Data-centric security in software-defined networks

Dr.-Ing. Konrad Wrona

Lecture 2: Software-defined networks: Principles and standards

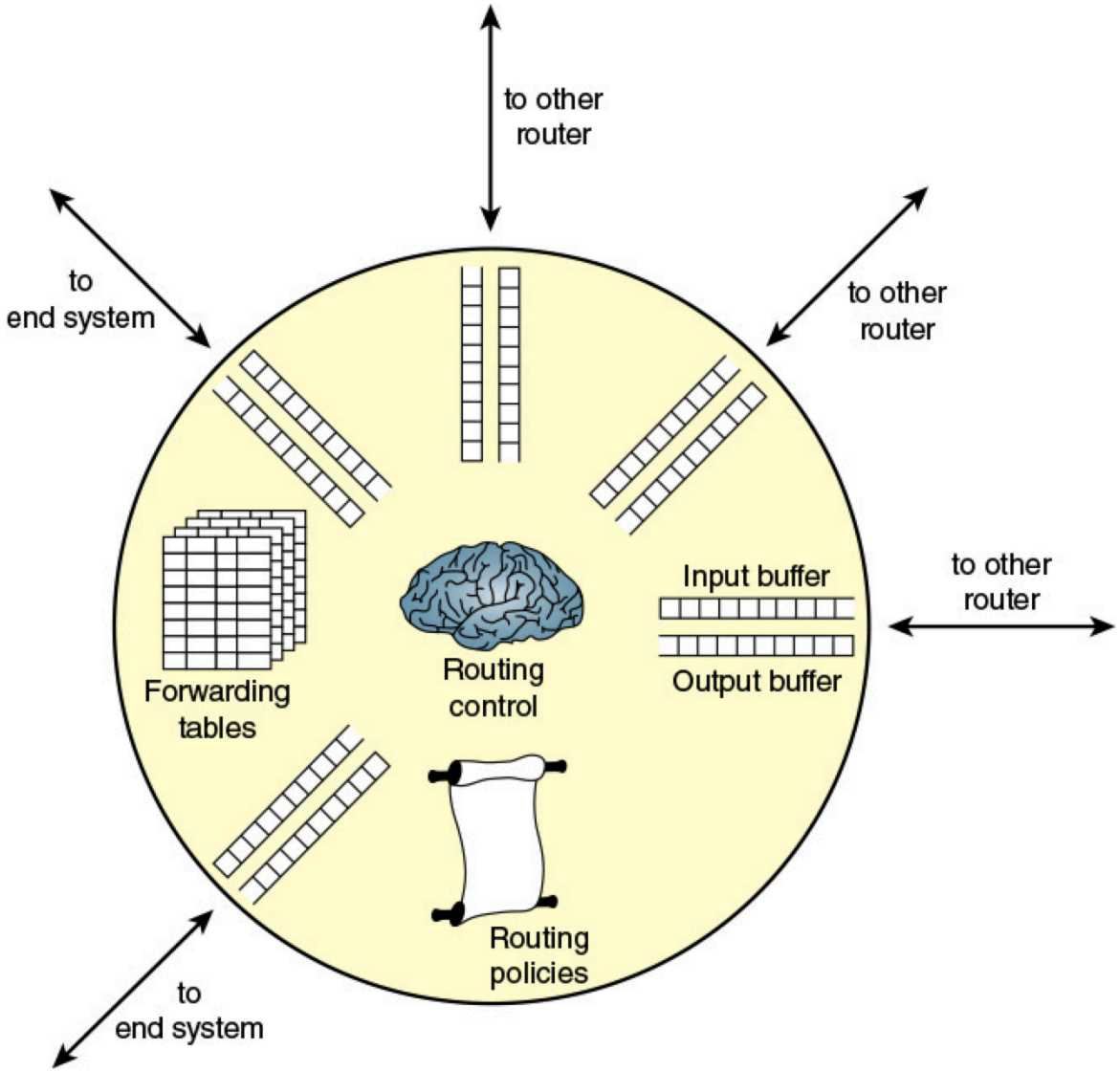
Basic concepts of SDN

- Software Defined Networking
  - Data Plane + Control Plane
  - Well defined API (i.e. OpenFlow)

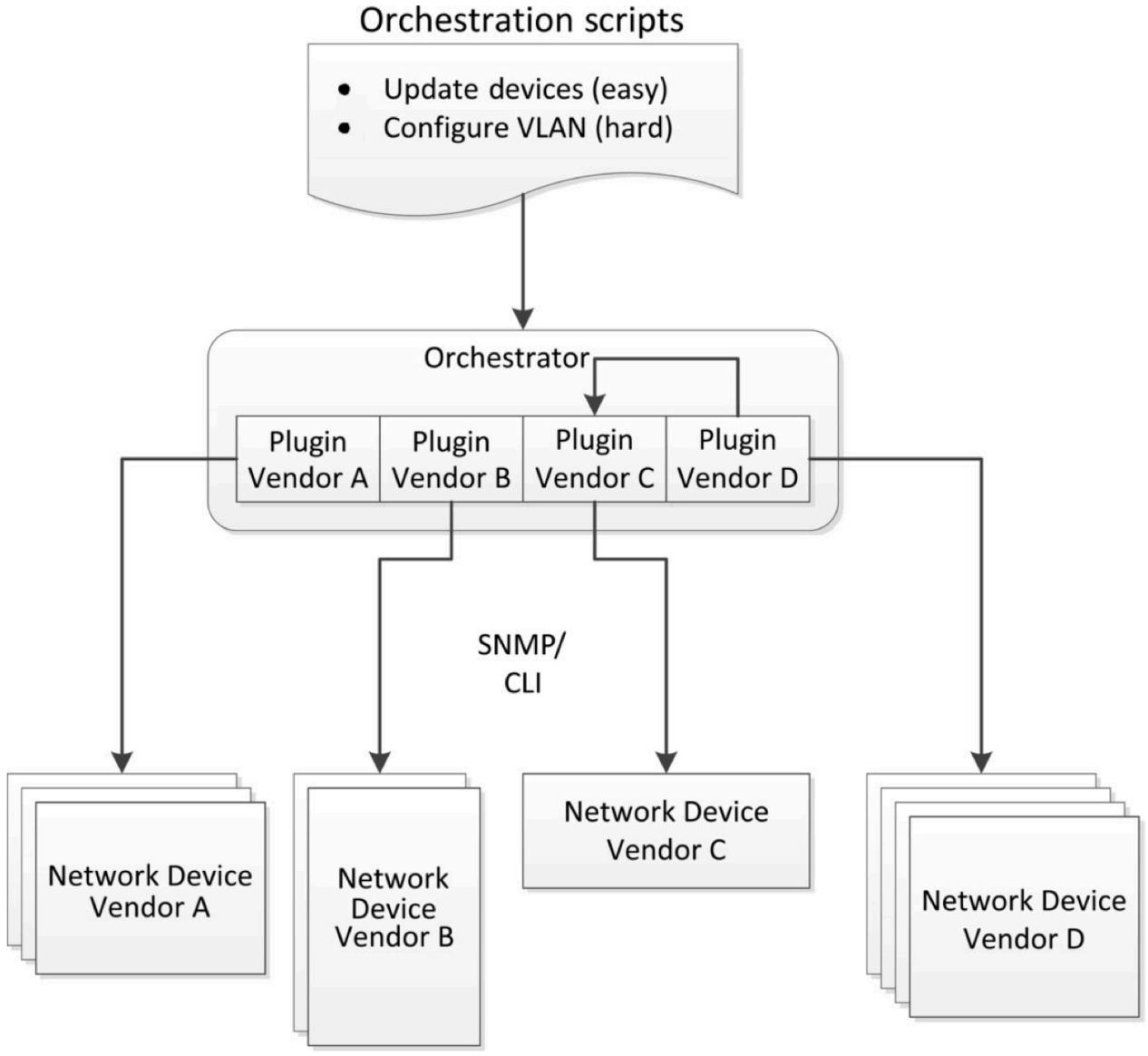
- More adequate is concept of Software Defined Infrastructure - going beyond layer 2 and 3

- Security can be a potential killer app for SDN justifying cost of replacing switches and of integrating the control plane

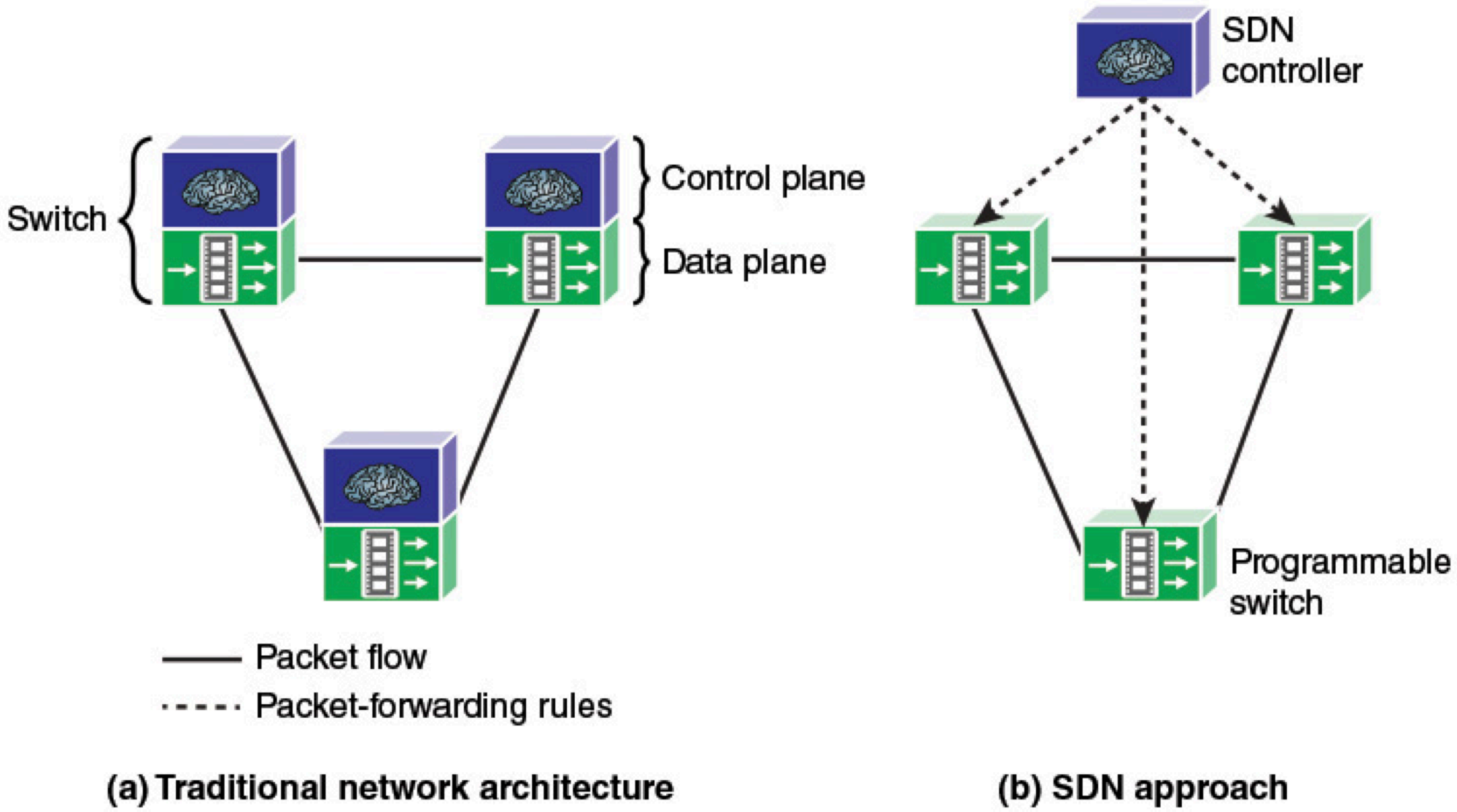
What does a router do?



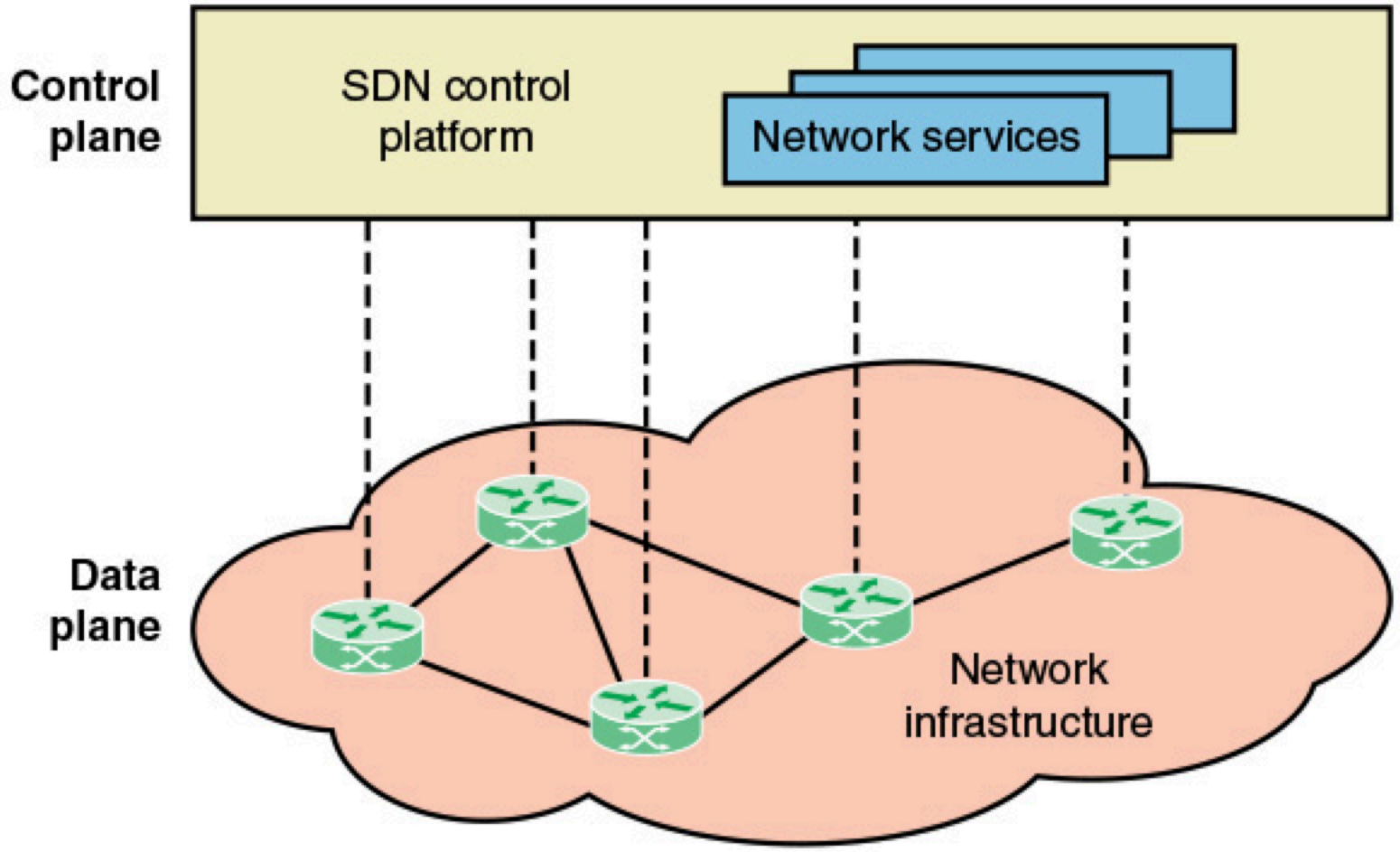
Dealing with configuration challenge



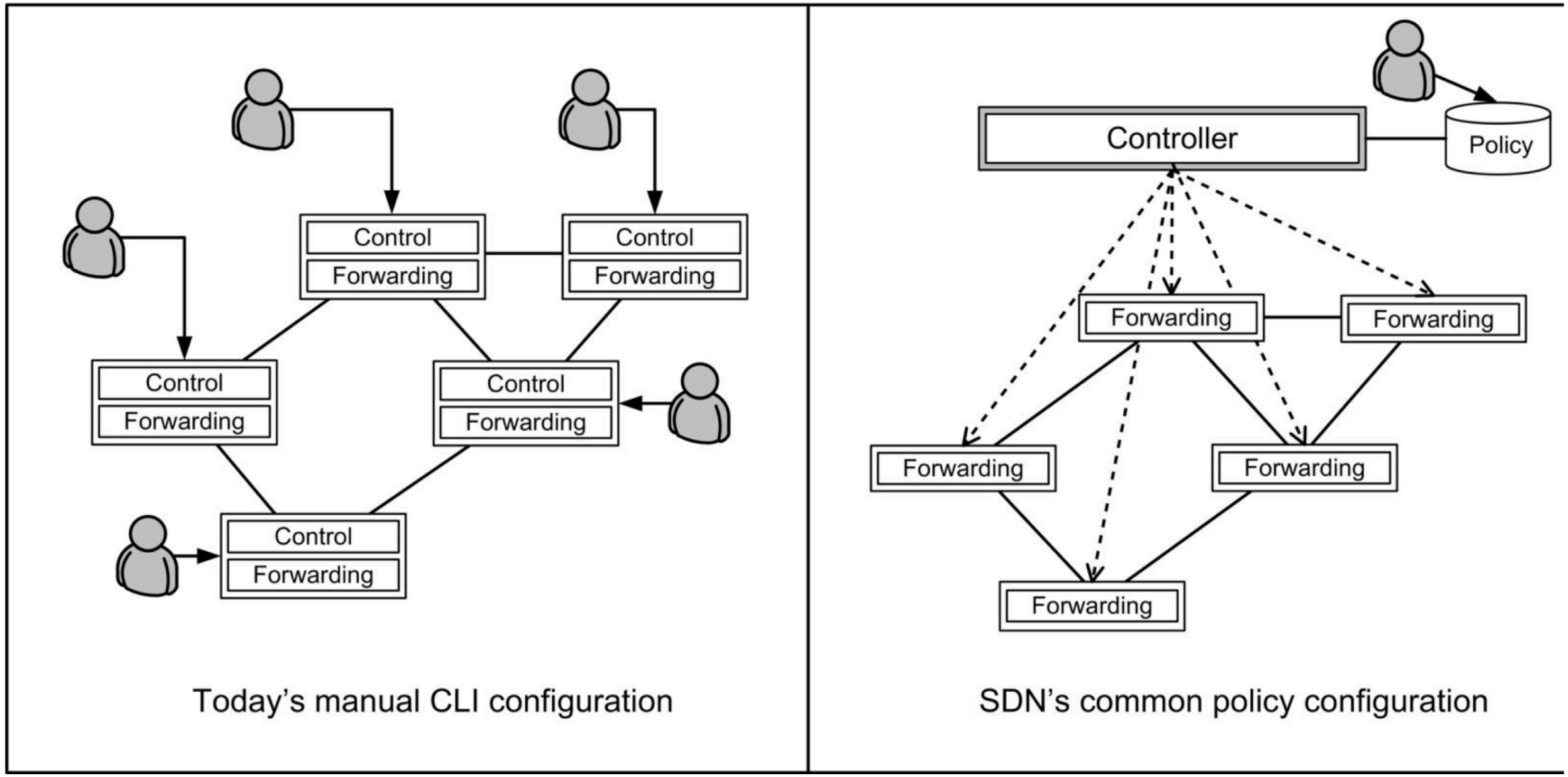
From appliances to software



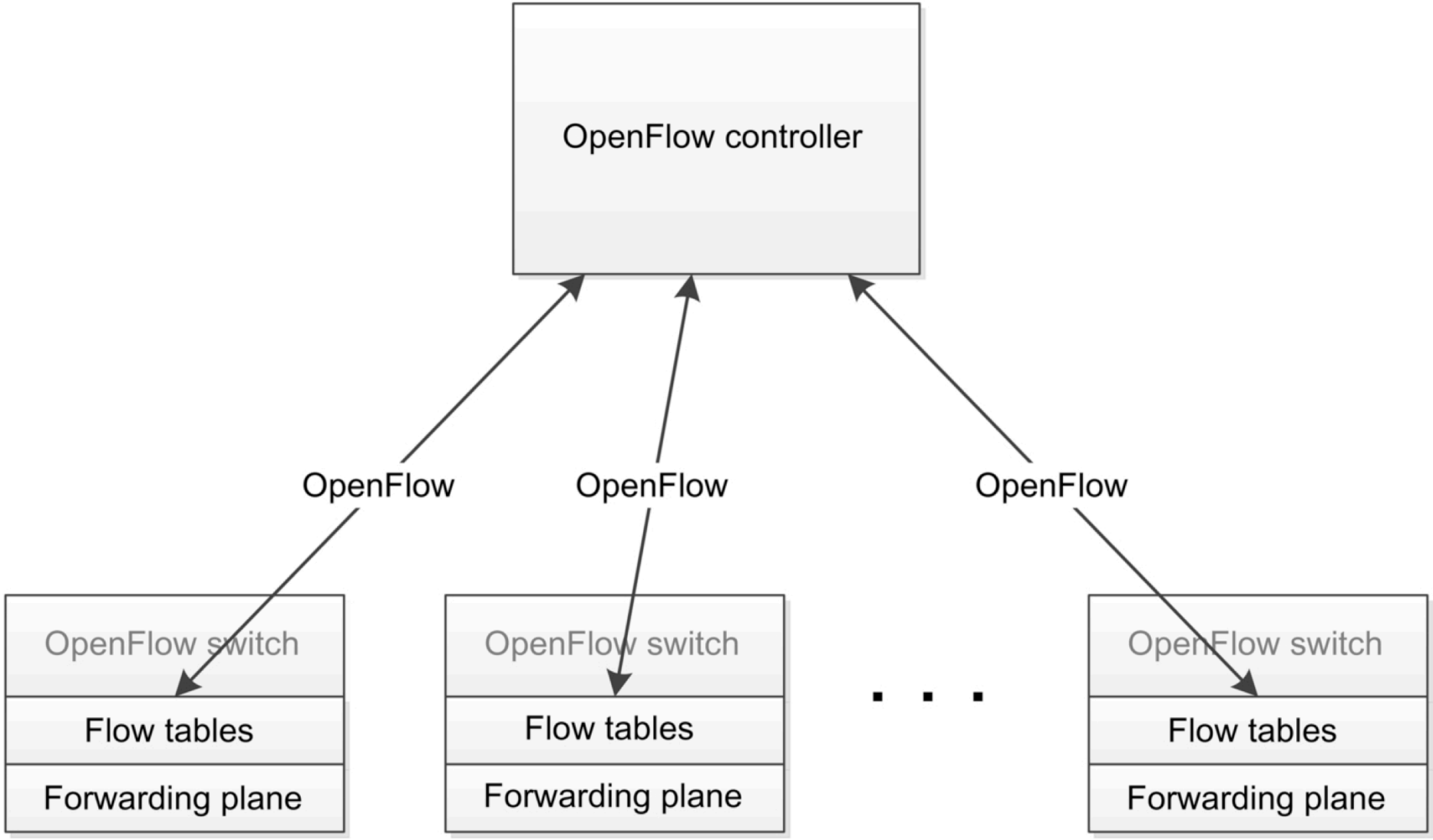
Main idea: Separation of control and data



