# Software Defined Networks (SDN)

ITN 4252 Advanced Topics in Networking

*Partially based on whitepapers and resources from Cisco, Palo Alto, HPE, Equinix, and Juniper.*

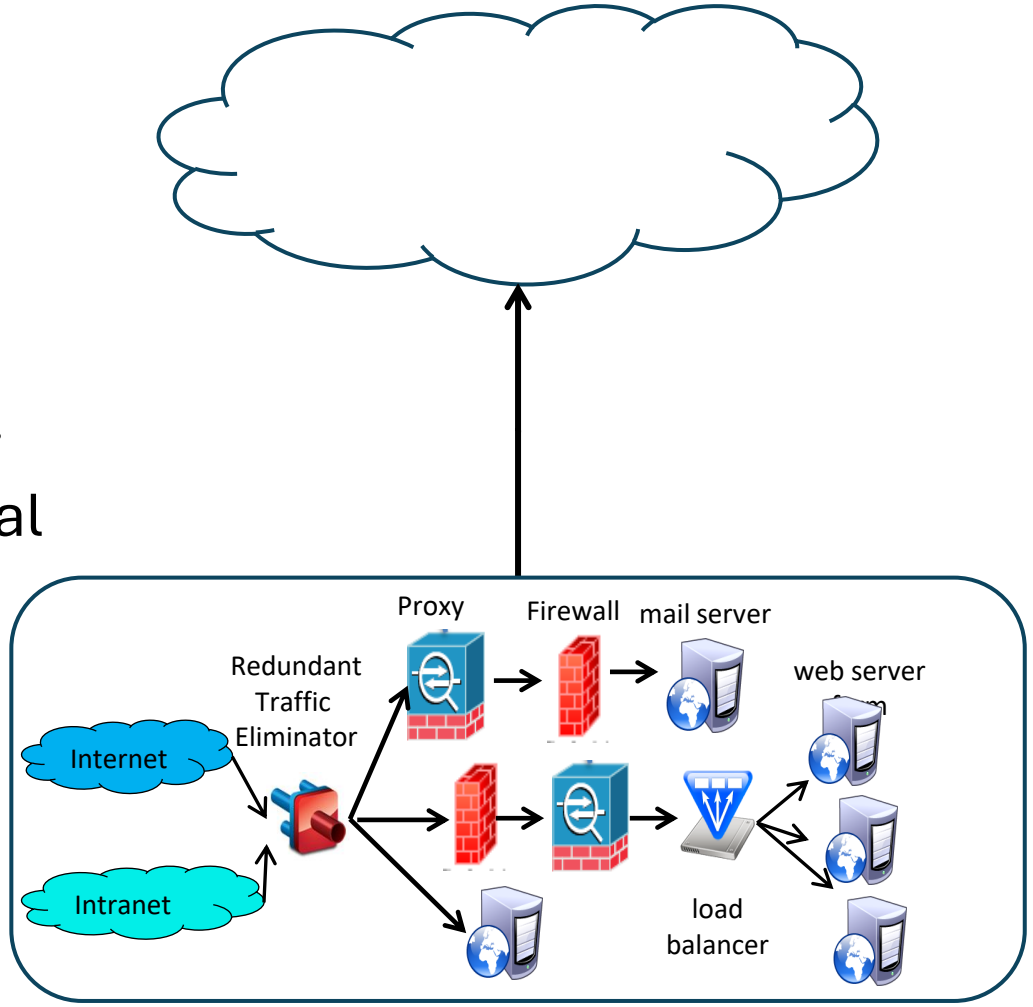
# Computing systems once upon a time

- Vertically integrated systems
  - Proprietary hardware
  - Proprietary applications
  - Highly reliable

- But…
  - Slow software innovation
  - Proprietary development
  - Small industry

# Moving to Cloud Computing

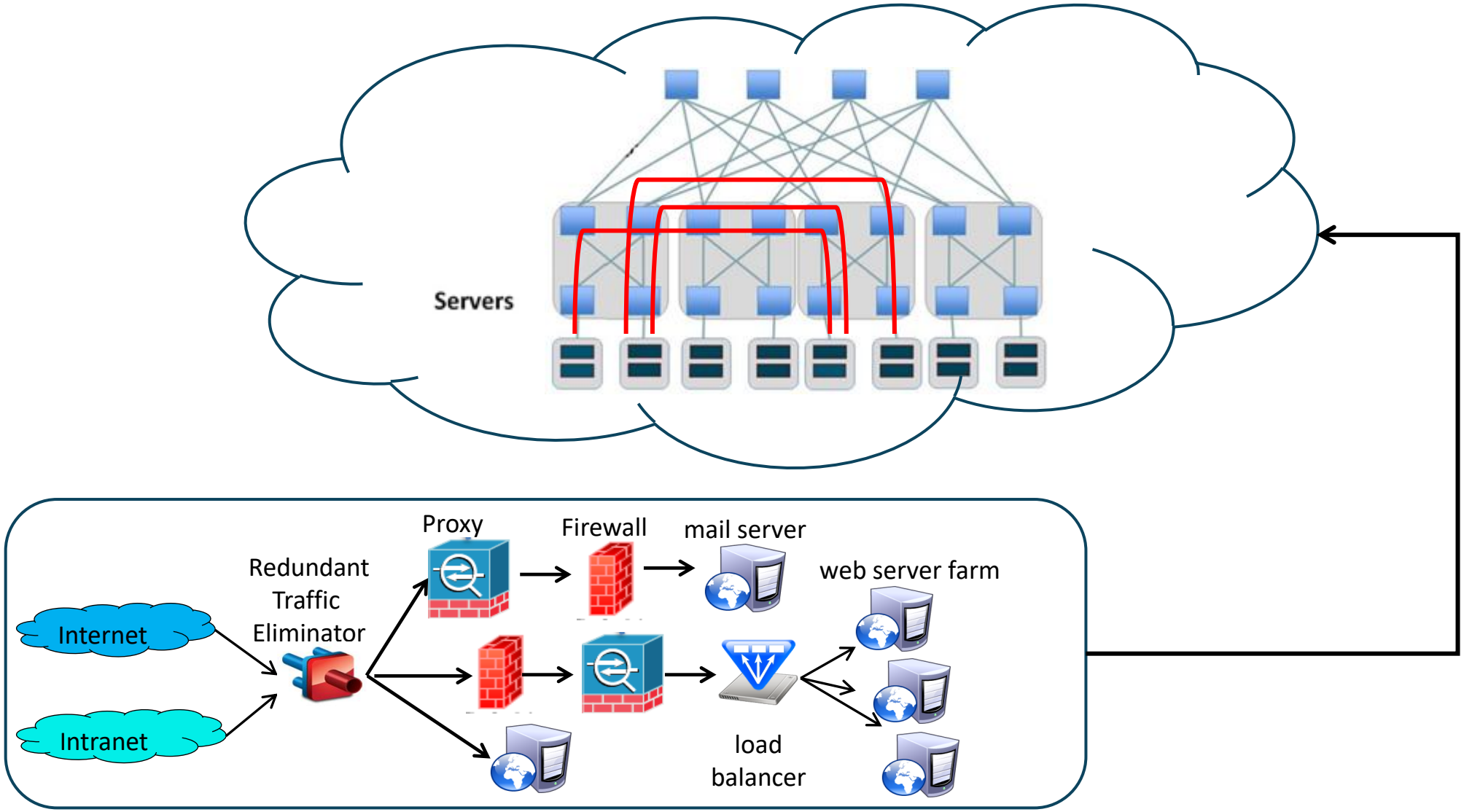
- Applications running on data centres can be moved into cloud computing environments
- However, moving an entire data centre into a cloud computing environment is complicated.
- In addition to the applications, there are several networking components running in a data centre.
  - e.g.: IDS, Proxy, Firewall etc.
- The challenge is to transition real-world networking platforms into a virtualised, cloud-based environment.



