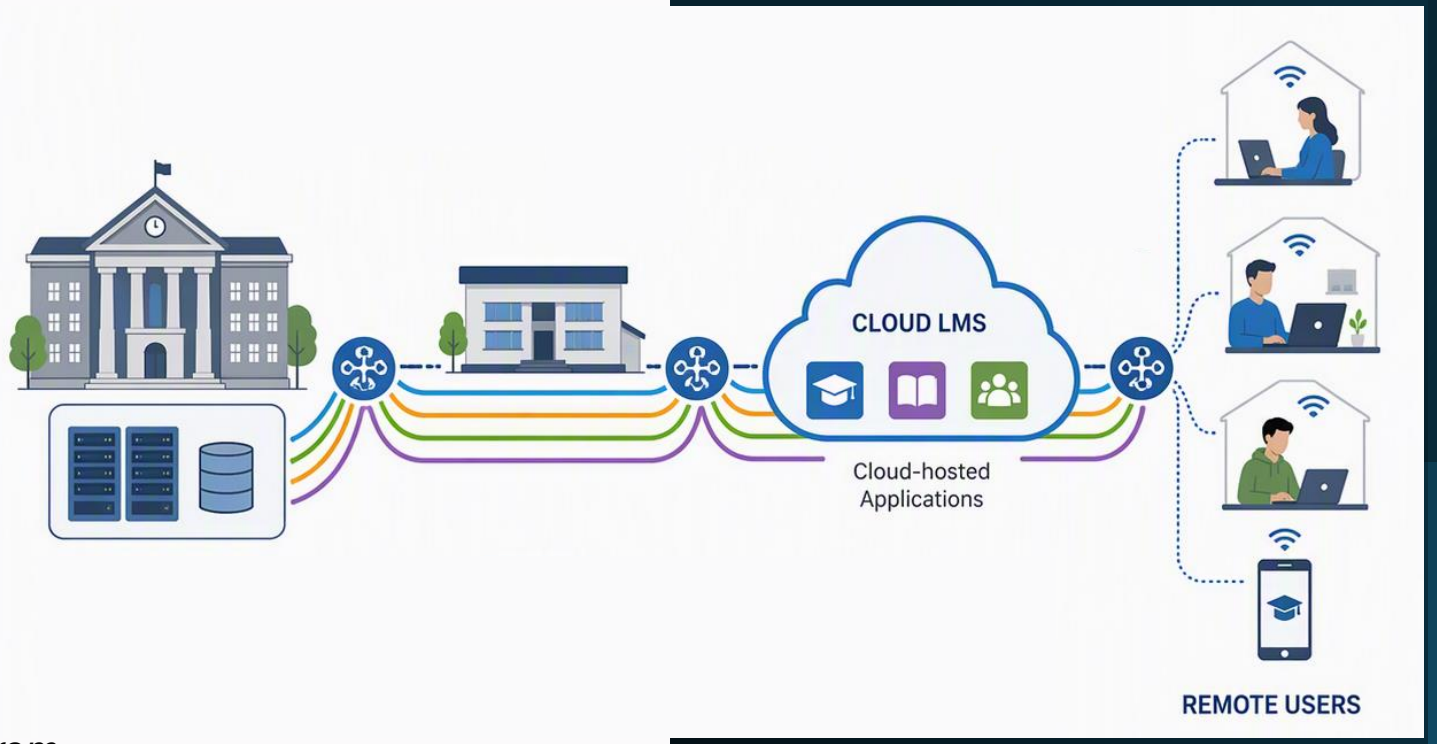
# Software-Driven Networking Paradigms




ITN 4252 Advanced Topics in Networking

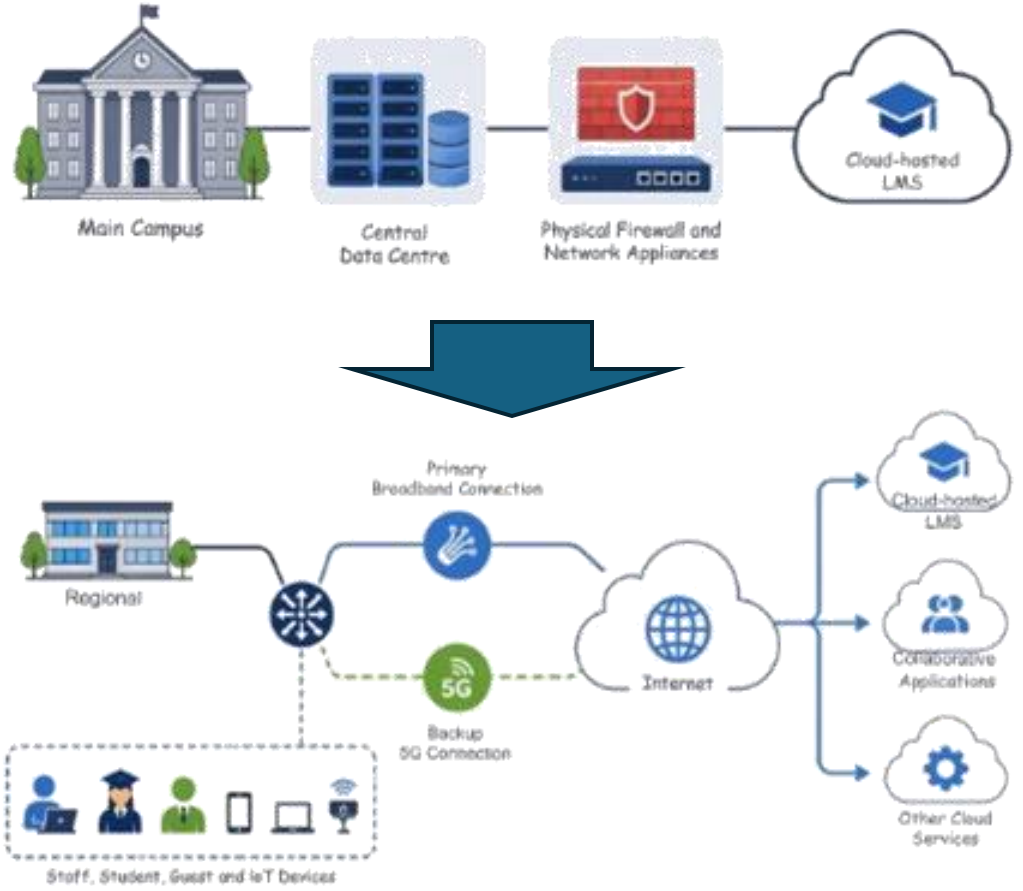
*Partially based on whitepapers and resources from Cisco, Palo Alto, HPE, Equinix, and Juniper.*

