Chapter 30-31

Network Management and Software Defined Networks

Terminology

- Network manager or network administrator is a person responsible for network
  - Planning
  - Installation
  - Operation
  - Monitoring
- Network refers to intranet
  - Owned and operated by a single organization
  - Contains many managed items such as routers, switches, servers, printers and hosts
  - May span multiple sites

An interesting problem

- Many protocol mechanisms have been created to overcome network problems automatically
  - Forward error correction
  - Retransmission
  - Routing protocols
- Consequence: protocols may hide problems from a manager!

The industry standard model

- Derived from ITU recommendation M.3400
- Known by abbreviation, FCAPS
- Acronym refers to five aspects of management

Abbreviation	Meaning
F	Fault detection and correction
C	Configuration and operation
A	Accounting and billing
P	Performance assessment and optimization
S	Security assurance and protection

Fault Isolation and Root-Cause Analysis

- Users report high-level symptoms
  - Example: I lost access to a shared file system
- Manager must relate symptoms to underlying cause
  - Cable cut
  - Power supply has failed or disk has crashed
  - Software configuration changed (e.g., file system renamed or moved)
  - Security changed (e.g., password expired)

Network Element

- Generic term for a managed entity
  - Physical device, or
  - Service (e.g., DNS)
- Examples

Manageable Network Elements	
Layer 2 Switch	IP router
VLAN Switch	Firewall
Wireless Access Point	Digital Circuit (CSU/DSU)
Head-End DSL Modem	DSLAM
DHCP Server	DNS Server
Web Server	Load Balancer

Element Management System

- Management tool that can manage one element at a time
- Typically, supplied by vendor of the network element
- Limitation of element management systems, examples:
  - When configuring MPLS tunnel across multiple routers, element management system only allows manager to configure one router at a time
  - If routers sold by multiple vendors, each vendor may have its own element management system
- Unfortunately, many networks only have element management

Types of Network Management Tools

- Physical Layer Testing
- Reachability And Connectivity
- Packet Analysis
- Network Discovery
- Device Interrogation
- Event Monitoring
- Performance Monitoring
- Flow Analysis
- Routing And Traffic Engineering
- Configuration
- Security Enforcement
- Network Planning

How should Management Systems operate?

- Some possibilities
  - Use a parallel physical network
  - Use a parallel logical network
  - Use a special link-layer protocol
  - Use the same links, equipment, and protocols as data
- Surprise: modern network management often follows the last approach

Simple Network Management Protocol (SNMP)

- Internet standard
- Allows software in a manager's computer (manager) to interact with software that runs in an element (agent)
- Specifies format and meaning of messages exchanged
- Runs as an application protocol over TCP or UDP
- Uses fetch-store paradigm

SNMP fetch-store paradigm

- Set of conceptual variables defined
- Each variable given a name
- Set of variables known as Management Information Base (MIB)
- SNMP offers two basic operations
  - GET to read the value of a variable
  - PUT to store a value into a variable
- All management functions are defined as side-effects of GET or PUT to a MIB variable
- Example: reboot defined as side-effect of PUT

SNMP encoding

- SNMP uses a standard known as Abstract Syntax Notation.1 (ASN.1)
- Variable-length encoding
- Example: integer encoded as length and value

Decimal Integer	Hexadecimal Equivalent	Length Byte	Bytes Of Value (in hex)
27	1B	01	1B
792	318	02	03 18
24,567	5FF7	02	5F F7
190,345	2E789	03	02 E7 89

MIB variable names

- Are hierarchical
- Begin with standard prefix
- Identify a specific protocol and variable
- Example: counter for IP packets received has name

  iso.org.dod.internet.mgmt.mib.ip.ipInReceives

- Name is encoded as integers:

  1.3.6.1.2.1.4.3

Arrays in a MIB

- ASN.1 does not define an array type
- Many MIB variables correspond to conceptual array
  - Routing table
  - ARP cache
  - Set of network interfaces
- Trick
  - The “index” is appended onto variable name
  - Manager software uses GET-NEXT operation to move through array

Example of indexing

- **IP routing table assigned variable name**

  standard-prefix.ip.ipRoutingTable

- **Each field has a name**
- **Issuing GET_NEXT operation gets first routing table entry**
- **For example, name of destination address field variable is**

  standard-prefix.ip.ipRoutingTable.ipRouteEntry.field.IPdestaddr

A plethora of MIBs

- Initially
  - One MIB
  - Defined variables for IP, TCP, UDP, ICMP
- Now
  - Many MIBs
  - Variables for routers, switches, modems, printers, hosts, and other network elements
  - Each vendor define a MIB for its devices

Summary

- Network management is complex and difficult
- Current tools are fairly primitive
- Life goes on anyway

Chapter 31

Software Defined Networking (SDN)

What is Software Defined Networking?