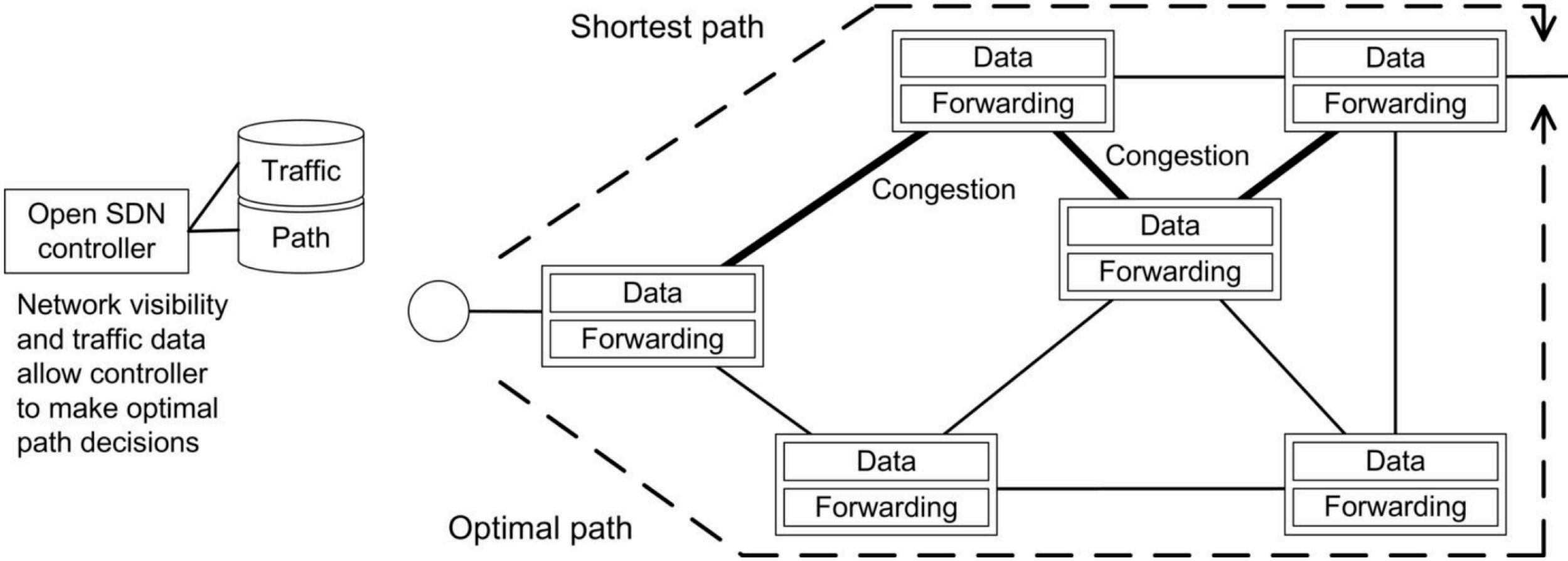
Advantages of SDN



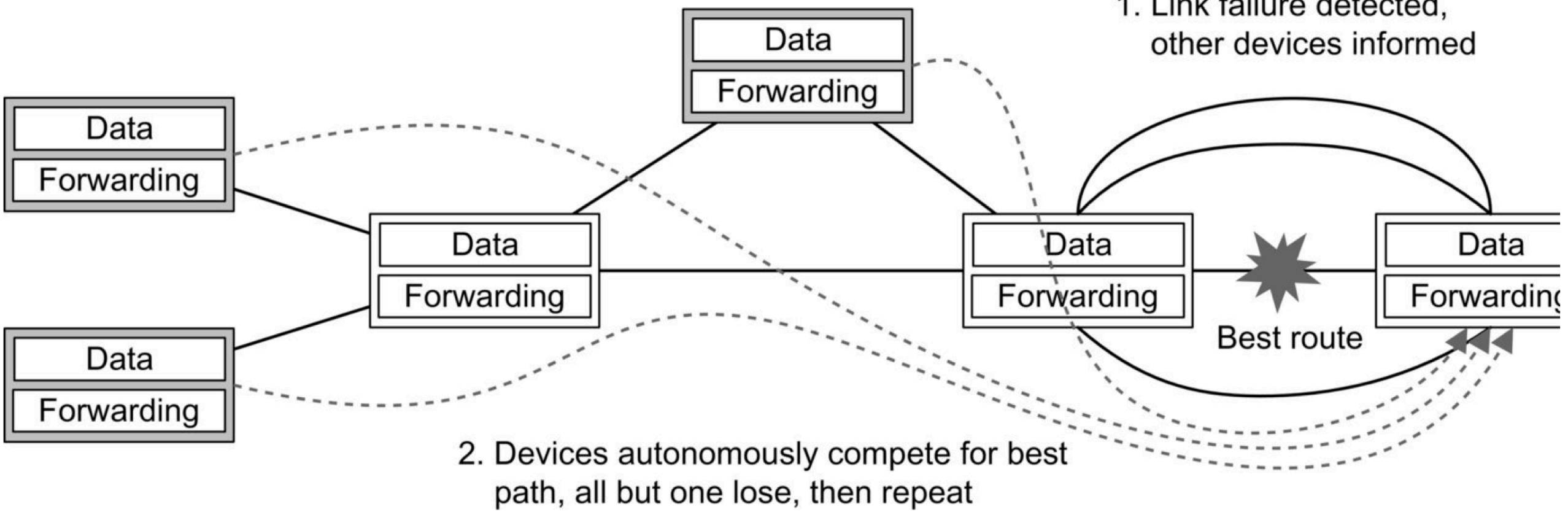
Global view of the network



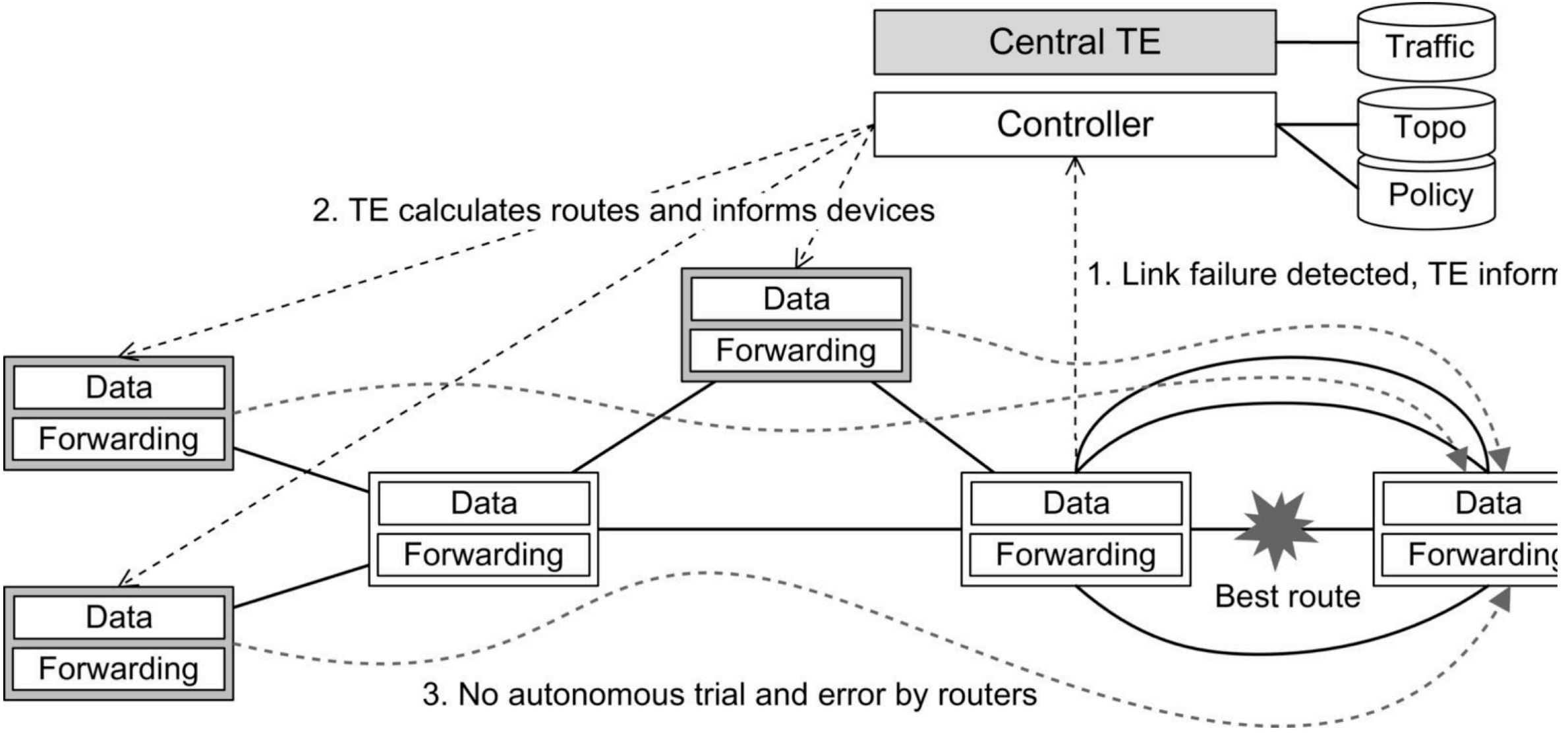
Optimal paths



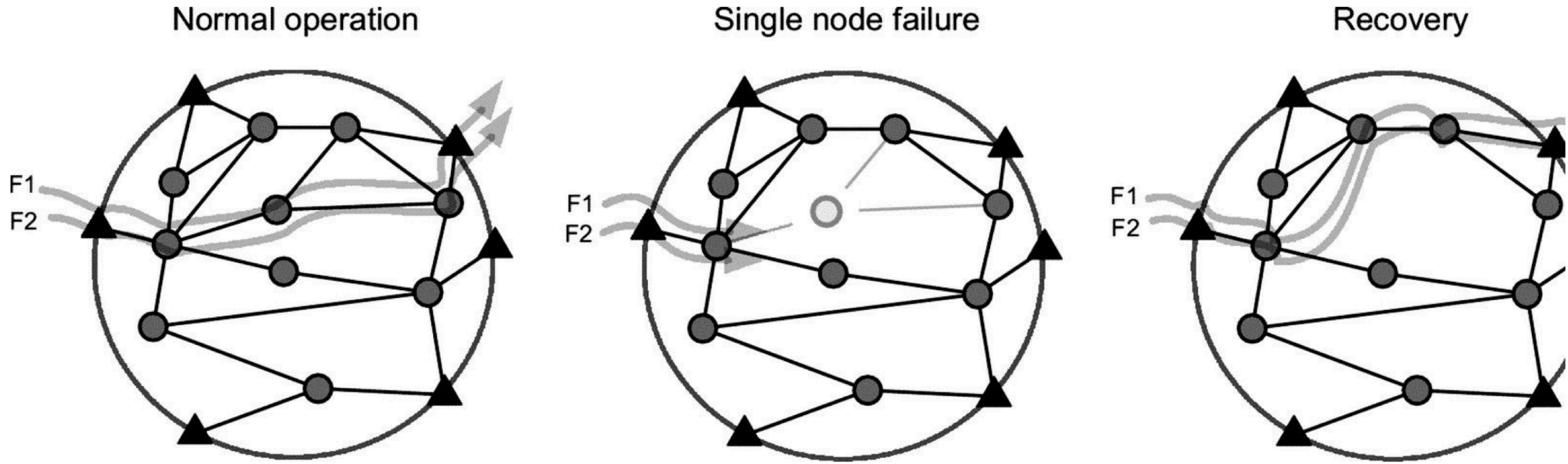
Reduction in network overhead and delay



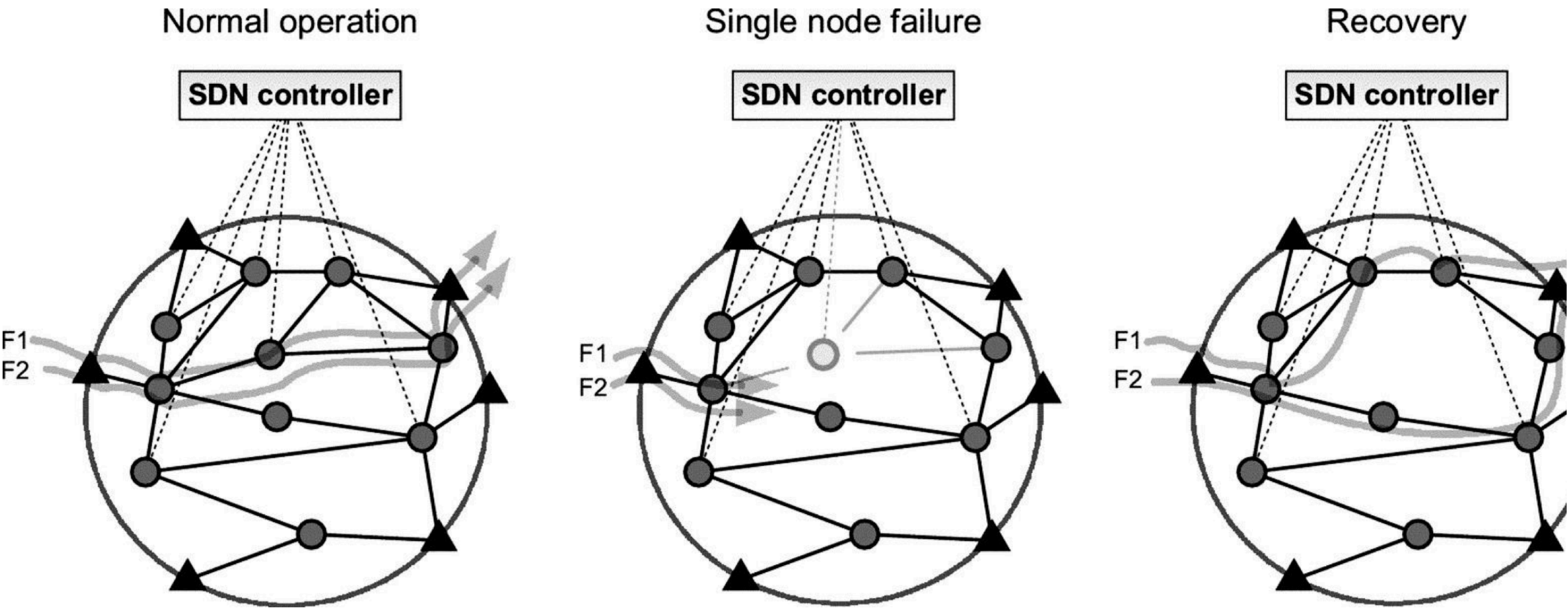
Reduction in network overhead and delay



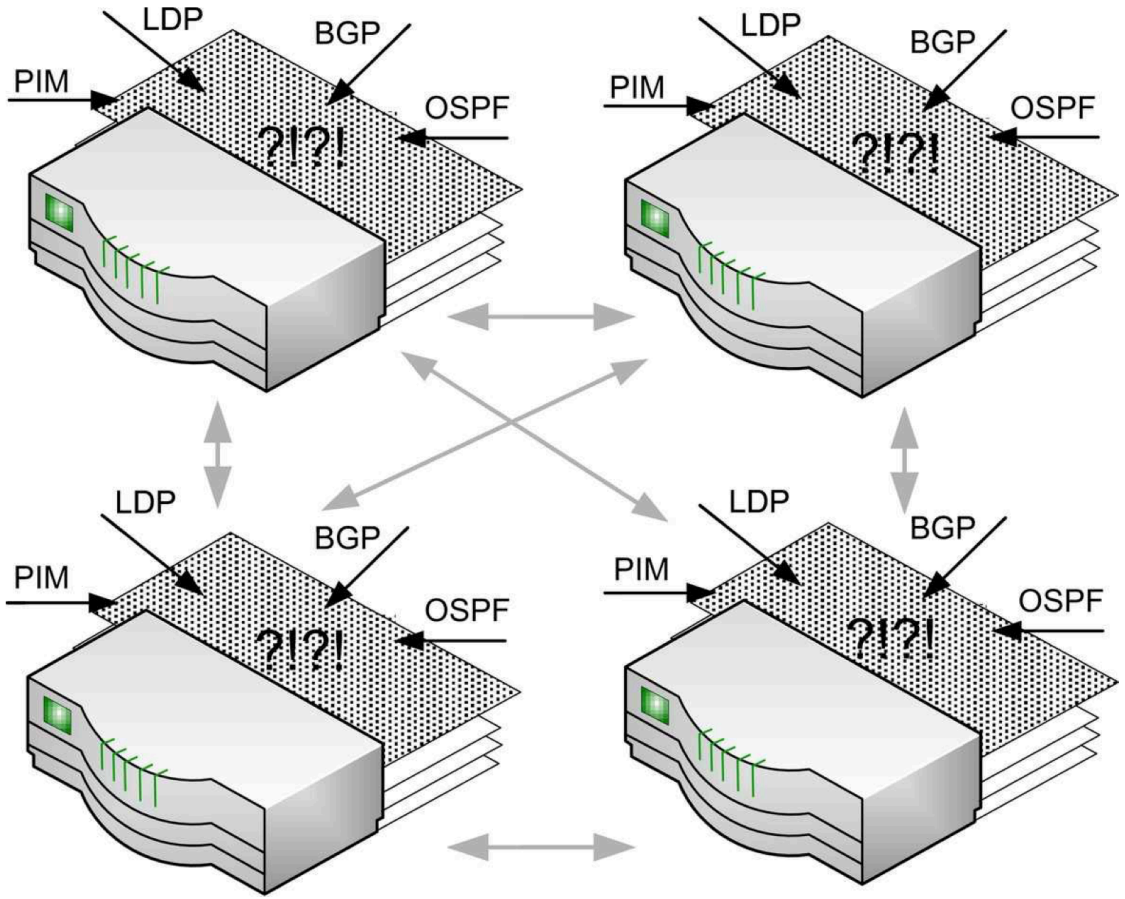
Better load balancing

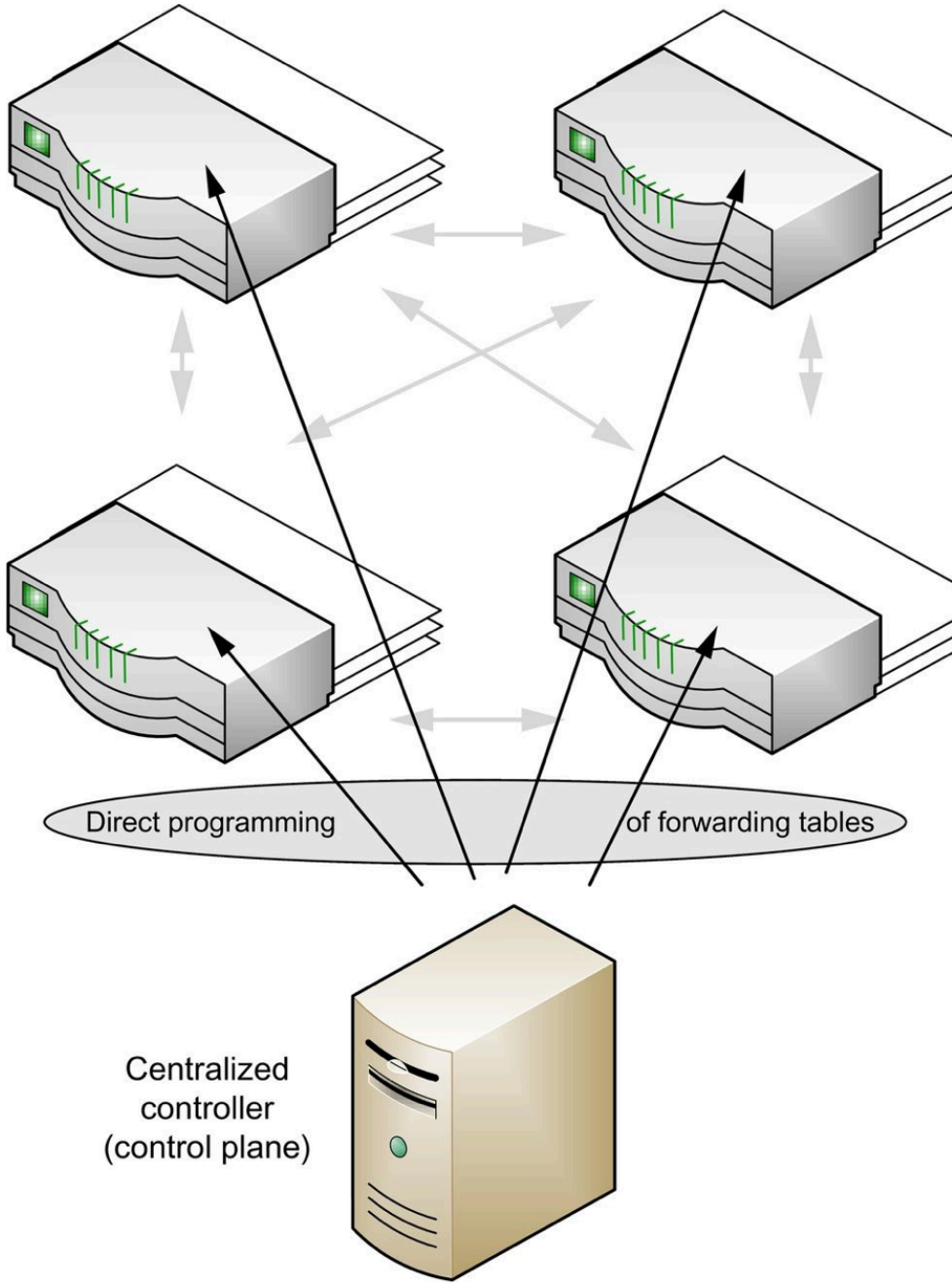


Better load balancing



Reduced requirements on switches

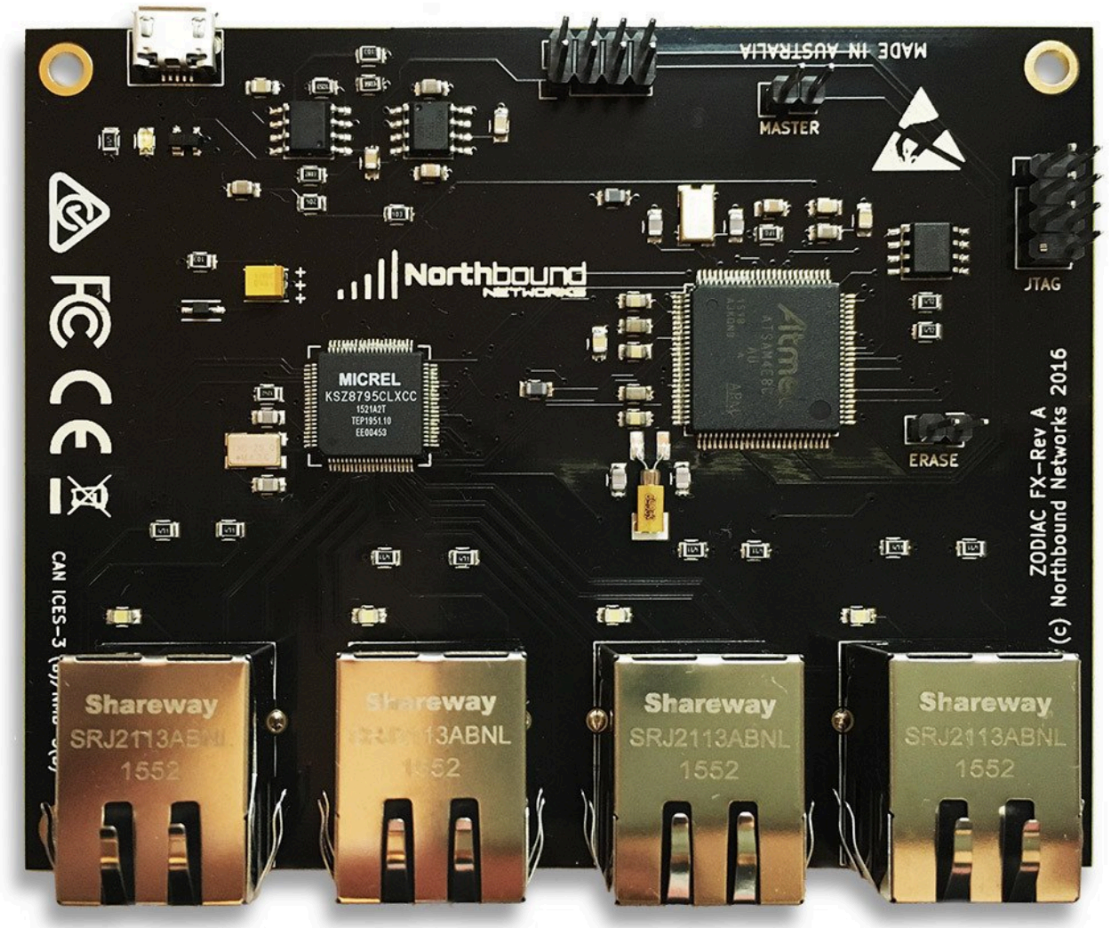




Switch can be cheap…

Northbound NETWORKS

HOME ZODIAC WX ZODIAC FX FLOW MAKER RESELLERS BLOG SUPPORT FORUM USD SIGN IN 0