# A new university campus is opening next week

The new location needs:

- Secure access to the cloud-hosted LMS
- Reliable video and collaboration services
- Separate staff, student and guest networks
- Central monitoring and consistent security policies
- Backup connectivity if the primary link fails

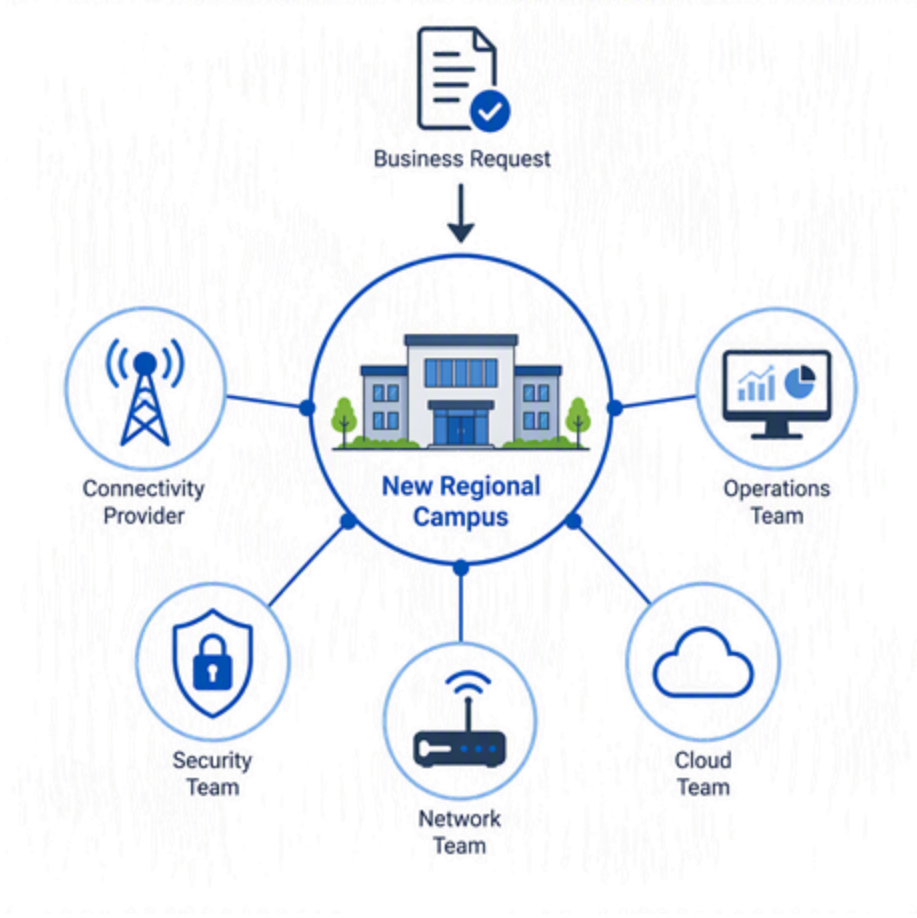
**Can the network be deployed as quickly as the service?**



# One location, many dependent changes

- Order and activate WAN connectivity
- Configure routing, addressing and segmentation
- Deploy firewall and network services
- Apply policy across multiple devices
- Integrate monitoring, logging and support