- One of the hottest topics in networking
- According to marketing, SDN is:
  - A way to eliminate all human error in Network Management
  - A technology that improves overall routing
  - An approach that eliminates 60% to 80% of operational costs
- In reality SDN is:
  - A technology that gives programmers more control over network equipment
  - An approach with the potential to make some improvements in network configuration and management

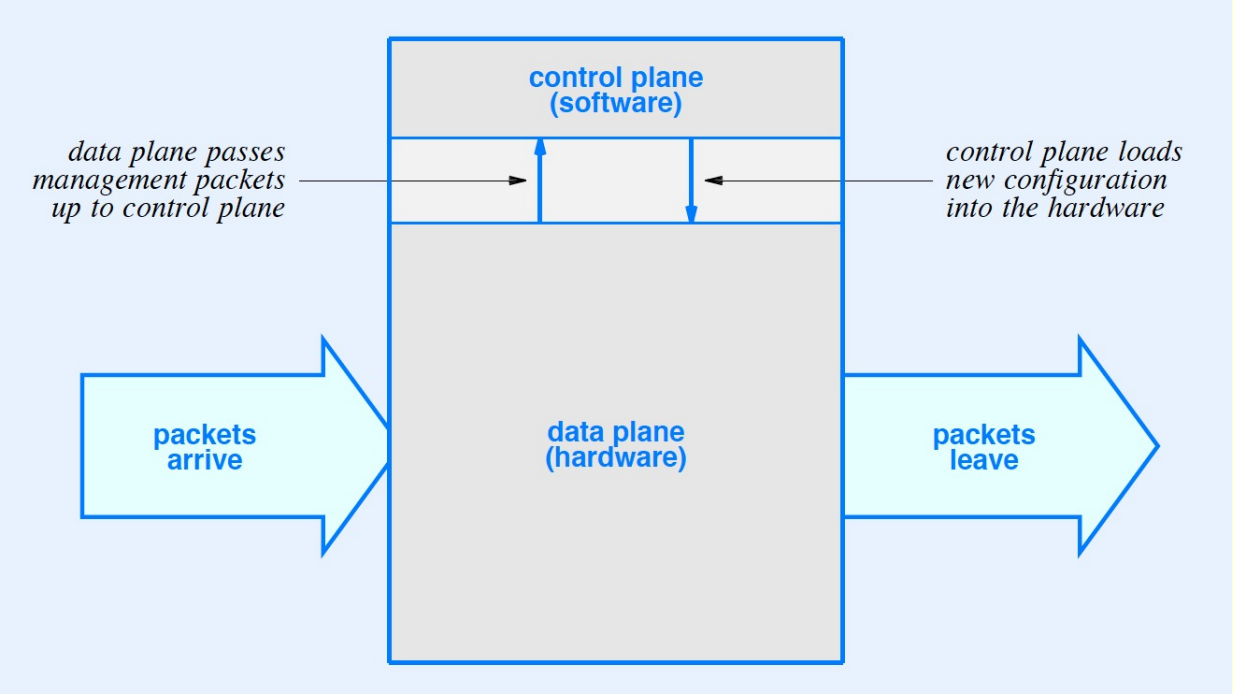
Motivation for SDN

- Switch from element management to network management
- Move from proprietary to open standards
- Automate and unify network-wide configuration
- Change from per-layer to cross-layer control
- Accommodate virtualization used in data centres

Background and Definitions

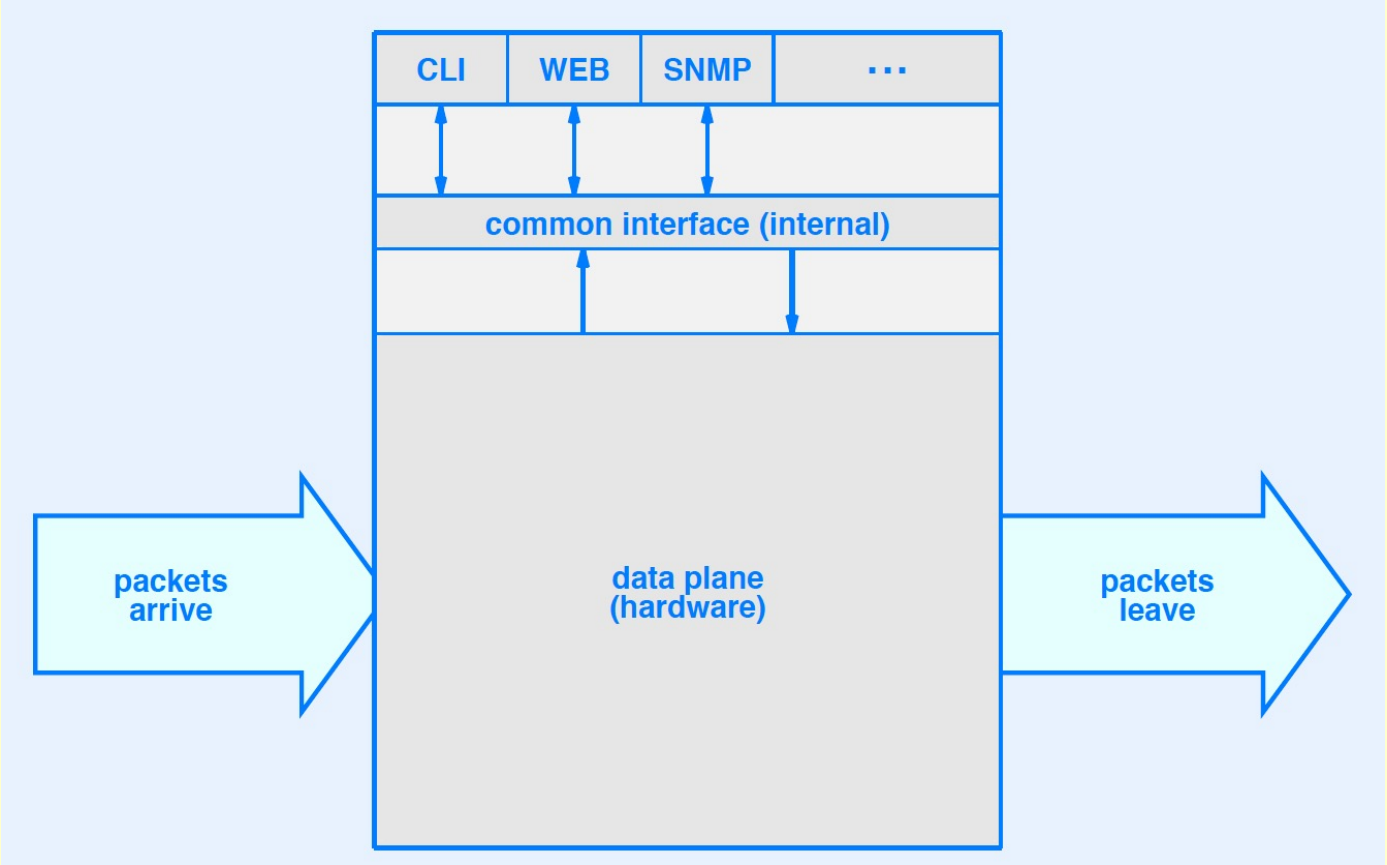
- Terminology adopted from network equipment engineers
- Data plane
  - Refers to packet processing mechanisms
  - Typical functions include packet classification and packet forwarding
  - Operates at wire speed
- Control plane
  - Refers to management
  - Typical functions include interacting with network manager and modifying forwarding tables
  - Operates slowly and only when changes are needed

