

SDN Basics

🕒 Created	@November 19, 2022 10:13 AM
☰ Week	Week 1

[SDN Basics](#)

[Evolutie van switches en routers](#)

[Voorlopers SDN en NAC](#)

[Voordelen SDN](#)

[Nadelen SDN](#)

[3 SDN categorieën](#)

[SDN via Overlays](#)

[SDN via Controller](#)

[SDN via APIs](#)

[SDN via Policy-level APIs](#)

[Cisco IOS](#)

SDN Basics

SDN is het scheiden van de control-plane (brein) en de data-plane.

SDN is ook transitie van complexe hard/software naar centrale intelligentie, 'dommere' hardware en nieuwe(re) protocollen

Van software (OS) naar hardware (tabellen in 'ram' geheugen)

Jip en Janneke-taal: Niet meer (alleen) werken vanaf de CLI, maar een controller (server) de configuratie (beslissingen) laten uitvoeren

Traditionele Switch Architectuur (Management, Control en Dataplane in 1 device):

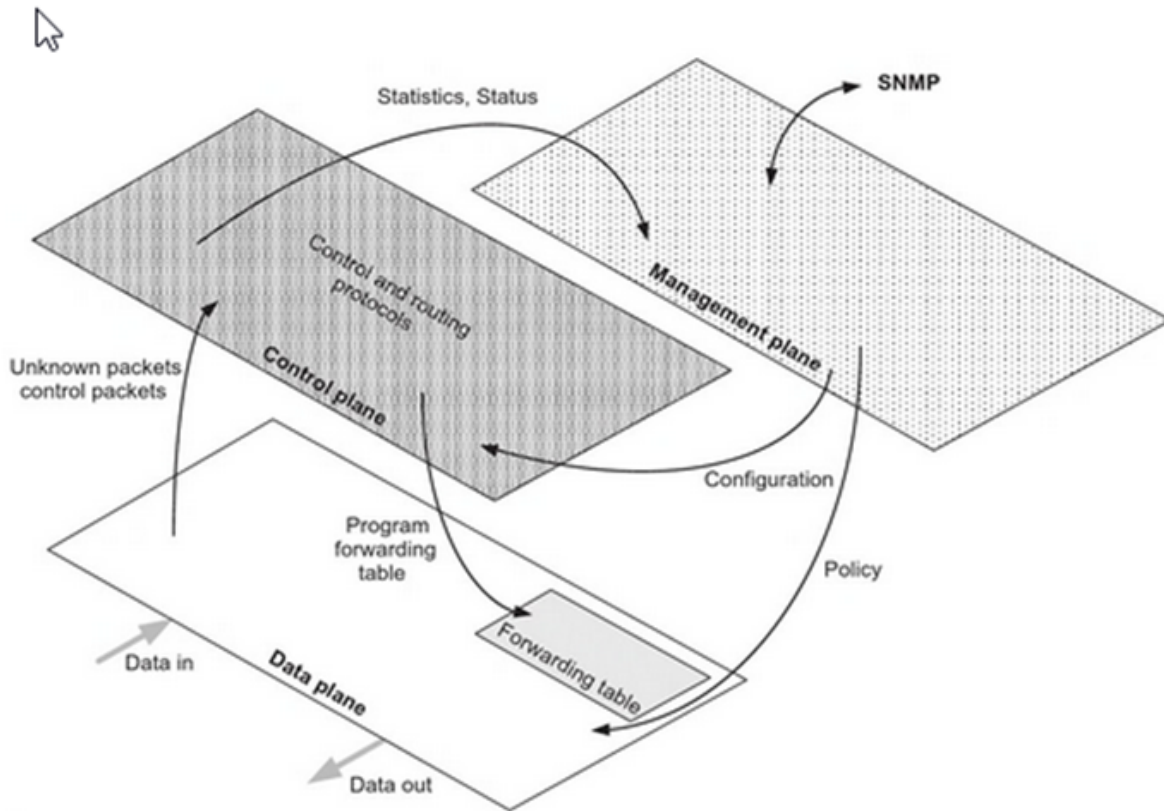
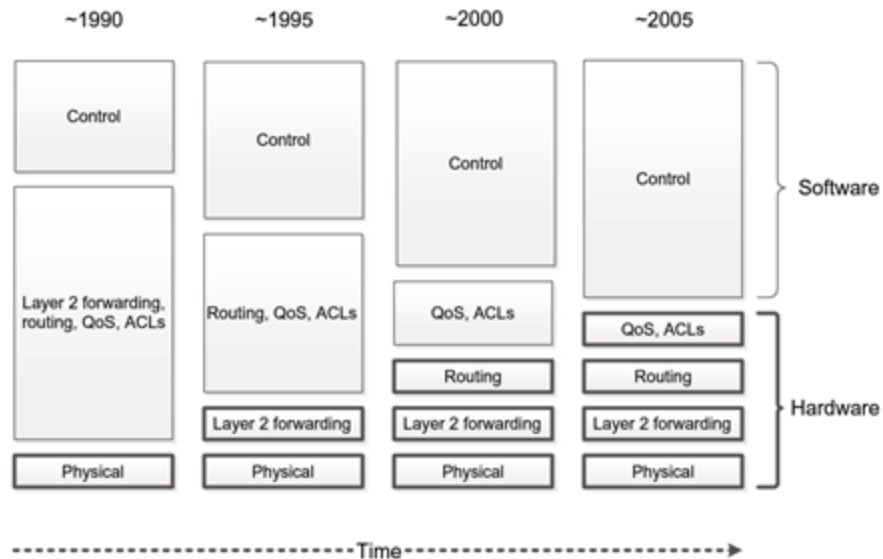