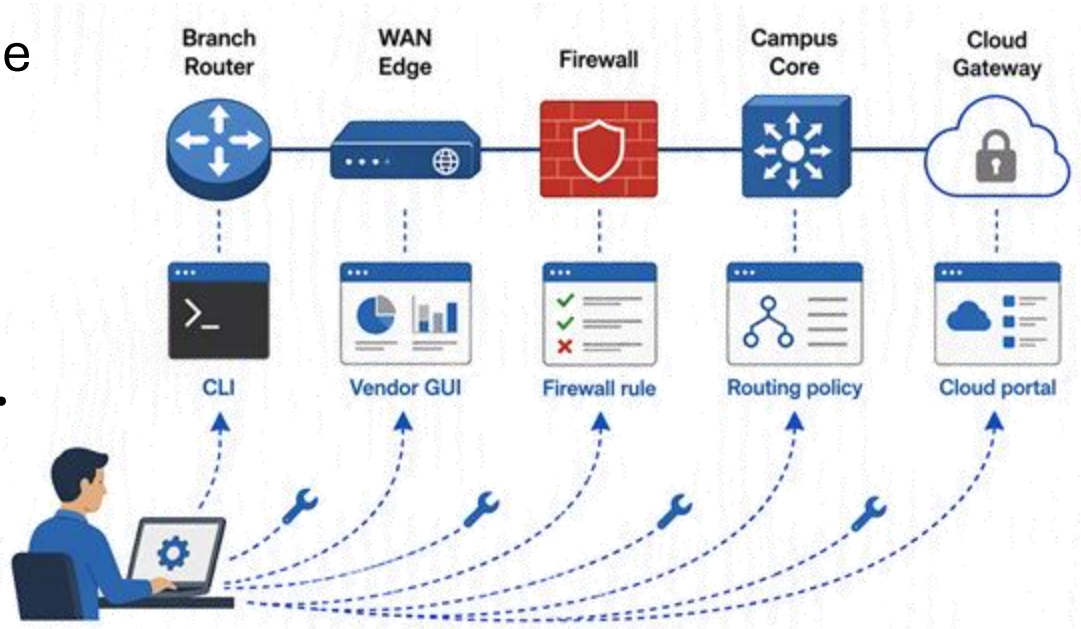
**The delay is often coordination, not connectivity.**



# Every device is configured separately

1. Interpret the network requirement
2. Translate it into vendor-specific commands
3. Configure each router, switch and firewall
4. Test each device and the end-to-end service
5. Repeat whenever the policy changes

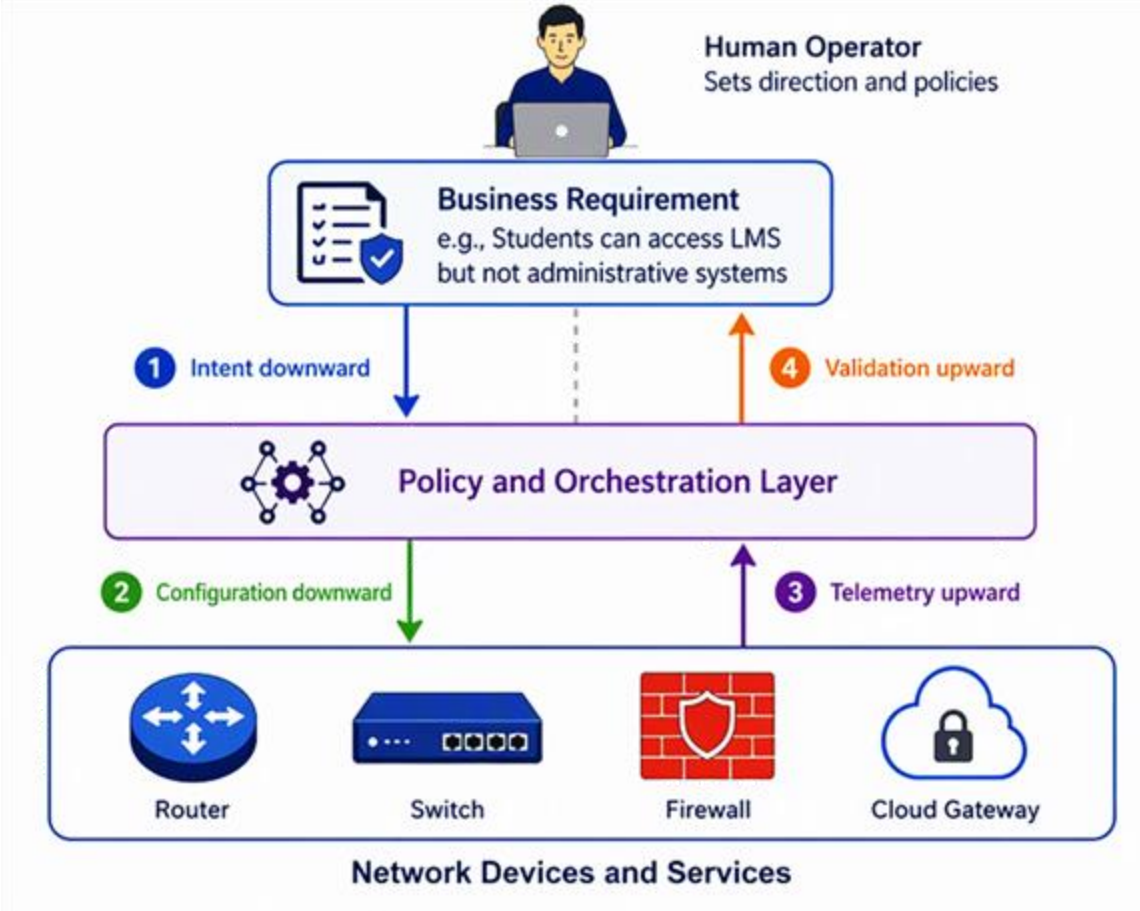
**The organisation defines one policy, but engineers implement it many times.**



