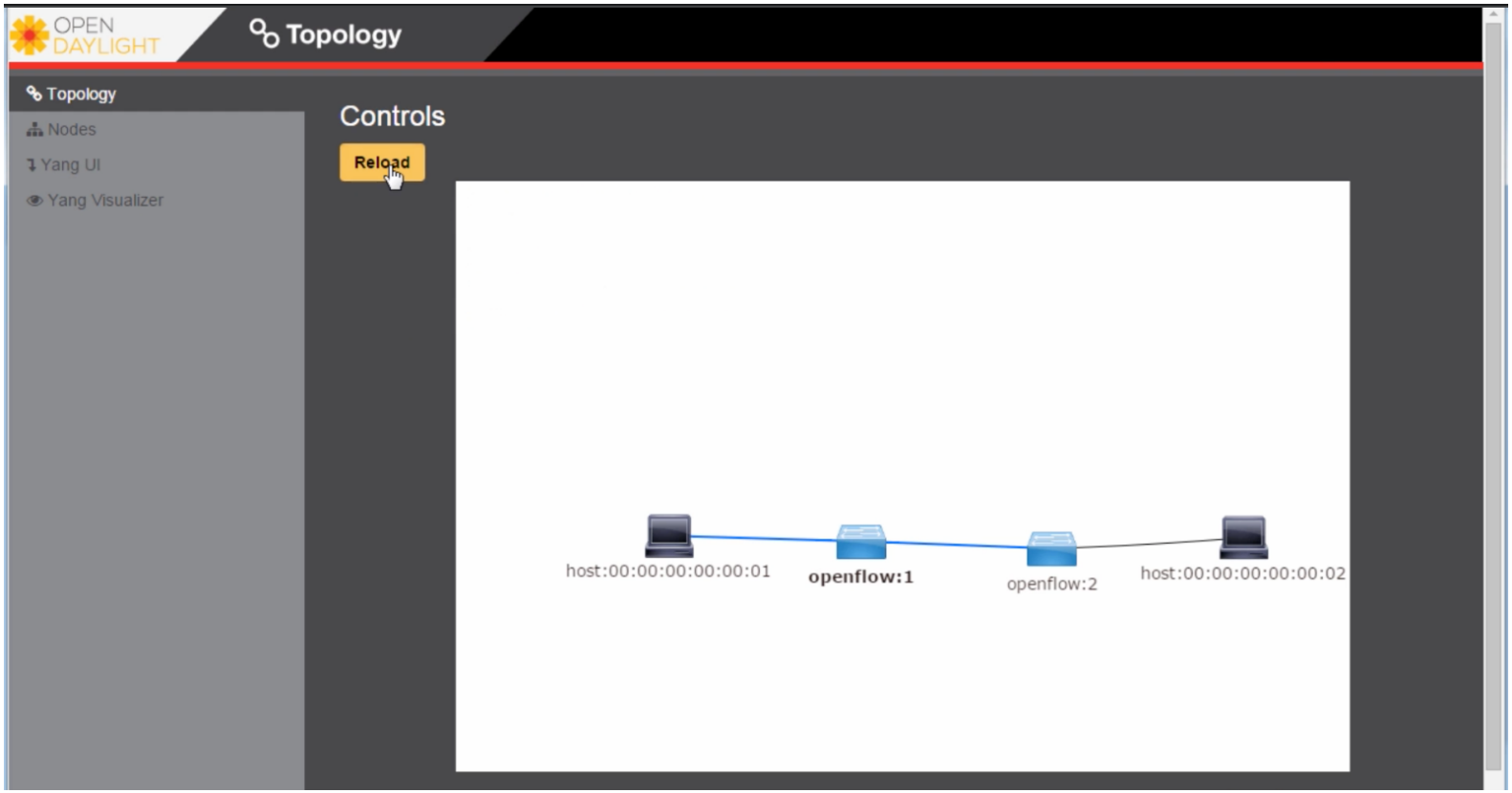

REACTIVE FLOW ENTRY
The controller dynamically learns where devices are in the topology
Controller
Packet-in message
Packet-out
Packet-in
Packet-out
2
2
1
PC 1
S1
?
S2
PC 2