# Networking the cloud era

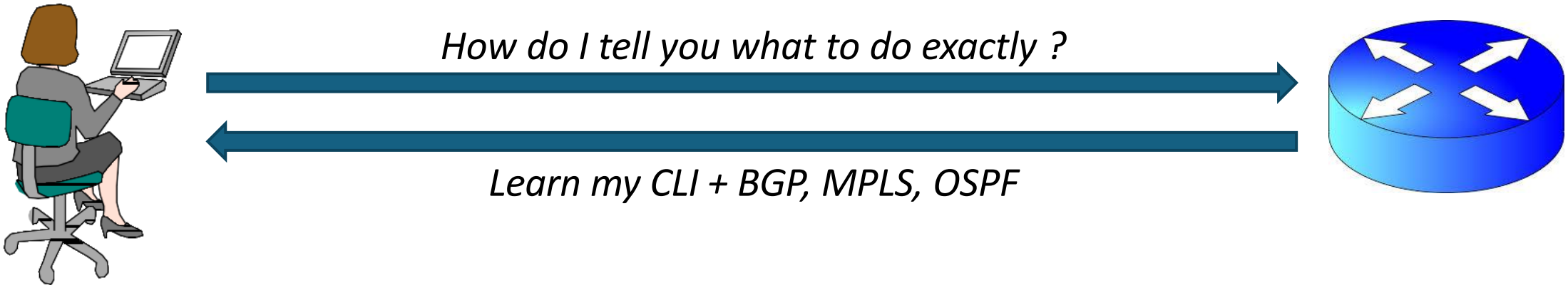
- Network administrators in the cloud usually don’t deal with physical routers, switches, and other infrastructure devices.
- Software Defined Networking (SDN) is a solution that enables this transition.
- SDN transforms physical devices like switches, routers, firewalls, and other networking infrastructure into a software-based platform for use in the cloud.
- This process involves breaking down the functions of a device like a switch into individual components.
- These components are then recreated as software versions that can be run in the cloud.

# Cloud data center



# Existing technologies

- Large data centres, different network boxes
- Network boxes speak protocols/algorithms that are not familiar to other IT personnel and only network people can comprehend
  - i.e. :  BGP, OSPF, MPLS, etc.
- Because interacting with the network required a language, that a few  people in the organisation understands
  - i.e.: Vendor specific CLI, and lots of vendors

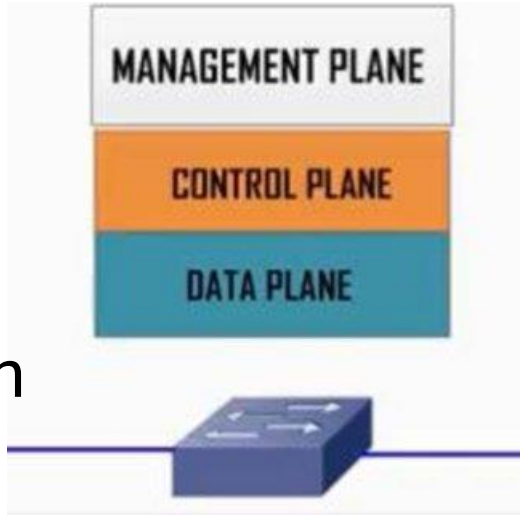


# Challenges with traditional networks

- Architecture:
  - Traditional networks use fixed and dedicated hardware devices such as routers and switches to control network traffic. This static, hardware-based architecture can be less flexible and adaptable.
- Scalability:
  - Traditional networks may struggle to scale efficiently in response to the dynamic needs of cloud computing.
- Management and Configuration:
  - Traditional networks often require manual configuration and management, which can be time-consuming and prone to errors.
- Interoperability:
  - Traditional networks may face compatibility issues with cloud software.
- Cost:
  - Traditional networks often involve significant capital expenditure (capex) on proprietary hardware.