# What should the network do differently?

- Separate
  - Decision-making from packet forwarding
- Abstract
  - Business policy from device-specific commands
- Automate
  - Repeatable configuration and lifecycle tasks
- Observe
  - Continuously verify network state and outcomes

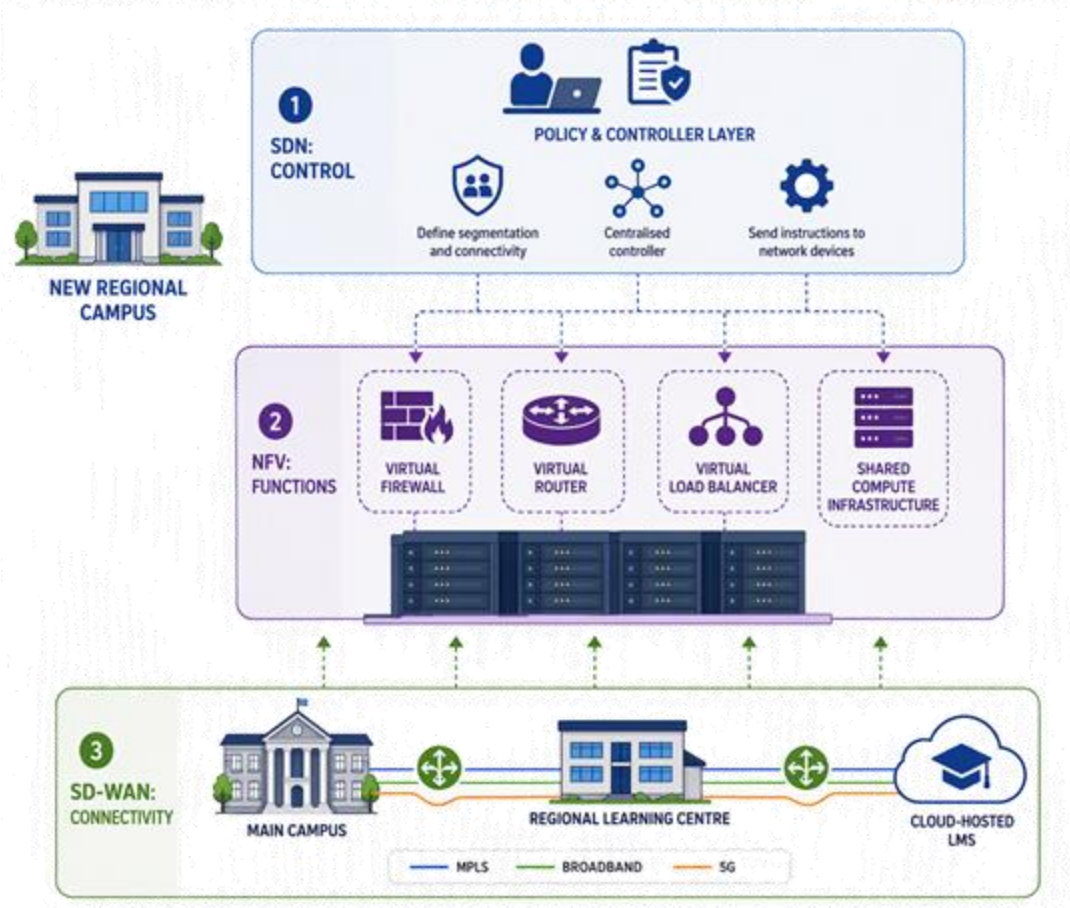
**Manage the network as a system, not as a collection of devices.**



# Three paradigms, three different problems

- SDN
  - How is network behaviour controlled?
  - Centralised policy, programmability and automation
- NFV
  - How are network functions delivered?
  - Firewalls, routers and load balancers implemented as software
- SD-WAN
  - How are distributed locations connected?
  - Application-aware policy across multiple WAN transports