ZODIAC FX

★★★★★ 11 reviews

$85.41 USD

QTY

1

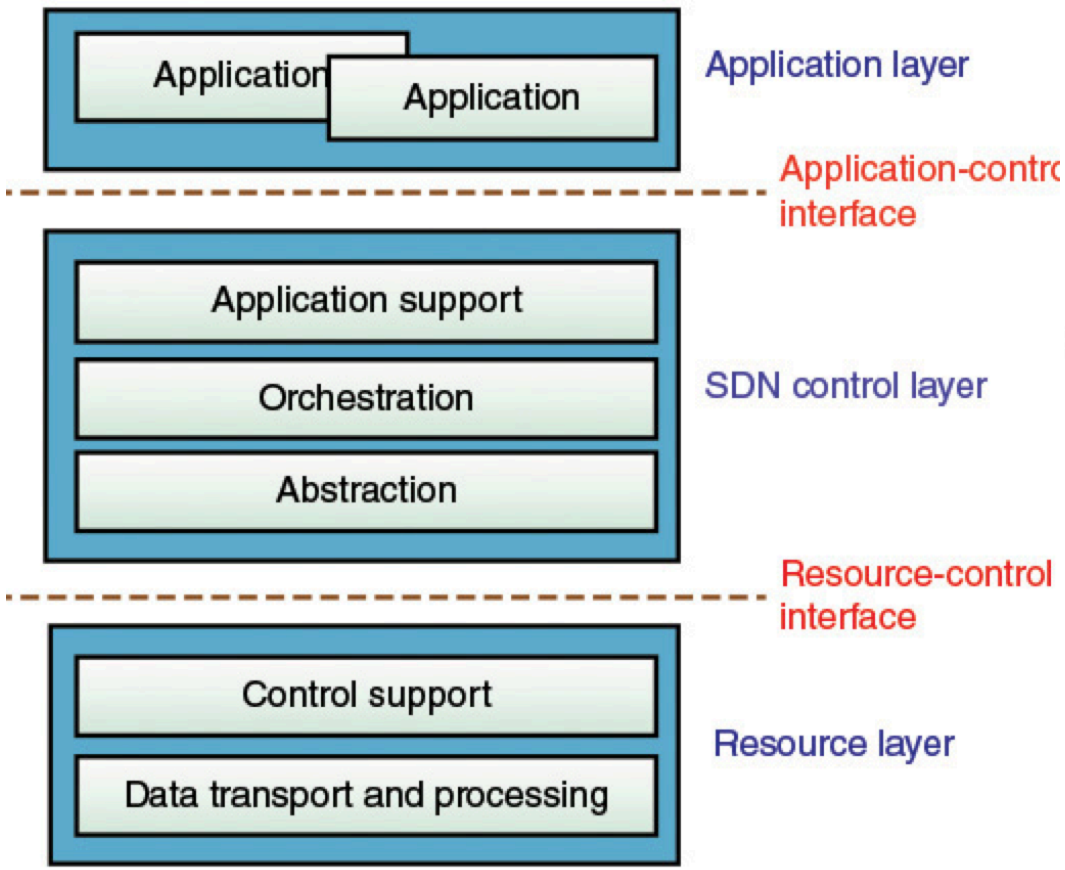
ADD TO CART

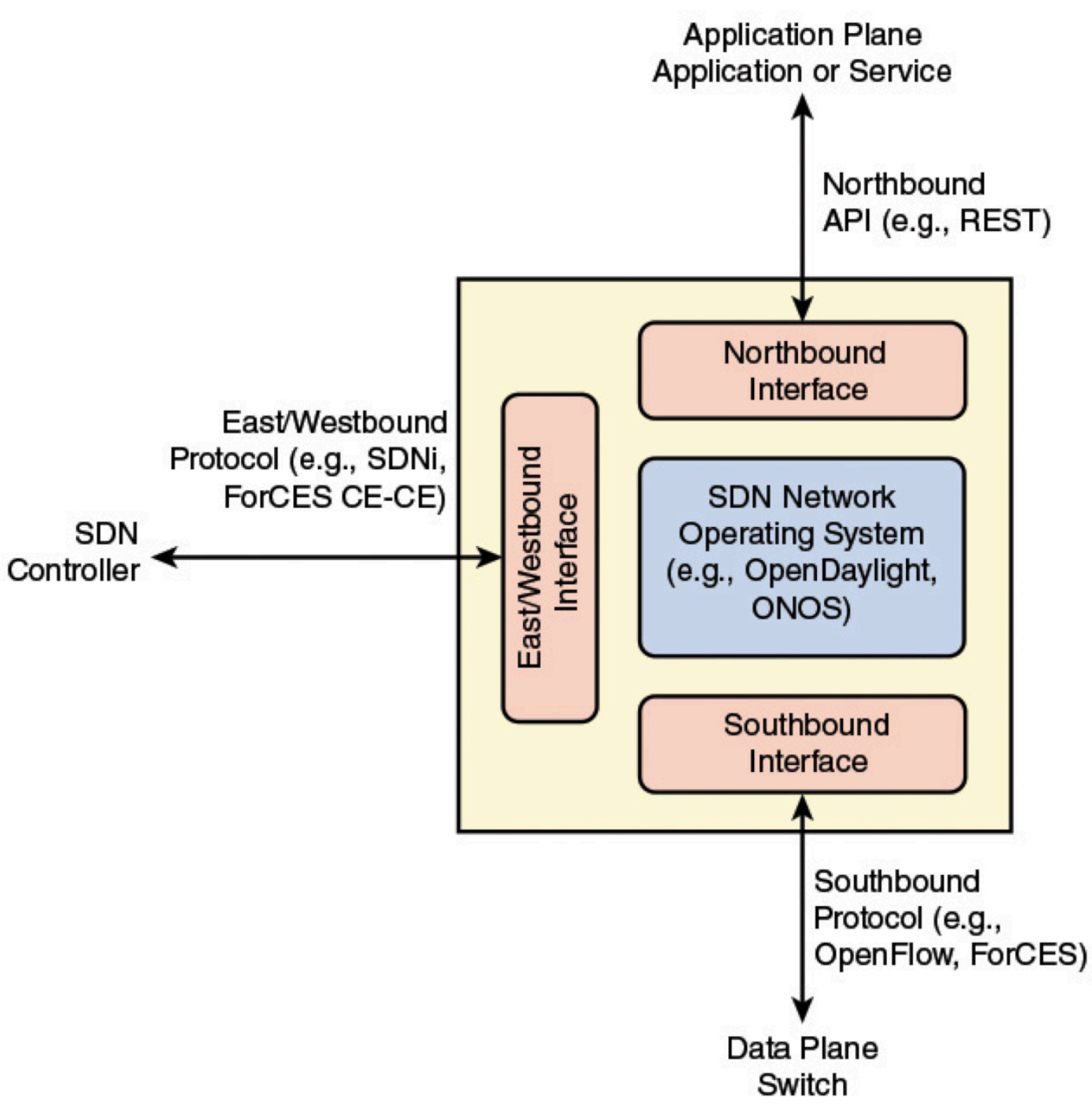
The Zodiac FX is the first OpenFlow switch designed to sit on your desk, not in a datacenter. Finally you can develop SDN applications using real traffic from real hardware. Until now the power of Software Defined Networking (SDN) was only available to the administrators of large corporate networks like Google and Facebook. Even though there are numerous free or open source SDN controllers the one thing that was missing was a small, affordable OpenFlow switch. That was until now...

PRICE INCLUDES FREE SHIPPING!