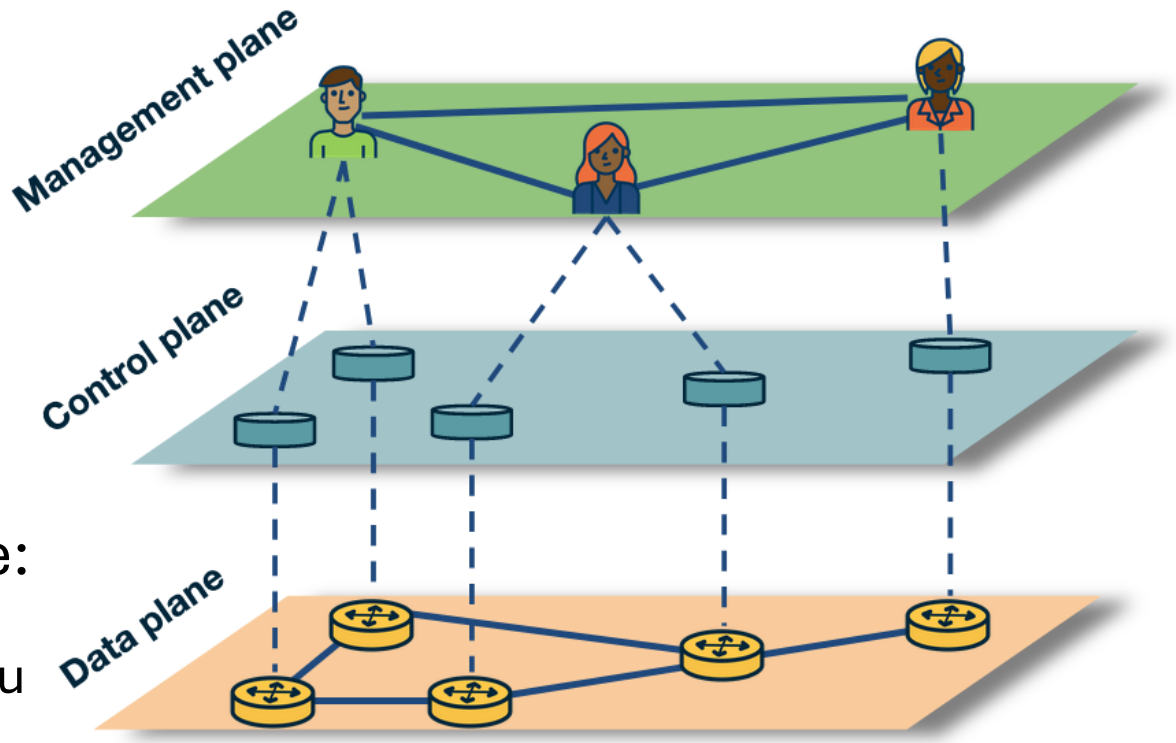
# Traditional networks

- There are three layers or ways to separate networking devices for consistency:
  1. infrastructure layer/data plane,
  2. control layer/control plane
  3. application layer/management plane
- Software for the control plane cannot be separated from forwarding hardware in data plane.
- Vertically integrated, complex, closed, proprietary



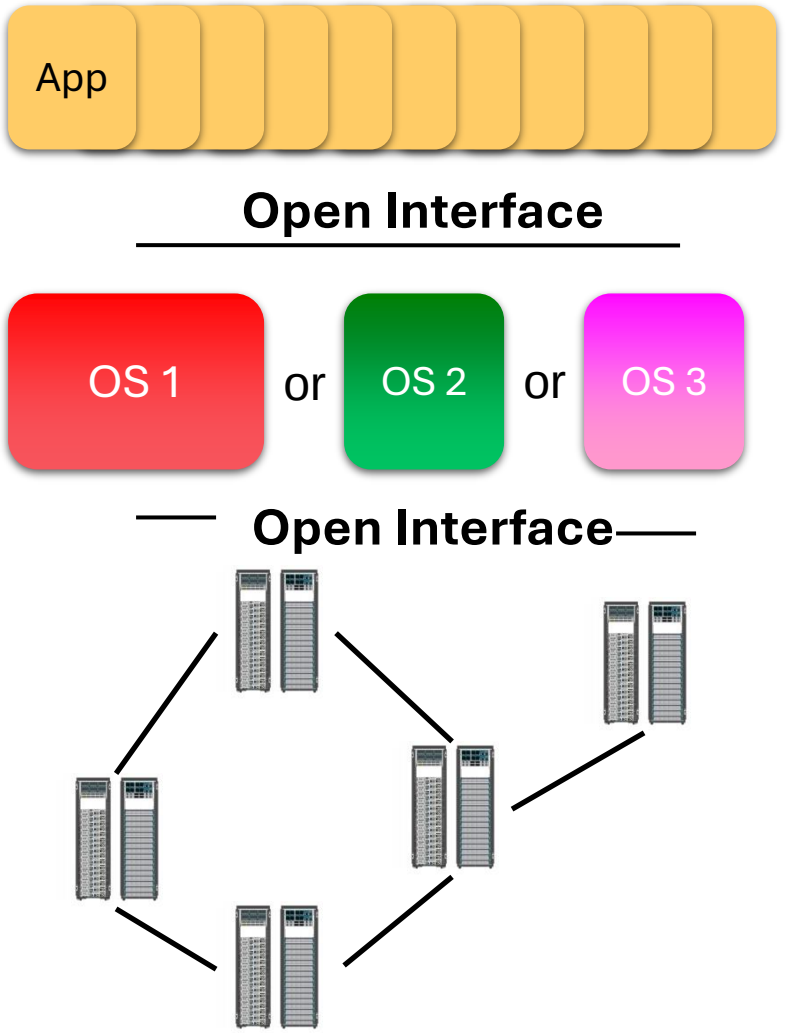
# Layered view of networking functionality

- Infrastructure Layer/Data Plane:
  - It handles forwarding, trunking, encrypting, network address translation, and other packet-level operations.
- Control Layer/Control Plane:
  - It contains references for traffic directions, such as dynamic routing protocols, forwarding tables in a switch, and NAT tables in a router.
- Application Layer/Management Plane:
  - It allows login or access to the device via an API for device management. When you SSH into a router or bring up a graphical front end of a firewall, you're managing the device from this plane.



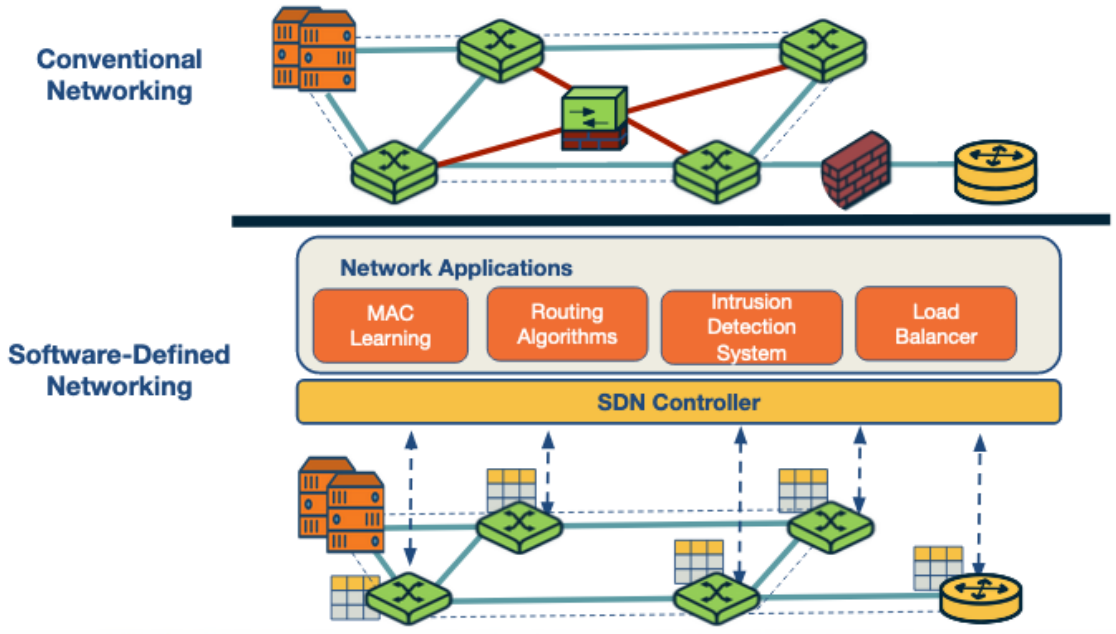
# Ideal networking system for innovation