FIG. 1.2

Roles of the control, management, and data planes.

Waarom is er zo weinig verandering in netwerkconfiguratie (geweest)?

- ... “het werkt toch”
- Behoeftte aan automatiseren (nog) niet groot;
- Hegemonie van specifieke vendors bepalen de toekomst;
- Het (nodig) hebben en/of ontbreken van specifieke functionaliteiten:
- Beperking en evolutie van Netwerk Operating System



NFV = Network Function Virtualization = Het automatiseren van virtuele netwerken en technieken

Van traditioneel configureren, monitoren en beheer van fysieke hardware:

- CLI
- SNMP
- Telnet
- SSH

Naar Centraal beheren van configuratie voor virtuele routers, switches

Evolutie van switches en routers

Vendors schrijven/schreven 'basic functions' in software;

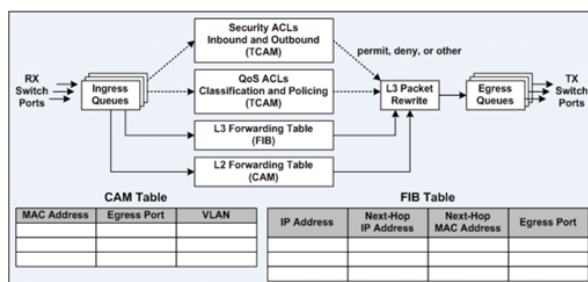
Over tijd zijn basis functies in software vervangen door hardware;

- Veel forwarding en filtering decisions volledig in hardware;
- Besluitvorming via tabellen die via software in hardware schrijft;
 - Doel verbeteren performance/cost ratio;

Hardware Components:

- Application Specific Integrated Circuits (ASICs);
 - Chip voor specifieke, beperkte functie, niet meer te wijzingen.
- Field-Programmable Gate Arrays (FPGAs);
 - Als ASIC, maar softwarematige wel te wijzingen.
 - Duurder dan ASICs ivm productie.
 - FPGA kan prototype voor ASIC worden.
- Ternary Content-Addressable Memories (TCAMs);
- P4 Programming Protocol-independent Packet Processors)

Performance upgrade to 40 Gbps >. (400Gbps)



Veel verschillende tabellen (in hardware) zorgt voor mindere prestaties

Voorlopers SDN en NAC

Devolved Control of ATM Networks (DCAN):

- Scheiden van controle en managementlaag van ATM Switches;

Open Signaling:

- Programmable interface vor ATM switching hardware;
- General Switch Management Protocol (GSMP) 1990;

Network Access Control (NAC);

- Access control op basis van policies;
- Tag Switching (TS) (Cisco); TS + GSMP = MPLS;

- O.a RADIUS and Common Open Policy Service (COPS);
- Authentication, Authorization and Accounting (AAA)

Voordelen SDN

- Simpel en Gecentraliseerd
- Lagere kosten qua
 - Management
 - Hardware
- Innovatie dmv nieuwe protocollen

Nadelen SDN

Veel NEMs (Network Equipment Manufactures) maken een eigen standaard en verwachten dat andere NEMs zich hierbij aansluiten. Hierdoor zijn er veel SDN controllers en applicaties.