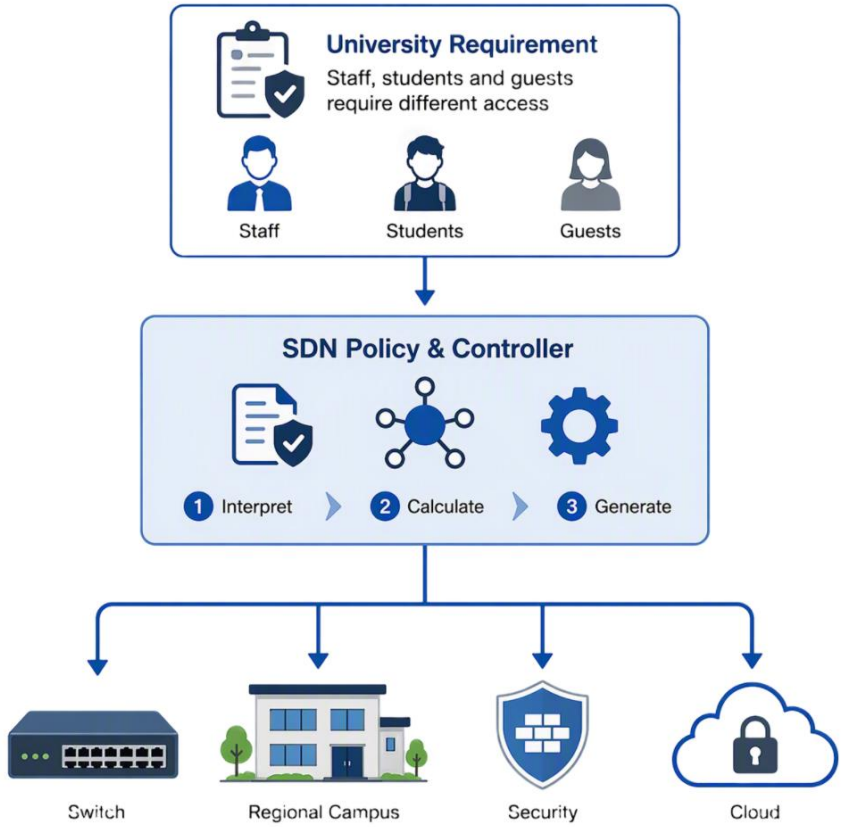
**They complement one another, but they are not interchangeable.**



# SDN: Programme the network as a system

- Separate control decisions from packet forwarding
- Maintain a logically centralised network view
- Express policy through software and APIs
- Apply changes consistently across multiple devices

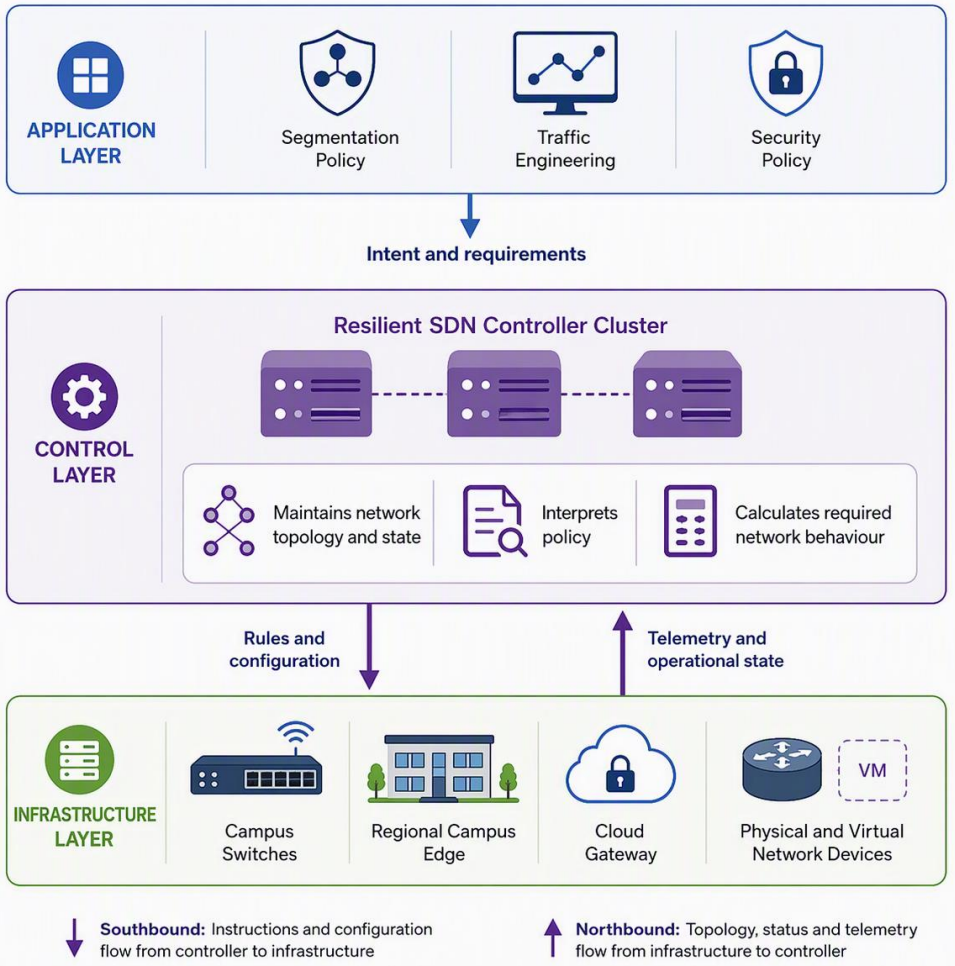
**Configure the required behaviour, not every device individually.**



# Three layers of SDN

- Application layer
  - Defines the required outcome
- Control layer
  - Translates policy into network instructions
- Infrastructure layer
  - Applies rules and forwards traffic