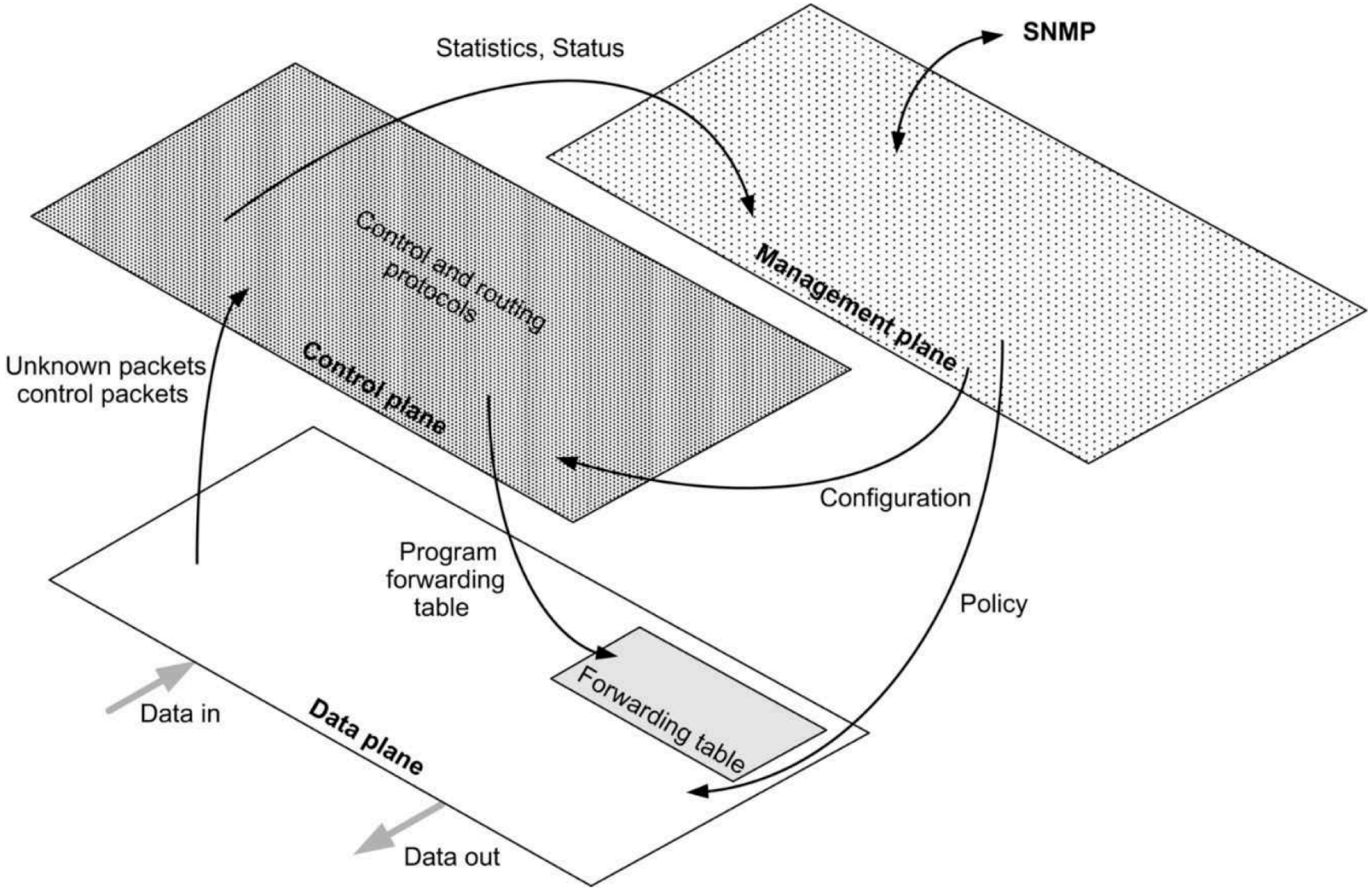
SHARE

SDN Architecture

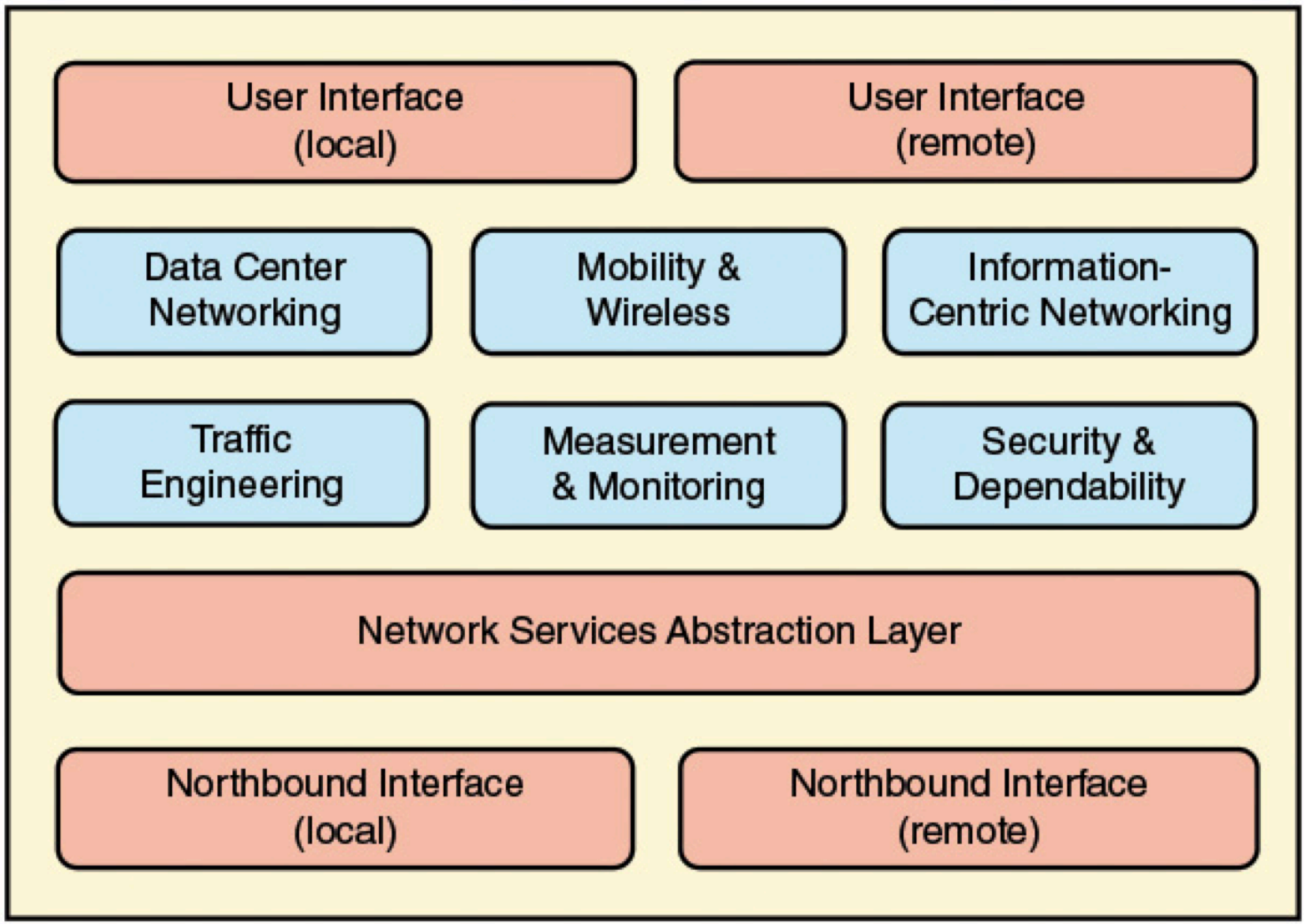




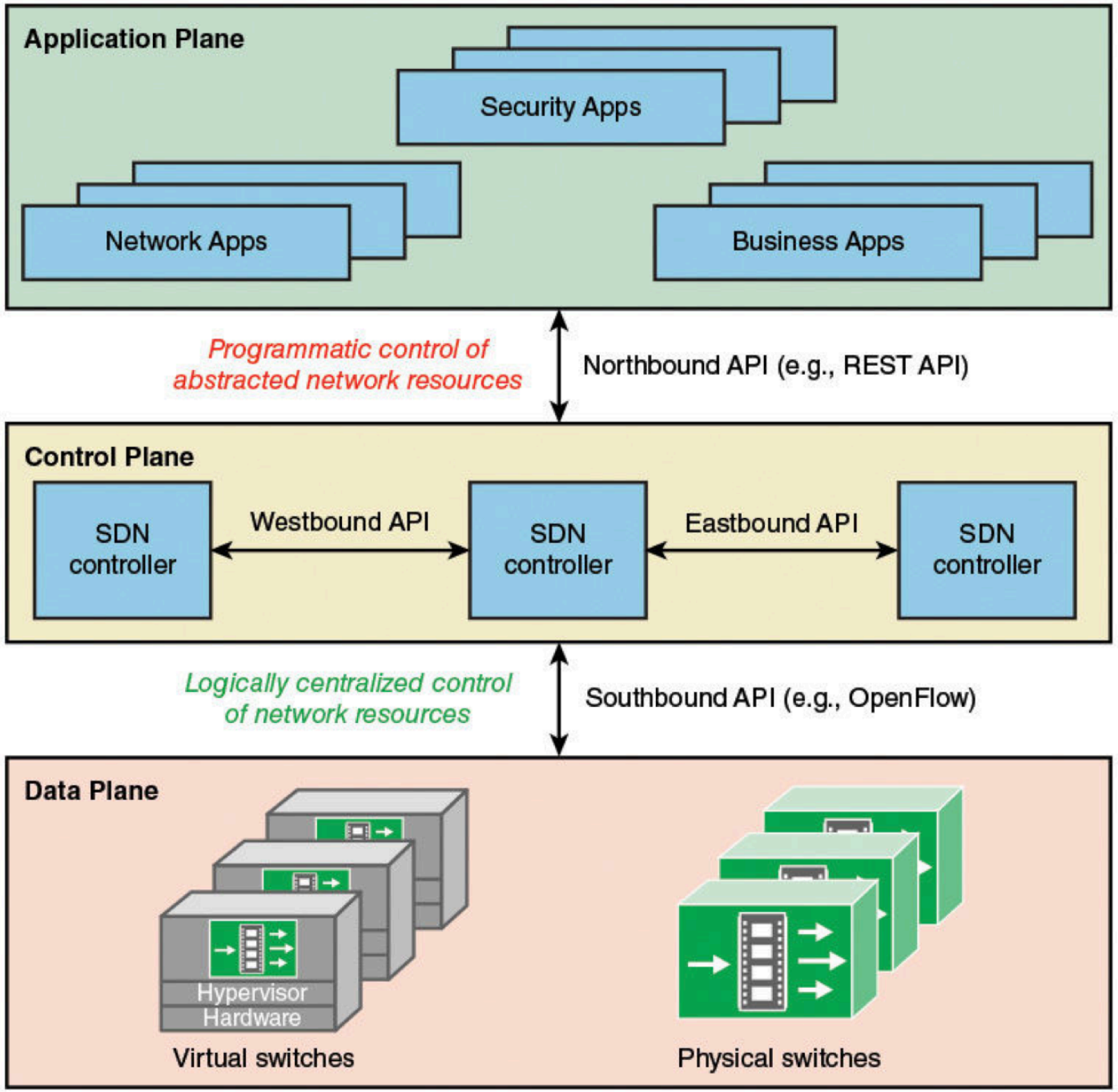
SDN Architecture

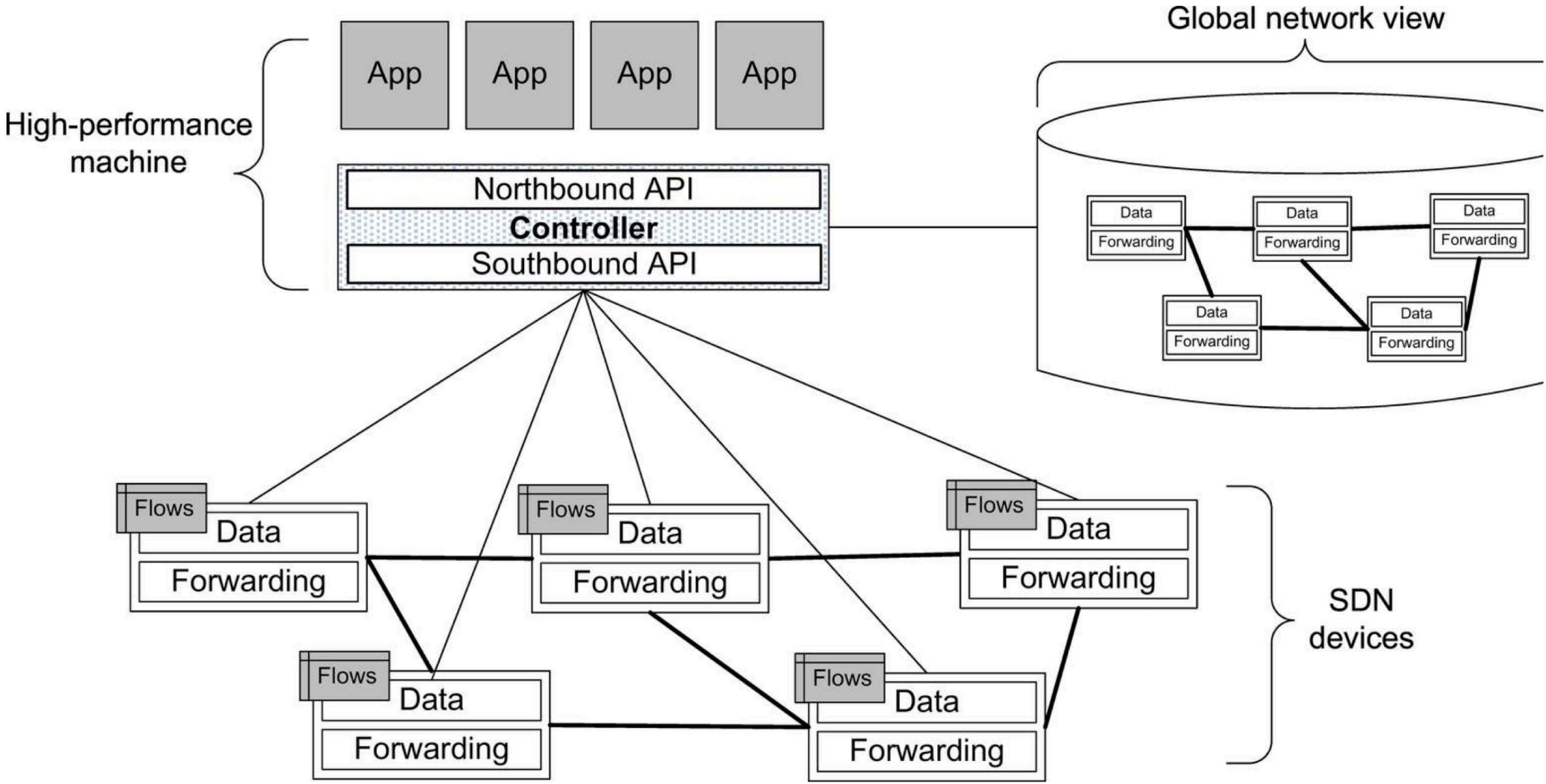


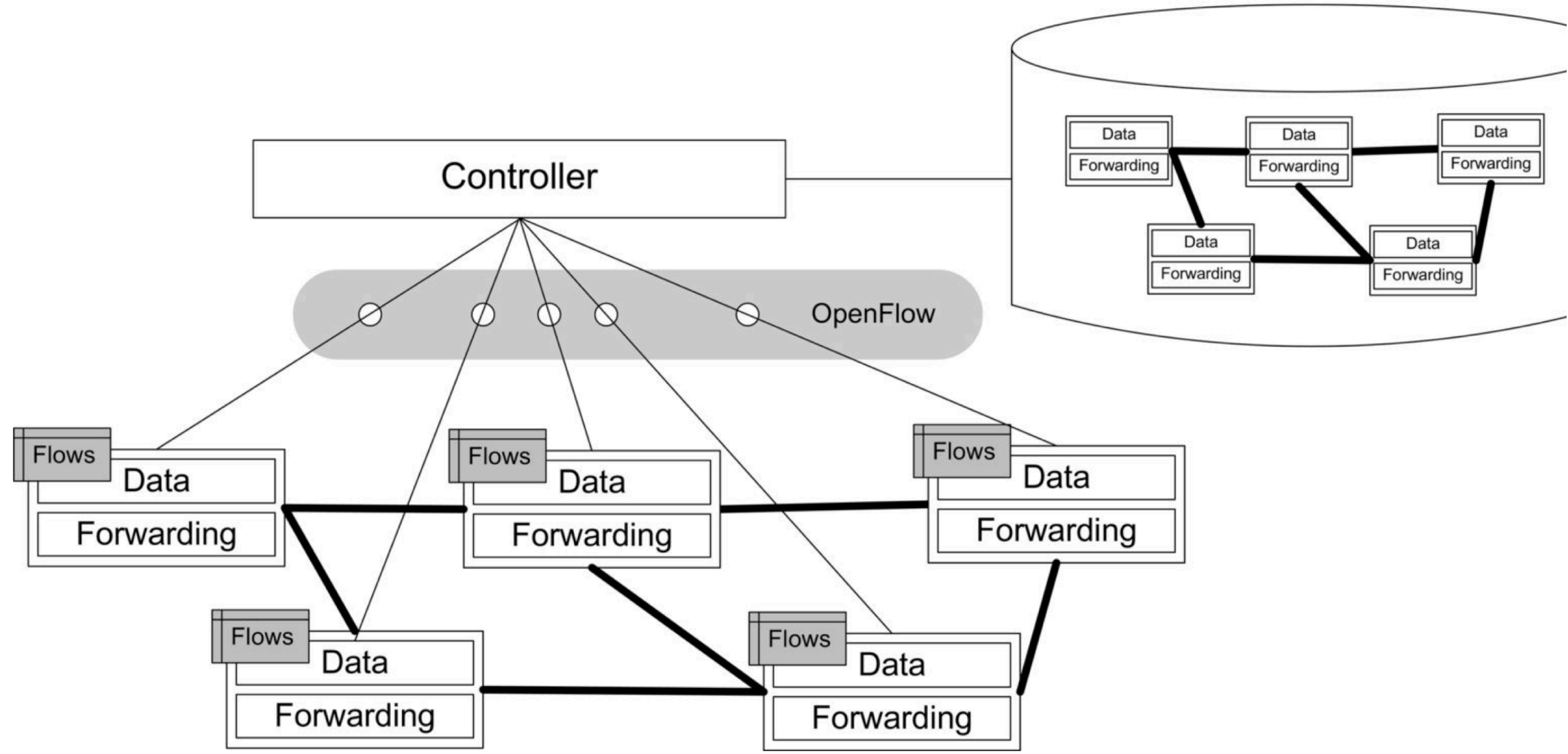
Management


User Interface (local)
User Interface (remote)
Data Center Networking
Mobility & Wireless
Information-Centric Networking
Traffic Engineering
Measurement & Monitoring
Security & Dependability
Network Services Abstraction Layer
Northbound Interface (local)
Northbound Interface (remote)

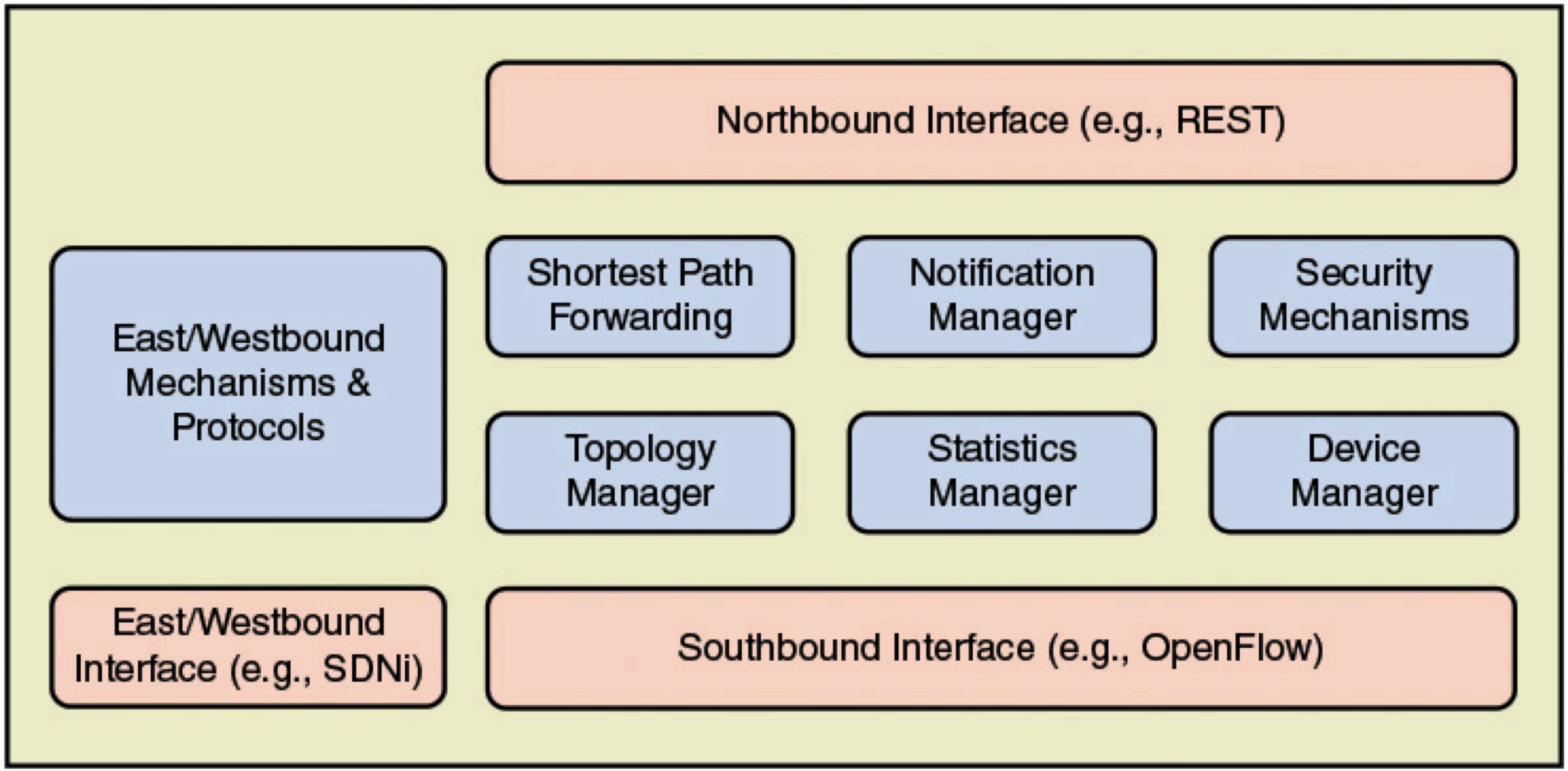
SDN Architecture



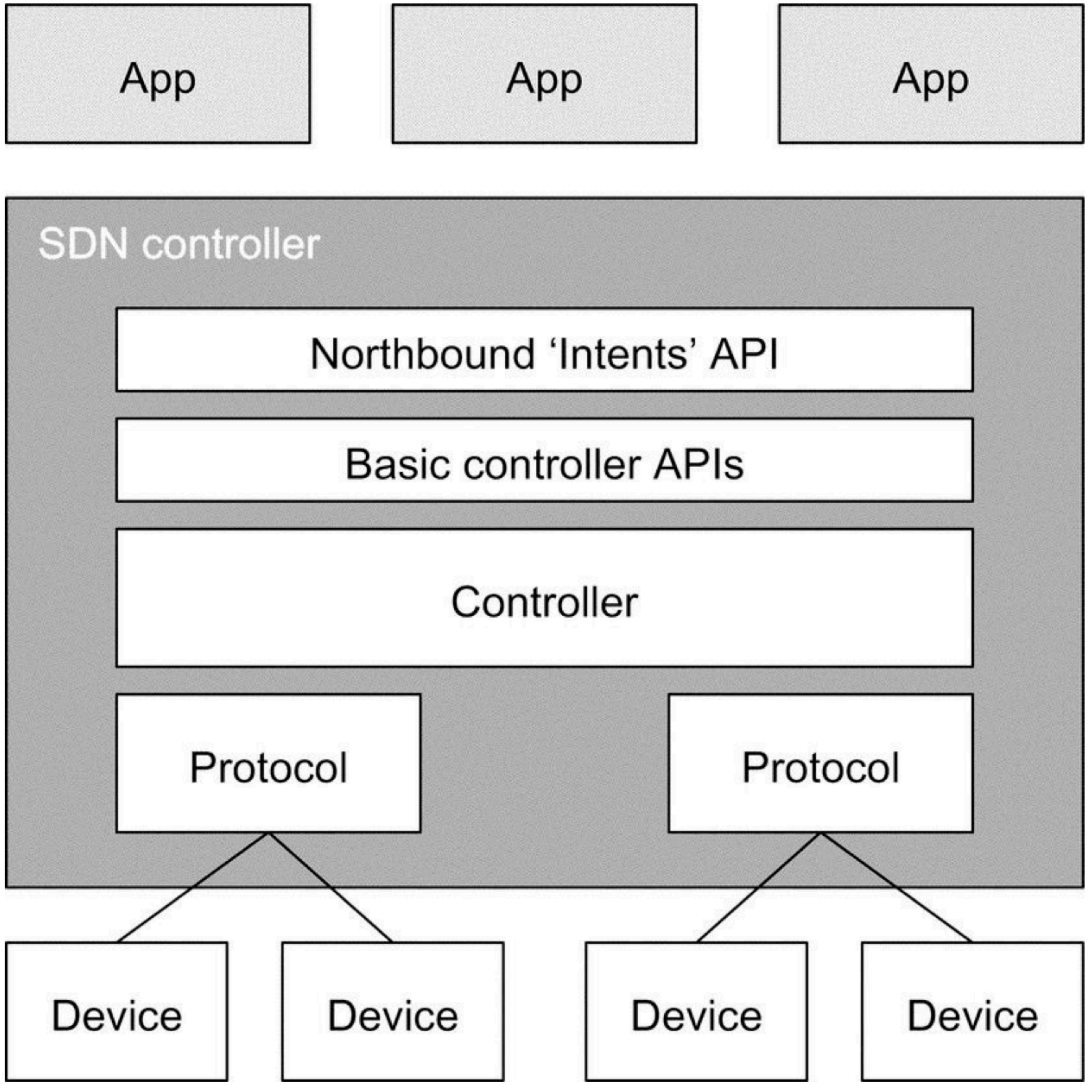

High-performance machine
App
App
App
App
Northbound API
Controller
Southbound API
Global network view
Data
Forwarding
Flows
SDN devices


Controller
OpenFlow
Flows
Data
Forwarding
Flows
Data
Forwarding
Flows
Data
Forwarding
Flows
Data
Forwarding
Flows
Data
Forwarding
Data
Forwarding
Data
Forwarding
Data
Forwarding
Data
Forwarding
Data
Forwarding

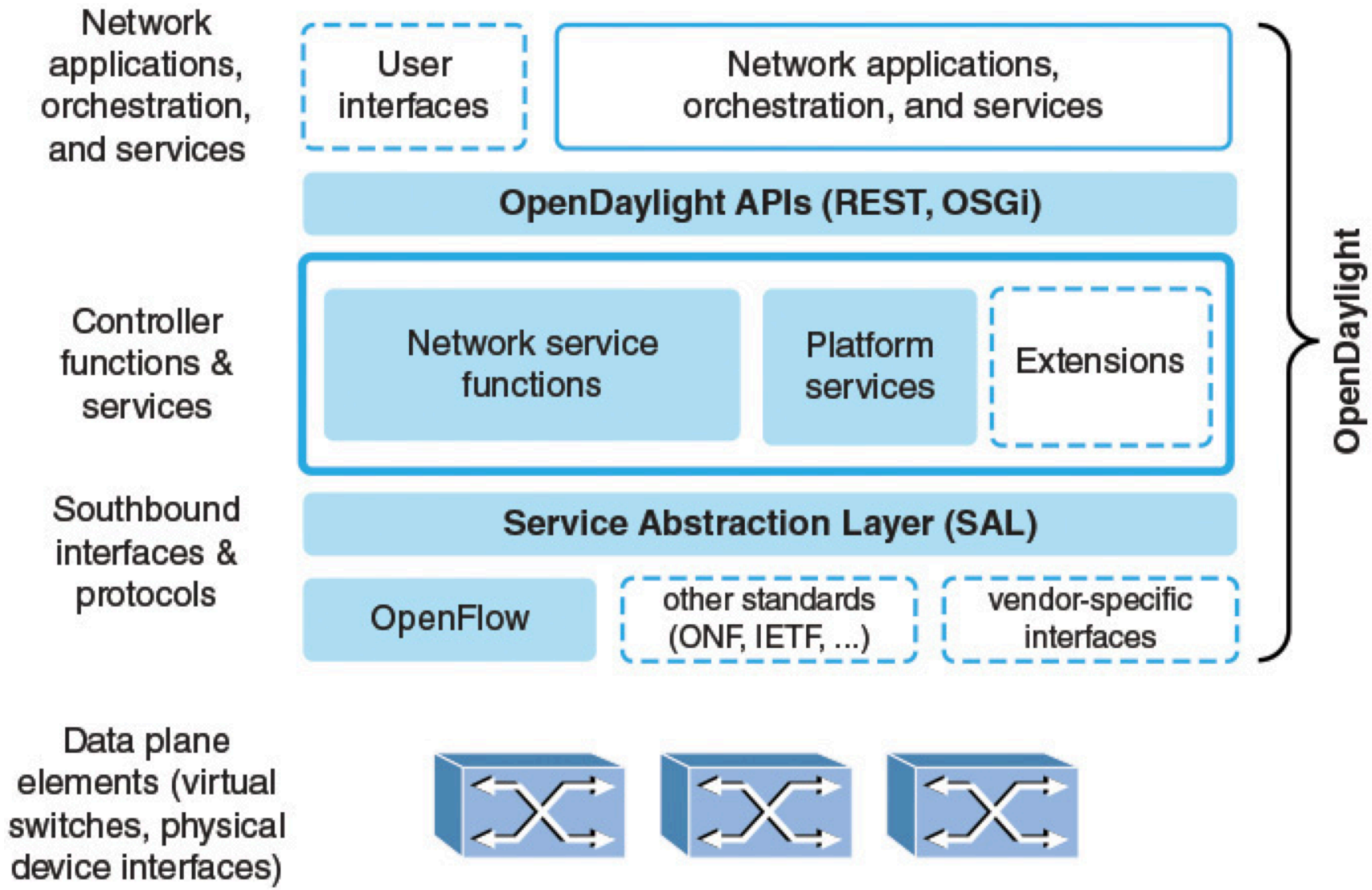
Controller


Northbound Interface (e.g., REST)
East/Westbound Mechanisms & Protocols
Shortest Path Forwarding
Notification Manager
Security Mechanisms
Topology Manager
Statistics Manager
Device Manager
East/Westbound Interface (e.g., SDNi)
Southbound Interface (e.g., OpenFlow)