PROACTIVE FLOW ENTRIES ARE BUILT BEFORE TRAFFIC ARRIVES

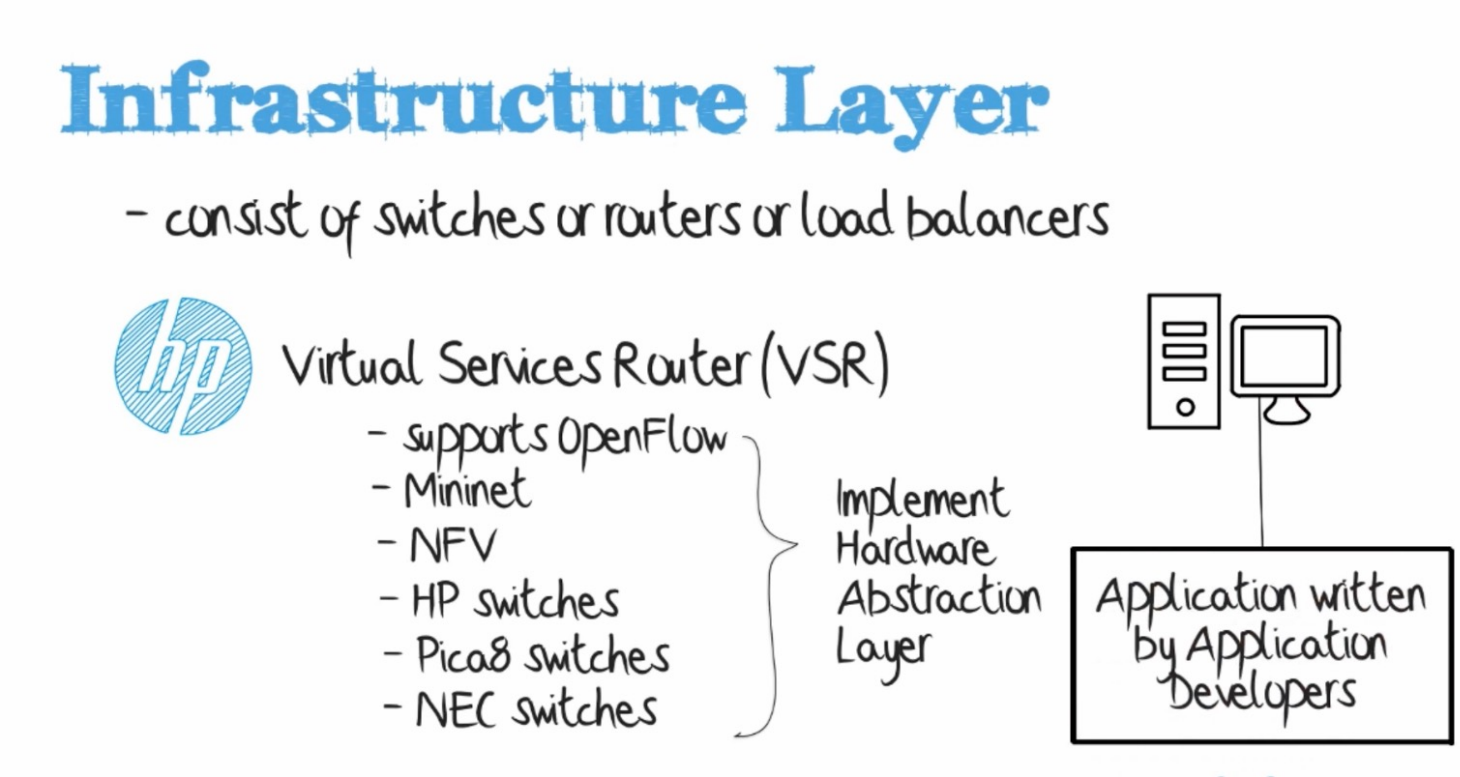


In OpenFlow = 1.0 1.1

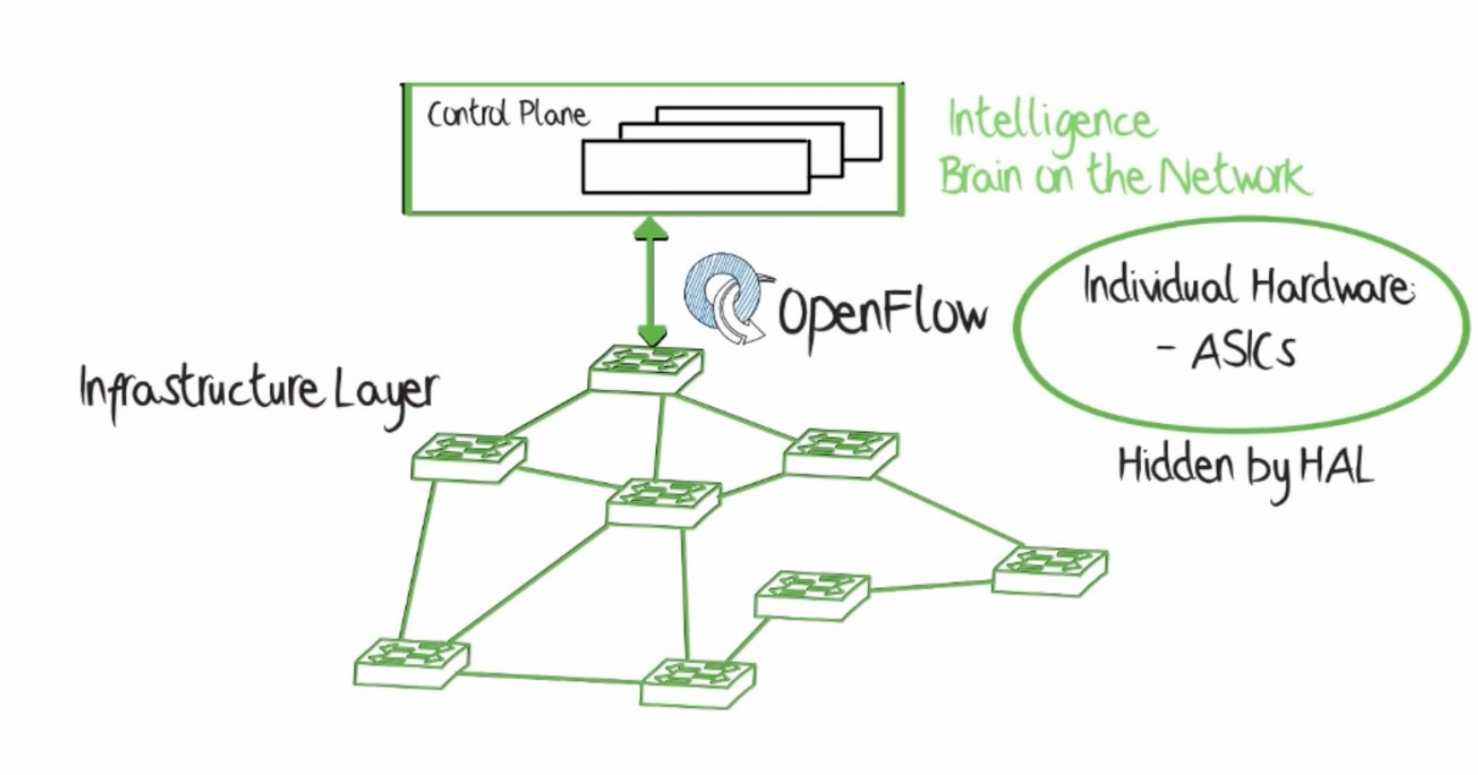
Example of Controller



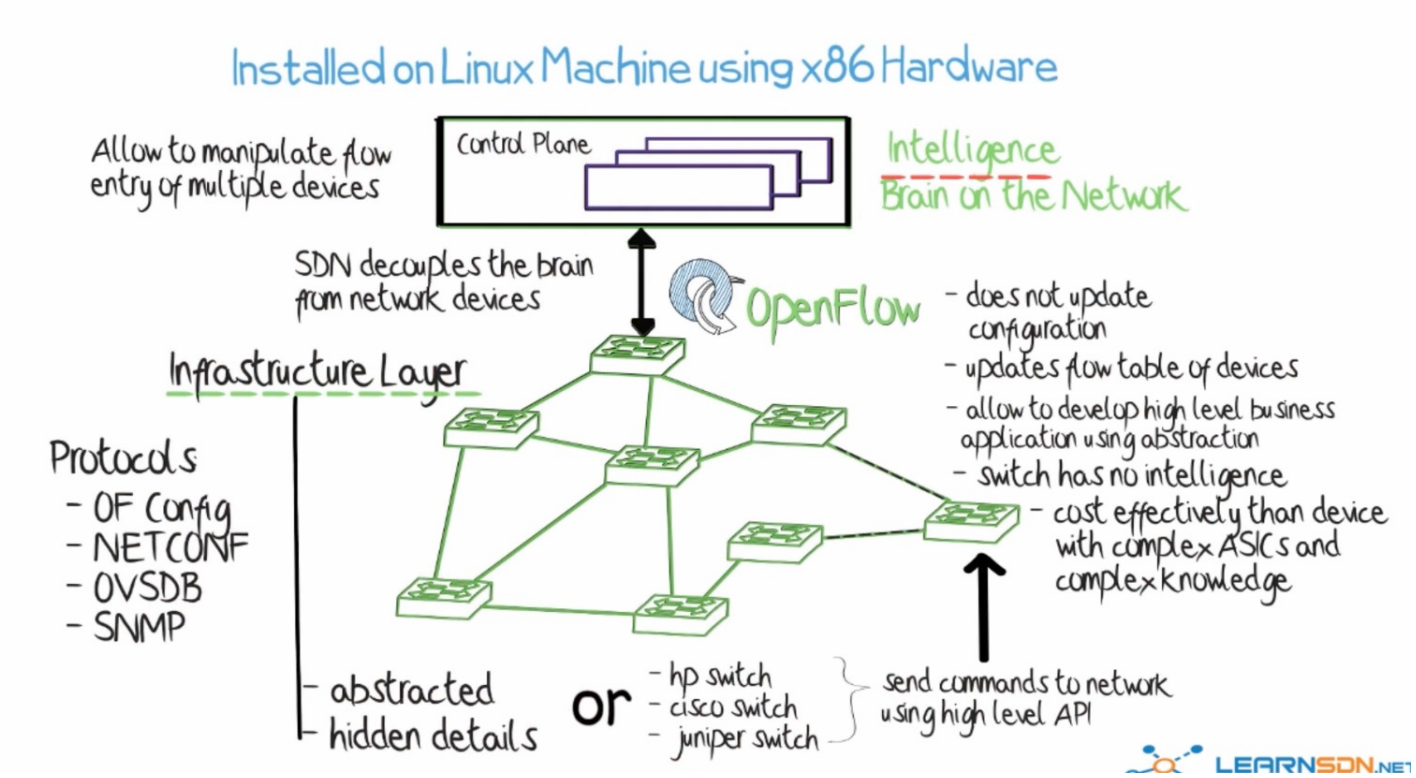
SDN Architecture



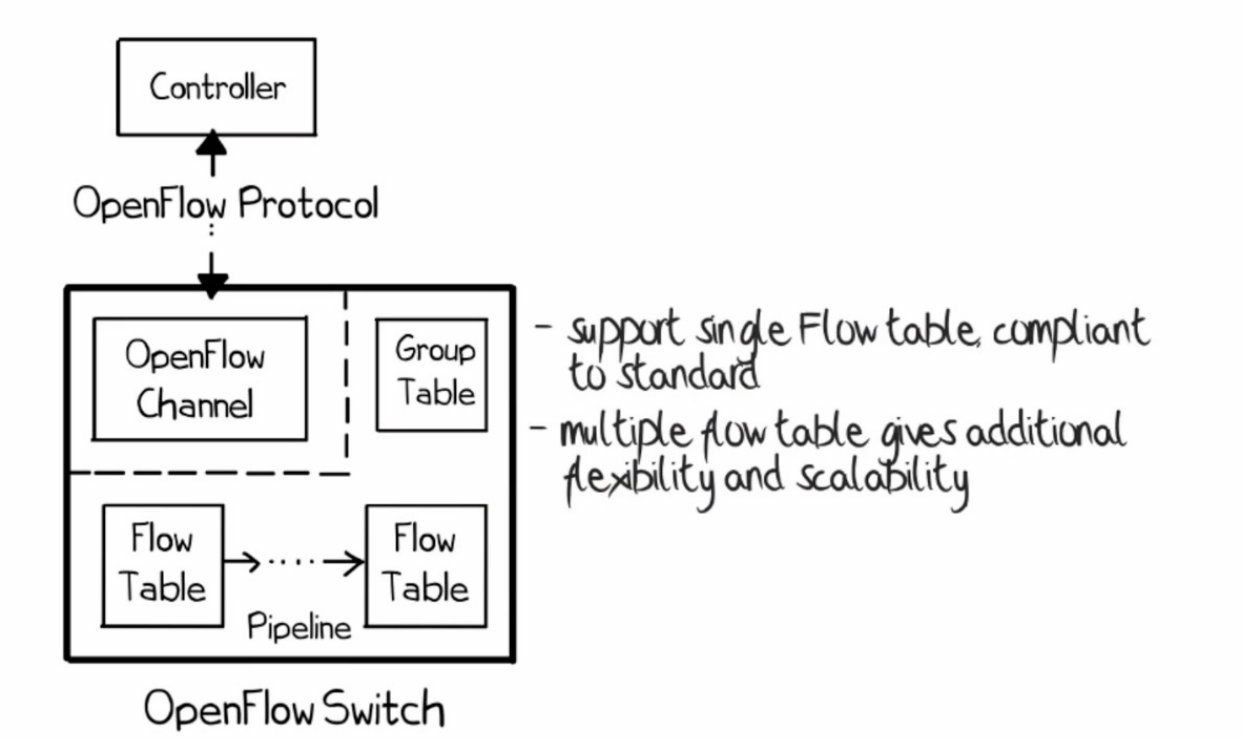
SDN Architecture