- Separate hardware from software
- Standardise the interfaces
- Each layer provides an abstraction
- This is the vision of SDN

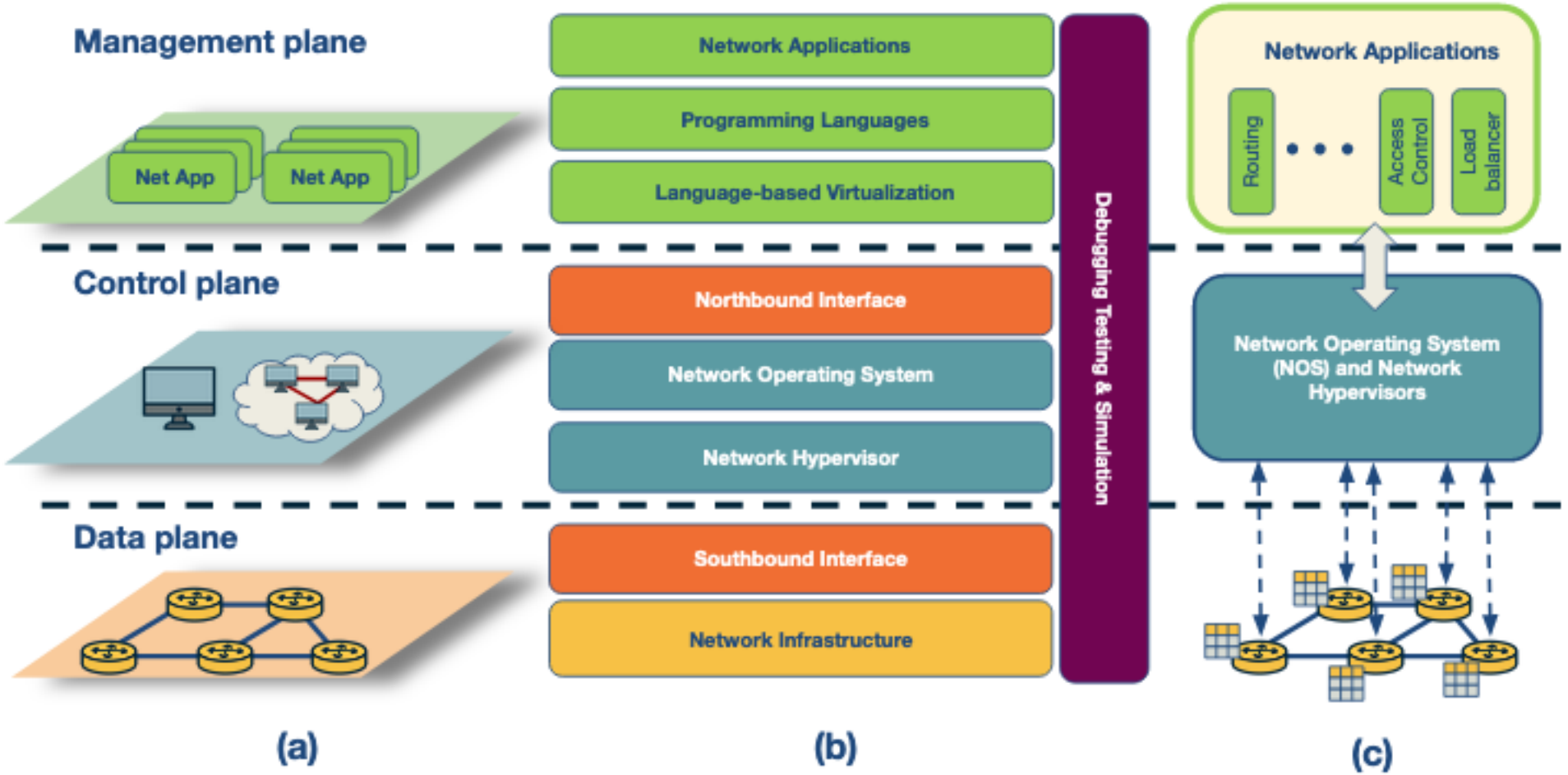


# Software Defined Networks (SDN)

- SDN is a networking approach that uses software controllers, driven by application programming interfaces (APIs), to communicate with hardware infrastructure and direct network traffic.
- SDN creates and operates a series of virtual overlay networks that work in conjunction with a physical underlay network.
- It separates the control plane (routing and packet forwarding functions) from the data plane (underlying infrastructure), and implements controllers above the network hardware.



# SDN Architecture




(a) a plane-oriented view, (b) the SDN layers, and (c) a system design perspective

# SDN Components

- Applications
  - Tasked with relaying information about the network or requests for specific resource availability or allocation.
- SDN controllers
  - Handle communication with the apps to determine the destination of data packets. The controllers are the load balancers within SDN.
- Networking devices
  - Receive instructions from the controllers regarding how to route the packets.
- Open-source technologies
  - Programmable networking protocols, such as OpenFlow, direct traffic among network devices in an SDN network. The Open Networking Foundation (ONF) helped to standardise the OpenFlow protocol and other open source SDN technologies.

# SDN Technologies

- Infrastructure
  - SwitchLight, Open vSwitch, Pica8, etc.
- Southbound interfaces
  - OpenFlow, ForCES, OVSDB, POF, OpFlex, OpenState, etc.
- Network virtualisation
  - VxLAN, NVGRE, FlowVisor, FlowN, NVP
- Network operating systems
  - OpenDayLight, OpenContrail, Onix, Beacon and HP VAN SDN
- Northbound interfaces
  - Floodlight, Trema, NOX, Onix and SFNet
- Language-based virtualisation
  - Pyretic, libNetVirt, AutoSlice, RadioVisor, OpenVirteX, etc.
- Network programming languages
  - Pyretic, Frenetic, Merlin, Nettle, Procera, FML, etc.
- Network applications
  - Hedera, Aster*x, OSP, OpenQoS, Pronto, Plug-N-Serve, SIMPLE, FAMS, FlowSense, OpenTCP, NetGraph, FortNOX, FlowNAC, VAVE, etc.

