SDN (Software Defined Networking)

Network programmability refers to the trend toward software-defined networking (SDN).

SDN decouples the data, control, and management planes from the physical device, virtualizes them, and defines the networking functions in software.

The control plane is centralized through SDN

This creates an architecture that can be more efficiently and effectively managed through programmatic control.

Data, Control, and Management Planes

- Data (Forwarding) Plane; Traffic which is forwarded through the device
- Control Plane; makes decisions about how to forward traffic. Control plan packets such as routing protocols or STP updates are destined to or locally originated on the device itself
- Management Plane; The device is configured and monitored in the management plane. For Example, at the CLI through Telnet or SSH, via a GUI using HTTPS or via SNMP or an API (Application Programming Interface)

Data and Control Plane Separation

- Network infrastructure devices are responsible for their own individual control and data planes in a traditional environment.
- Software Defined Networking decouples the data and control planes.
- The network infrastructure devices are still responsible for forwarding traffic, but the control plane moves to a centralized SDN controller.
- Rules for packet handling are sent to the network infrastructure devices from the controller.
- The network infrastructure devices query the controller for guidance as needed, and provide it with information about traffic they are handling.

Data Plane

A traditional networking device contains two planes. The data plane is responsible for forwarding data as quickly as possible. To do so, it relies on tables built by the control plane. Actions taken by the data plane include the following:

- L2 and L3 encapsulation and de-encapsulation
- Addition or removal of an 802.1Q trunking header
- MAC address table lookups
- IP routing table lookups
- Data encryption and addition of a new IP header (as in VPNs)
- Change to the source or destination IP address (with NAT)
- Message discard due to a filter (such as an ACL or port security)

control plane

does all the calculations for populating tables used by the data plane and manages control messages between other networking devices.

Figure 3-6 Control and Data Plane Example

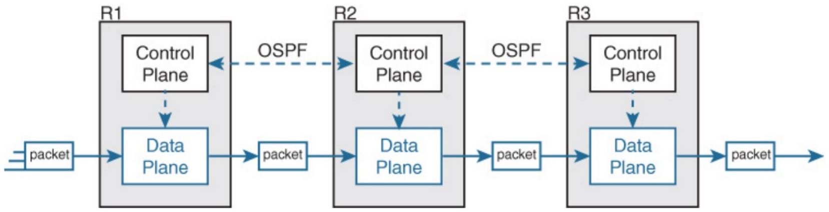


Figure 3-6 provides an example of OSPF operating on the control plane while the data plane is responsible for forwarding packets using the best route.

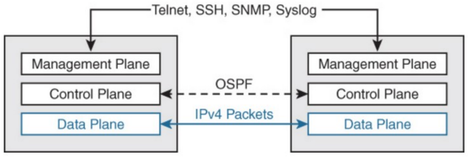
The following are the most common control plane protocols:

- Routing protocols (OSPF, EIGRP, RIP, BGP)
- IPv4 ARP
- IPv6 NDP
- Switch MAC learning
- STP

Management Plane

The management plane is responsible for all functions that are not directly related to controlling the data plane.