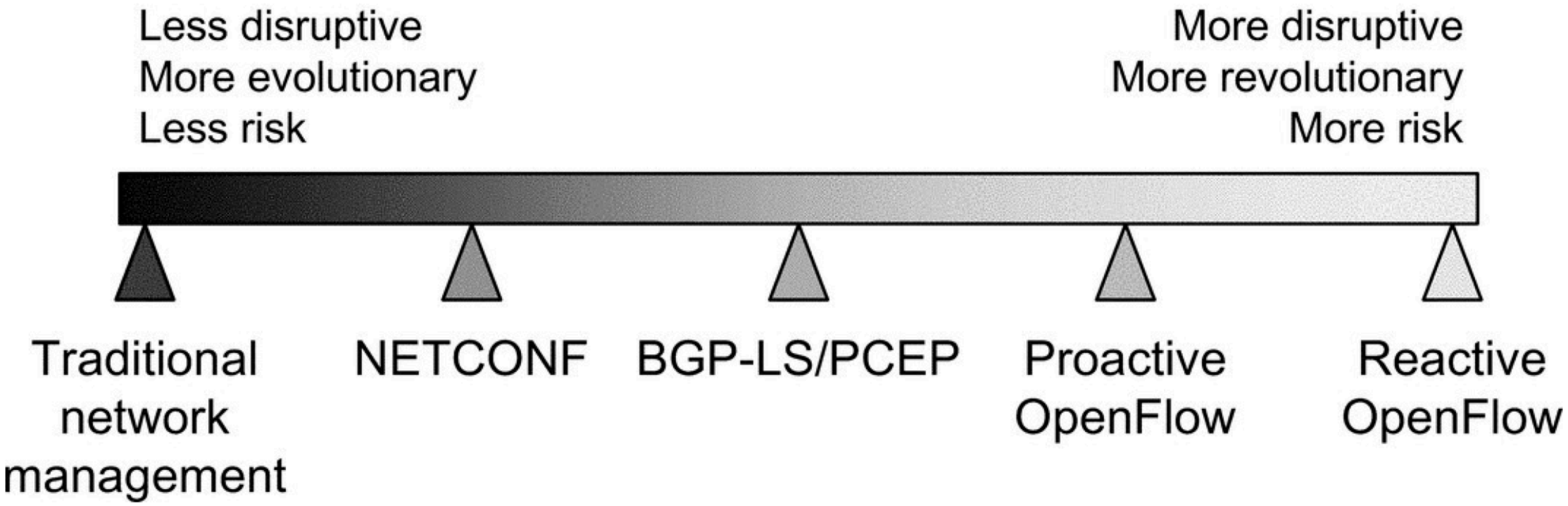
SDN is not only OpenFlow



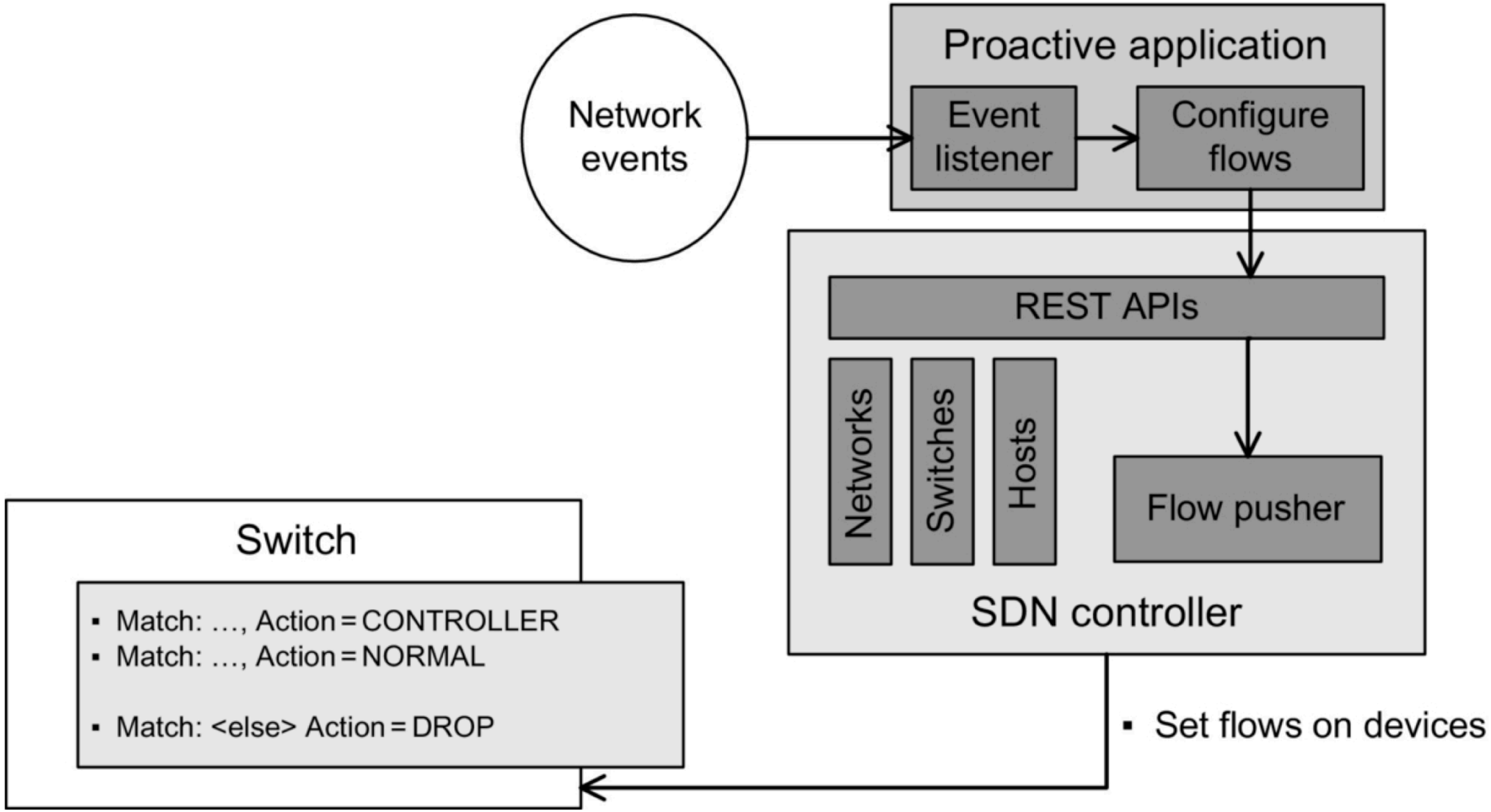
Multiple protocol support: OpenDaylight



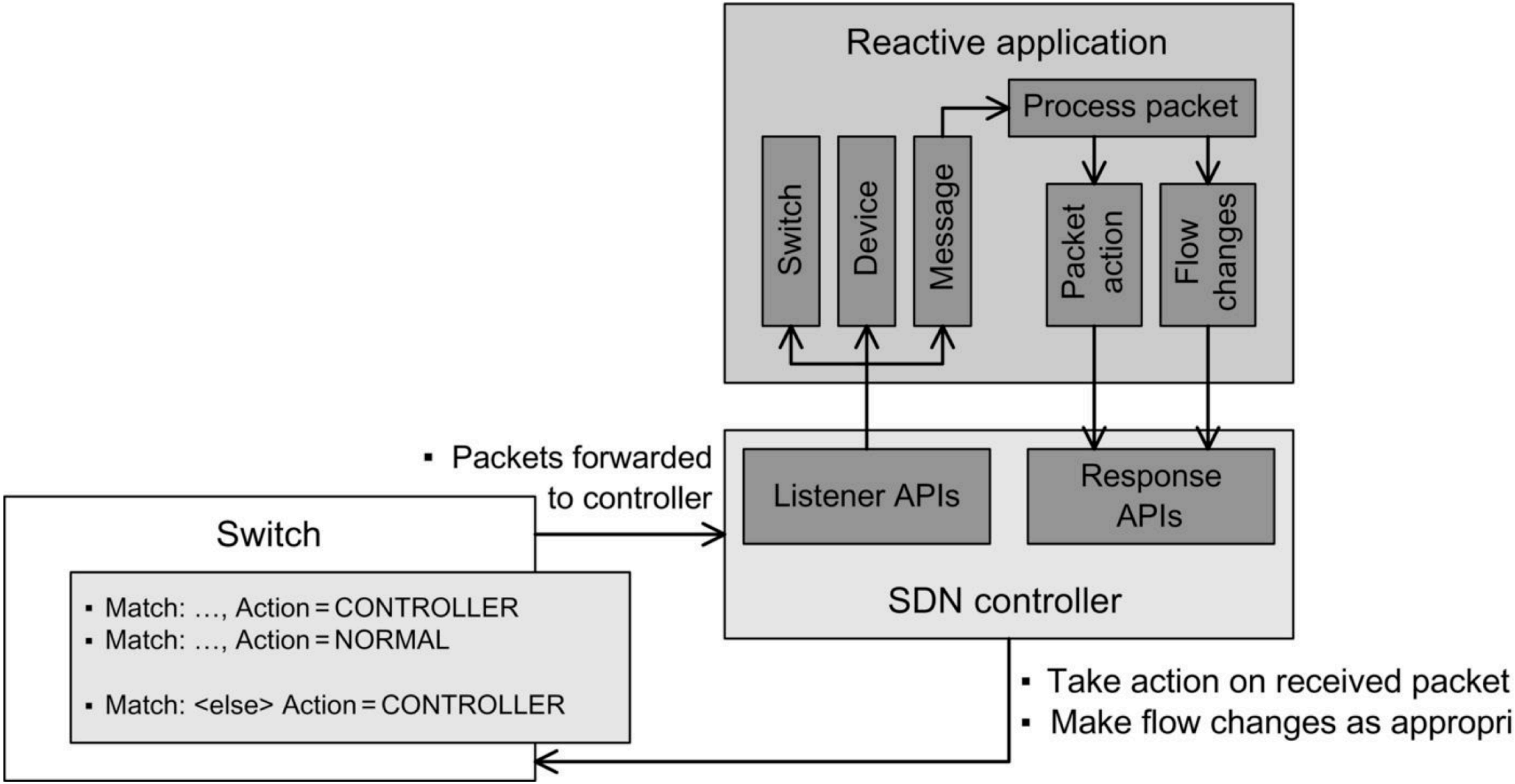
Spectrum of SDN technologies



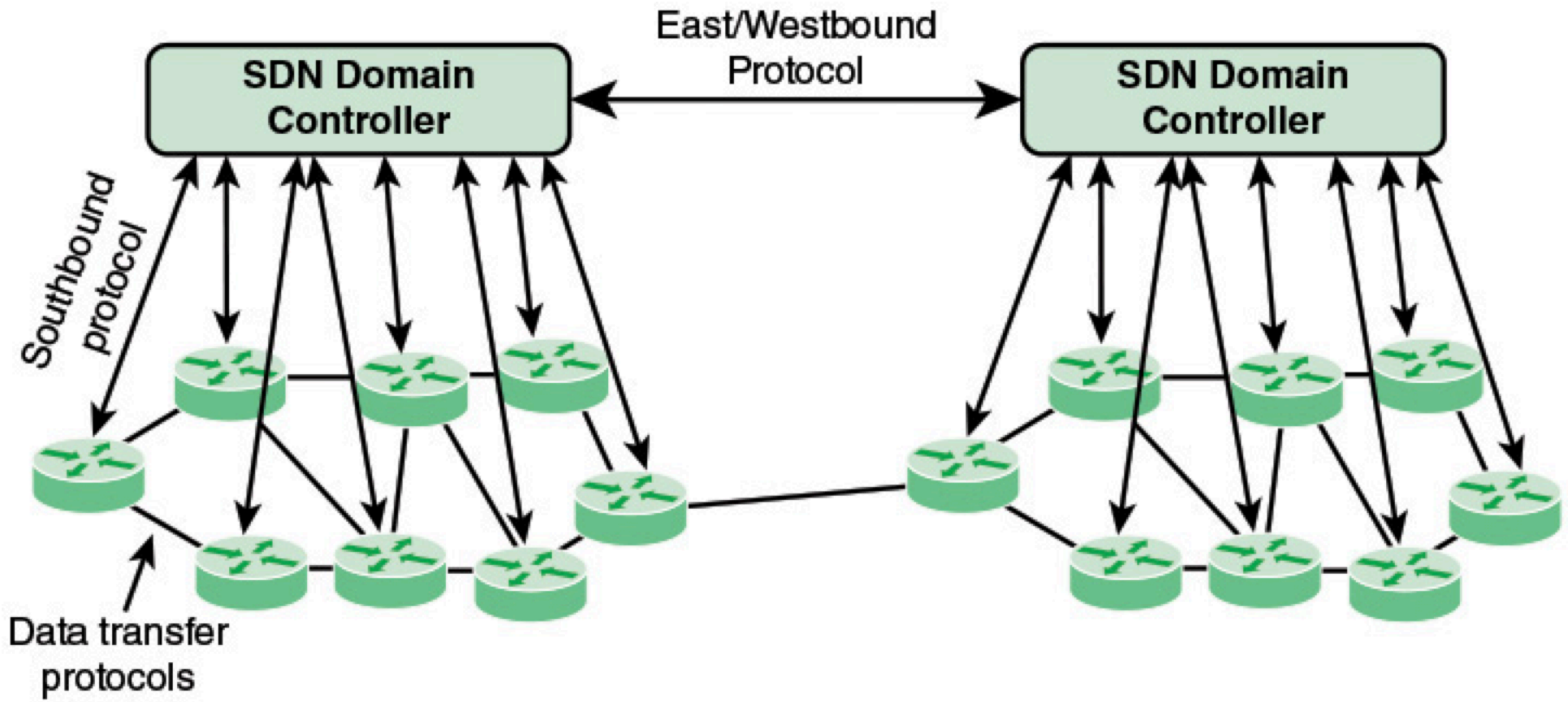
Proactive applications



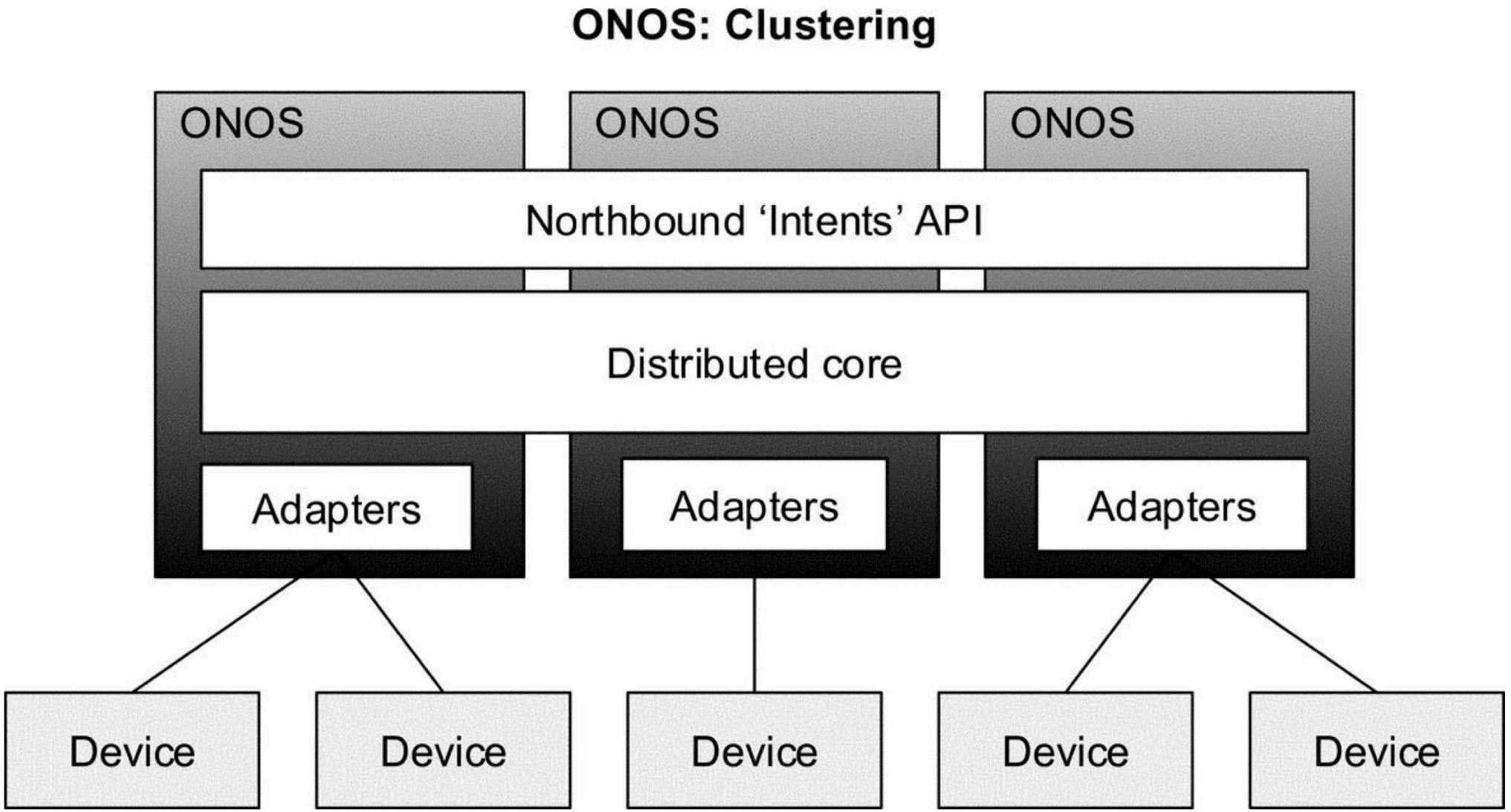
Reactive applications



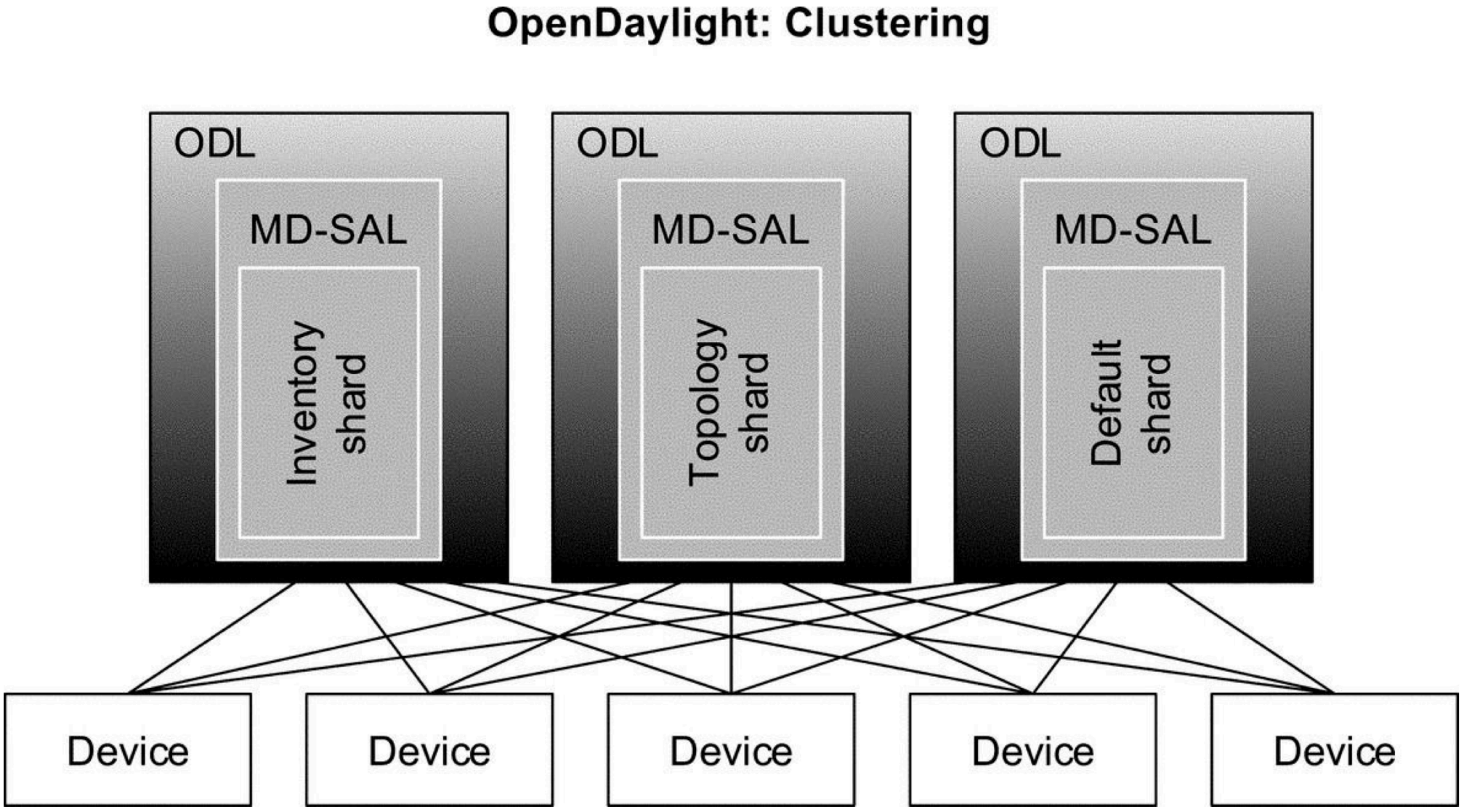
Clustering of controllers



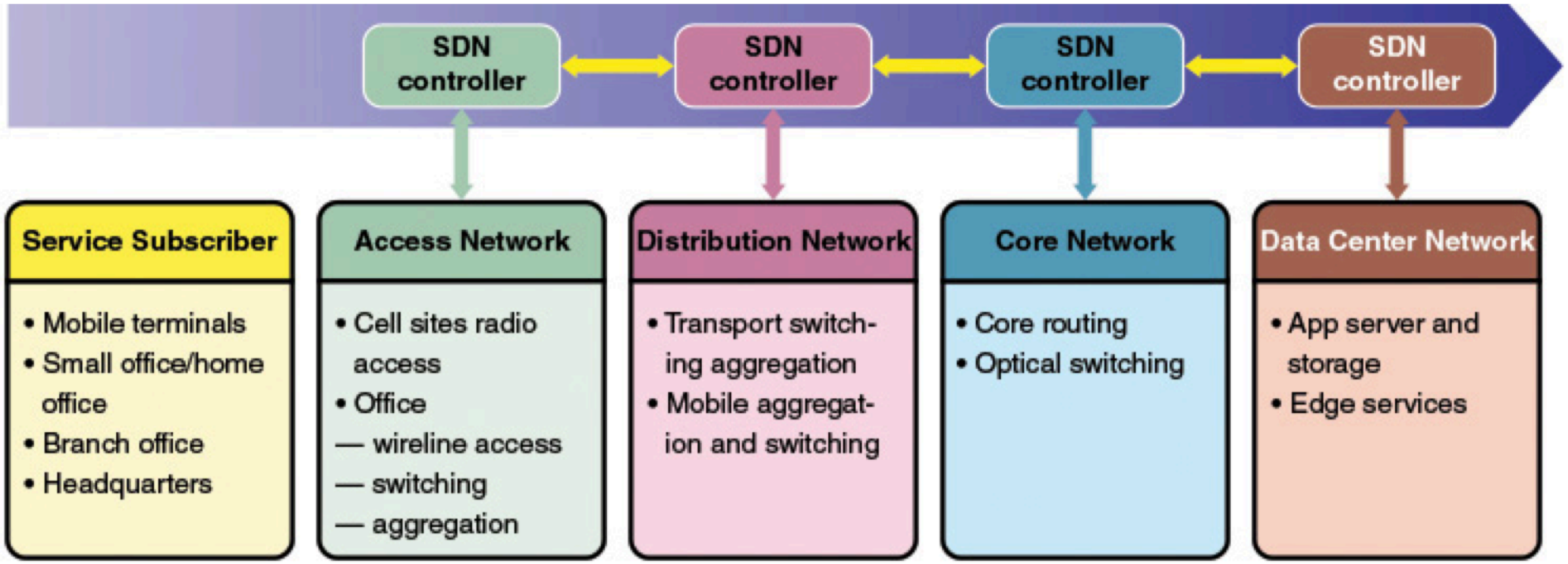
Various types of clustering



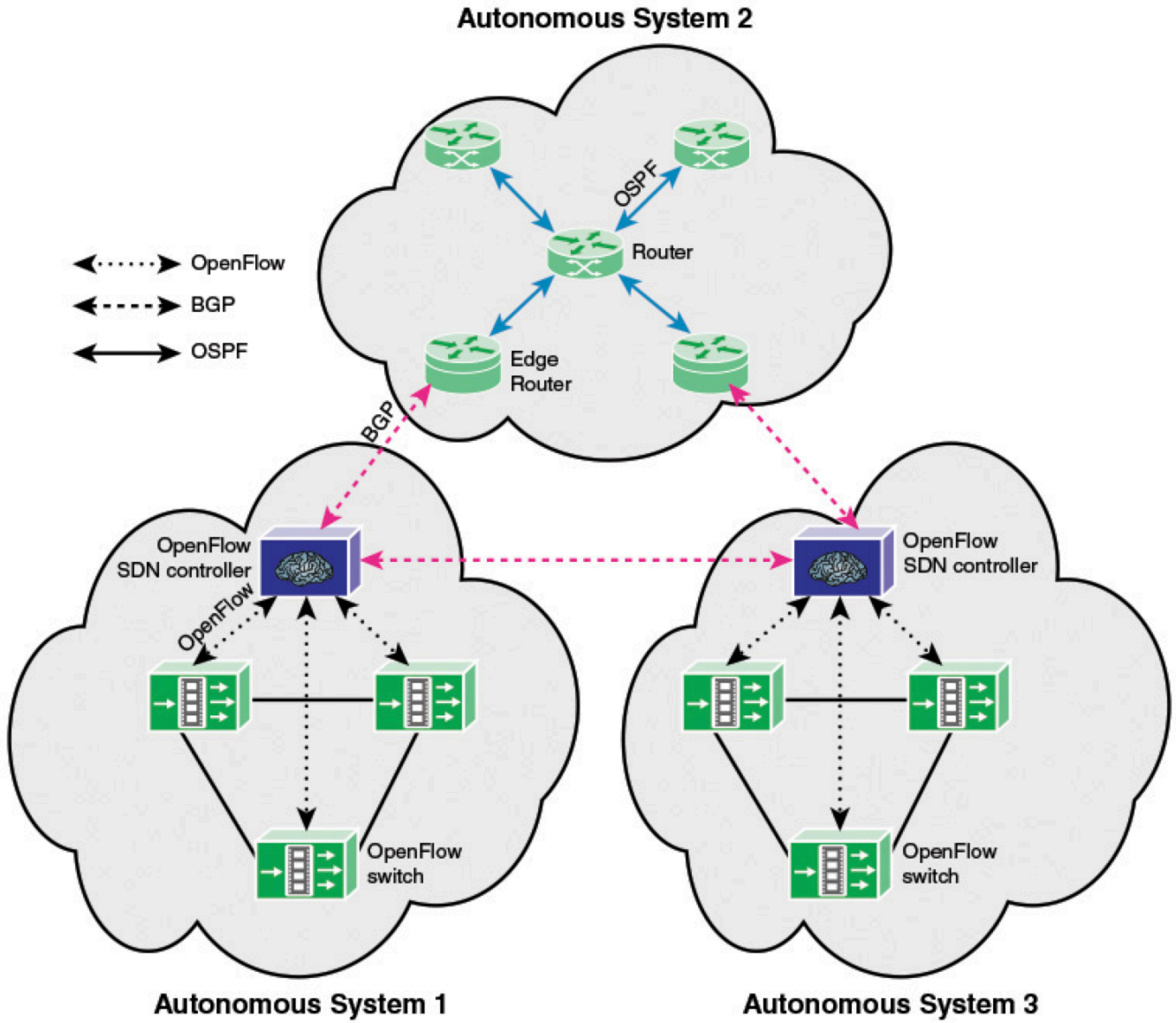
Various types of clustering



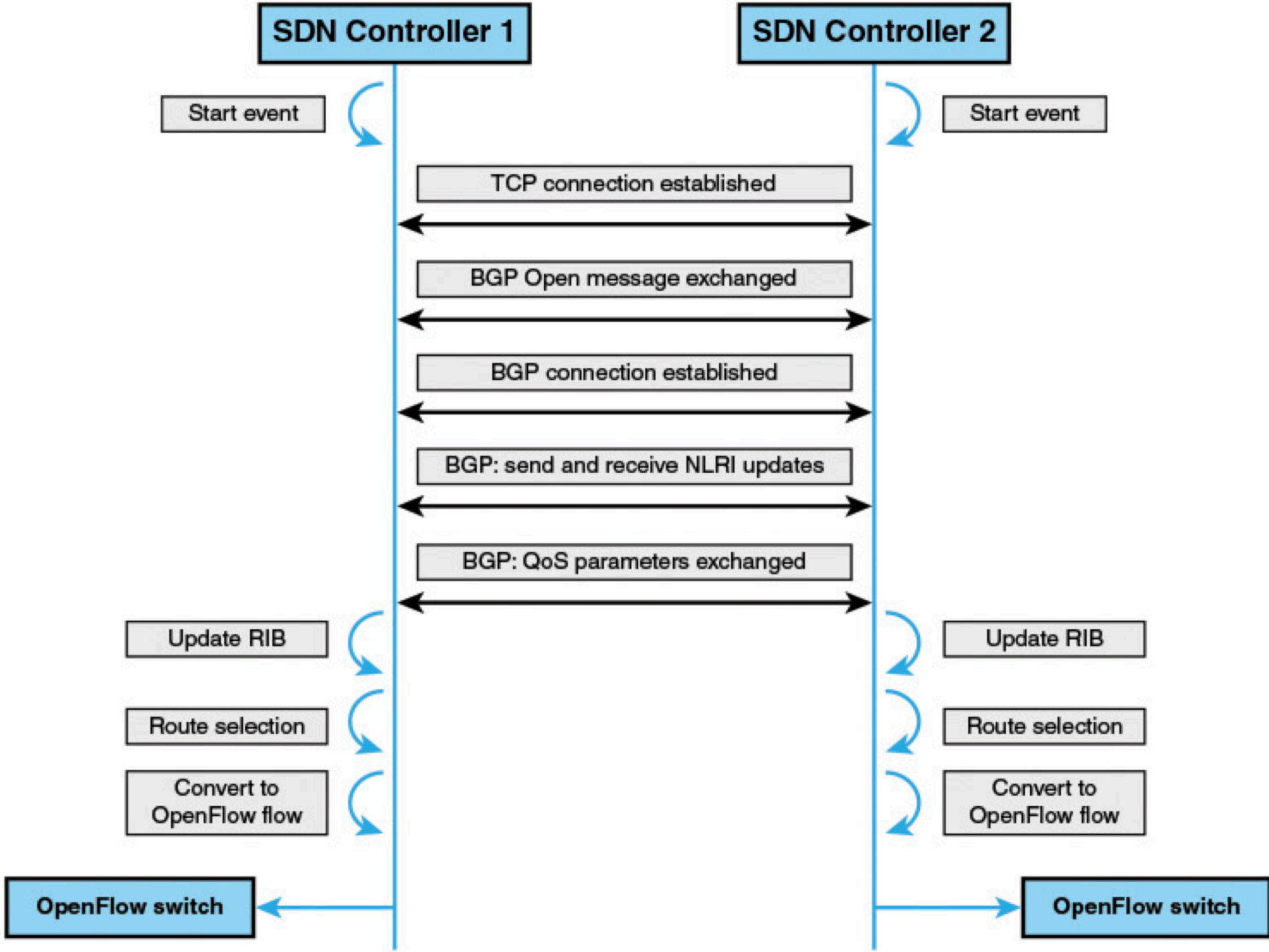