# SDN Security

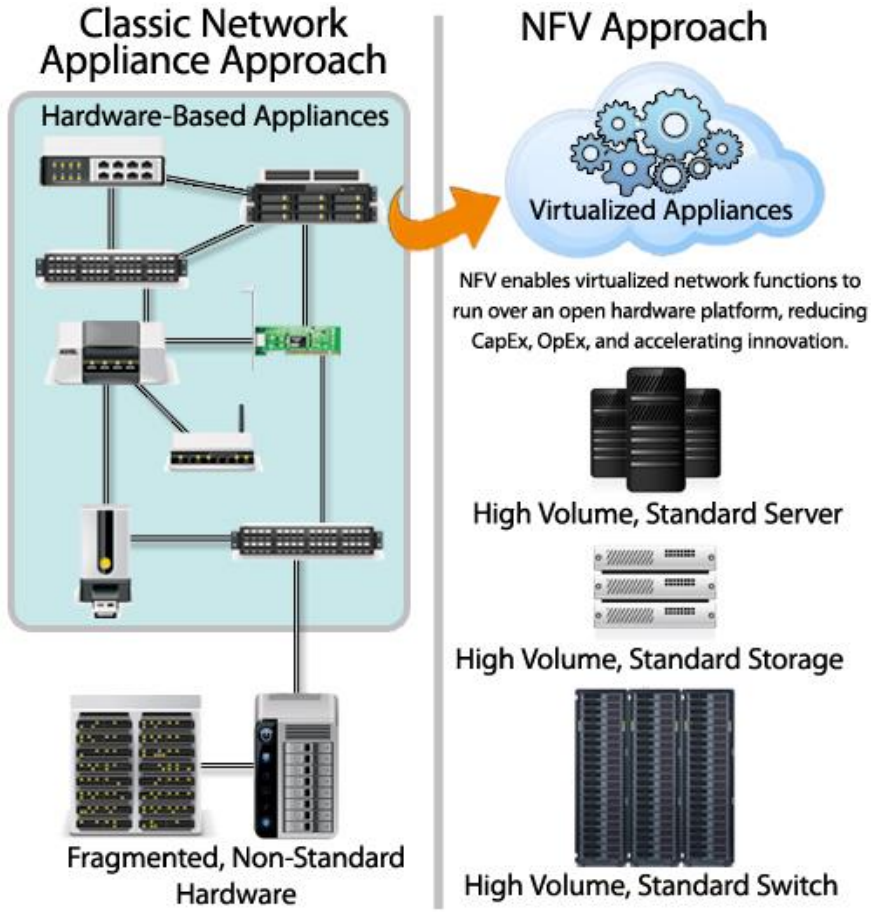
- Centralised Policy Management:
  - SDN controllers configure policies centrally, translating and pushing them to all networking devices.
- Efficient Endpoint Segmentation:
  - Simplifies segmentation of different endpoint groups.
- Business-Focused Configuration:
  - Aligns network configuration with business interests, avoiding tedious IP addressing schemes.

# SDN Advantages

- Flexible Architecture:
  - Unlike traditional networks that rely on fixed, dedicated hardware devices, SDN uses a software-based, programmable architecture. This allows for greater flexibility and adaptability.
- Efficient Scalability:
  - SDN can efficiently control traffic and scale as needed, making it more suitable for the dynamic needs of cloud computing than traditional networks.
- Automated Management:
  - SDN allows for automated, centralised network management. This is more efficient and less error-prone compared to the manual configuration and management often required in traditional networks.
- Improved Interoperability:
  - SDN software can integrate with any underlying hardware, overcoming the compatibility issues that traditional networks may face with cloud software.
- Cost-Effective:
  - SDN can lead to cost savings by using generic hardware and reducing operational expenditure (opex) costs. This is a significant advantage over traditional networks that often involve significant capital expenditure (capex) on proprietary hardware.

# Network Functions Virtualisation (NFV)

- Virtualises network services, such as routers, firewalls, and load balances, that have traditionally been run on proprietary hardware, and allows these services to be hosted on virtual machines
- Collapses various functions into a physical server, reducing overall cost
- Delivers high-performance networks with greater scalability, elasticity, and adaptability at lower costs



# SDN vs. NFV

**SDN**

- Separates control plane from forwarding plane, centralising control and programmability.
- Focuses on data centres.
- Uses OpenFlow as a communication protocol.
- Managed as a complete entity for better integration.