Verschillende oplossingen voor 1 probleem:

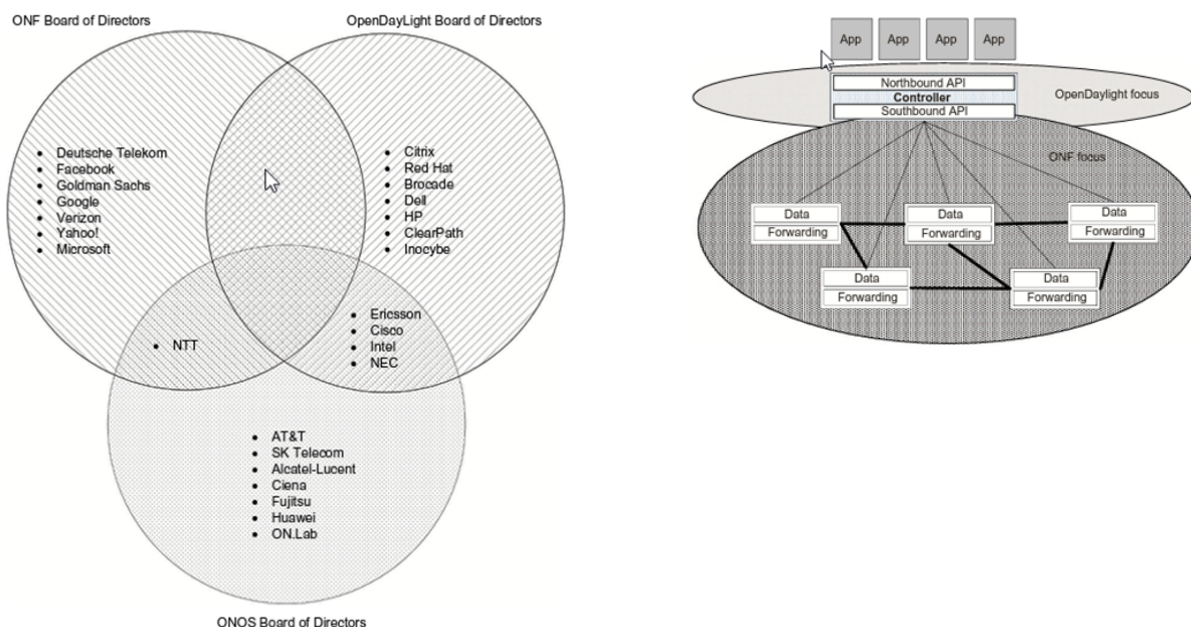
- VXLAN: Virtuele tunnel (Laag 2 frames) over fysieke of virtuele infrastructuur.
- NVGRE: (Microsoft Tunnel)
- STT: (VMware Tunnel)

Vendor	SDN Devices	SDN Controller	SDN Applications
Cisco	SDN via APIs OpenFlow: Nexus	COSC APIC-DC APIC-EM VAN	WAE
Hewlett-Packard	OpenFlow: 3500, 5400, and 8200		Security (Sentinel)
Brocade	OpenFlow: NetIron CER, CES	Brocade SDN Controller (Vyatta)	
VMware	SDN via APIs		
Big Switch	OpenFlow: Open vSwitch (OVS) OpenFlow: Indigo OpenFlow: Switch Light	NVP (NSX) Big Network Controller	NVP (NSX) Big Cloud Fabric Big Tap SDN VE
IBM	OpenFlow: RackSwitch and Flex System	Programmable Network Controller	
NEC	Programmable Flow 5240 and 5820	Programmable Flow Controller	DOVE Virtual Tenant Networks Firewall, others
Extreme	OpenFlow	ADARA	
Juniper	OpenFlow: MX, EX series	Contrail	
Alcatel-Lucent ^a	SDN via APIs	Nuage VSC	
Arista	OpenFlow: 7050 series SDN via APIs	VMware NVP Nuage VSC	

^aAlcatel-Lucent is now part of Nokia.

Hierdoor komen er nieuwe 'vendors' en hopen een internationale inter-vendor standaard maken.

- Open Networking Foundation (ONF);
- OpenDaylight (ODL): SDN Controller;
- ONOS;
- Open Stack;
- OpenSwitch;
- IETF.