Inter-controller communications



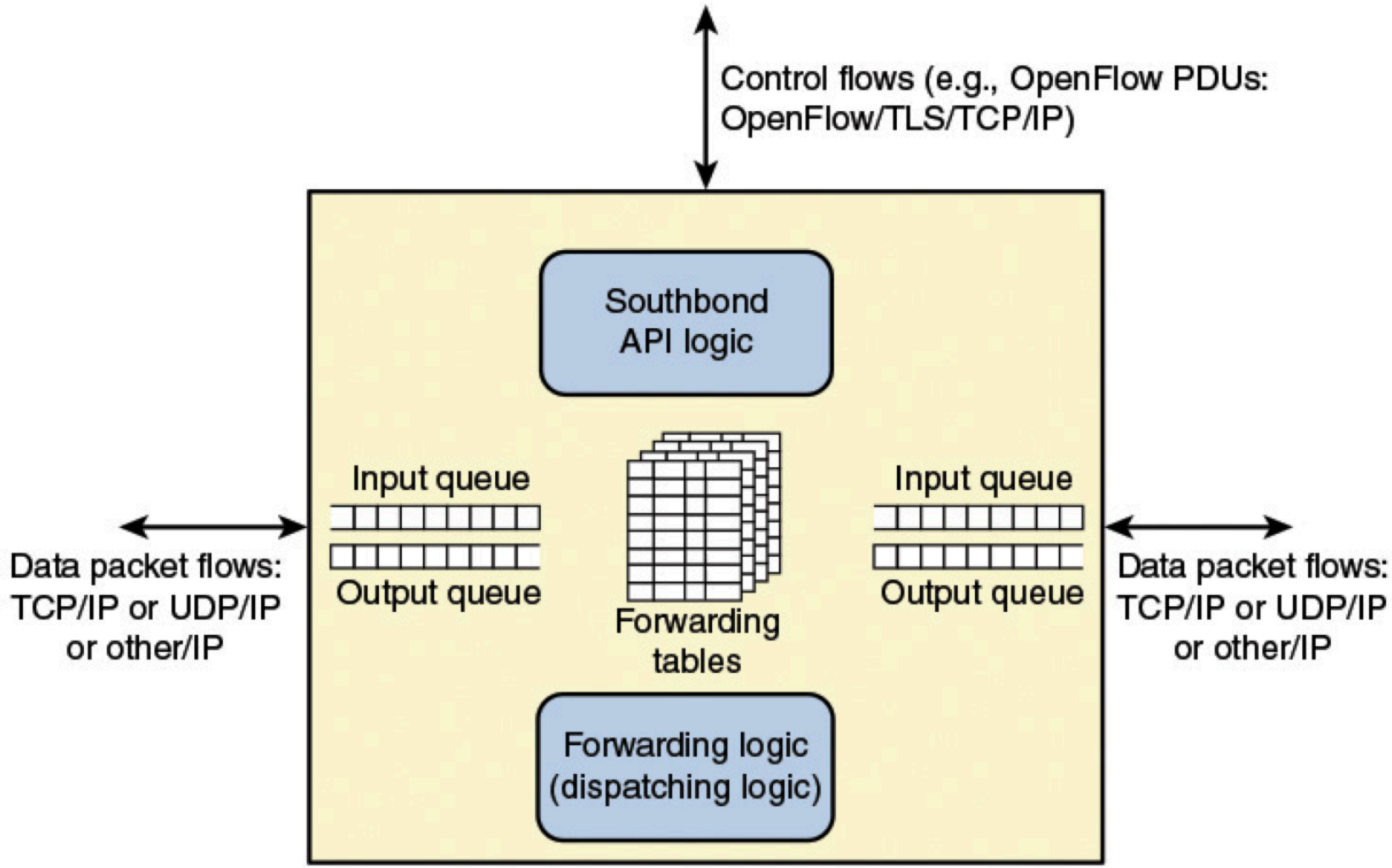
Inter-controller communications



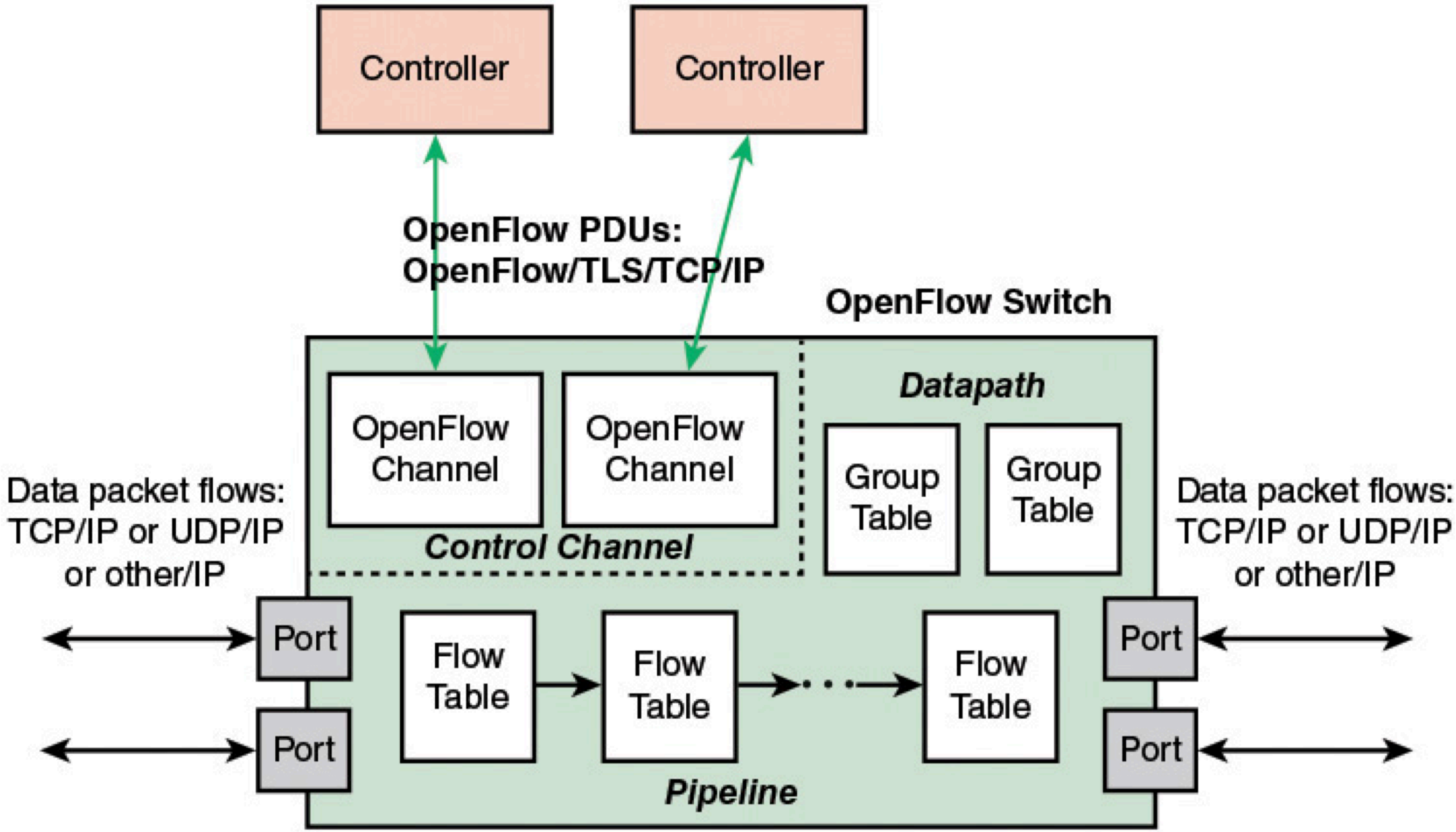
East-west


SDN Controller 1
SDN Controller 2
Start event
Start event
TCP connection established
BGP Open message exchanged
BGP connection established
BGP: send and receive NLRI updates
BGP: QoS parameters exchanged
Update RIB
Update RIB
Route selection
Route selection
Convert to OpenFlow flow
Convert to OpenFlow flow
OpenFlow switch
OpenFlow switch

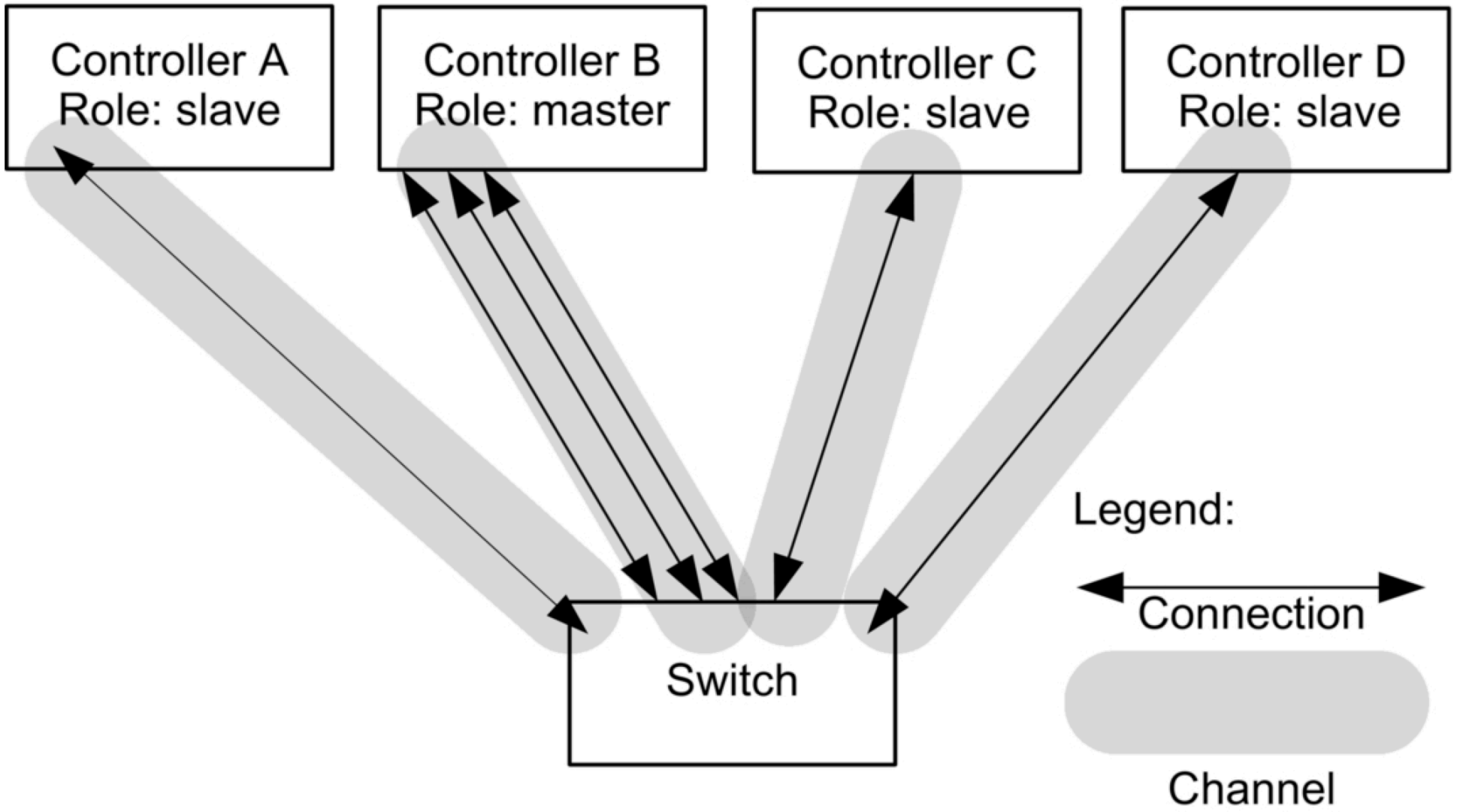
What does switch do?



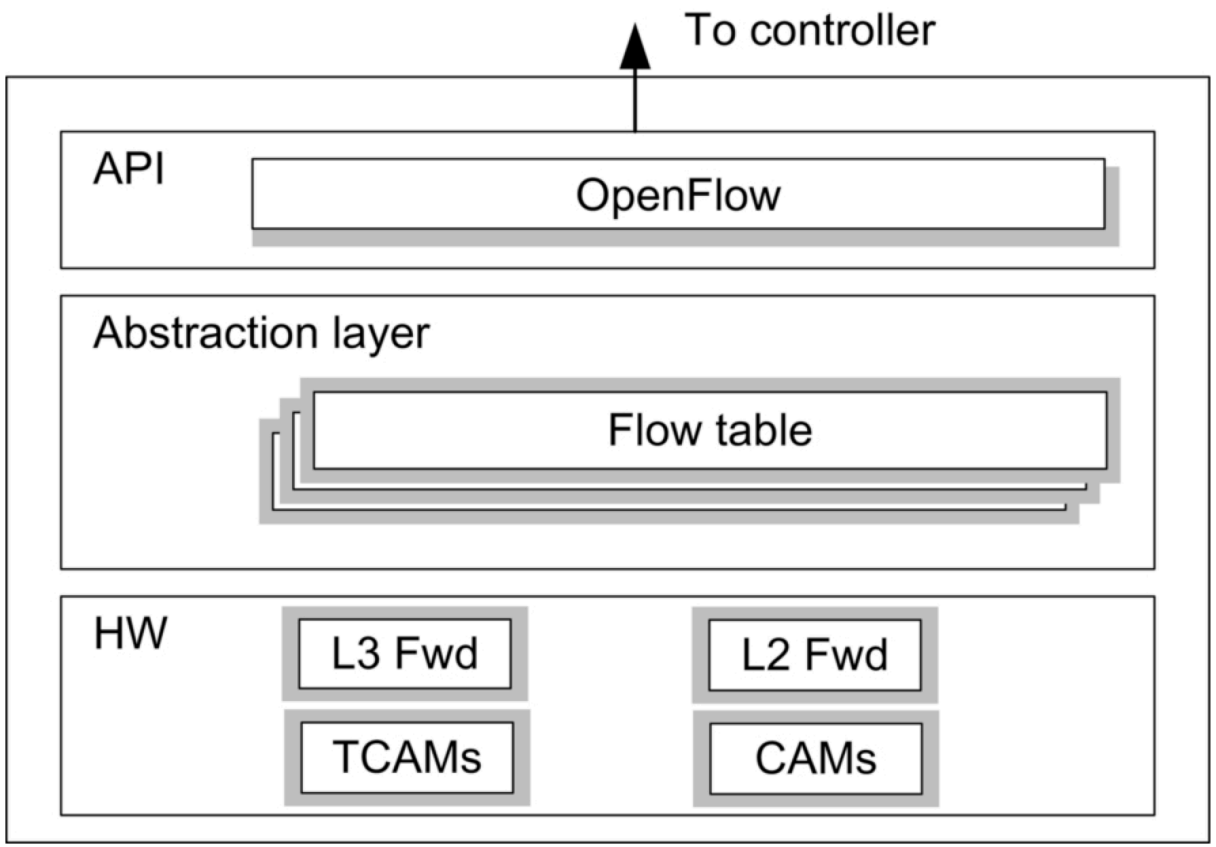
What does switch do?