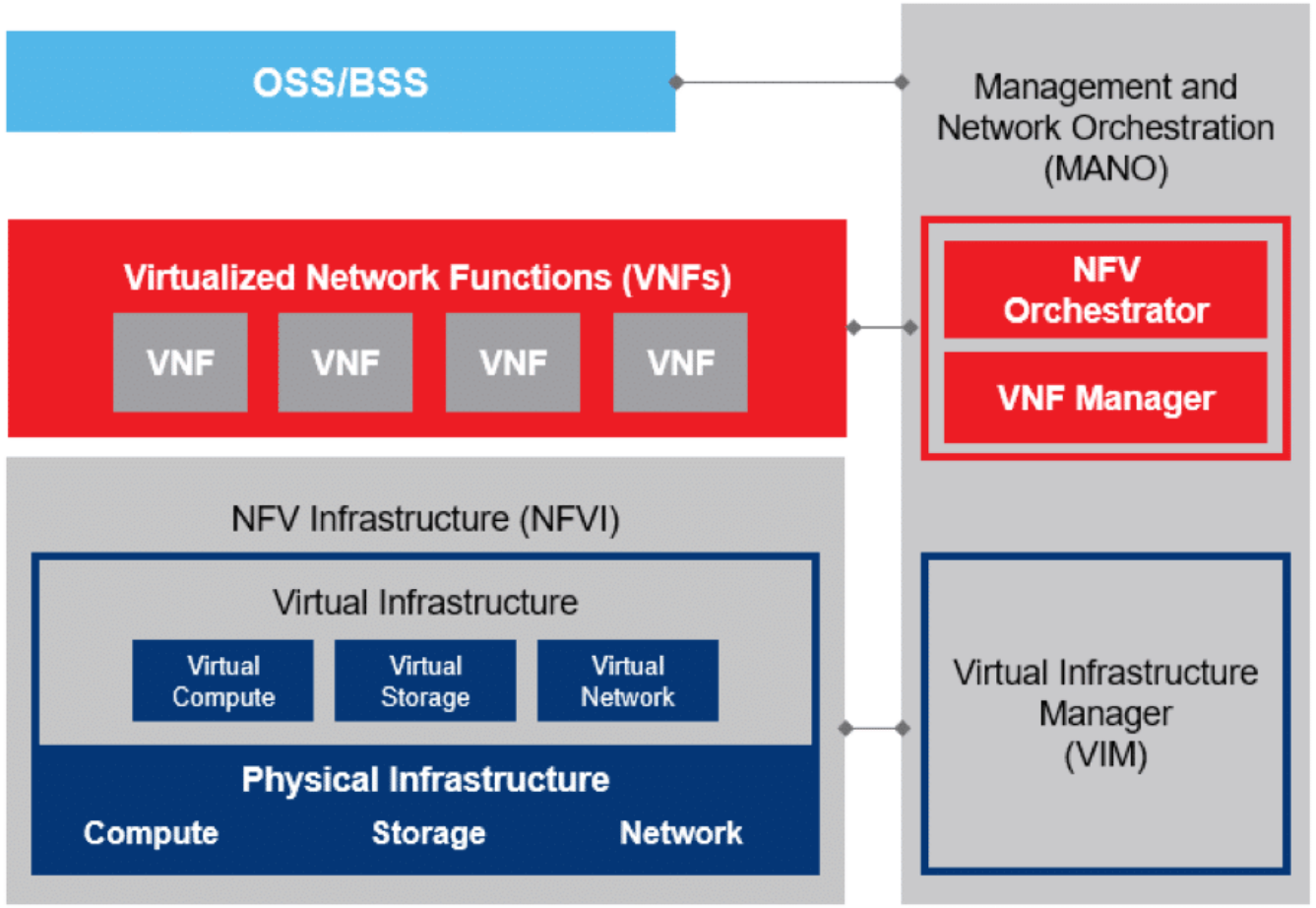
**NFV**

- Virtualises network functions like routing, firewalls and SD-WAN.
- Targeted at service providers.
- Runs virtual network functions (VNFs) on high-performance servers.
- Module-based, with functions created and joined as needed.

•**Similarities:** Both leverage virtualisation for flexible, agile network infrastructures.

•**Differences:** SDN virtualises the network itself, while NFV virtualises network services or functions.