Openheid is nodig: Nu bepalen veelal de fabrikanten wat mogelijk is

- Hardware; (Closed: dus je kunt het niet 'eigen maken')
- Low level firmware; (OS is geschreven door de fabrikant)
- Software (Closed: fabrikant dicteert services, protocollen,;

Als er al mogelijkheden zijn dan ben je gebonden aan:

- Development methods en talen (Java, ...);
- Software (OS,...) en Hardware functionaliteiten

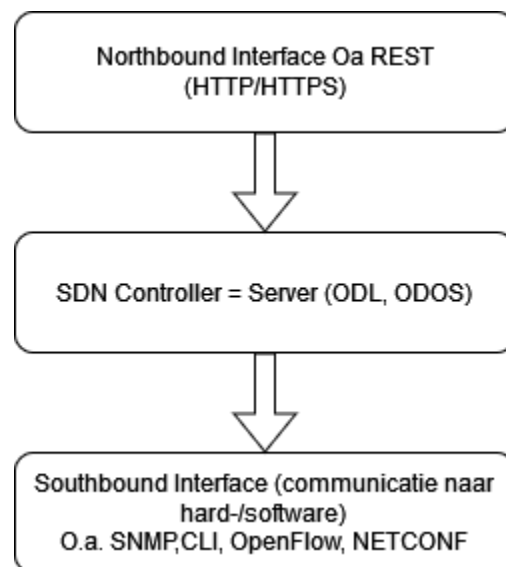
Openheid en innovatie voor de fabrikanten:

- Betere, sneller en competitieve producten;
- Openheid zorgt (vaak) ook voor meer veiligheid en innovatie
- Better margins (servers + 5% margin)

3 SDN categorieen

1. SDN via een controller (OpenSDN)
2. SDN via Overlays
3. SDN via API's

SDN communicatie en onderdelen:



SDN via Overlays

SD-WAN/ SD-Access

Software, beheer van netwerk (under- en overlay, LAN, WAN, en applicatie-based)
(meestal via web-dashboard)

O.a. Cisco Meraki

Virtual network komt bovenop het fysieke netwerk;
(Virtual Tunnel)Endpoints weten niets van de tunnel en/of het virtuele netwerk.;
Overlay / tunnelling encapsulation gebruikt o.a.;
MAC in IP tunnelling;
VXLAN;
NVGRE;
STT .

SDN via Controller

- Breaking the control plane and data plane;
- Centralized PBRs (Policy Based Routing);
- Specialized network appliances direct into Switch (o.a. IDS);
- Edit forwarding / Flow tables;
- Inspect and (potentially) modify Layer two, three and four protocol header modification.

SDN via APIs

Belangrijke kenmerken / verbeteringen:

Programmeerbaarheid en Centrale controle

SDN via APIs:

- Traditionele methodes: CLI, SNMP, SSH, Telnet, ...;
- Interface to the Routing System (I2RS);
 - RESTful APIs: (HTTP(S) / TCP)
 - NETCONF

4 kenmerken van I2RS:

1. Programmatisch, asynchroon en fast interface (toegang)
2. Structured routing information
3. Mogelijkheden voor netwerkmanagement

4. Bieden van standaard data-models en methoden

Benefits and Limitations of SDN via APIs

Voordelen:

- Gebruikt legacy management interfaces (Console poort, SSH, Telnet, ...) en dus werkt met 'oude' hardware en commando's ;
- Geeft mogelijkheden voor: agility en automation;
- Bepaalde mate van centrale controle
- Potentiele mogelijkheid voor meer 'openness' tussen de vendors;

Nadelen:

- there is practically no controller at all
- Geeft niet een 'network-wide view'
- Control plane en applicatie heeft synchronisatie nodig

SDN via Policy-level APIs

API's 'boven' de controller.