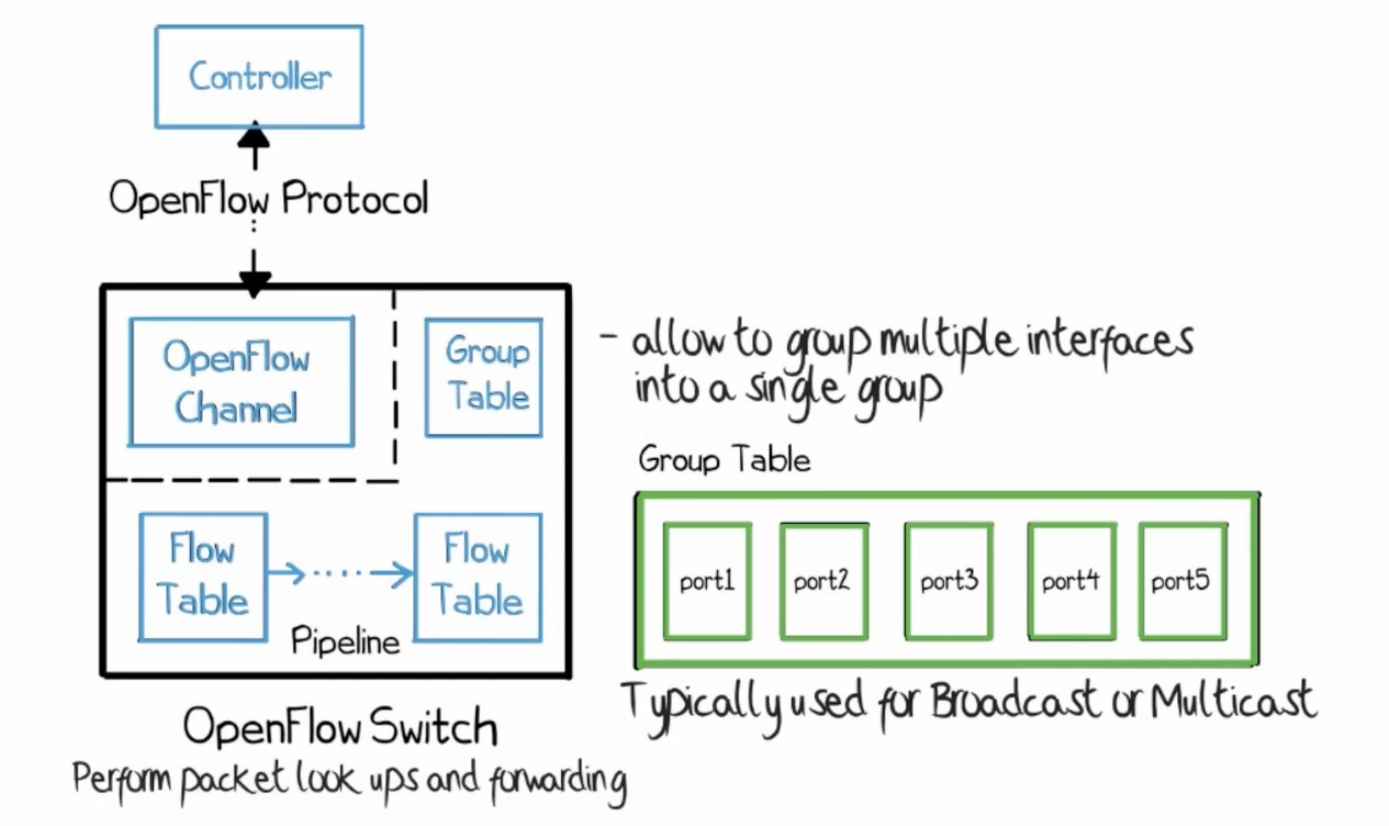
SDN Architecture



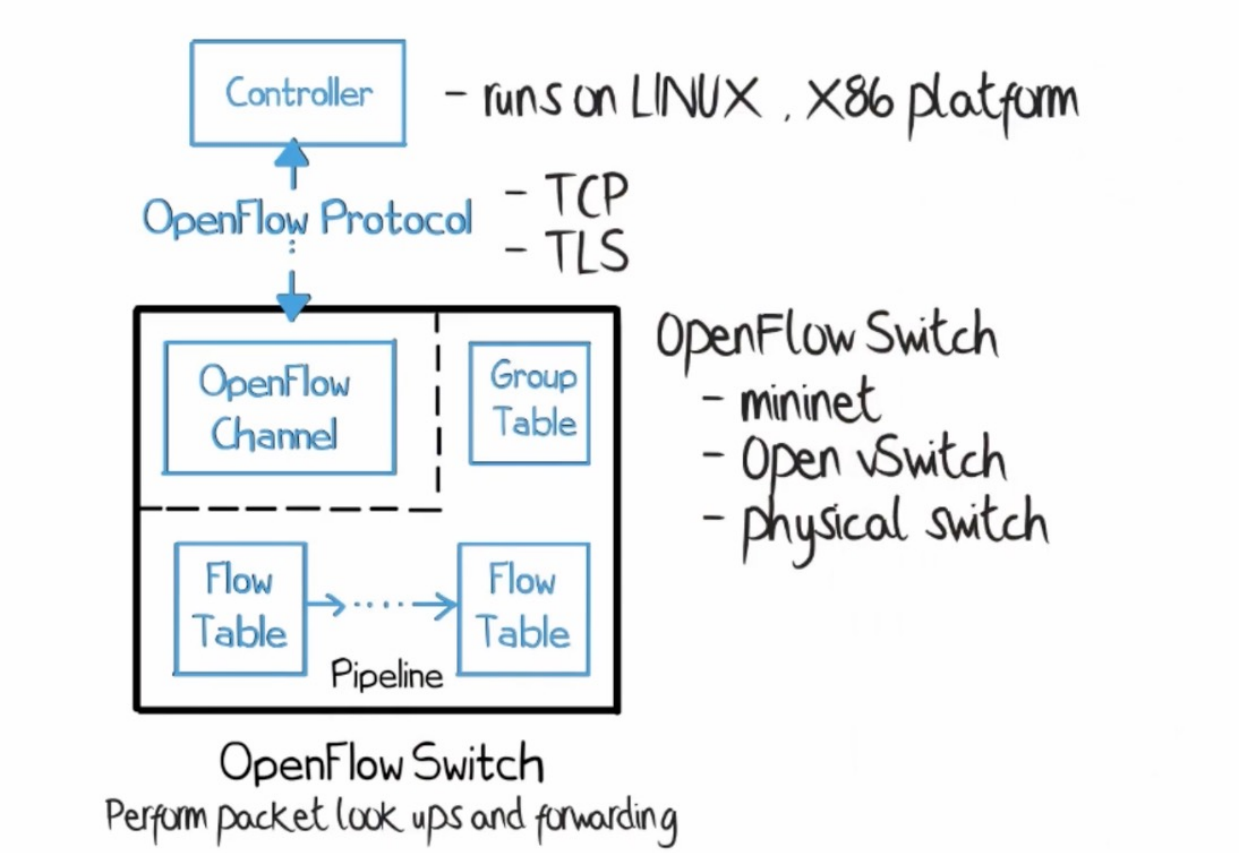
OpenFlow Switch



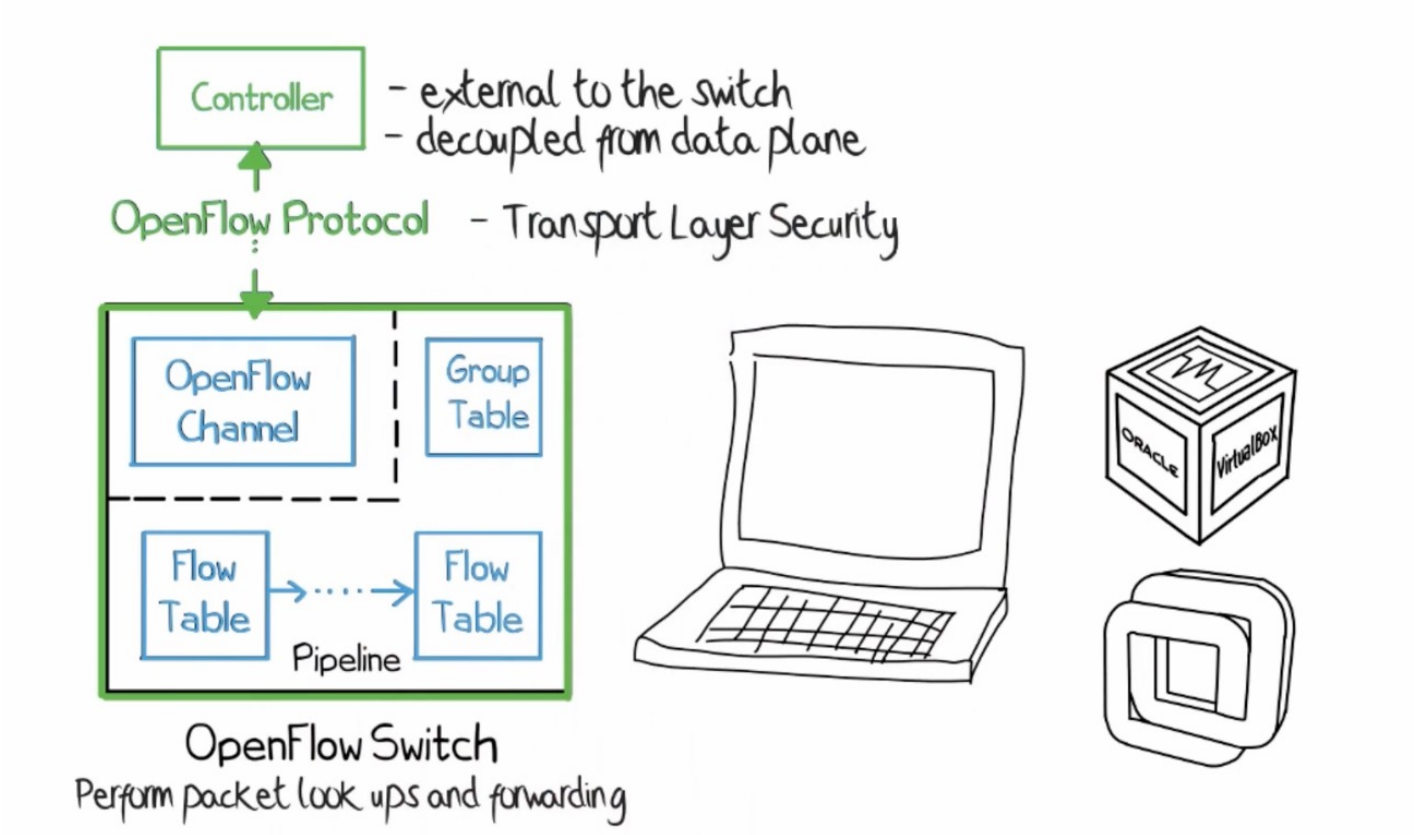
OpenFlow Switch



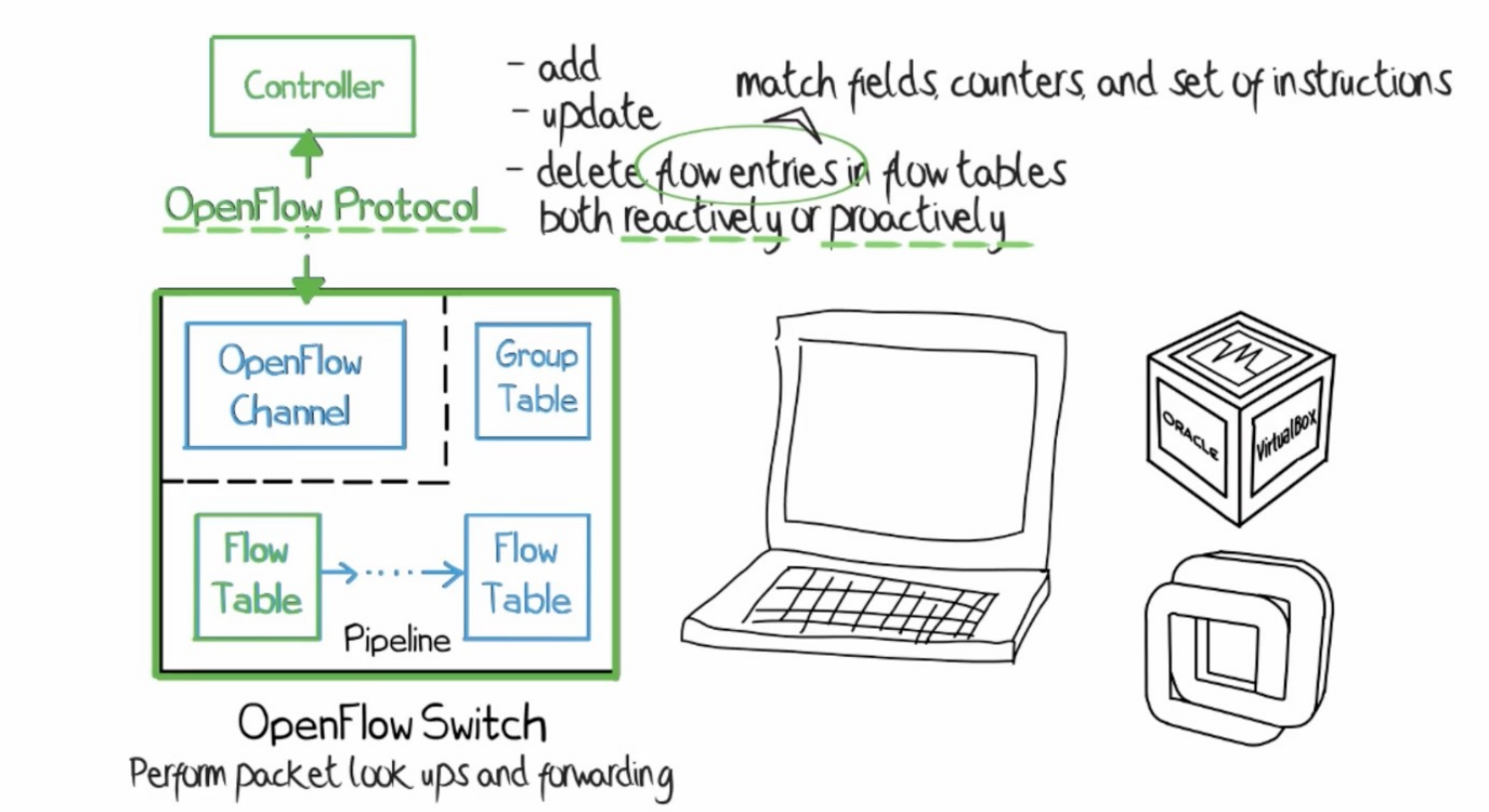
OpenFlow Switch



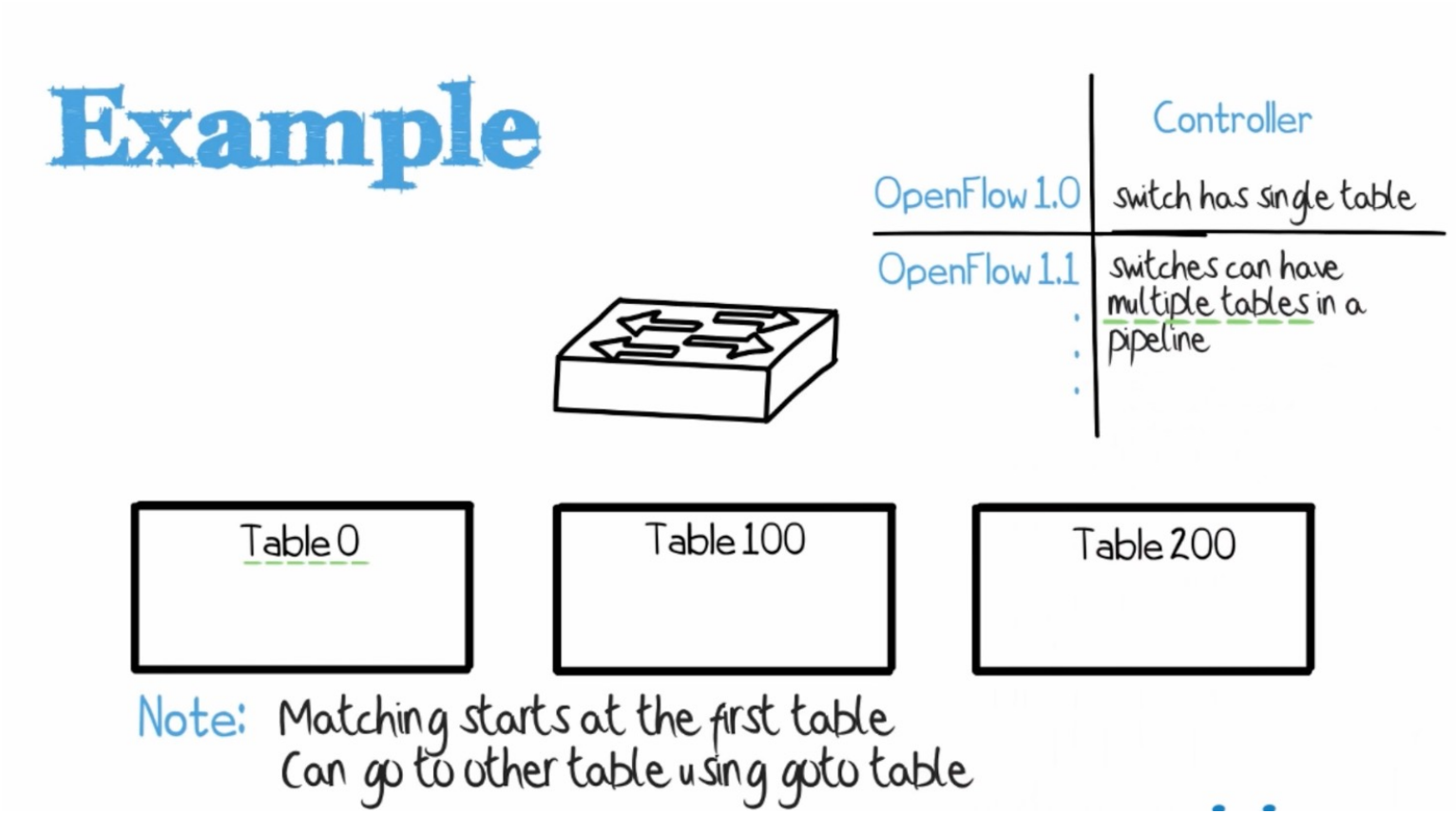
OpenFlow Switch



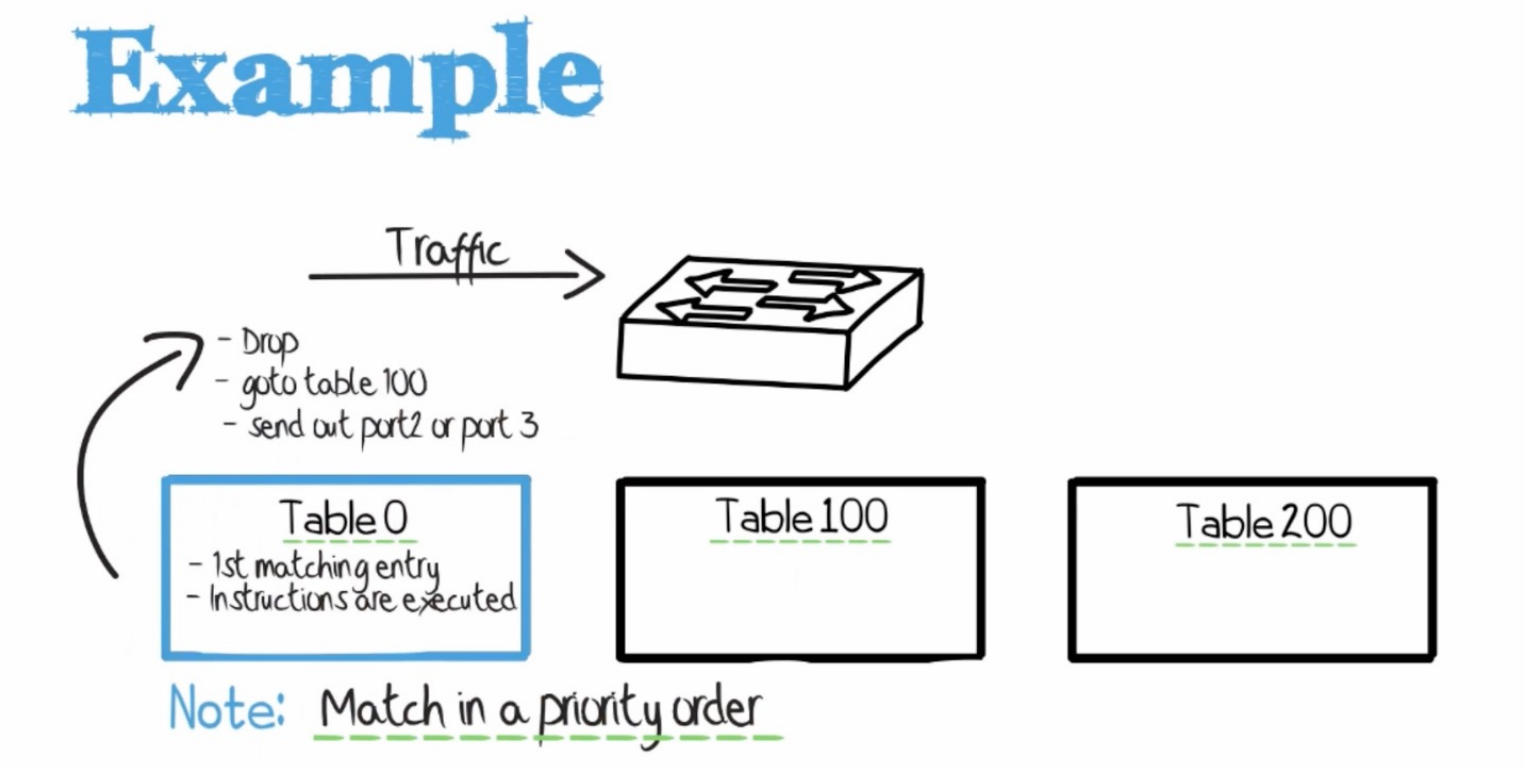