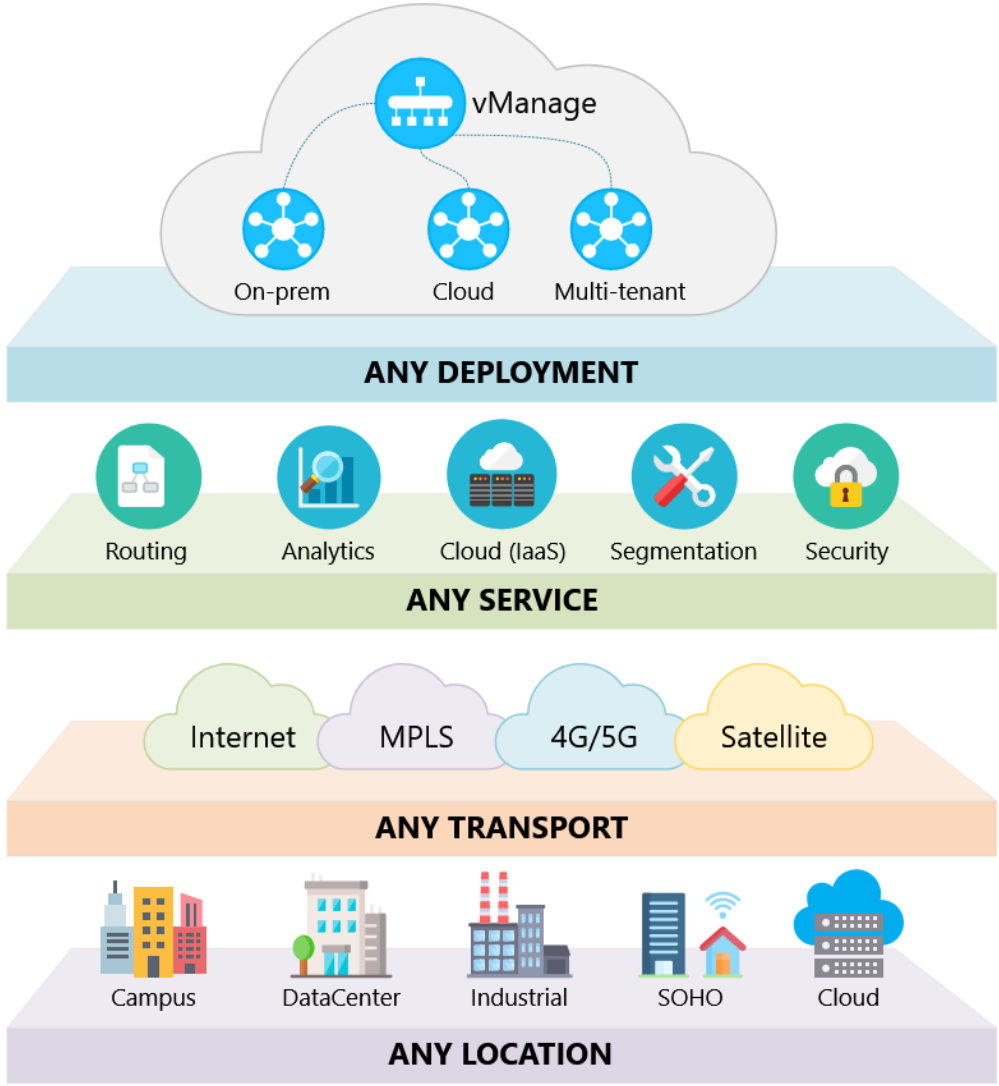
# NFV Architecture



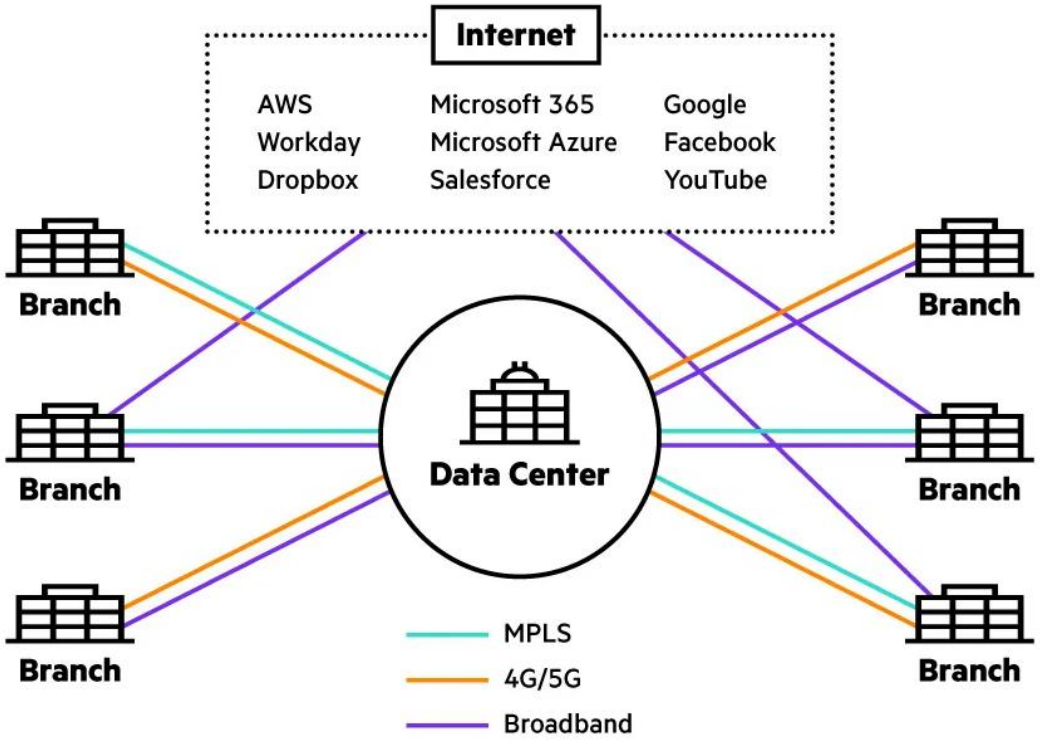

- Virtual Network Functions (VNFs):
  - Software-based network services running on generic hardware.
- NFV Infrastructure (NFVI):
  - The compute, storage, and network infrastructure supporting VNFs.
- NFV Management and Network Orchestration (MANO):
  - Framework for coordinating and managing NFVI and VNFs.

# What is SD-WAN?

- SD-WAN, or Software-Defined Wide Area Network, is a virtual WAN architecture.
- Like Software-Defined Networking (SDN), SD-WAN separates the control plane from the data plane.
- The software then uses a centralised control function to steer traffic securely and intelligently across the WAN and directly to trusted providers in the cloud.



# SD-WAN architecture

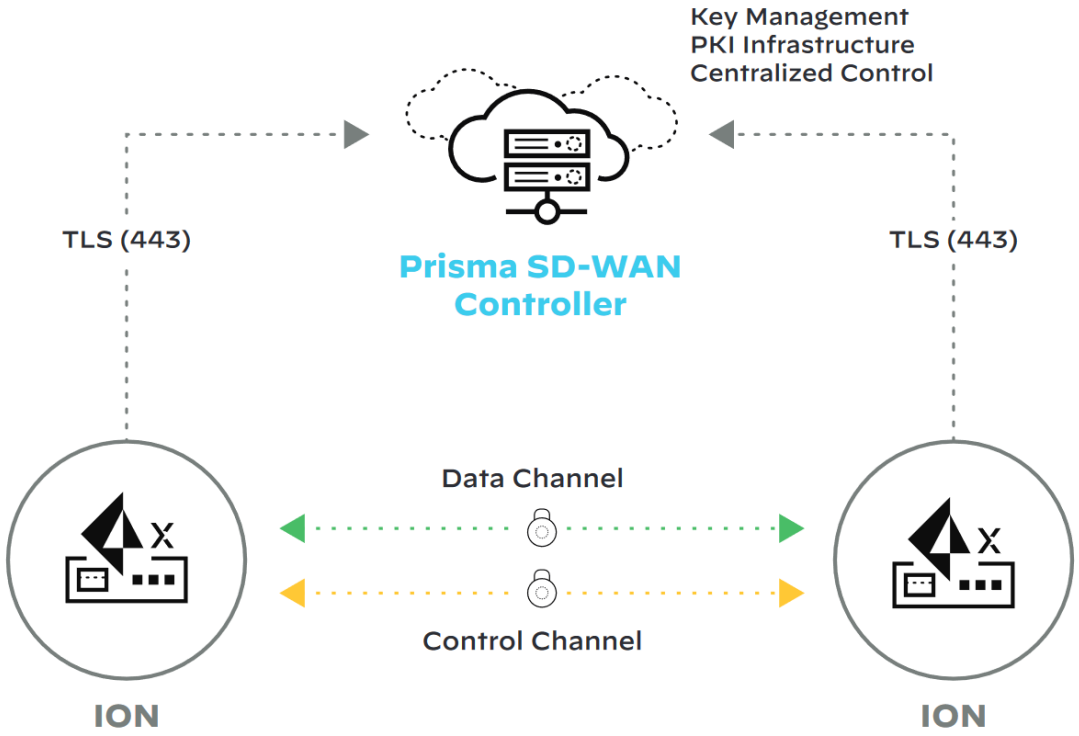



- Delivers superior application quality of experience (QoEx).
- Provides intelligent, application-aware routing.
- Ensures appropriate QoS and security policy enforcement.
- Supports secure local internet breakout for IaaS and SaaS traffic.
- Enhances cloud performance and protects against threats.