Conceptual Organization Of Network Devices



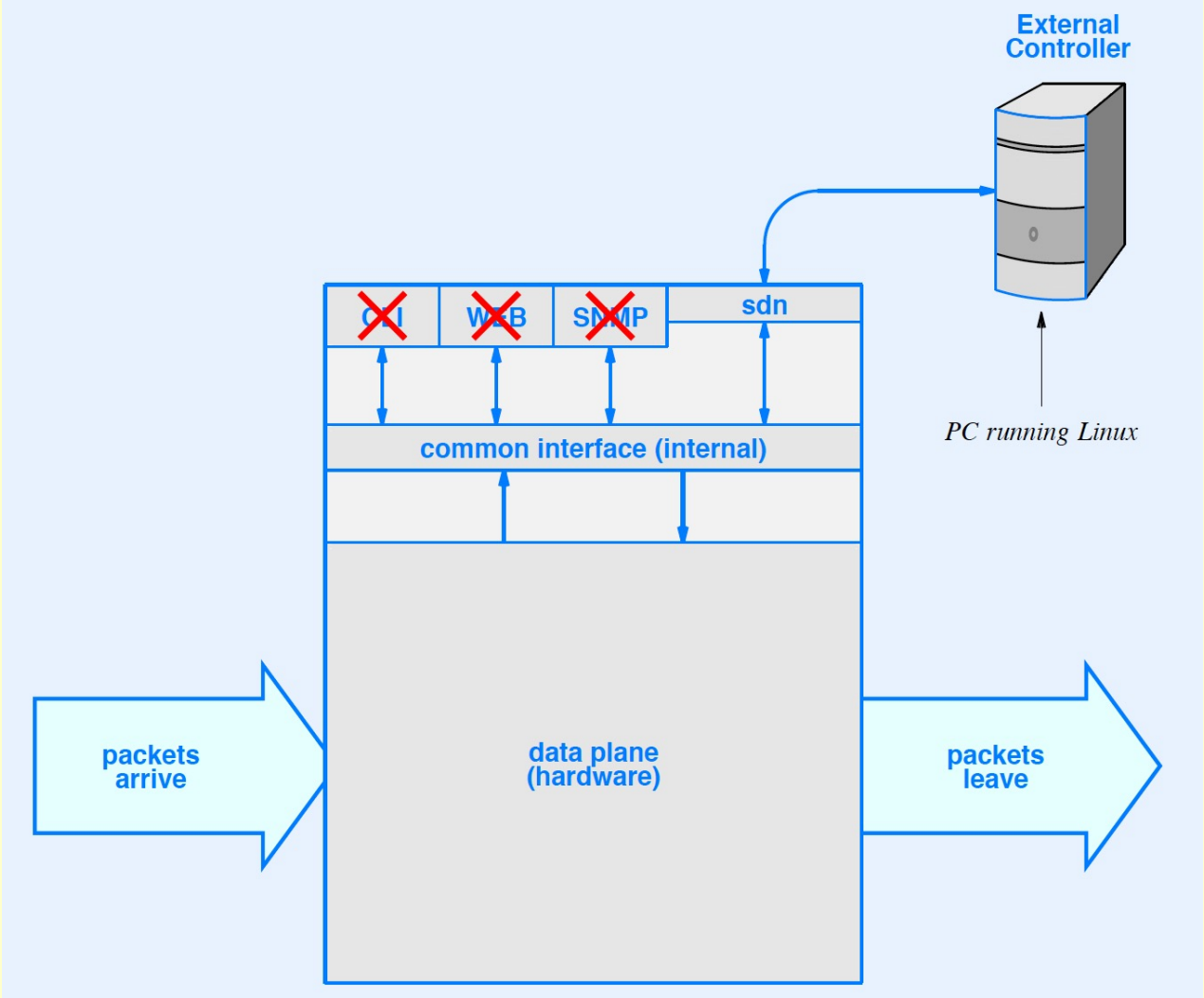
- Data plane may use ASIC hardware for speed
- Control plane includes a TCP/IP stack