OpenFlow Switch



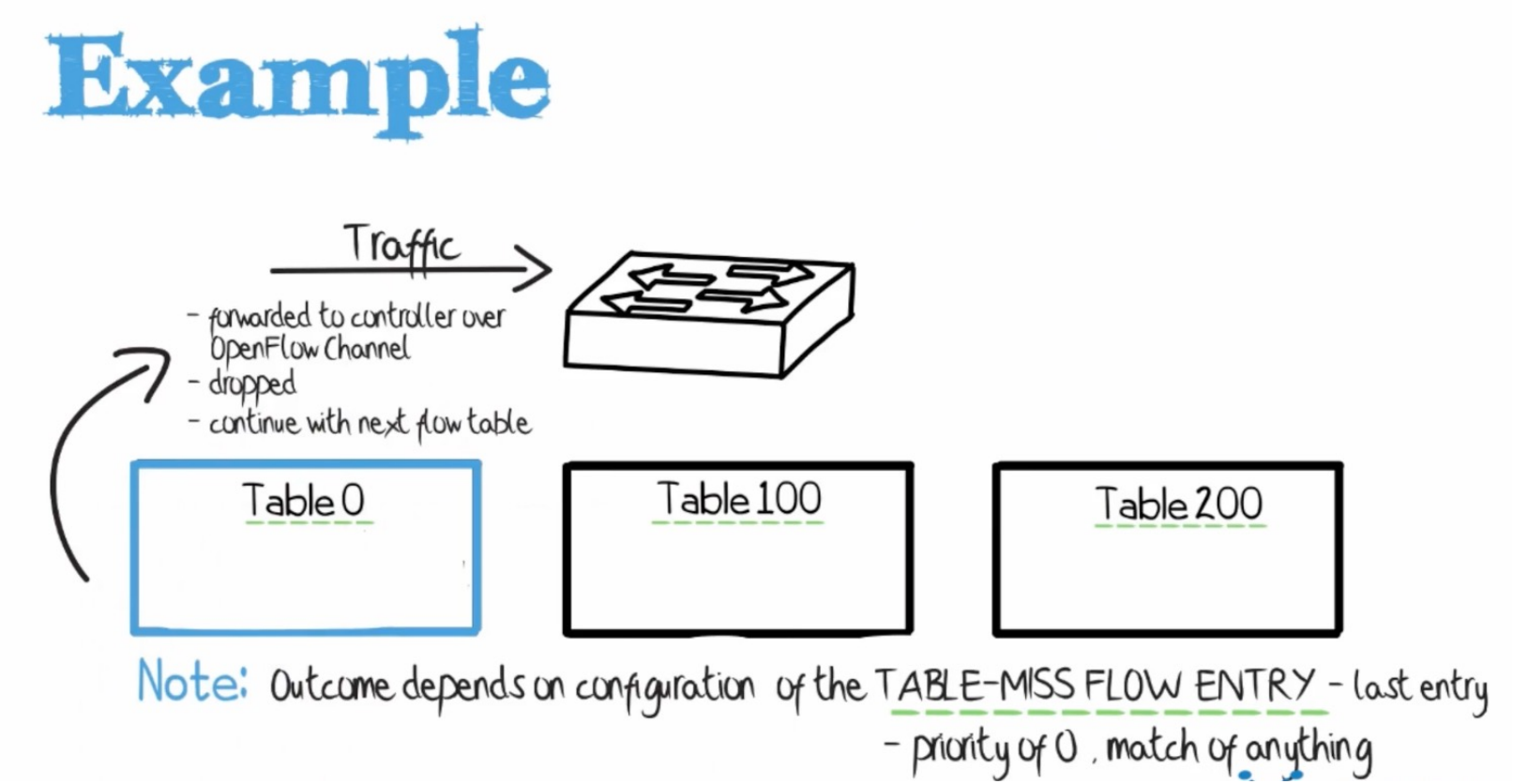
Traffic Matching



Traffic Matching

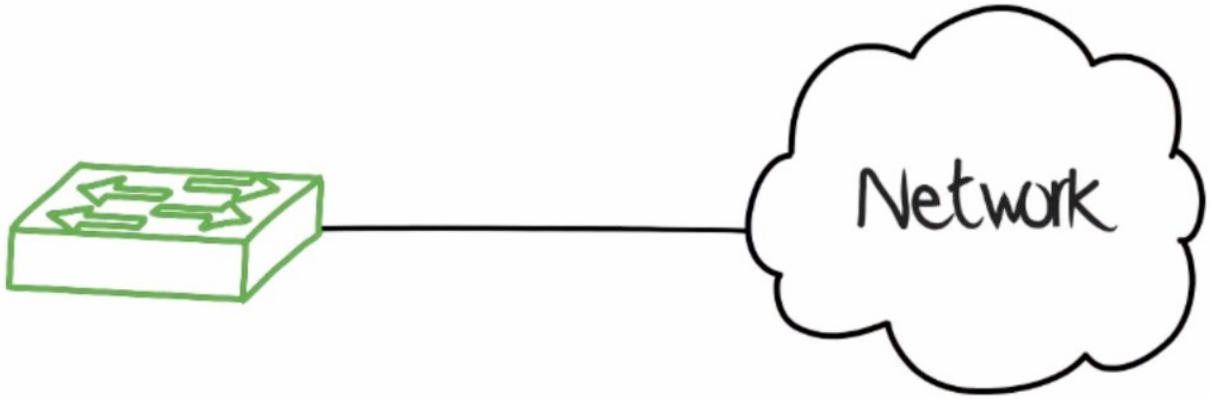


Traffic Matching

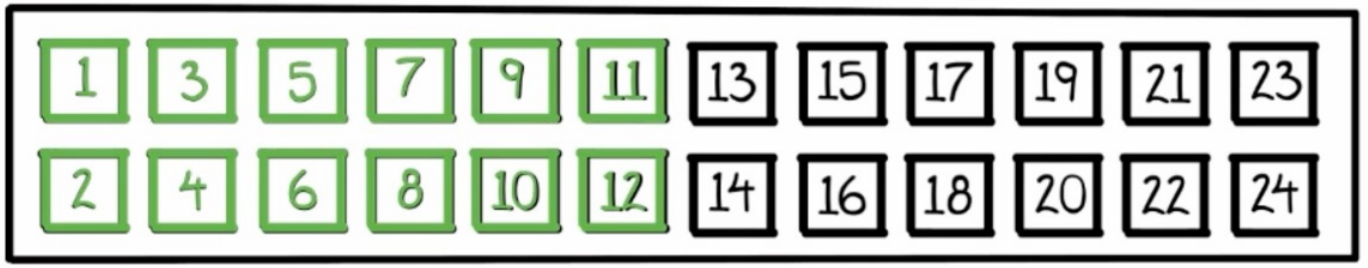


OpenFlow Ports

- the network interfaces for passing packets between OpenFlow processing and the rest of the network