# SD-WAN Benefits

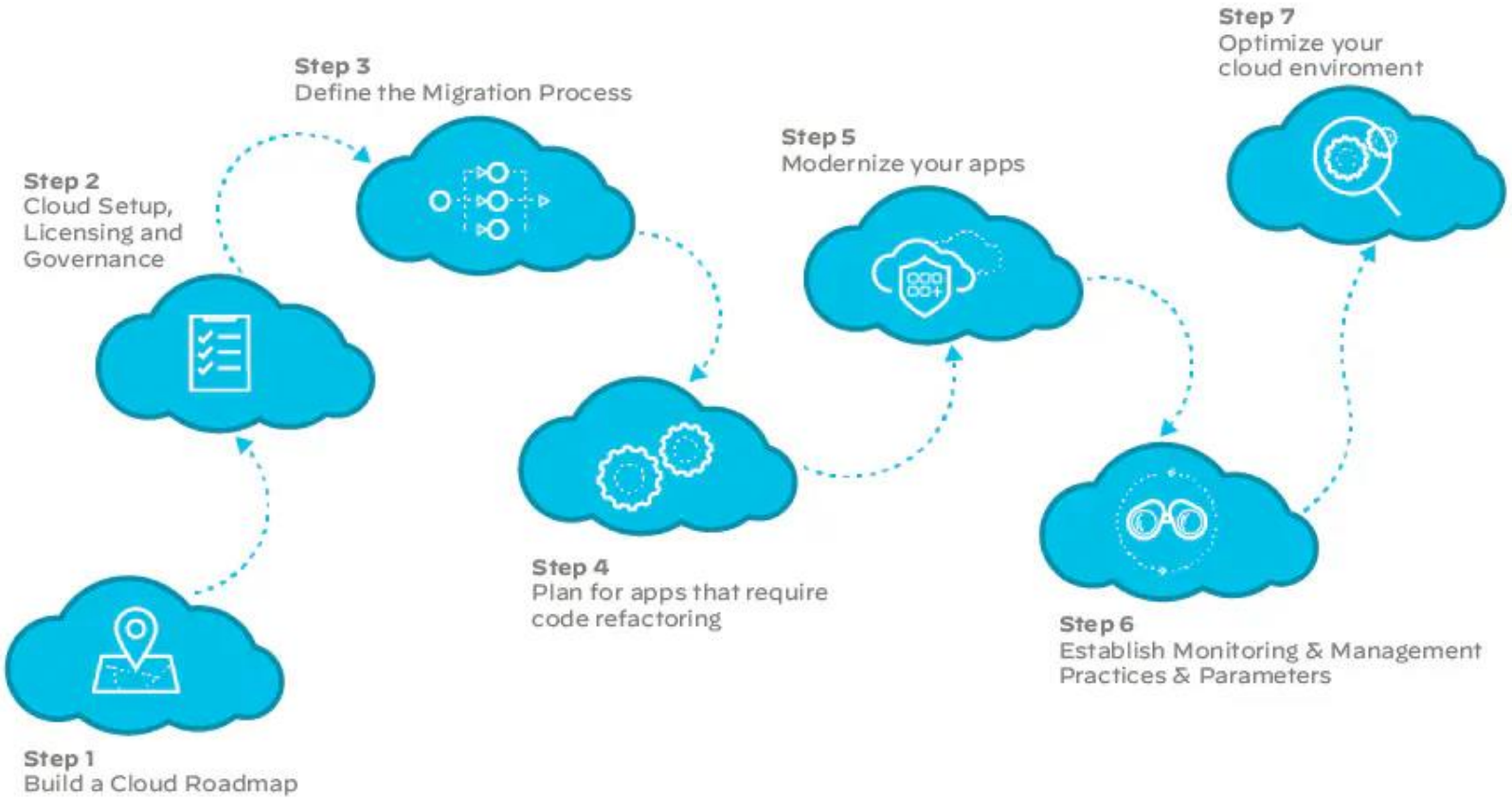
- Enhances bandwidth efficiency and cloud access.
  - Allows enterprises to leverage any combination of transport services – including MPLS, LTE, and broadband internet services – to securely connect users to applications.
- Simplifies WAN management and reduces costs.
  - Simplifies WAN infrastructure management by providing a single dashboard for network operations, offering visibility and control over deployment.
  - Allows companies to utilise less expensive internet connections such as broadband, 4G, or 5G wireless, leading to significant cost savings.
- Improves application performance, productivity, and customer satisfaction.
  - Uses a centralised control function to intelligently direct traffic across the WAN, increasing application performance and delivering a high-quality user experience.
- Maintains security and data privacy, reducing business risk.
  - Has built-in security features that help secure traffic going to applications. It can segment the network based on identity or roles, secure connections through data encryption, and tightly integrate with cloud security functions.

# SD-WAN Security




- High-Frequency Key Rotation:
  - Hourly key rotation for large-scale VPN networks (full-mesh, partial-mesh, hub-and-spoke).
- Unique Encryption Keys:
  - Each tunnel has unique encryption keys; session keys are only visible to tunnel endpoints.
- Controller Independence:
  - Endpoints can rotate keys without the controller; dataplane is isolated from the controller.
- Centralised Control:
  - Authorisation, security, and network policies are centrally managed.
- Secure Communication:
  - Policies and encrypted data are communicated via secure TLS 1.2 sessions; endpoints send anonymised statistics back to the controller.

# Next-Generation SD-WAN



# What is Next-Generation SD-WAN?

- Advanced Technologies:
  - Utilises AI, machine learning, and automation for superior performance and management.
- Cloud Integration:
  - Seamlessly integrates cloud services, improving access and reducing latency.
- Cost-Effective Broadband:
  - Leverages affordable broadband connections while maintaining high performance.
- Enhanced Security:
  - Centralised management, traffic segmentation, and advanced threat detection for better protection.

# Benefits of Next-Generation SD-WAN

- Exceptional User Experience:
  - Ensures application availability with real-time performance SLAs, delivering a 10x improvement in performance. Traditional WANs struggle with high bandwidth demands of cloud services and SaaS applications.
- Simplified Operations:
  - Reduces trouble tickets by up to 99%, simplifying network functions and expediting SASE migrations. Manual network management is inefficient and costly.
- Improved Security Outcomes:
  - Applies best-in-class security, reducing breaches by 45% with ZTNA 2.0. Enhanced security measures are required to protect against modern threats.
- Flexible Connectivity:
  - Supports adaptable and scalable network solutions, including direct internet, 5G, and MPLS.

# Requirements of Next-Generation SD-WAN

- Elastic Networks:
  - Zero-routing network with centralised controller, supporting direct internet, 5G, and MPLS.
- Direct-to-App Access:
  - Ensures exceptional user experience and application availability for SaaS, cloud, and business-critical apps.
- Zero Trust Security:
  - Integrated, granular security services for apps, users, and IoT devices, enforcing least-privilege access.
- AI-Powered Operations:
  - Advanced AI/ML for automating IT and NOC functions, increasing productivity, and reducing MTTR.
- Session-Based Architecture:
  - Creates a smart routing fabric based on each session's unique needs, providing greater visibility into user experience and network performance.
- Tunnel-Free Networking:
  - Eliminates VPNs and IPsec-based tunnels that consume resources.
- Secure Access Service Edge (SASE):
  - Ensures high performance and security for a mobile workforce with centralised, simple security policies and role-based access.

# Summary

- SDN Overview:
  - Uses software controllers and APIs to direct network traffic, creating virtual overlay networks over physical infrastructure.
- Benefits of SDN:
  - Delivers application environments as code, increases visibility and flexibility, and efficiently controls traffic.
- Components of SDN:
  - Includes applications, SDN controllers, networking devices, and open-source technologies like OpenFlow.
- SD-WAN Advantages:
  - Improves performance, enhances security, simplifies operations, and reduces costs with affordable broadband connections.
- Cloud Integration:
  - Ensures seamless access to cloud applications, improving overall network performance and management.