Gebruikt policy i.p.v. individuele configuratie

```

prefix-set rfc1918
  10.0.0.0/8 le 32,
  172.16.0.0/12 le 32,
  192.168.0.0/16 le 32
end-set

route-policy inbound-tx
  if destination in too-specific or destination in rfc1918 then
    drop
  endif
  set med 1000
  set local-preference 90
  set community (2:1001) additive
  if community matches-any ([101..106]:202) then
    prepend as-path 2.30 2
    set community (2:666) additive
    if med is 666 or med is 225 then
      set origin incomplete
    else
      set origin igp
    endif
  endif
  else
    set community (2:999) additive
  endif
end-policy

router bgp 2
  neighbor 10.0.1.2 address-family ipv4 unicast route-policy inbound-tx in

```

Cisco IOS

- Cisco IOS (1980)
 - In het begin weinig geheugen (256 Kb)
 - Monolitisch
 - Beheer met CLI
- Cisco IOS XR (2004 >)
 - Multicore
 - Microkernel (safety)
- Cisco IOS XE (2007 >)
 - Linux Kernel (x64)

- containers en VM's
- CLI, GUI, API
- Ondersteuning Python, Ruby, Golang
- Cisco IOS NX
 - is XE/XR voor in datacenter
 - Virtueel + Fysiek

Datacenter Netwerken

East-West Traffic; Within the Datacenter;
North-South Traffic. 'Outside' the Datacenter;

80% + is East-West verkeer

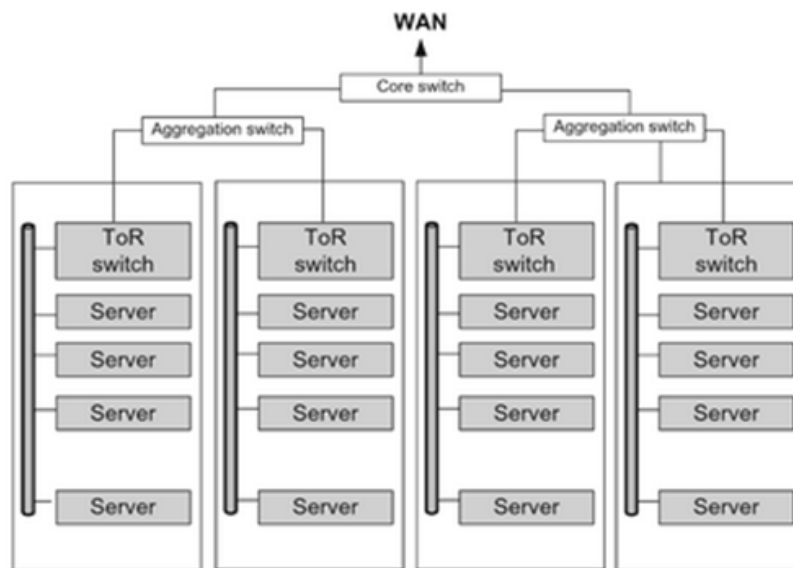


FIG. 1.1

Typical data center network topology.

ToR switch = Top of the Rack switch (1 main switch/switch cluster per rack)

OpenFlow

OpenFlow Protocol beschrijft communicatie tussen OpenFlow Switches en een centrale controller.

OpenFlow 'ontwikkelt in 2008; Impact o'p netwerk industry in 2011;

Basic operation of OpenFlow:

Controller 'populates flow table van een OF switch';

'Switch evaluates the header of incoming packets';

Geen Match gevonden, dan gaat een packet naar de controller;

Controller updates flow table entries as new packet patterns are recieved;

Controller kan werken met wildcard rules.

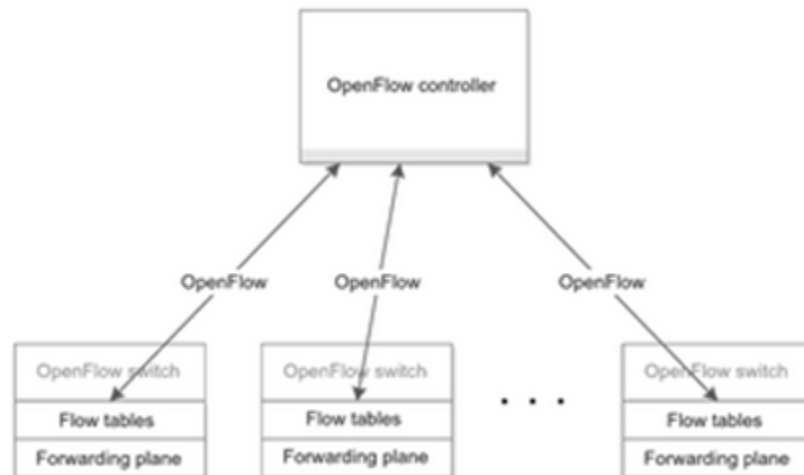


FIG. 3.7

General OpenFlow design.