Control Plane Interface Modules

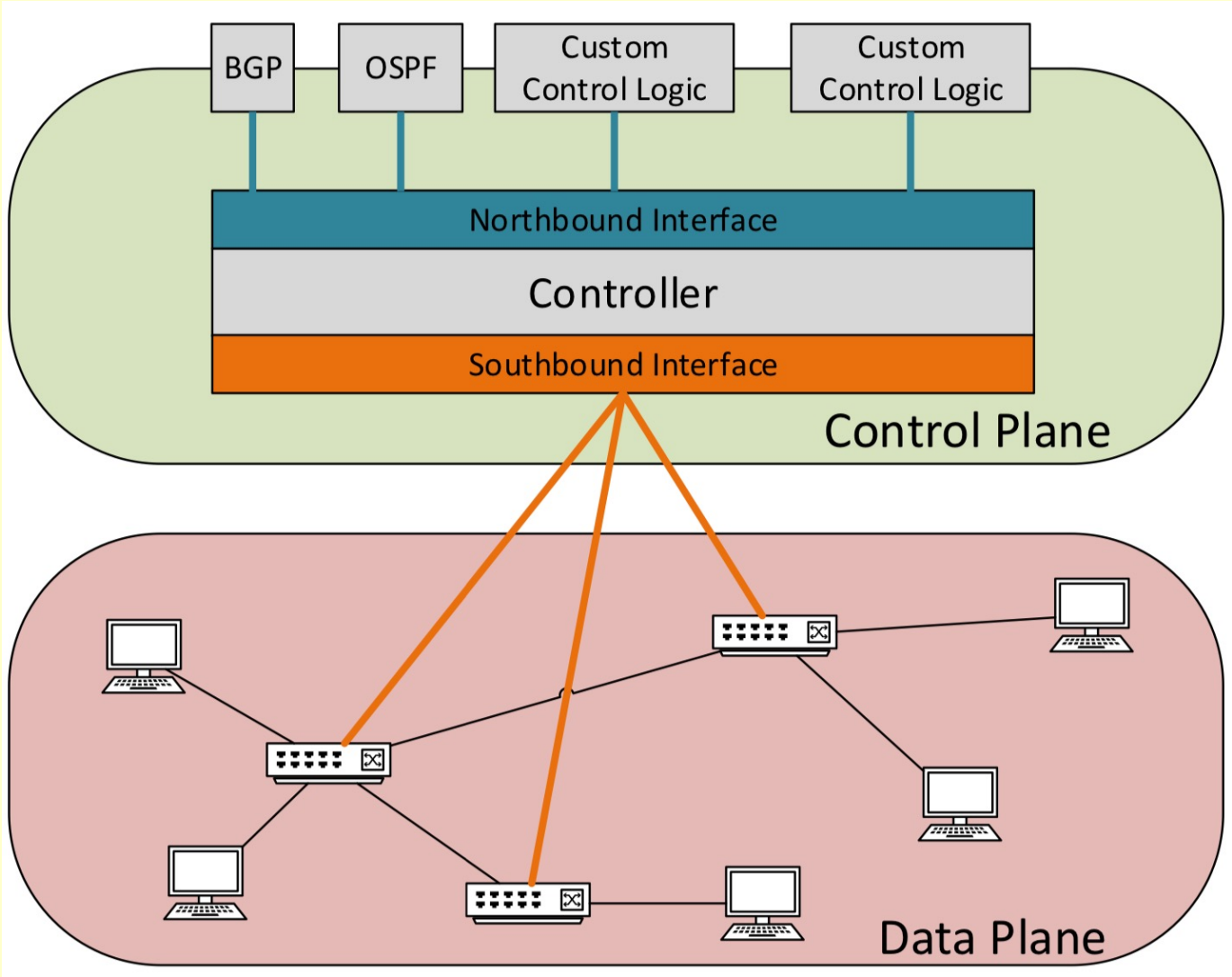


- Managers can choose among command line interface, web interface and SNMP

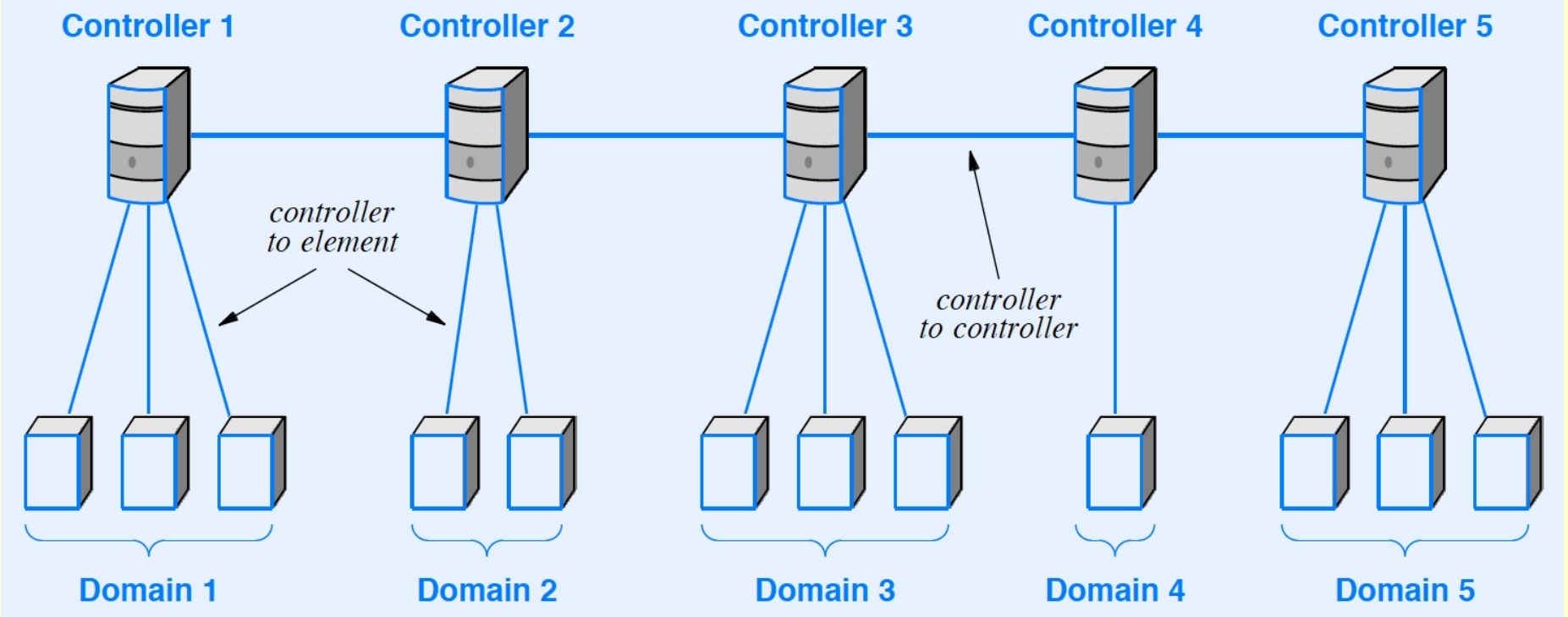
The SDN approach: an external controller