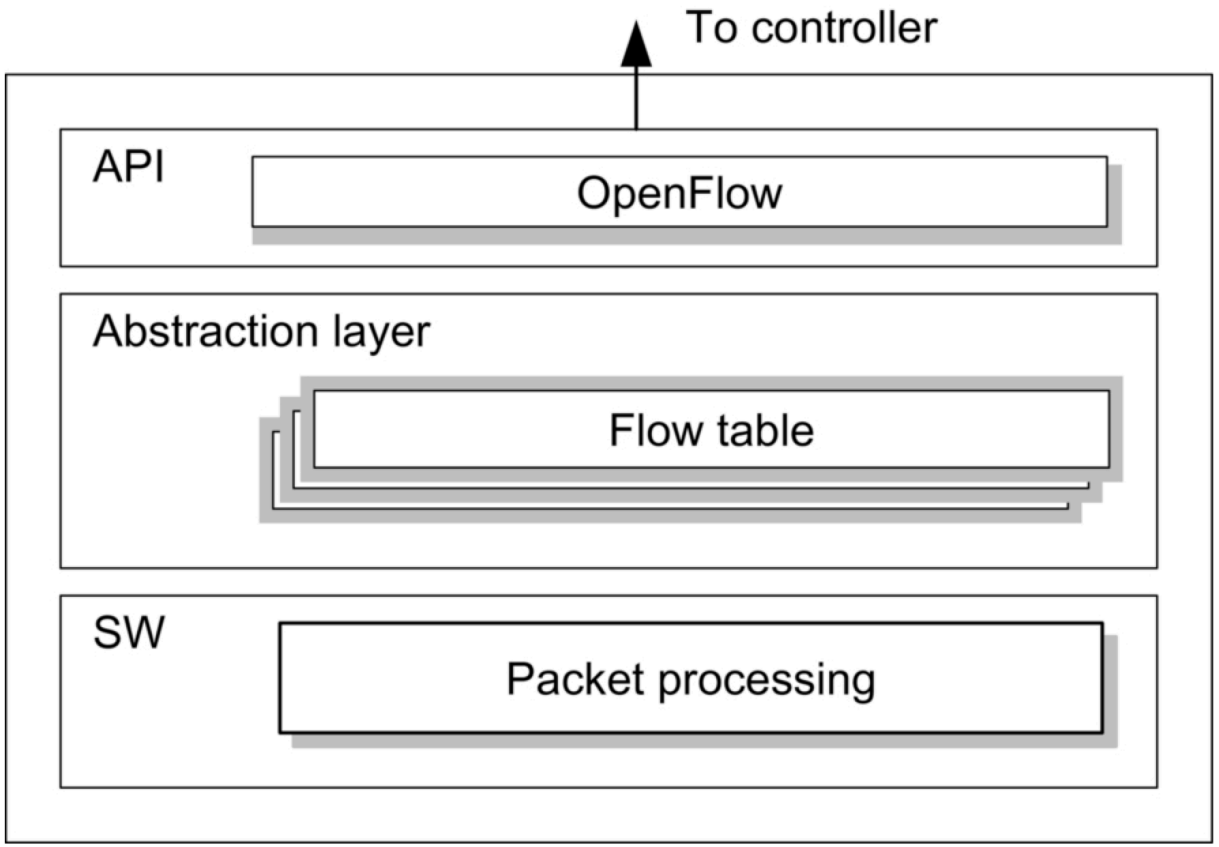


How many controllers control a switch?

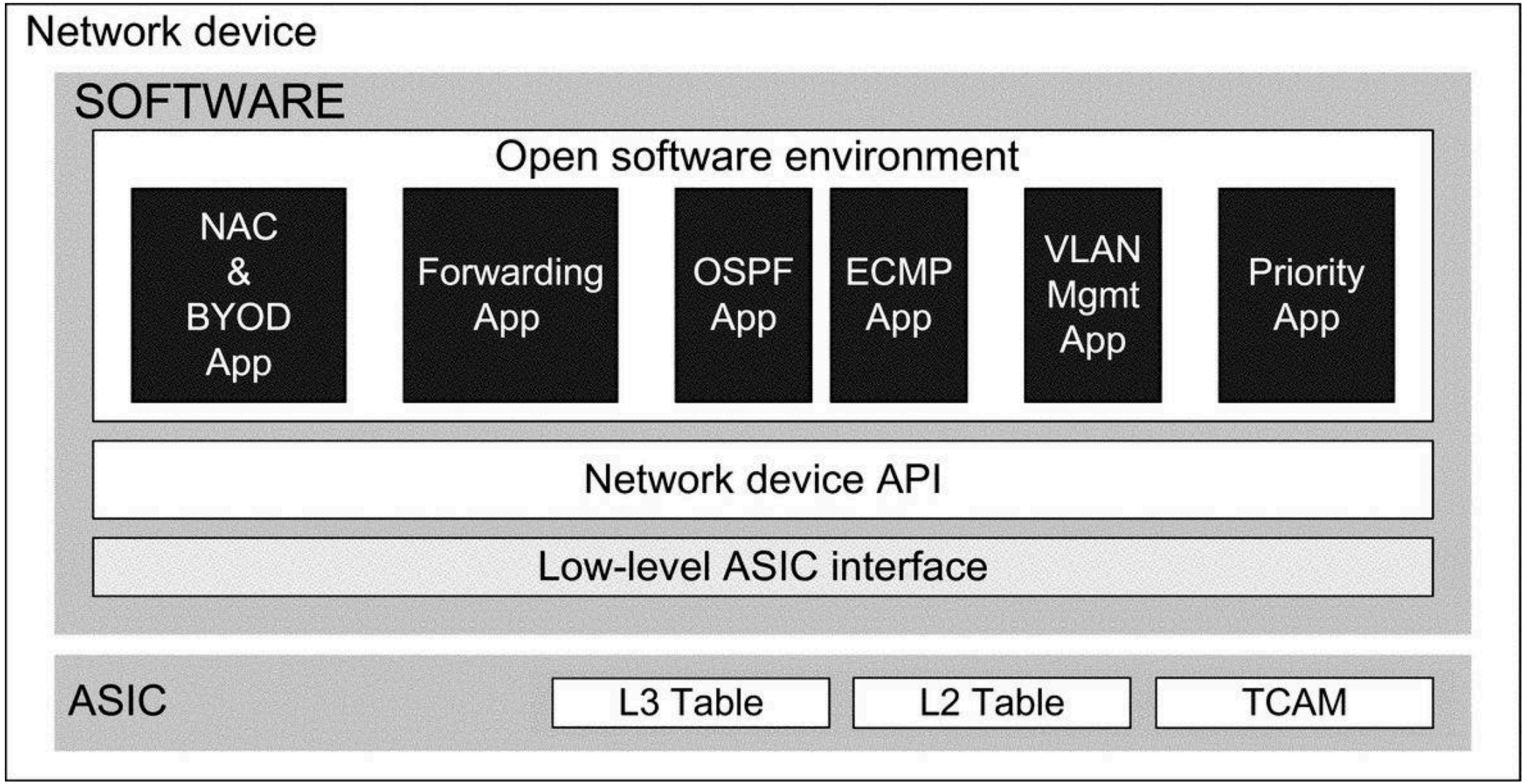


Hardware vs software switch

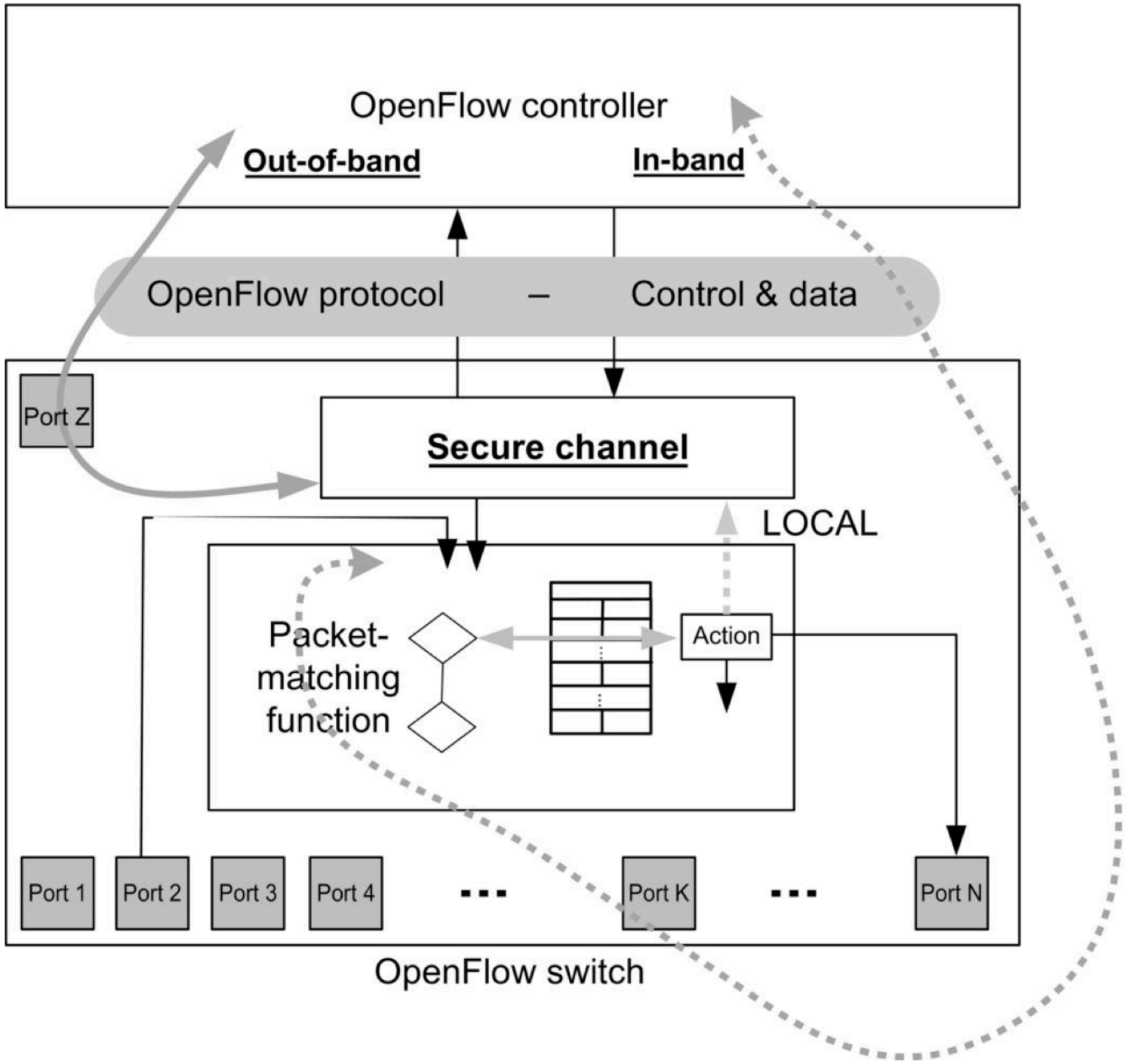




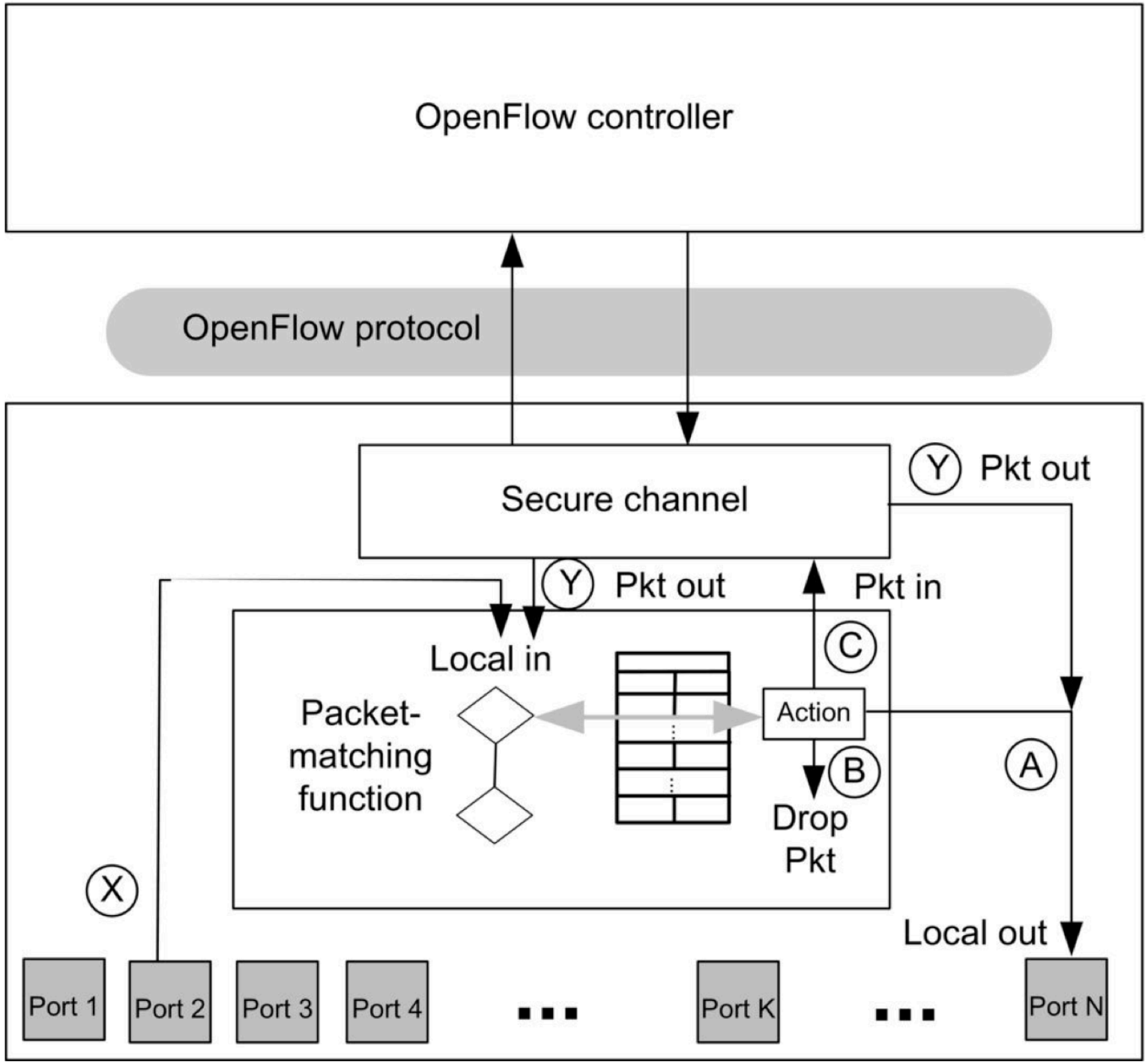
Open switches



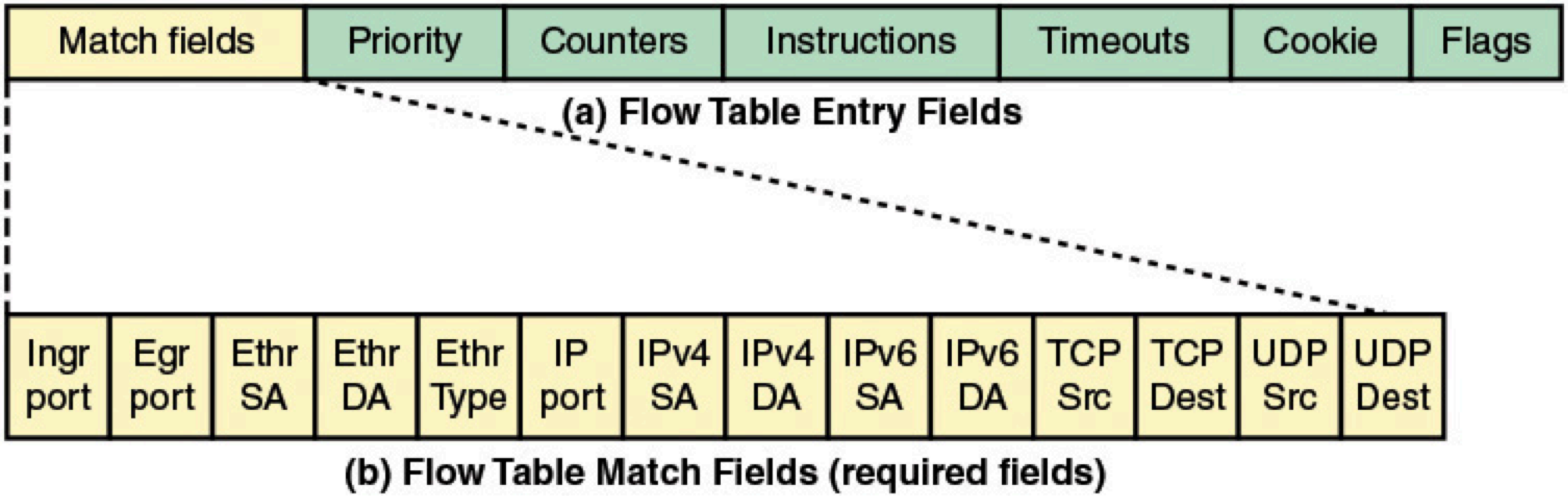
Flow processing

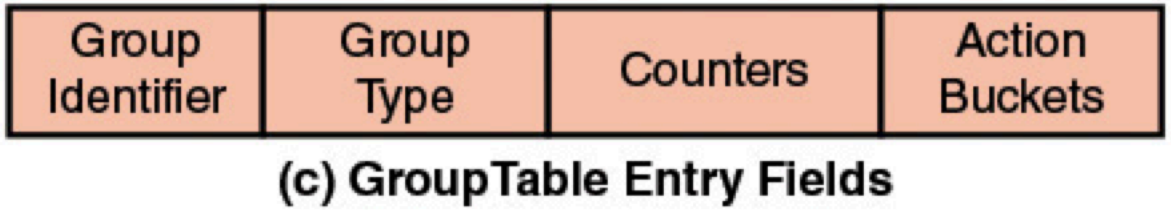


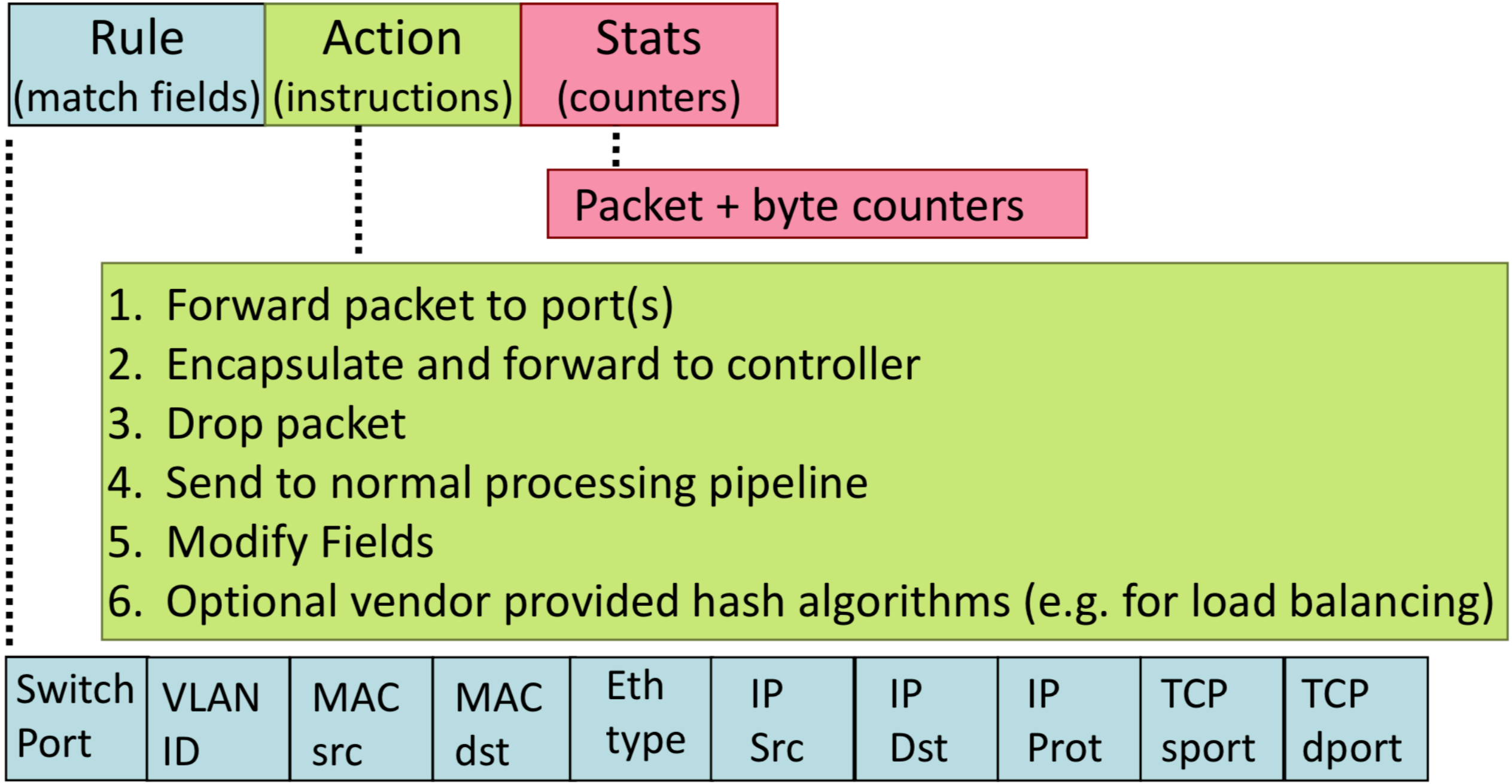
Flow processing



Flow tables


Match fields
Priority
Counters
Instructions
Timeouts
Cookie
Flags
(a) Flow Table Entry Fields
Ingr port
Egr port
Ethr SA
Ethr DA
Ethr Type
IP port
IPv4 SA
IPv4 DA
IPv6 SA
IPv6 DA
TCP Src
TCP Dest
UDP Src
UDP Dest
(b) Flow Table Match Fields (required fields)


Group Identifier
Group Type
Counters
Action Buckets
(c) GroupTable Entry Fields


Rule
(match fields)
Action
(instructions)
Stats
(counters)
Packet + byte counters
1. Forward packet to port(s)
2. Encapsulate and forward to controller
3. Drop packet
4. Send to normal processing pipeline
5. Modify Fields
6. Optional vendor provided hash algorithms (e.g. for load balancing)
Switch Port
VLAN ID
MAC src
MAC dst
Eth type
IP Src
IP Dst
IP Prot
TCP sport
TCP dport

Standard switching on MAC addrs

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	00:1f:..	*	*	*	*	*	*	*	port6

Switching based on application-level flow

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
port3	00:20..	00:1f..	0800	vlan1	1.2.3.4	5.6.7.8	4	17264	80	port6

Firewall / filtering rules

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Forward
*	*	*	*	*	*	*	*	*	22	drop