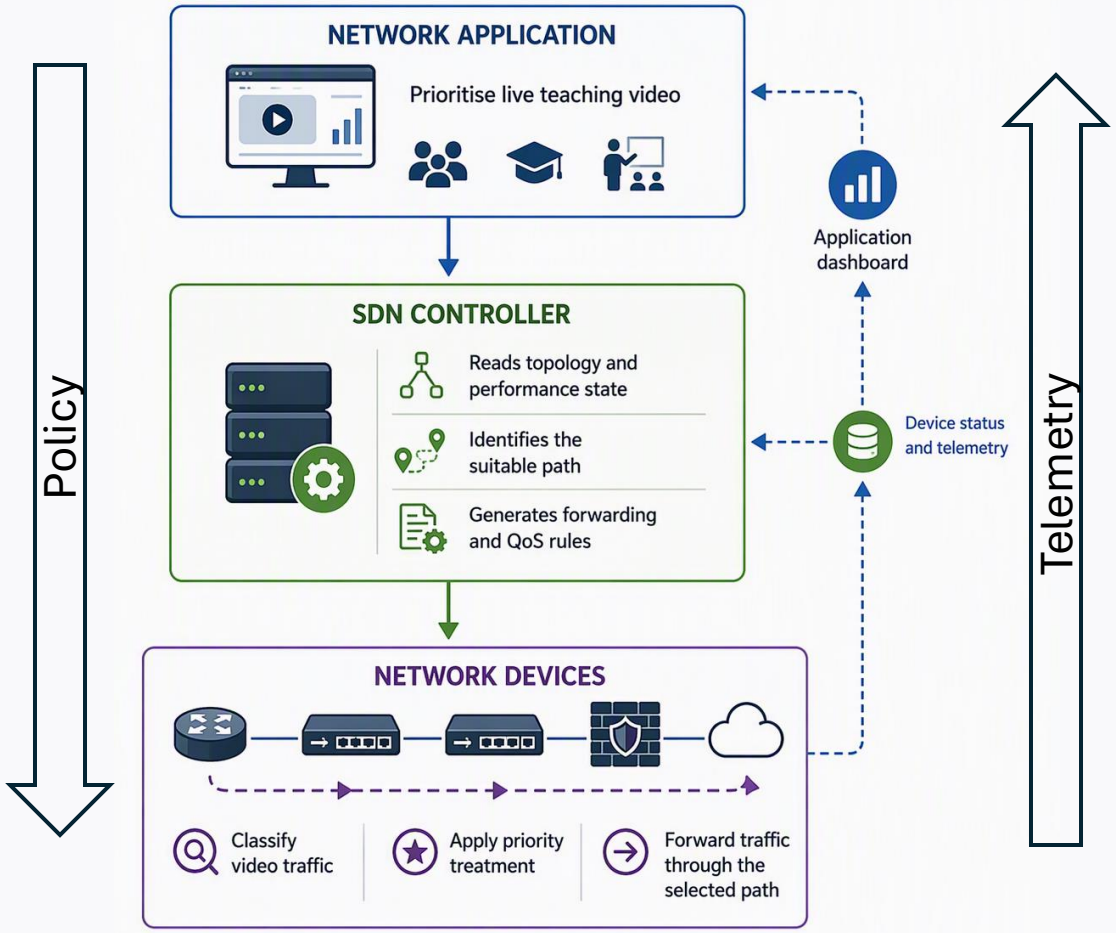
**Intent flows down.**
**Network state flows up.**



# Responsibilities of each SDN component

- Network applications
  - Define policies and required services
- SDN controller
  - Maintains state and coordinates network behaviour
- Network devices
  - Apply rules and forward traffic locally

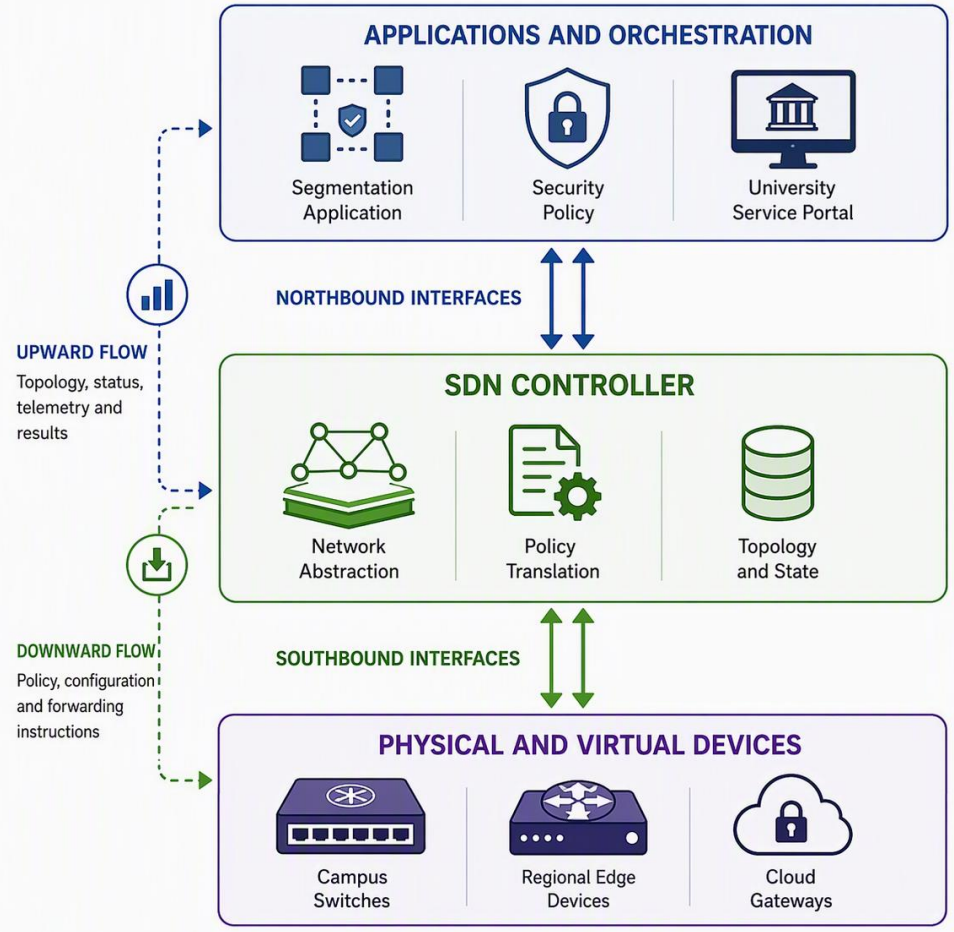
**Applications request.**
**The controller decides.**
**Devices execute.**