Example

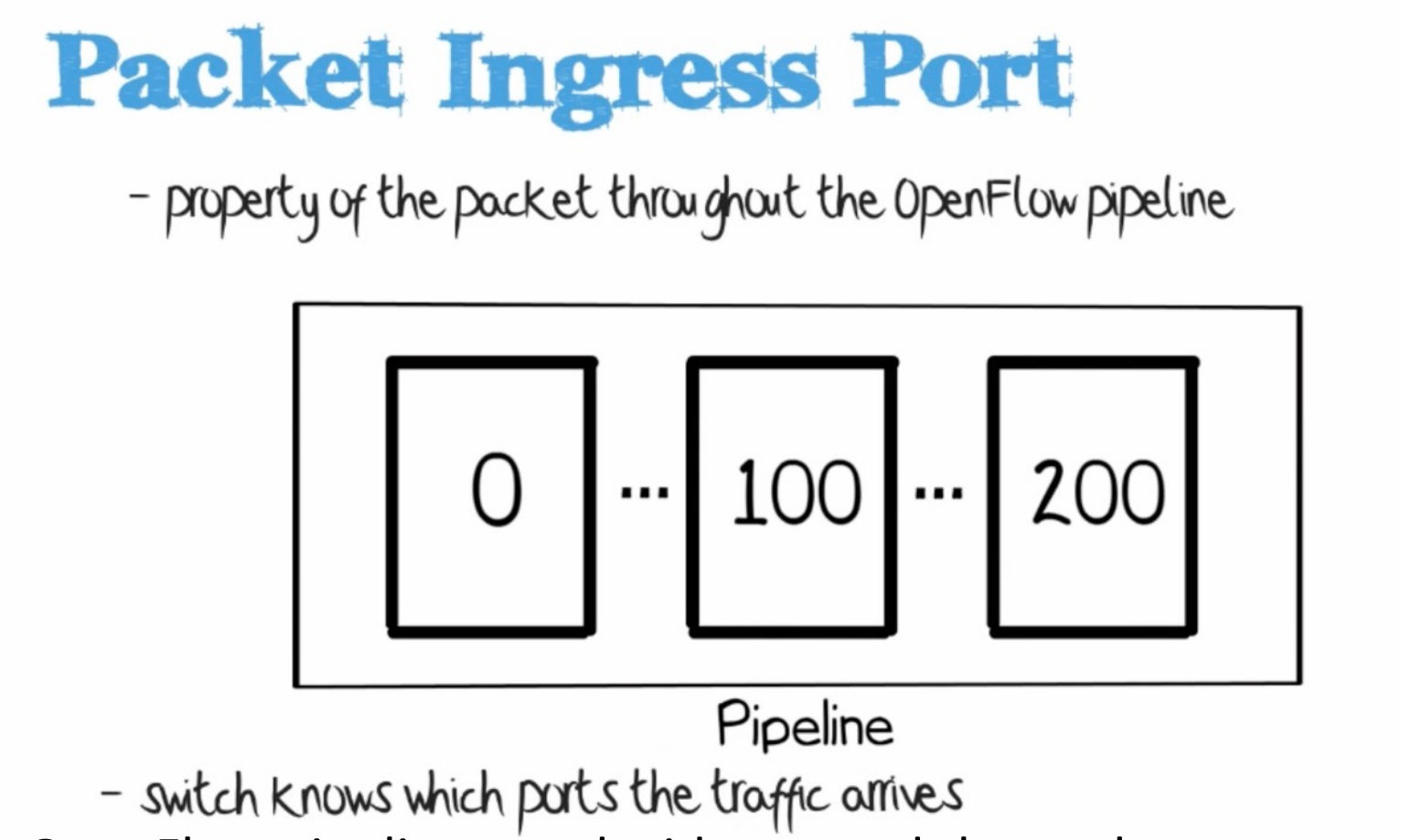


- OpenFlow packets are received on an ingress port and processed by the OpenFlow pipeline

OpenFlow 1.5 - egress port matching was introduced

OpenFlow 1.3 - basis, FOUNDATION

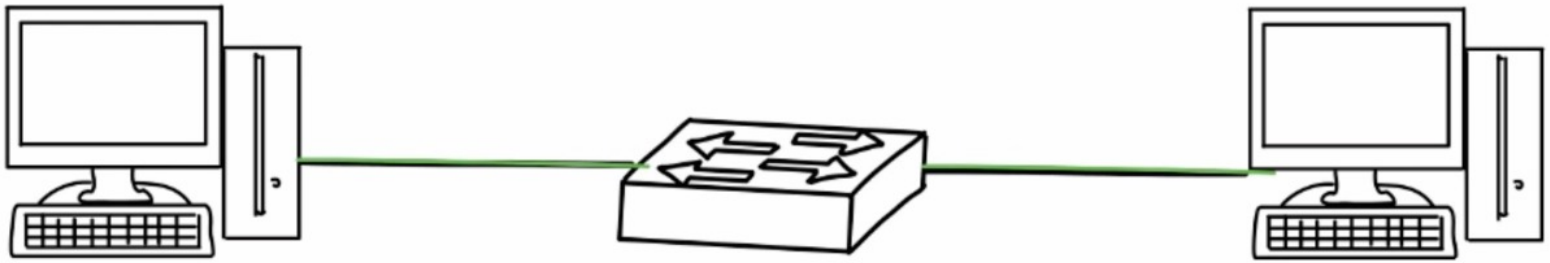
Networking devices and controllers don't support OpenFlow 1.4 or 1.5 . . .



- The OpenFlow pipeline can decide to send the packet on an output port using the output action.

Physical Ports

- are switch defined ports that correspond to a hardware interface of the switch

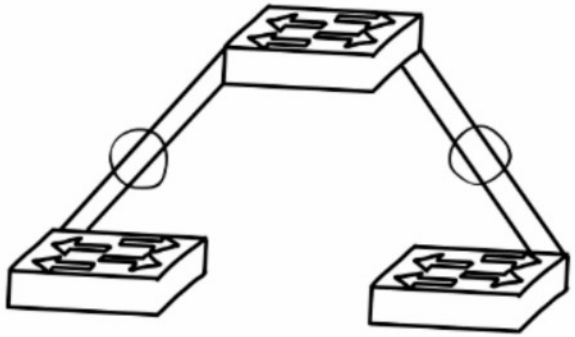


- may be virtualized over switch hardware
- may represent a virtual slice of the corresponding hardware interface of the switch

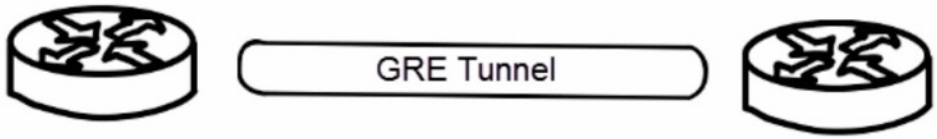
Logical Ports

- are switch defined ports that don't correspond directly to a hardware interface of the switch
- using non-OpenFlow methods

Link Aggregation

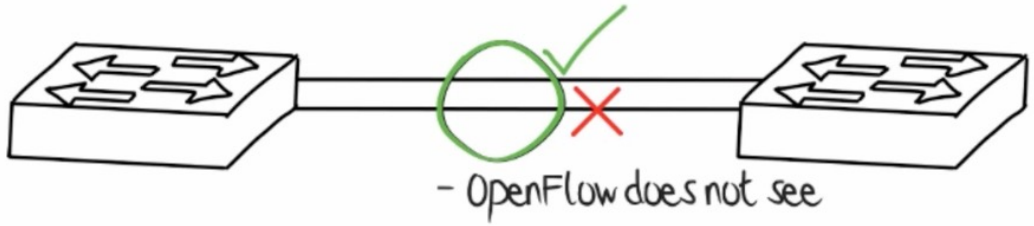


Tunnel



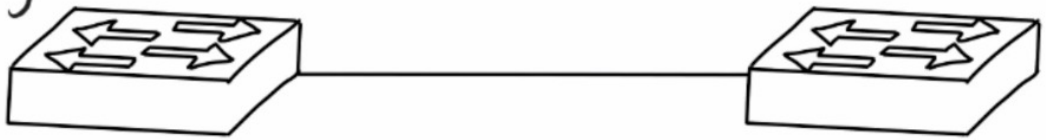
Logical Ports

- are switch defined ports that don't correspond directly to a hardware interface of the switch
- using non-OpenFlow methods
- may include packet encapsulation
- must be transparent in OpenFlow processing



- OpenFlow does not see

Logically



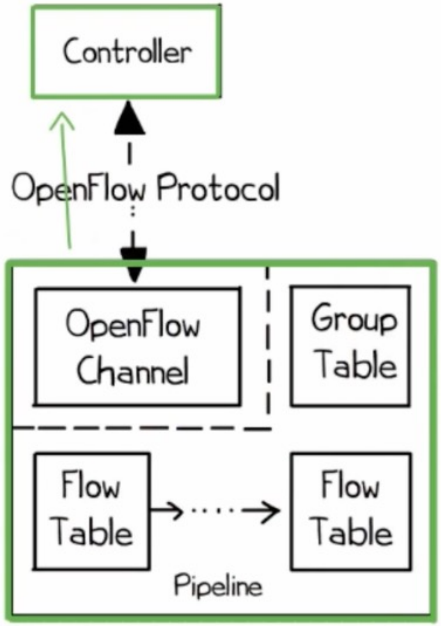
Reserved Ports

Specify generic forwarding actions

- sending to the controller
- flooding traffic out of ports
- forwarding using non-OpenFlow methods

Reserved Ports

Controller - represents the control channel with the OpenFlow Controller

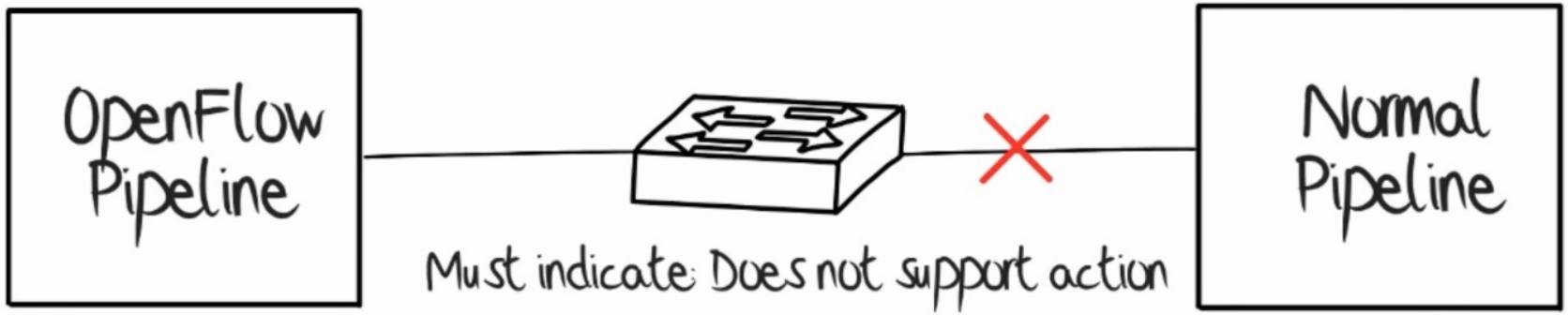


- can be used as an ingress port
- can be used as output port
  - encapsulate the packet in a packet-in message