Architecture of a Software Defined Network



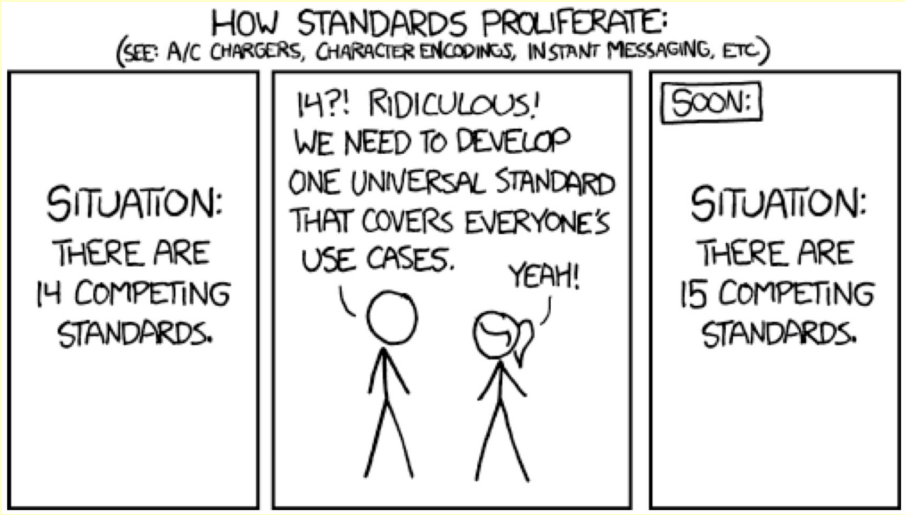
In practice



- Each controller can operate multiple devices
- Controllers coordinate to provide consistent configuration

SDN Communication

- Two conceptually separate types
  - Controller to network element
  - Controller to controller (in this area there is no standard developed yet, each manufacturer provide different tools. There also exist some open source tools)
- Protocols used can differ



OpenFlow

- Specification for controller-to-element communication
- Devised at Stanford
- Now a de facto industry standard for SDN
- Defines
  - Secure communication (over TLS)
  - Message format
  - Items to be managed
- Completely unlike SNMP

OpenFlow Model

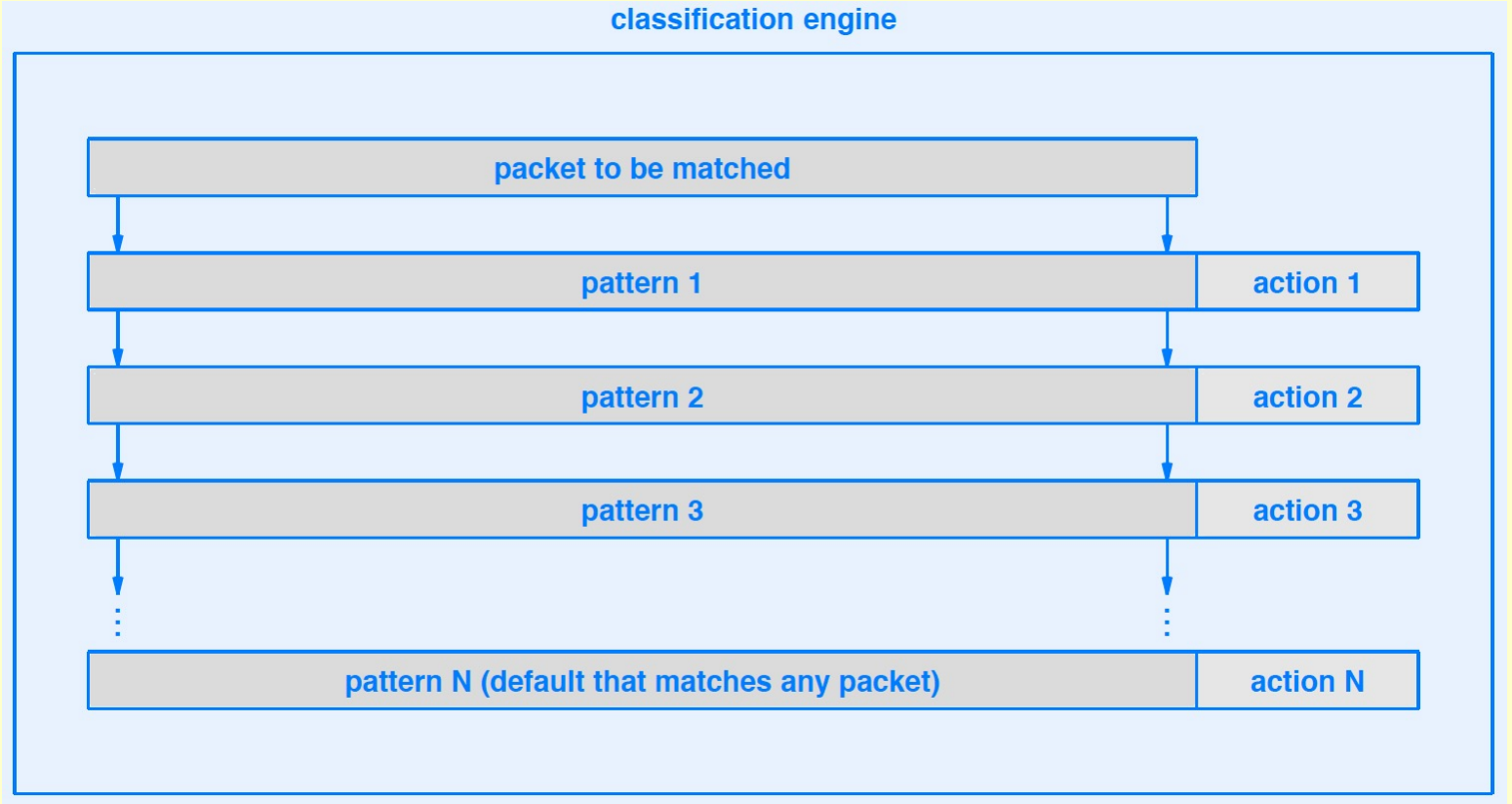
- Uses flow table abstraction
  - Data plane is assumed to have a sequence of flow tables
  - Each flow table specifies how to parse packets and handle them
- OpenFlow allows manager to set values in each flow table
- Important note: flow table model closely matches classification hardware found in Ethernet switches