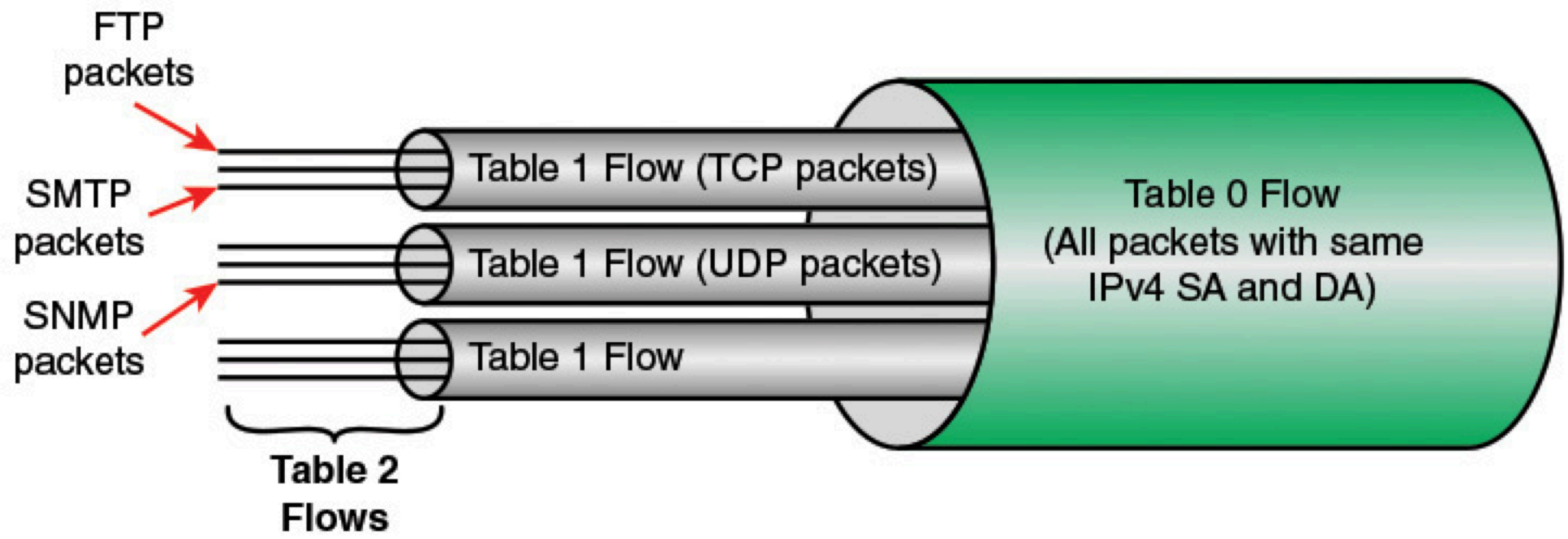
IP destination-based routing

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	*	*	*	*	5.6.7.8	*	*	*	port6

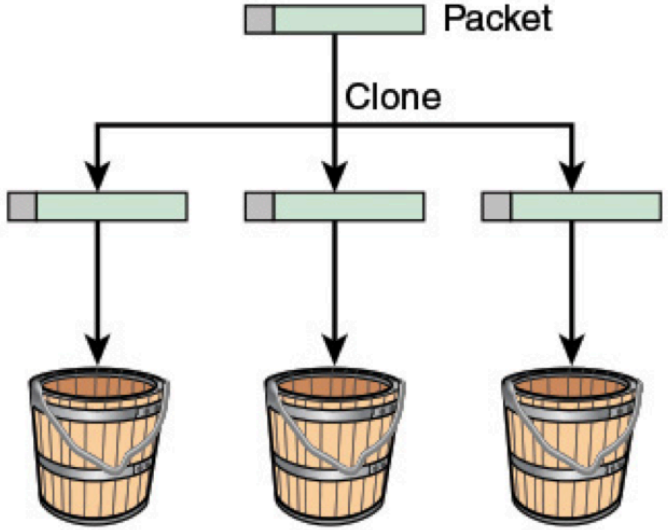
MAC address switching with VLAN check

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	00:1f..	*	vlan1	*	*	*	*	*	port7

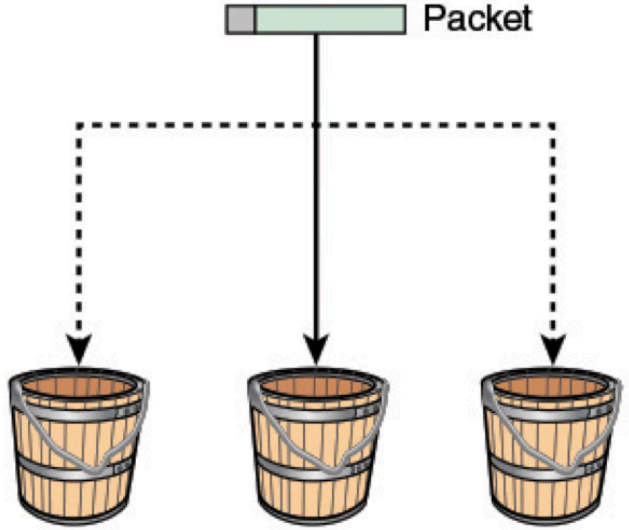
Flows


FTP
packets
SMTP
packets
SNMP
packets
Table 1 Flow (TCP packets)
Table 1 Flow (UDP packets)
Table 1 Flow
Table 0 Flow
(All packets with same
IPv4 SA and DA)
Table 2
Flows

Group tables

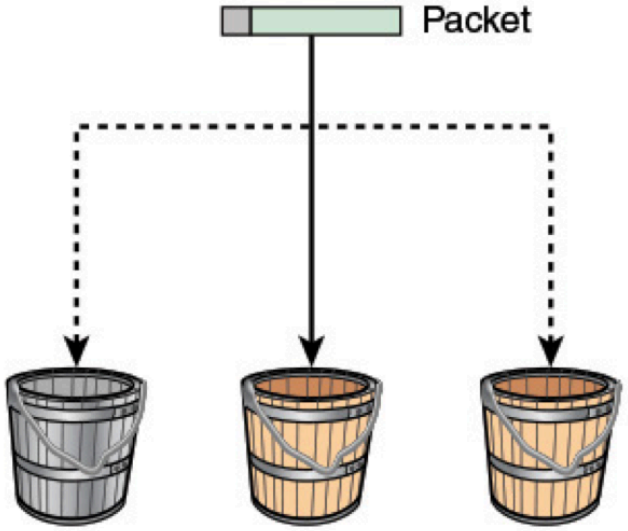


(a) Type = all



Random selection

(b) Type = select

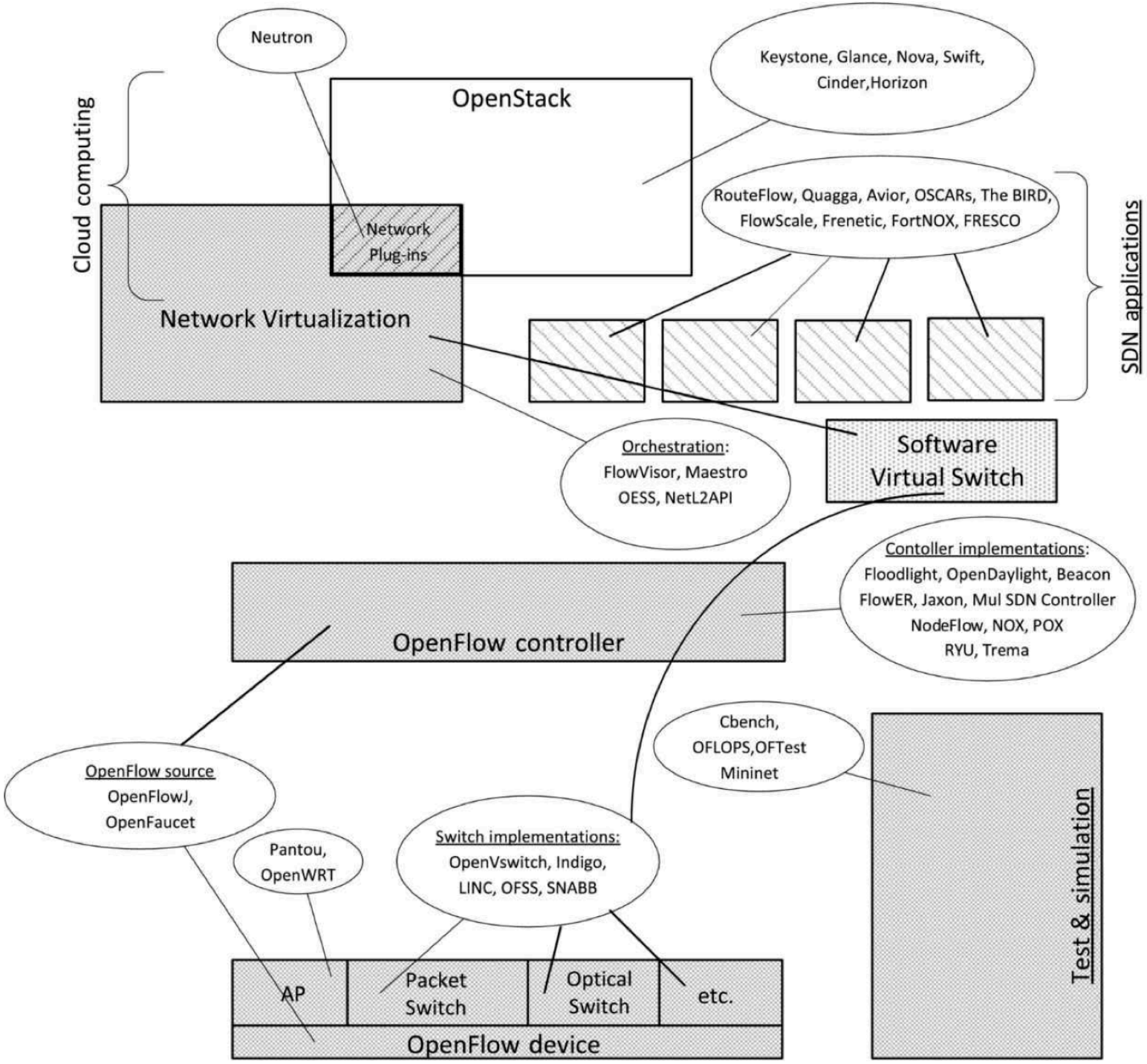


First live bucket

(c) Type = fast failover

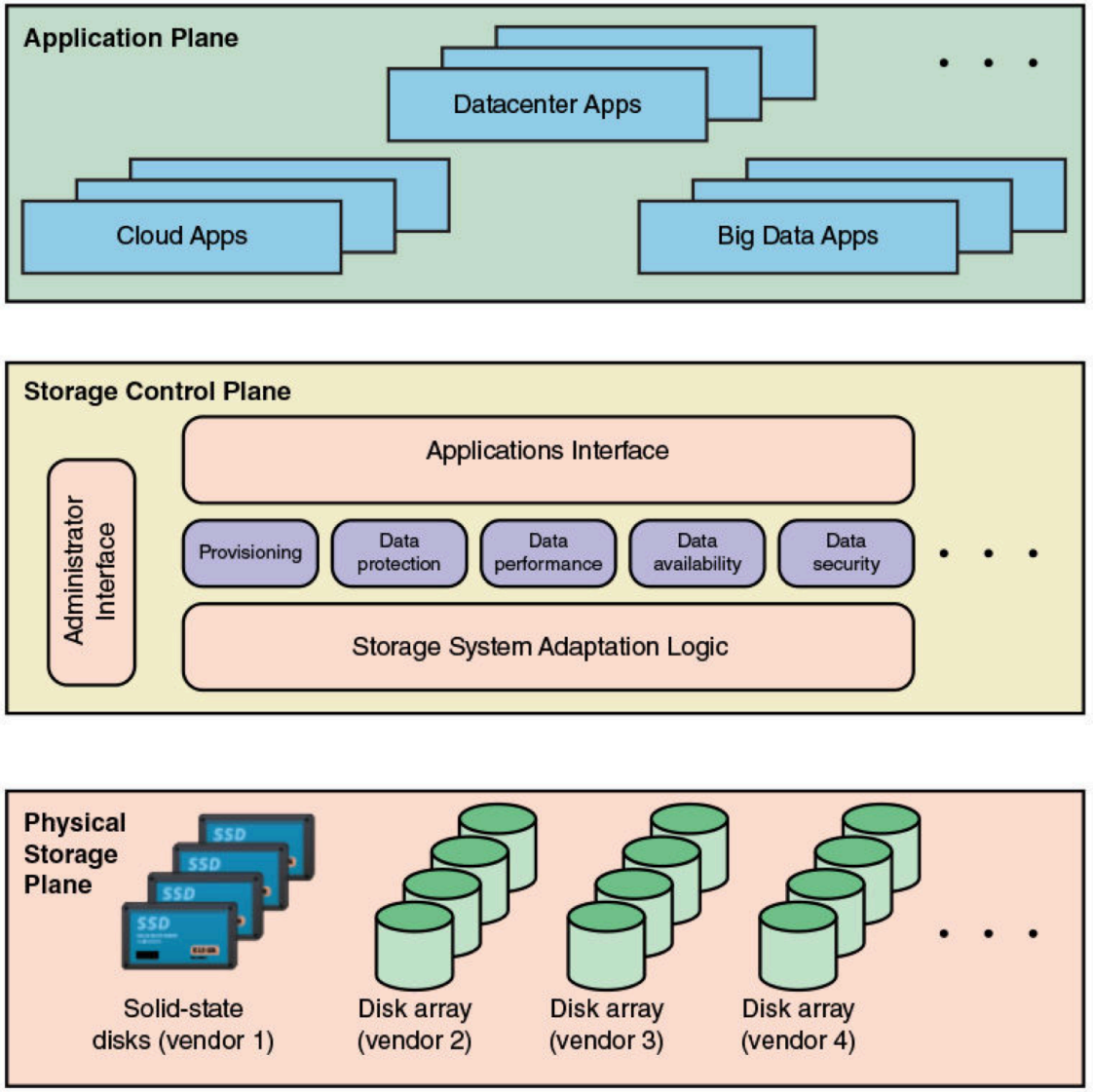
(d) Type = indirect

Open Standards

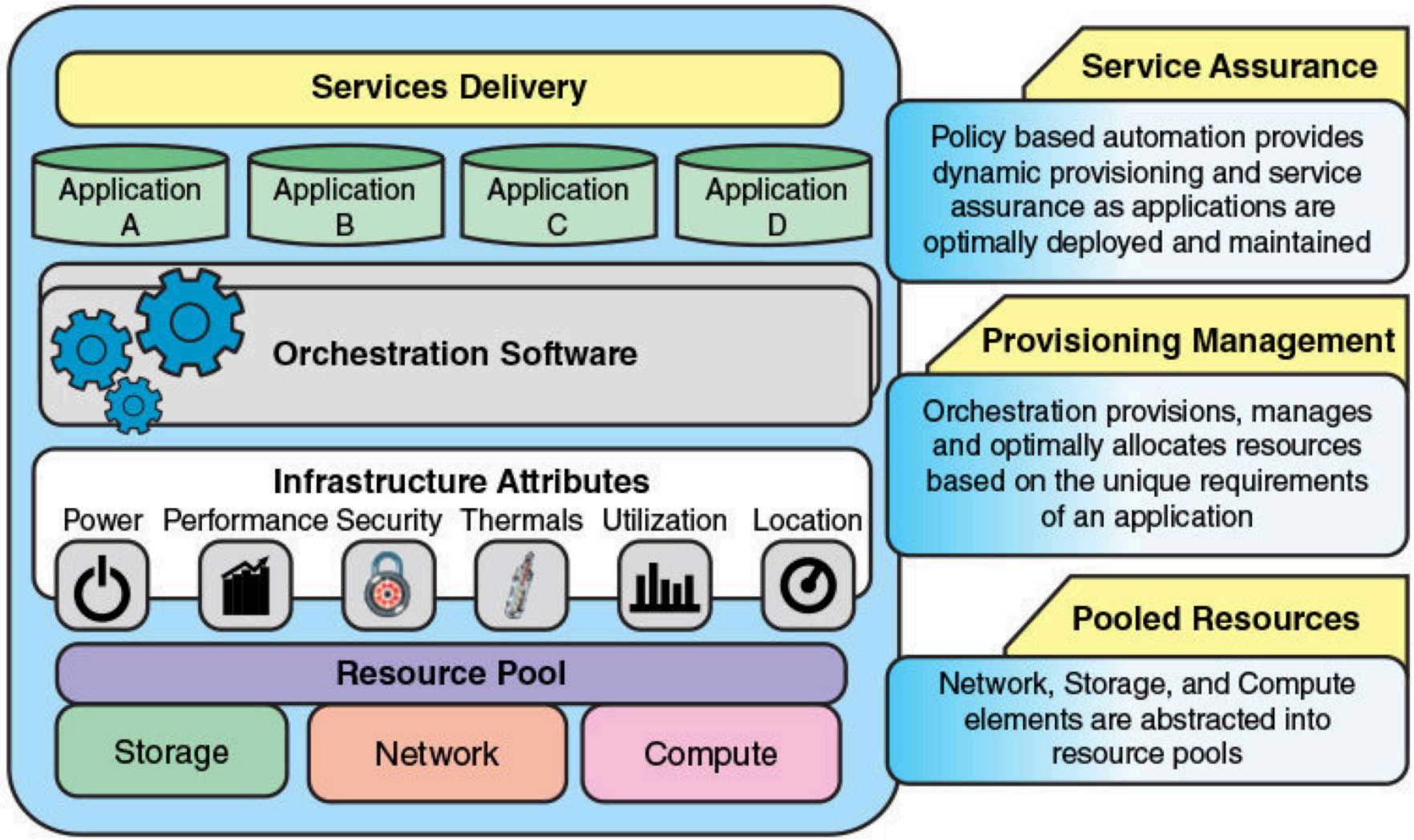


	POX	Ryu	Trema	FloodLight	OpenDaylight
Interfaces	SB (OpenFlow)	SB (OpenFlow) +SB Management (OVSDB JSON)	SB (OpenFlow)	SB (OpenFlow) NB (Java & REST)	SB (OpenFlow & Others SB Protocols) NB (REST & Java RPC)
Virtualization	Mininet & Open vSwitch	Mininet & Open vSwitch	Built-in Emulation Virtual Tool	Mininet & Open vSwitch	Mininet & Open vSwitch
GUI	Yes	Yes (Initial Phase)	No	Web UI (Using REST)	Yes
REST API	No	Yes (For SB Interface only)	No	Yes	Yes
Productivity	Medium	Medium	High	Medium	Medium
Open Source	Yes	Yes	Yes	Yes	Yes
Documentation	Poor	Medium	Medium	Good	Medium
Language Support	Python	Python-Specific + Message Passing Reference	C/Ruby	Java + Any language that uses REST	Java
Modularity	Medium	Medium	Medium	High	High
Platform Support	Linux, Mac OS, and Windows	Most Supported on Linux	Linux Only	Linux, Mac & Windows	Linux
TLS Support	Yes	Yes	Yes	Yes	Yes
Age	1 year	1 year	2 years	2 years	2 Month
OpenFlow Support	OF v1.0	OF v1.0 v2.0 v3.0 & Nicira Extensions	OF v1.0	OF v1.0	OF v1.0
OpenStack Networking (Quantum)	NO	Strong	Weak	Medium	Medium

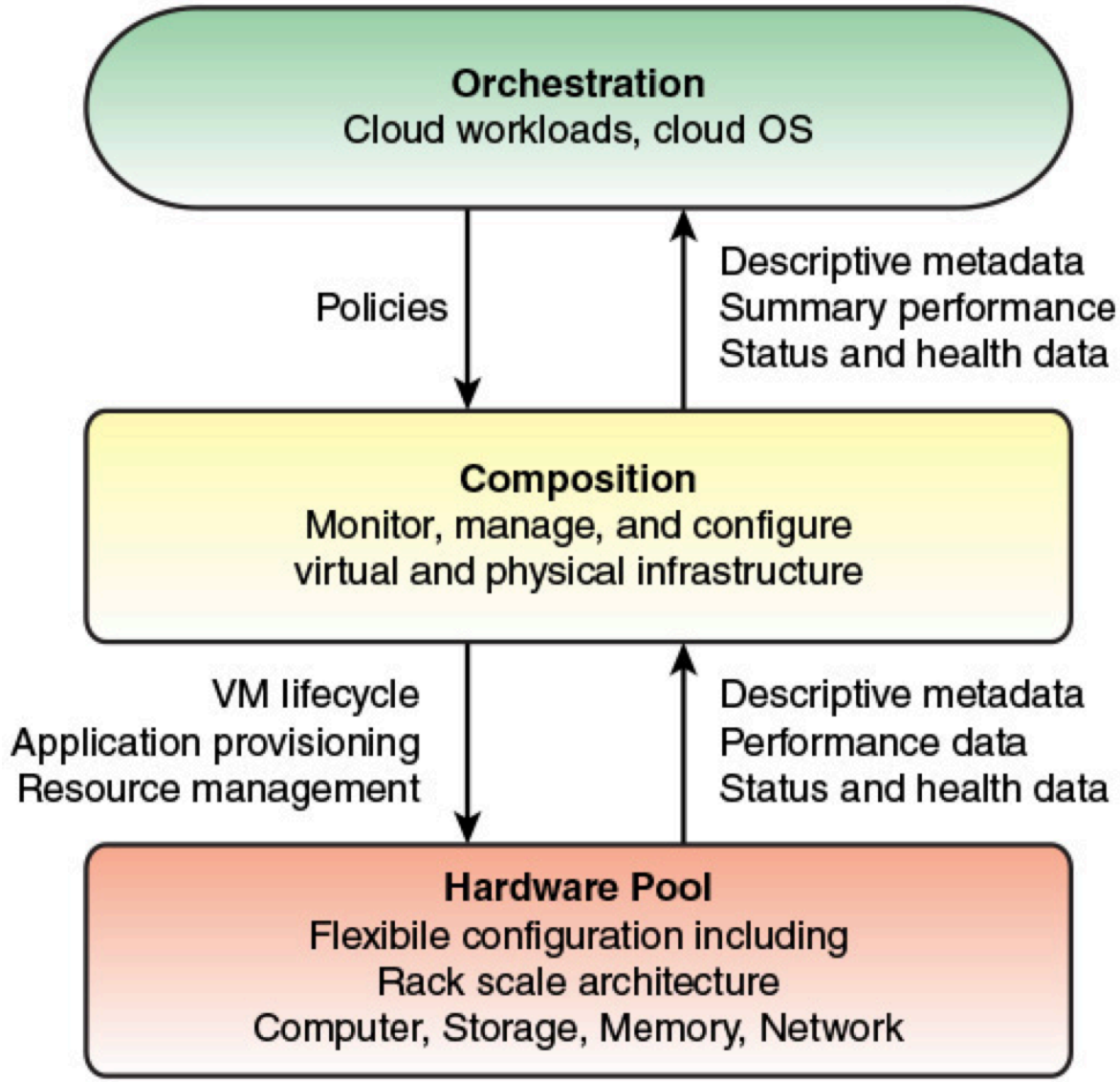
Not only network can be software-defined…



Software-defined infrastructure



Software-defined infrastructure



Network Function Virtualization