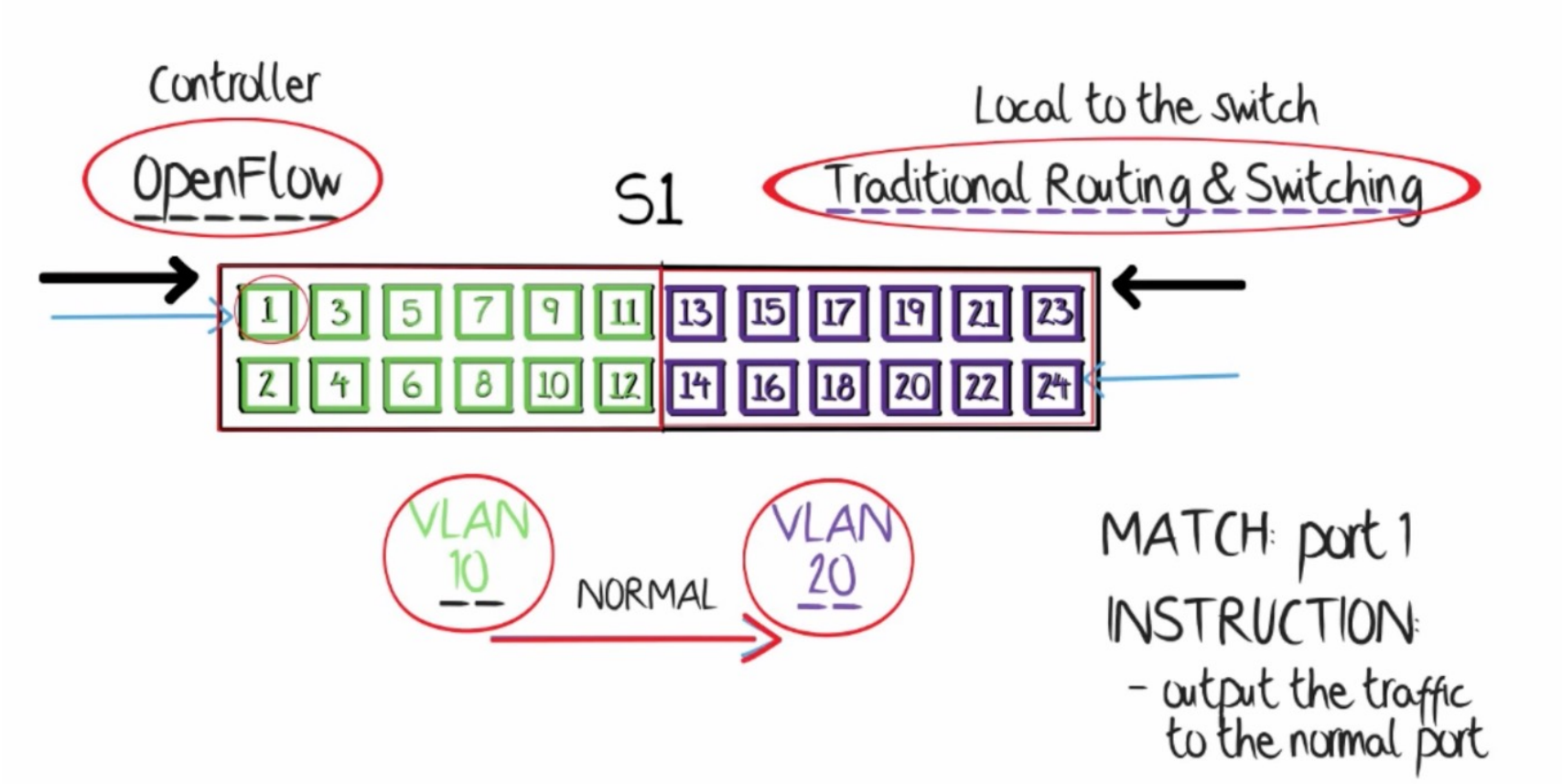
Reserved Ports

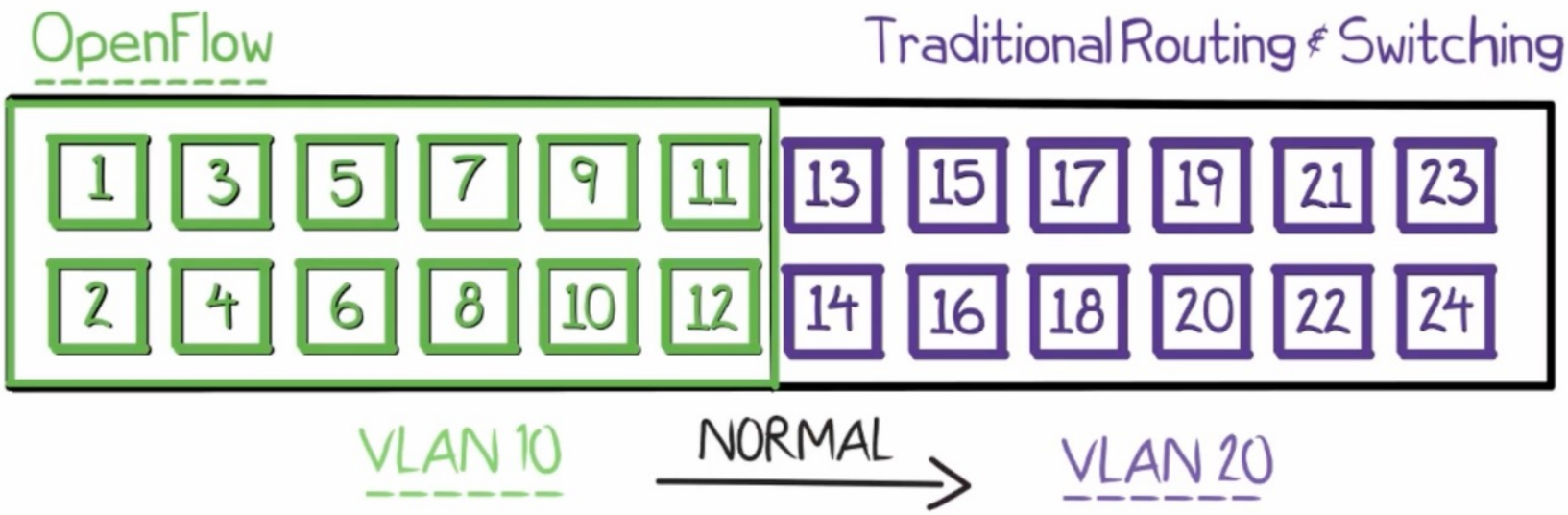
Controller - represents the control channel with the OpenFlow Controller

Normal Port - represents the traditional non-OpenFlow pipeline of the switch
- can only be used as an output port and processes the packet using normal pipeline