Classification

- Alternative to packet demultiplexing
- Examines headers from multiple layers at the same time
- Uses an array of pairs

  (pattern, action)
- Where
  - Pattern is a pattern that is matched against packets
  - Action specifies steps to be taken if the match succeeds. Possible actions are for example to drop the packet, forward it through one or multiple ports and/or modify the packet headers

Classification Hardware



- Hardware checks all patterns in parallel
- Result is extremely high speed classification

TCAM

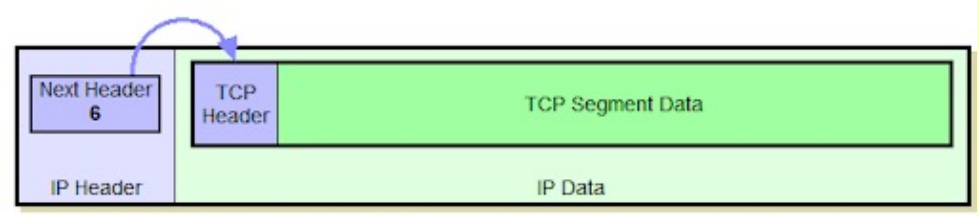
- Acronym for Ternary Content Addressable Memory (a special type of associative memory)
- Hardware technology used for high-speed classification
- Pattern is ternary because value for each bit can be 0, 1, or x = “don’t care”
- TCAM matches all patterns at once, and performs the action on the first matching table entry
- A typically SDN switch have a couple of thousand TCAM registers.

Example of IPv4 classification

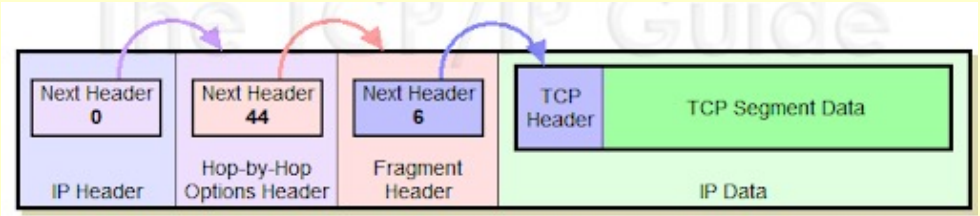
- The challenge
  - An ethernet frame arrives
  - What is the minimum number of steps needed to determine whether the frame carries an IPv4 datagram destined for a web server?
- The answer
  - Check whether the frame type field specifies IPv4 (0x0800)
  - Check whether the IP protocol field specifies TCP (6)
  - Check whether the TCP destination port specifies a web server (80)

IPv6 classification

- Simplest case (only a base header)
  - Frame type field specifies IPv6 (0x86DD)
  - Next Header field specifies TCP (6)
  - TCP destination port specifies a web server (80)
- Additional patterns needed for extension headers (fig. below)
- Example: base header plus two extension headers
  - Frame type field specifies IPv6 (0x86DD)
  - Three steps of Next Header eventually points to TCP (6)
  - TCP destination port specifies a web server (80)



IPv6 Datagram With No Extension Headers Carrying TCP Segment



IPv6 Datagram With Two Extension Headers Carrying TCP Segment

Example items in an OpenFlow pattern

Field	Meaning
Layer 2 fields	
Ingress Port	Switch port over which the packet arrived
Metadata	64-bit field of metadata used in the pipeline
Ether src	48-bit Ethernet source address
Ether dst	48-bit Ethernet destination address
Ether Type	16-bit Ethernet type field
VLAN id	12-bit VLAN tag in the packet
VLAN priority	3-bit VLAN priority number
ARP opcode	8-bit ARP opcode
Layer 3 fields	
MPLS label	20-bit MPLS label
MPLS class	3-bit MPLS traffic class
IPv4 src	32-bit IPv4 source address
IPv4 dst	32-bit IPv4 destination address
IPv6 src	128-bit IPv6 source address
IPv6 dst	128-bit IPv6 destination address
IPv4 Proto	8-bit IPv4 protocol field
IPv6 Next Header	8-bit IPv6 next header field
TOS	8-bit IPv4 or IPv6 Type of Service bits