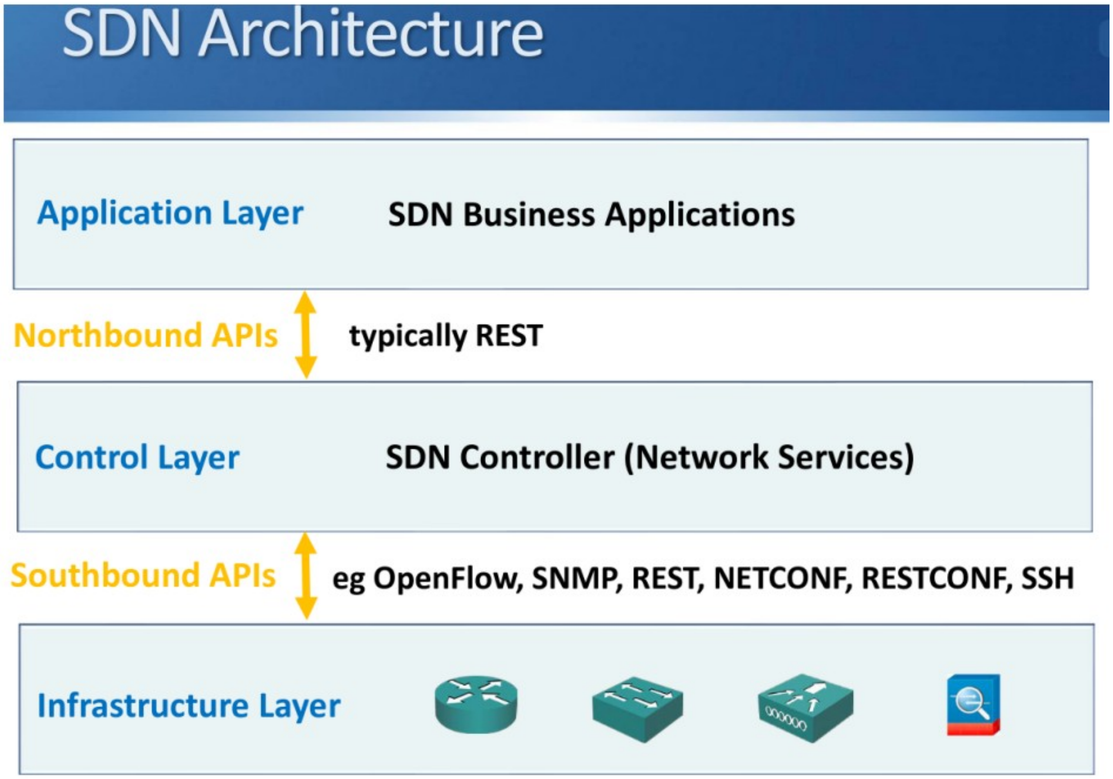
Figure 3-7 Management Plane Example



Management protocols, such as the ones in Figure 3-7, are examples of management plane functions.

Pure vs Hybrid SDN

- With a pure SDN – the control plan runs purely on an SDN controller, and the data plane runs purely on the network devices
- Hybrid SDN – the majority of the control plane intelligence is provided by an SDN controller, but network devices retain some control plan intelligence, along with their data plane operations
- Most implementations use a hybrid SDN



SDN Architecture

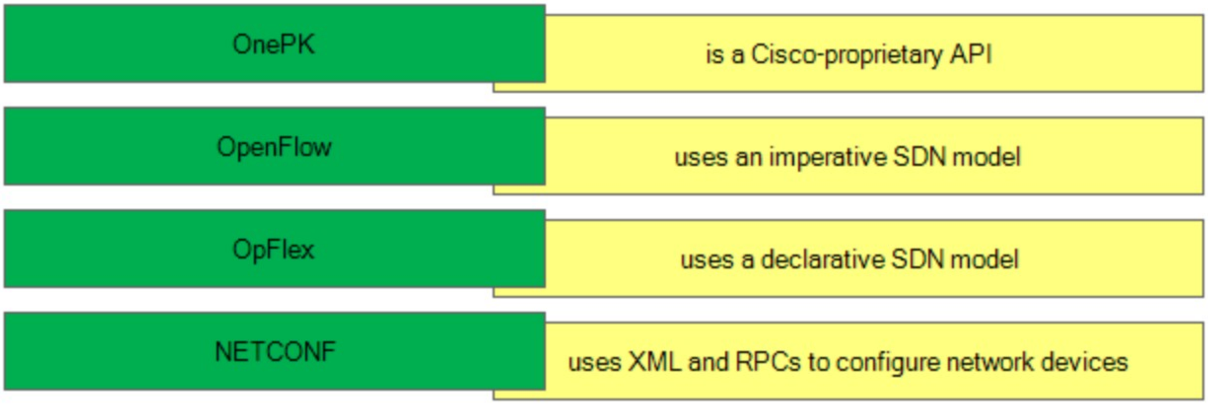
Application Layer — SDN Business Applications

Northbound APIs — typically REST

Control Layer — SDN Controller (Network Services)