OpenFlow Hybrid Switch





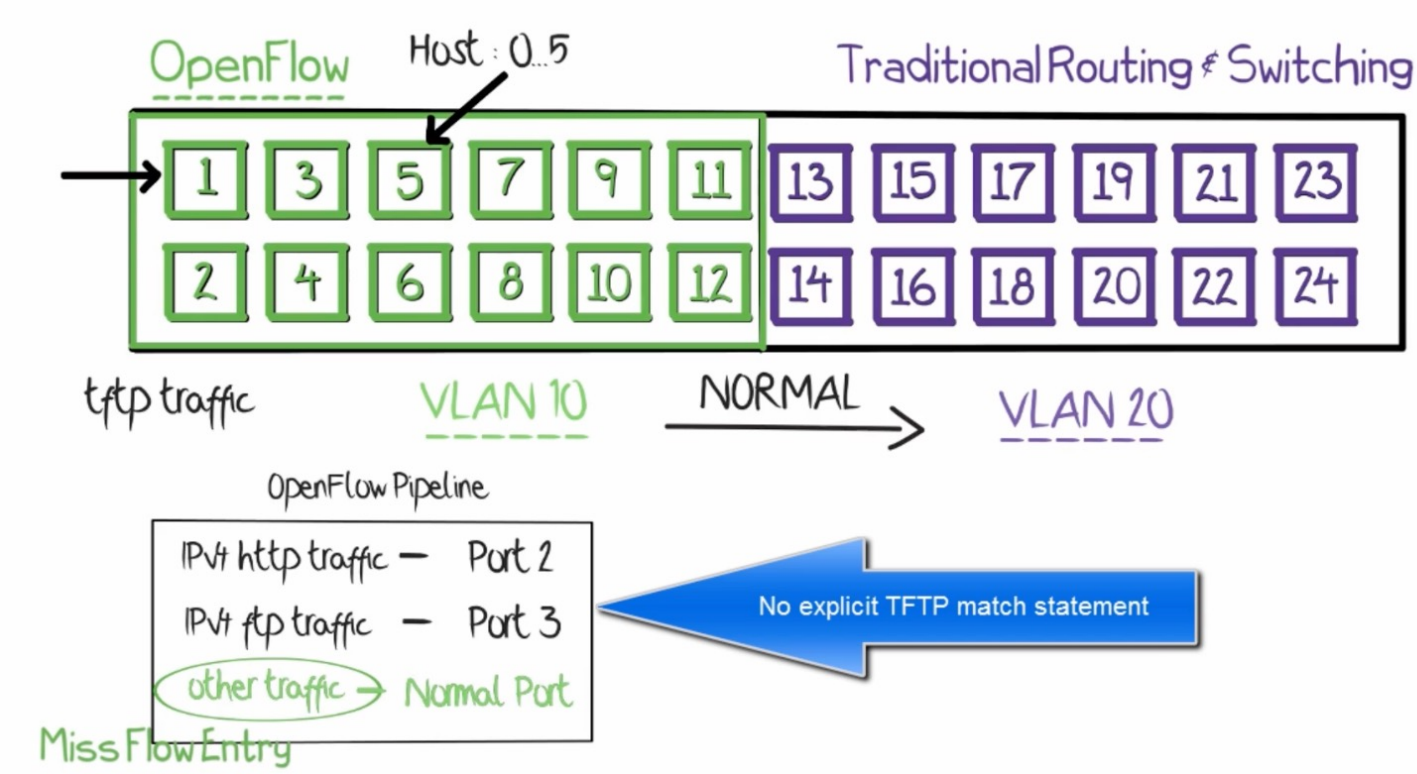
Normal Forwarding

- traditional non-OpenFlow pipeline of the switch

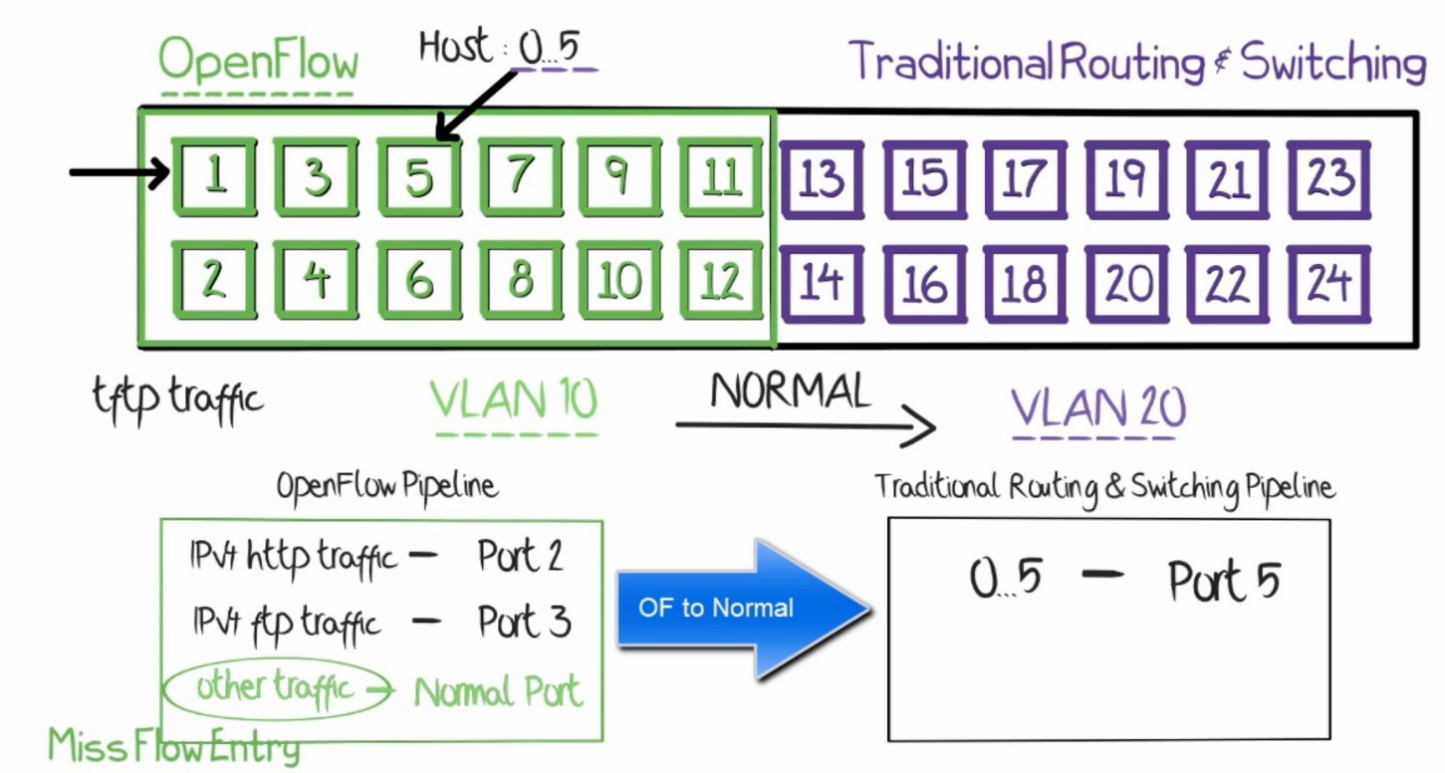
OpenFlow Hybrid Switches

- support both OpenFlow operation and normal Ethernet switching operation

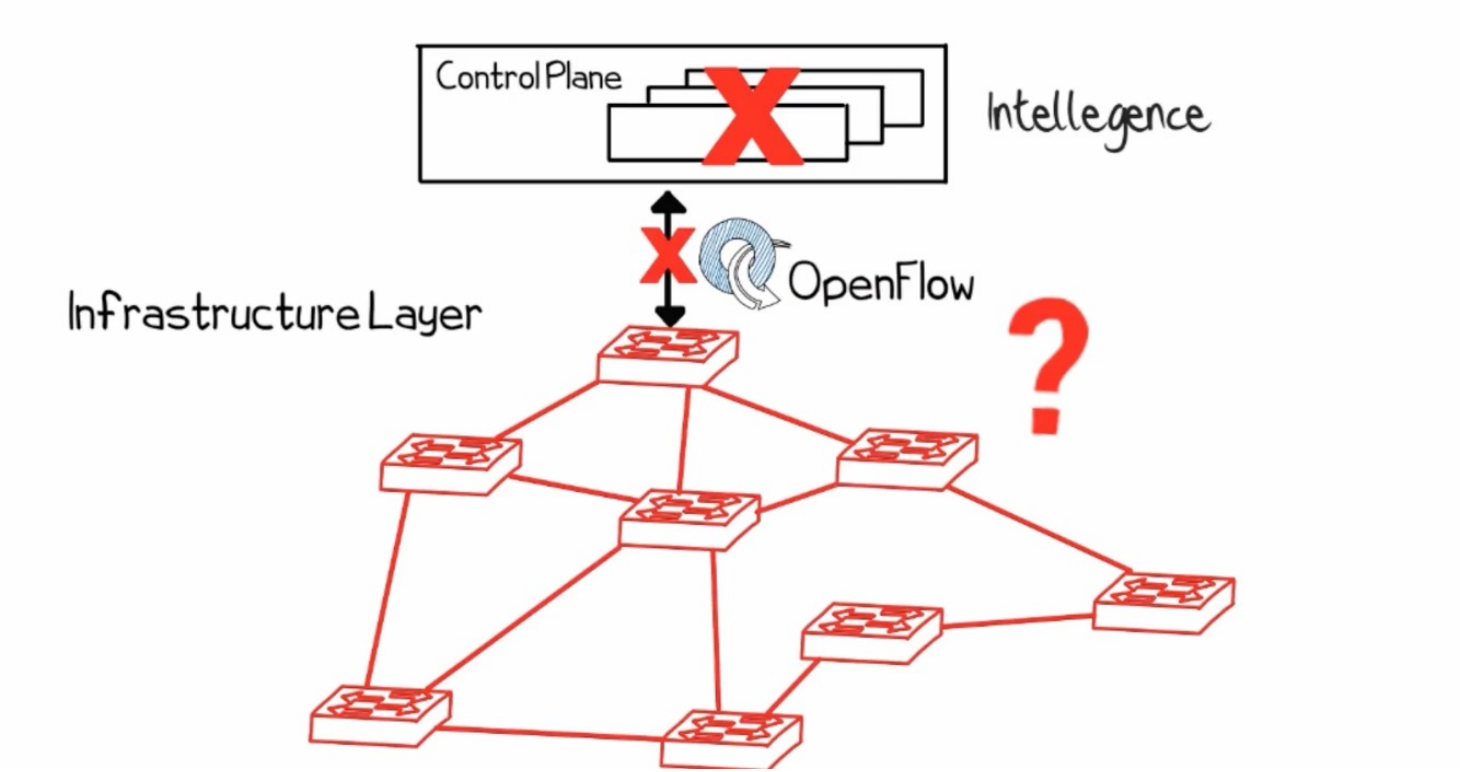
Example Flow Traffic



Example Flow Traffic

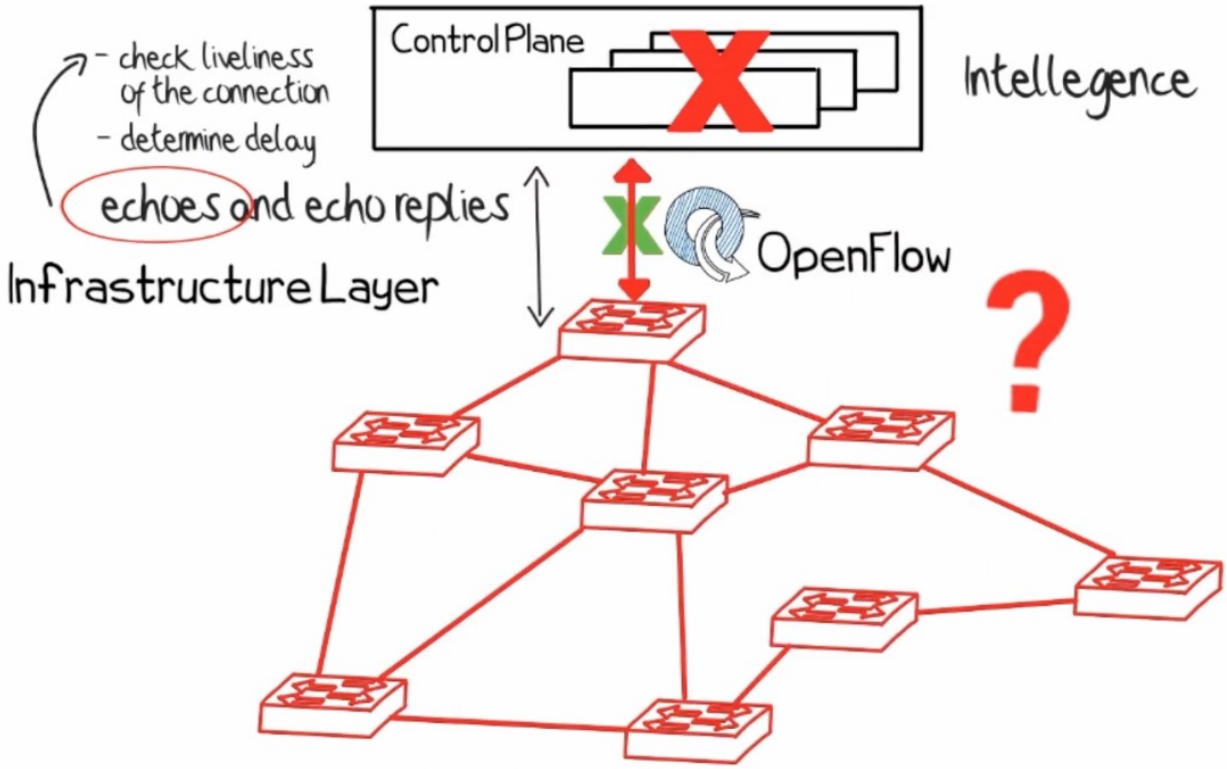


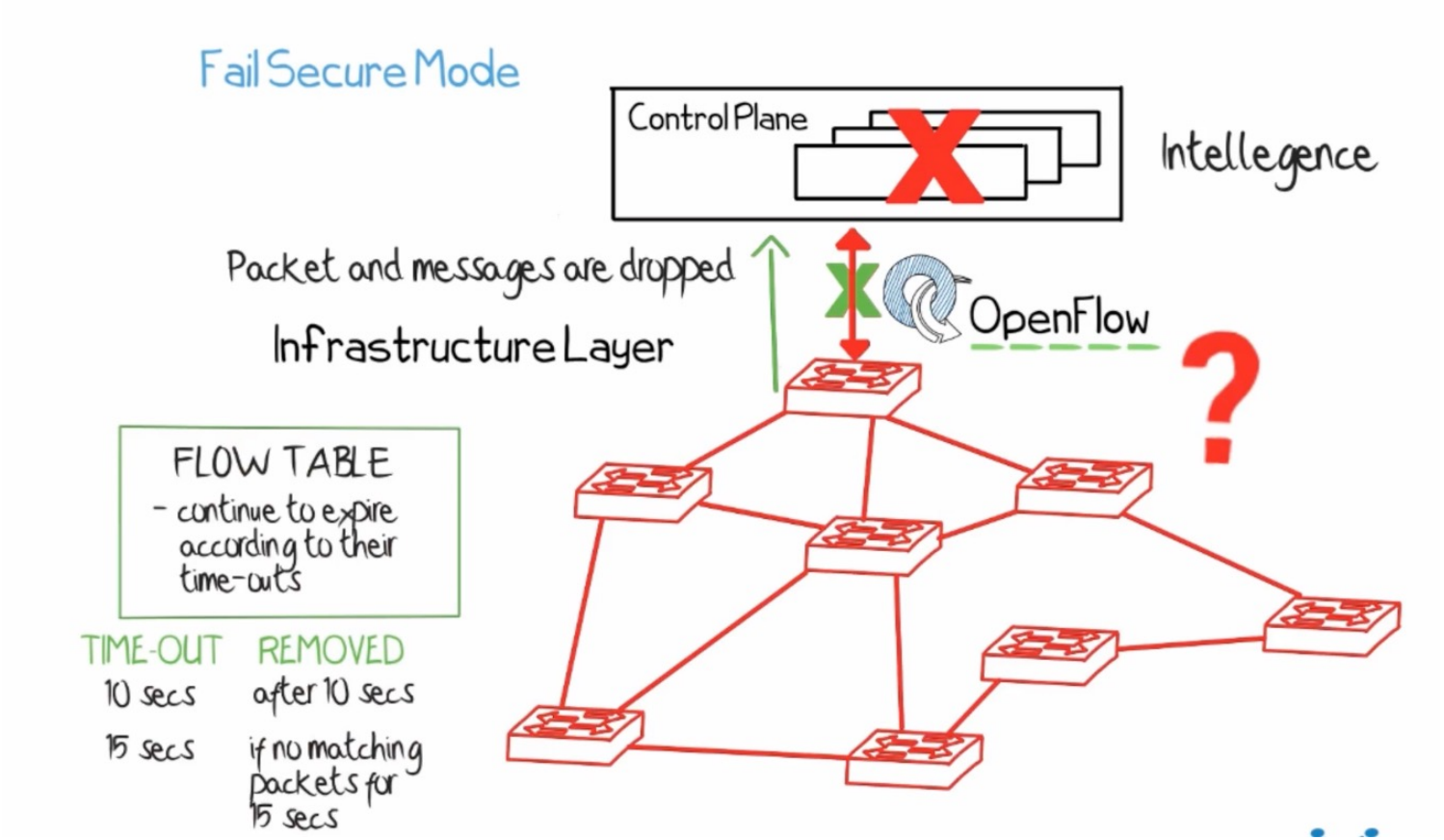
What happens when a controller fails? Network Down?