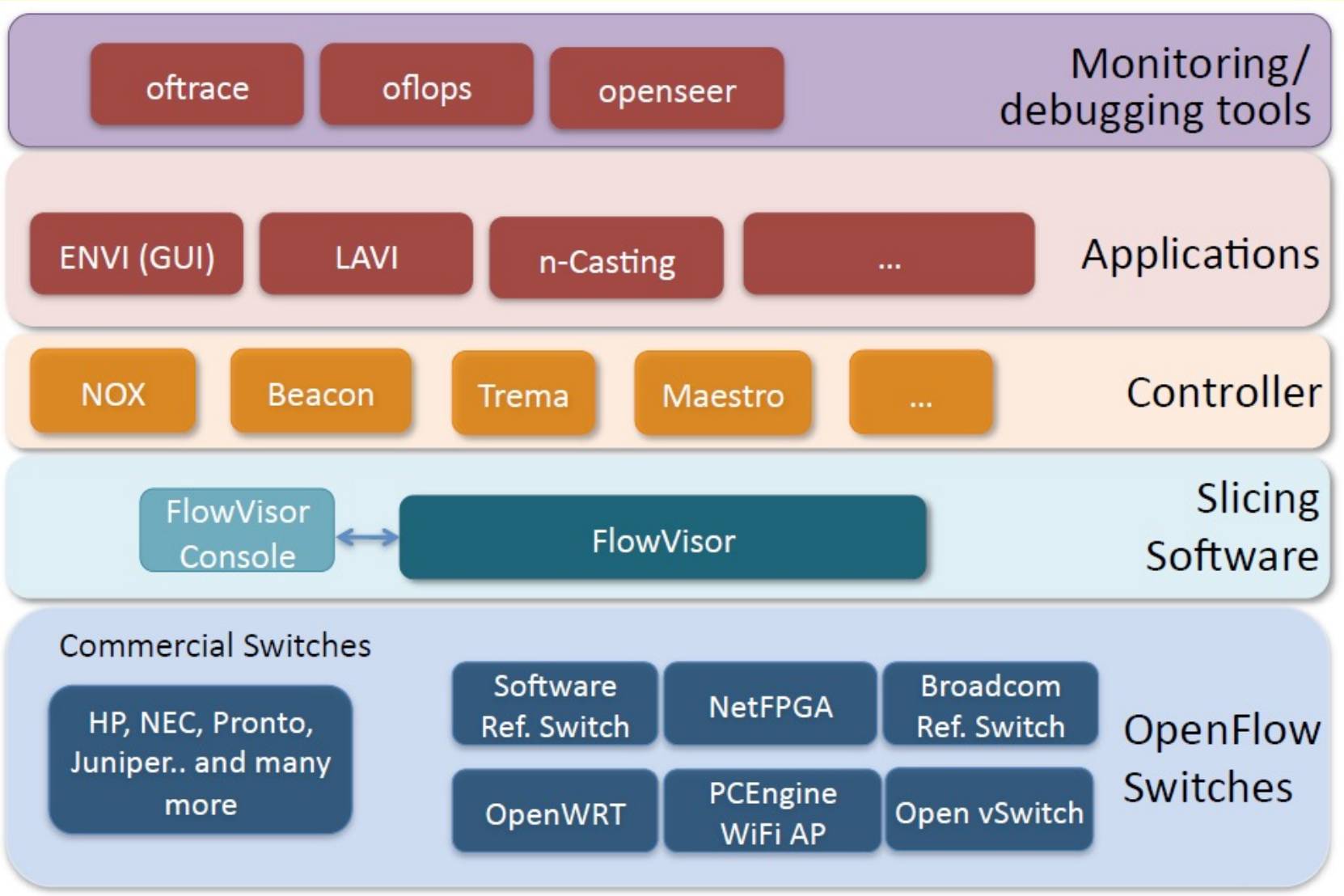
Example items in an OpenFlow pattern (continued)

Field	Meaning
Layer 4 fields	
TCP/UDP/SCTP src	16-bit TCP/UDP/SCTP source port
TCP/UDP/SCTP dst	16-bit TCP/UDP/SCTP destination port
ICMP type	8-bit ICMP type field
ICMP code	8-bit ICMP code field

Examples of SDN functionality

- End-to-end layer 2 paths
- Forwarding based on source as well as destination
- All traffic from a specific MAC address sent along a specific path
- Segregation of traffic based on application type
- Multipath forwarding based on hash of 4-tuple (IP sender/destination and port sender/destination)
- Transport of nonstandard layer 3 protocols

The SDN stack



Examples of OpenFlow Hardware

Juniper MX-series

NEC IP8800

WiMax (NEC)