# APIs connect the SDN layers

- Northbound interfaces
  - Applications request policy, services and network information
- Southbound interfaces
  - Controllers configure devices and collect operational state
- Common purpose
  - Replace device-specific interaction with defined software interfaces

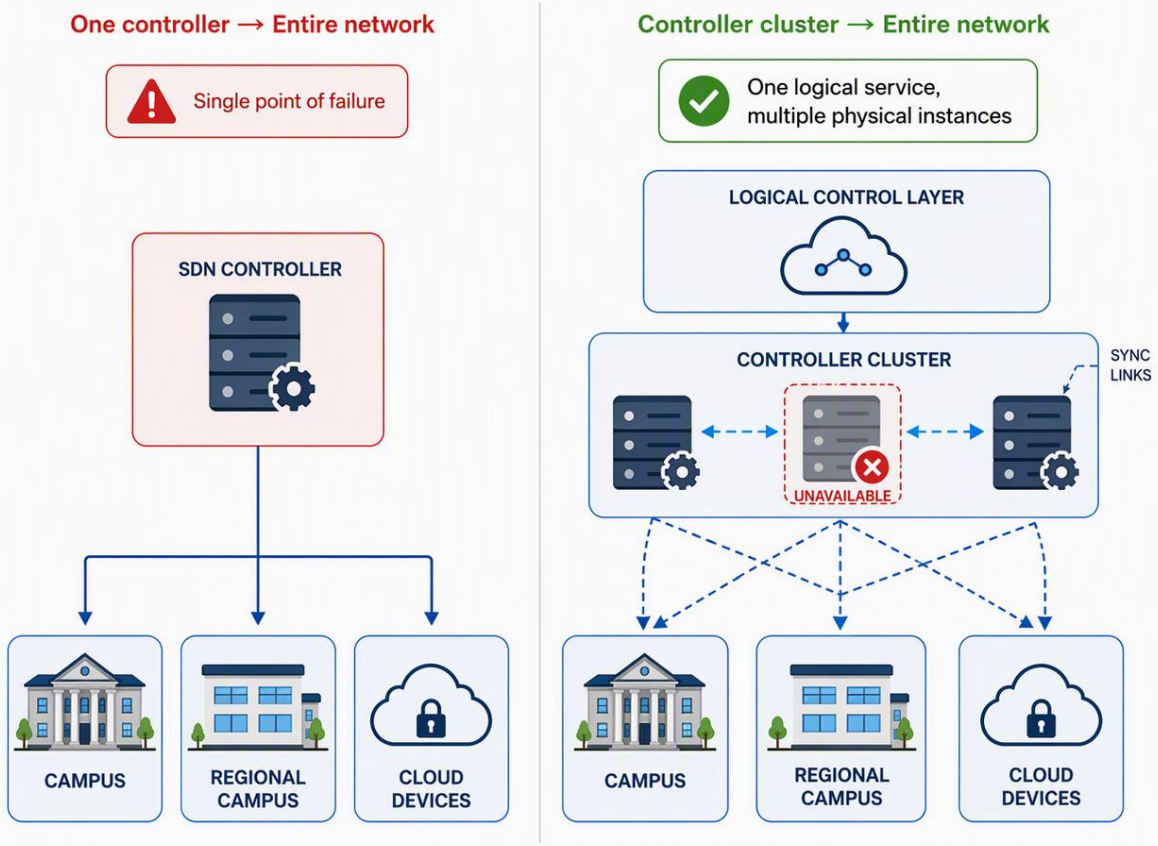
**Applications describe what is required. Devices receive how to implement it.**



# Logically centralised, but not one controller

- One logical network view
  - Applications interact with the controller as a coordinated system
- Multiple controller instances
  - Control services can be distributed across resilient nodes
- Synchronised state
  - Controllers maintain consistent topology, policy and device information
- Failover
  - Another controller continues control functions if one instance fails