Connection Interruption

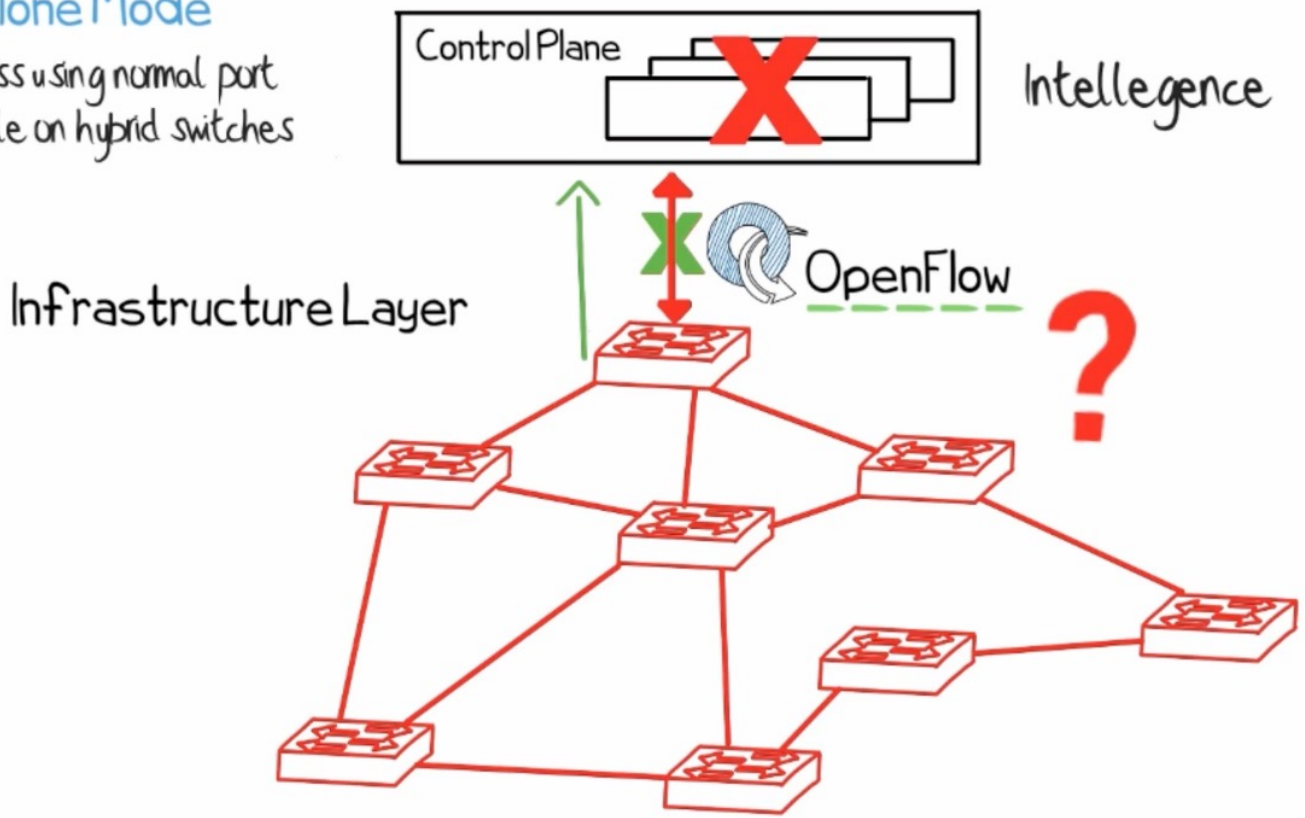
- immediately enter either "fail secure mode" or "fail standalone mode"
- depending on switch implementation and configuration



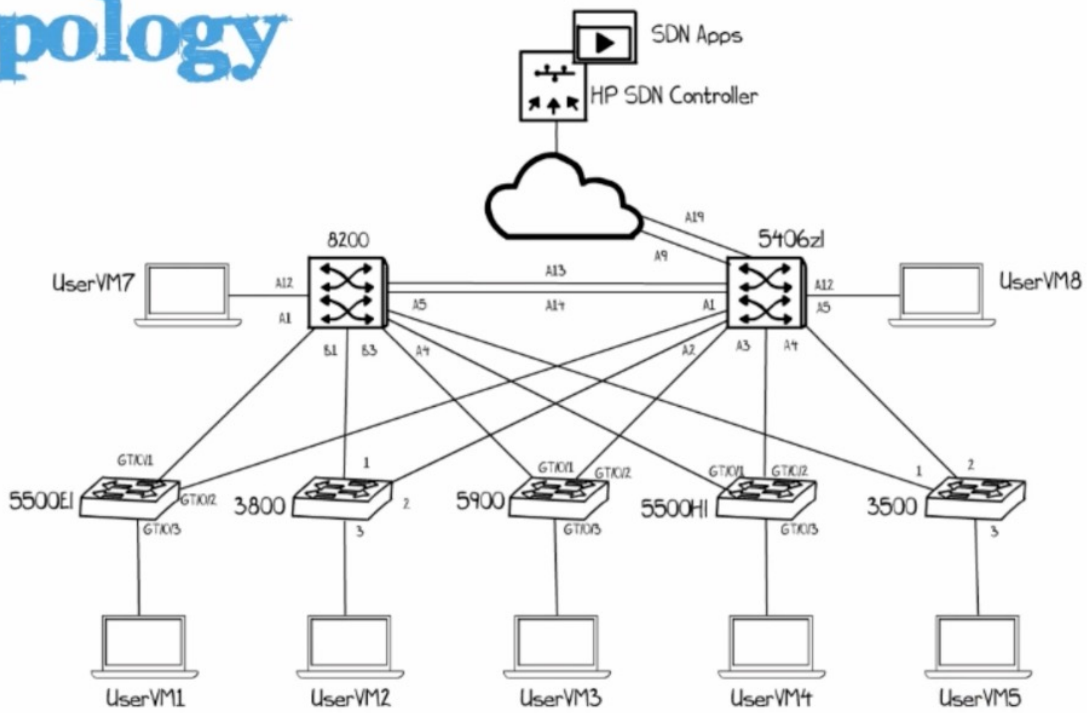

Fail Secure Mode
Control Plane
Intellegence
Packet and messages are dropped
Infrastructure Layer
OpenFlow
?
FLOW TABLE
- continue to expire according to their time-outs
TIME-OUT
REMOVED
10 secs
after 10 secs
15 secs
if no matching packets for 15 secs

Fail Standalone Mode

- switch process using normal port
- only available on hybrid switches



Topology

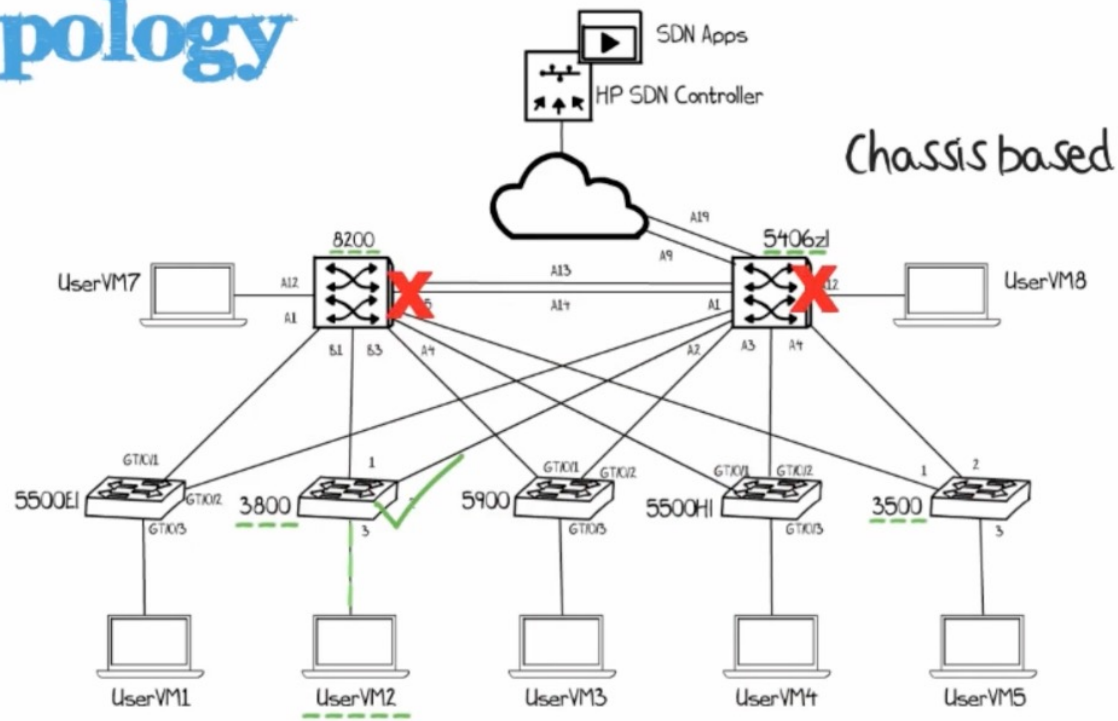


Upgrade Firmware of the switch to get OpenFlow Functionality

Do you need to do fork lift upgrade?
Do you need to replace all switches?

} depend on vendor

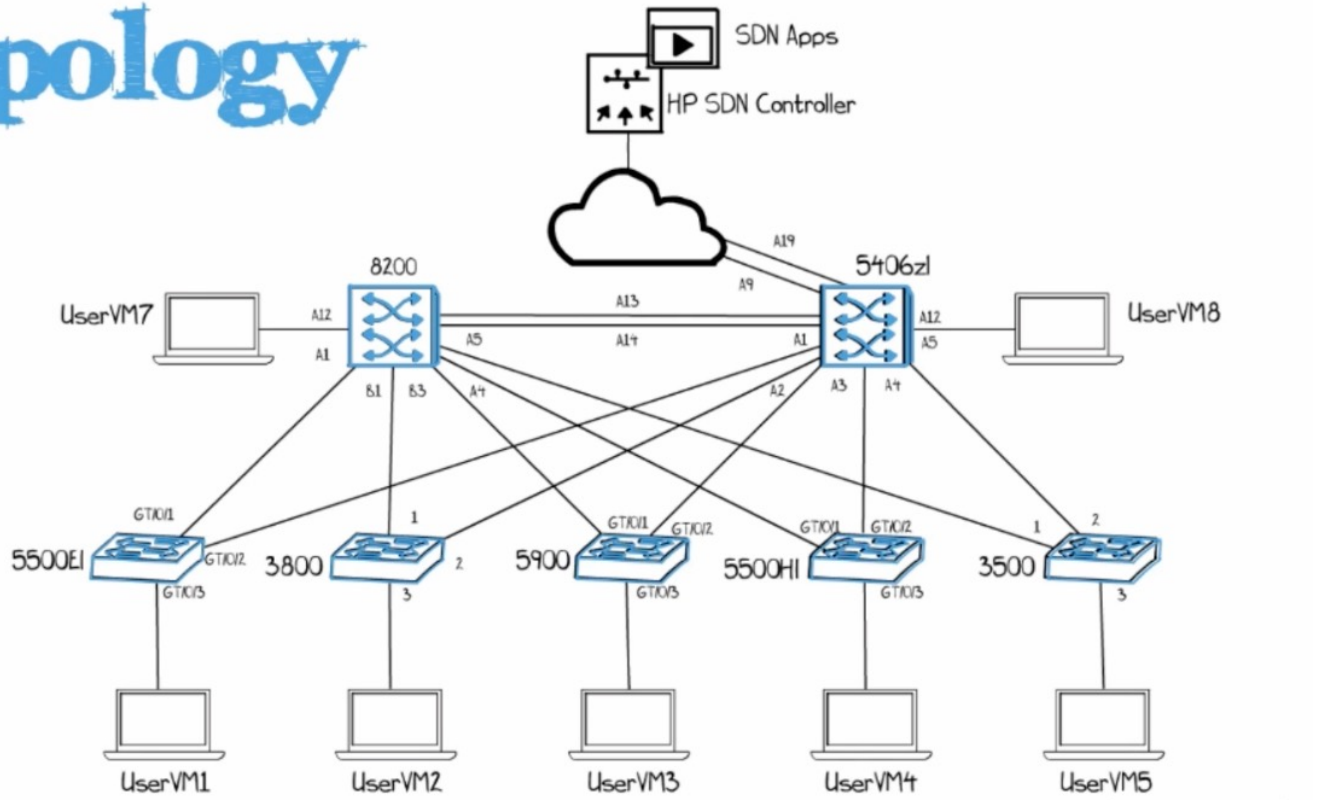
Topology



Chassis based HP switches

Do I need to enable OpenFlow everywhere in my network? NO

Topology



Does a single controller need to control the entire network? NO