HP Procurve 5400

Netgear 7324

PC Engines

Pronto 3240/3290

Ciena Coredirector

Examples of Open Controllers

Name	Lang	Platform(s)	License	Original Author	Notes
OpenFlow Reference	C	Linux	OpenFlow License	Stanford/ Nicira	not designed for extensibility
NOX	Python, C++	Linux	GPL	Nicira	actively developed
Beacon	Java	Win, Mac, Linux, Android	GPL (core), FOSS Licenses for your code	David Erickson (Stanford)	runtime modular, web UI framework, regression test framework
Maestro	Java	Win, Mac, Linux	LGPL	Zheng Cai (Rice)	
Trema	Ruby, C	Linux	GPL	NEC	includes emulator, regression test framework
RouteFlow	?	Linux	Apache	CPqD (Brazil)	virtual IP routing as a service

Comparing SDN and MPLS

- Benefits of SDN routing
  - Cost reduction
  - Overhead reduction
  - Physical vs. Virtual Networking Management
  - Reduced downtime
  - Central Networking Management Tool
  - Centralized Control

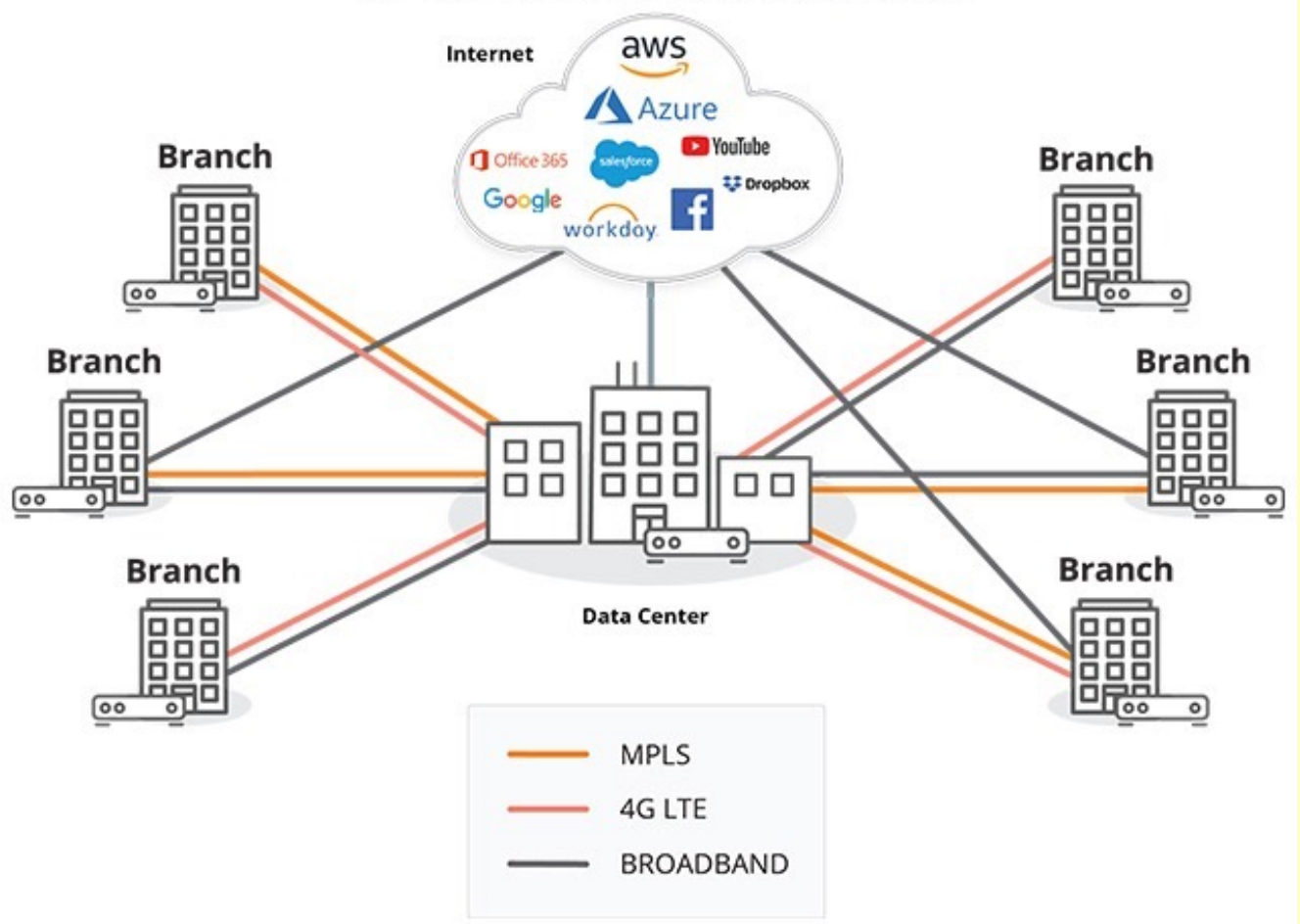
Comparing SDN and MPLS

- Advantages of MPLS over SDN:
  - One Carrier circuit can support MPLS, Internet and SIP
  - Domestic MPLS takes 30 days typically to install.
  - Carriers provide next-gen firewall
  - Carrier Managed Solutions such as Firewall, VOIP, etc.
  - MPLS port pricing is practically the same as Internet port pricing
  - MPLS supports many transport types including Ethernet, Broadband, DSL

Software-defined networking in a wide area network (SD-WAN)

- The main goal of SD-WAN (SDWAN) technology is to deliver a business-class, secure, and simple cloud-enabled WAN connection with as much open and software-based technology as possible. This can be used to deliver basic WAN connectivity, or it can be used for premium business services such as VPN, WAN optimization, and applications delivery control (ADC).
- It can replace traditional a WAN or an MPLS solution.
- It does not use the same technology as SDN, but share the idea of virtualization and flows.

SD-WAN Architecture



Source: https://www.arubanetworks.com/faq/what-is-sd-wan/