Southbound APIs — eg OpenFlow, SNMP, REST, NETCONF, RESTCONF, SSH

Infrastructure Layer



OnePK	is a Cisco-proprietary API
OpenFlow	uses an imperative SDN model
OpFlex	uses a declarative SDN model
NETCONF	uses XML and RPCs to configure network devices

Controllers

Traditional Networking

- the control plane has been part of the device OS and has been distributed across every device.
- every device must spend some resources calculating and maintaining Layer 2 and Layer 3 data structures (ARP tables, routing tables, and so on).
- When viewed as a whole, the network’s control plane is distributed across all the networking devices.

In SDN

- the functions of the control plane can be completely removed from the physical networking devices and placed in a centralized application called a controller.
- This frees up the devices to focus on data plane tasks.
- The controller sits at the top of a network topology diagram, and the connections to the networking devices are called the **southbound interface (SBI)** (see Figure 3-8).

the *southbound interface* (*SBI*) - connections to the networking devices. Heads south/down from the control to networking device (Syslog, SNMP, OpenFlow, REST, NETCONF, RESTCONF, SSH)

northbound interface (NBI) - exists between the SDN controller and the applications that are installed on the controller. These applications are what enable network programmability. (APIs)

SDN Controllers

APIC (Application Policy Infrastructure Controller)

- The main component of the Cisco ACI (Application Centric Infrastructure
- Designed to manage data center environments with Nexus switches

CISCO DNA Center

- Digital Network Architecture Center (DNAC)
- Designed to manage enterprise environments (campus, branch, and WAN)
- Can be thought of as an upgrade to APIC-EM (EM = Enterprise Module)
- Uses intent-based Networking (IBN), uses a software delivered approach to automating and assuring services across your WAN and Campus and Branch Networks

Intent Based Networking (IBN)

- Intent Based Networking transforms a traditional manual network into a controller led network that translates the business needs into policies that can be automated and applied consistently across the network.
- The goal is to continuously monitor and adjust network performance to help assure desired business outcomes

3 of the main building blocks of Cisco DNA and Software Defined Architecture are:

- DNA Center
- SD-Access
- SD-WAN

SD-Access Software Defined Access

● SD-Access is a newer method of network access control which solves the limitations

of the traditional implementation

- Traffic flow security is based on user identity, not physical location and IP address
- Users log in from and can move to any physical location in the network
- Two components are required for SD-Access:
- Users are authenticated by the ISE Identity Services Engine
- The security policy (permitted and denied communication between groups) is configured on the DNA Center
  Underlay and Overlay Network
- SD-Access uses an underlay and overlay network
- An underlay network is the underlying physical network. It provides the underlying
- physical connections which the overlay network is built on top of.
- An overlay network is a logical topology used to virtually connect devices. It is built over the physical underlay network.
- The combination of underlay and overlay forms the SD-Access 'network fabric'

SD-WAN (Software Defined WAN)

- Cisco acquired Viptela in 2017 to enhance their SD-WAN solution (previously called
- 'IWAN')
- It provides automated setup of WAN connectivity between sites
- Monitoring and failover is automated
- Traffic flow control is application aware
- SD-WAN Benefits
- Automated, standardized setup of connectivity between sites
- Transport independent
- Simplified, integrated operations
- More flexibility and easier to migrate WAN services
- The required, predictable performance for important applications
- Integration with the latest cloud and network technologies
- Lower cost

Where is the interface between the control plane and data plane within the software-defined architecture?

Control Layer and infrastructure layer

How Do SDN Southbound APIs Work?

Southbound APIs facilitate control over the network and enable the SDN Controller to dynamically make changes according to real-time demands and needs.

OpenFlow, which was developed by the Open Networking Foundation (ONF), is the first and probably most well-known southbound interface.

OpenFlow defines the way the SDN Controller should interact with the forwarding plane to make adjustments to the network, so it can better adapt to changing business requirements. With OpenFlow, entries can be added and removed to the internal flow-table of switches and routers to make the network more responsive to real-time *traffic* demands.

OpenFlex