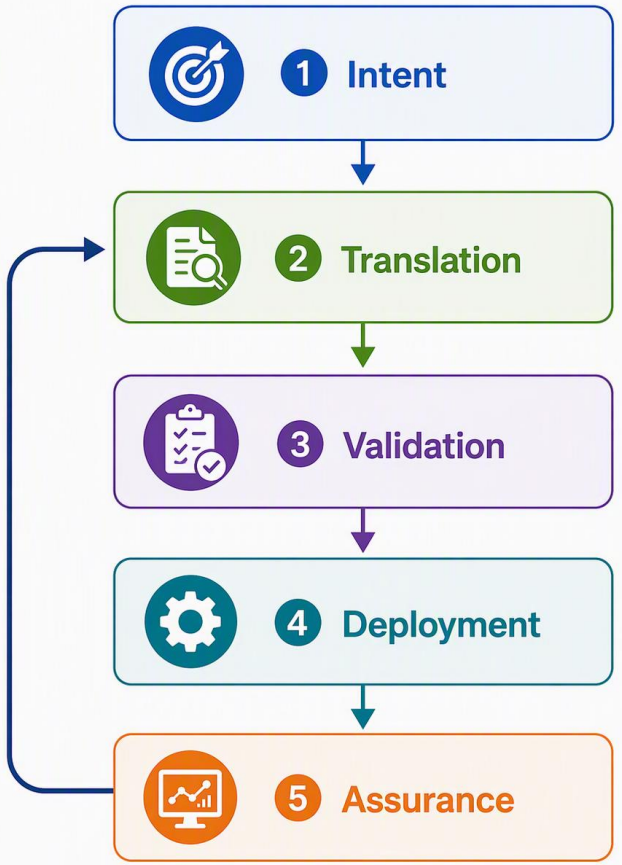
**Centralise the decision model, not the point of failure.**



# How does intent become network behaviour?

- Define the required outcome
- Translate intent into policy
- Validate against topology and constraints
- Deploy rules to enforcement points
- Assure the outcome using telemetry

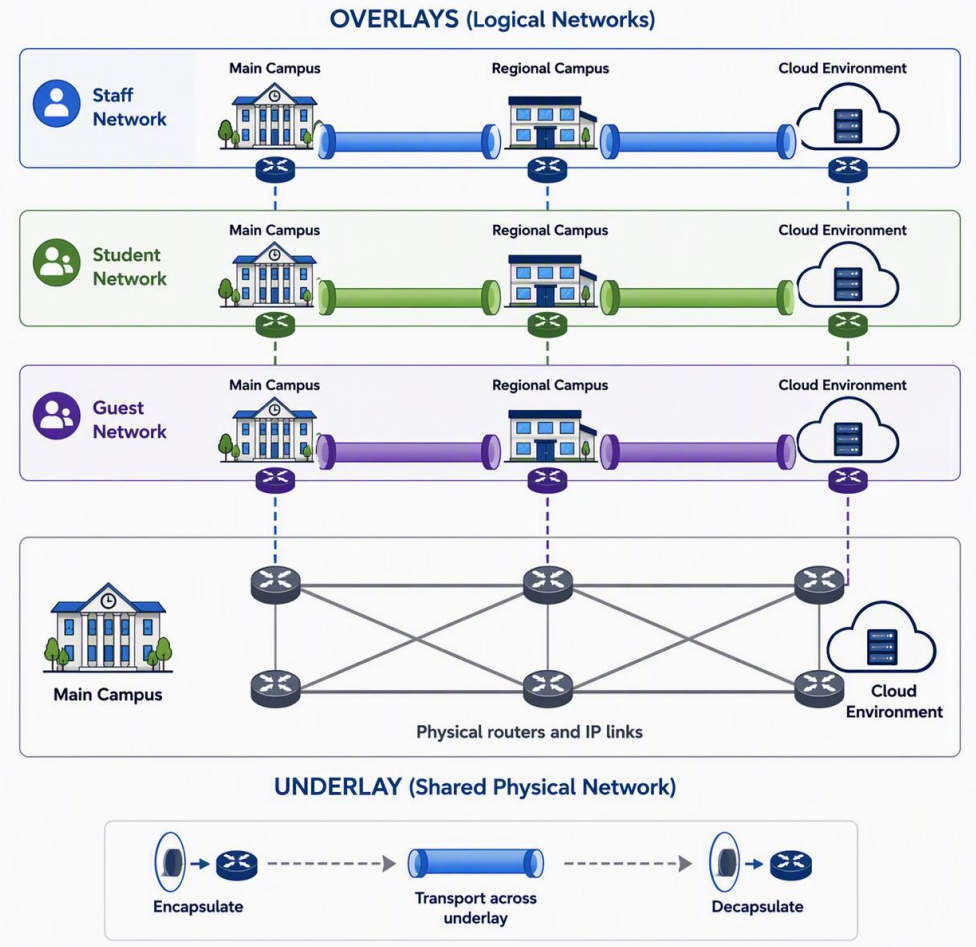
**Automation is incomplete until the result is verified.**



# One physical network, many logical networks

- Underlay
  - Provides physical and IP connectivity
- Overlay
  - Creates logical networks across the underlay
- Encapsulation
  - Carries overlay traffic between tunnel endpoints
- Policy
  - Controls segmentation and communication

**The underlay provides reachability.**
**The overlay provides logical structure.**



# SDN creates capability, not outcomes

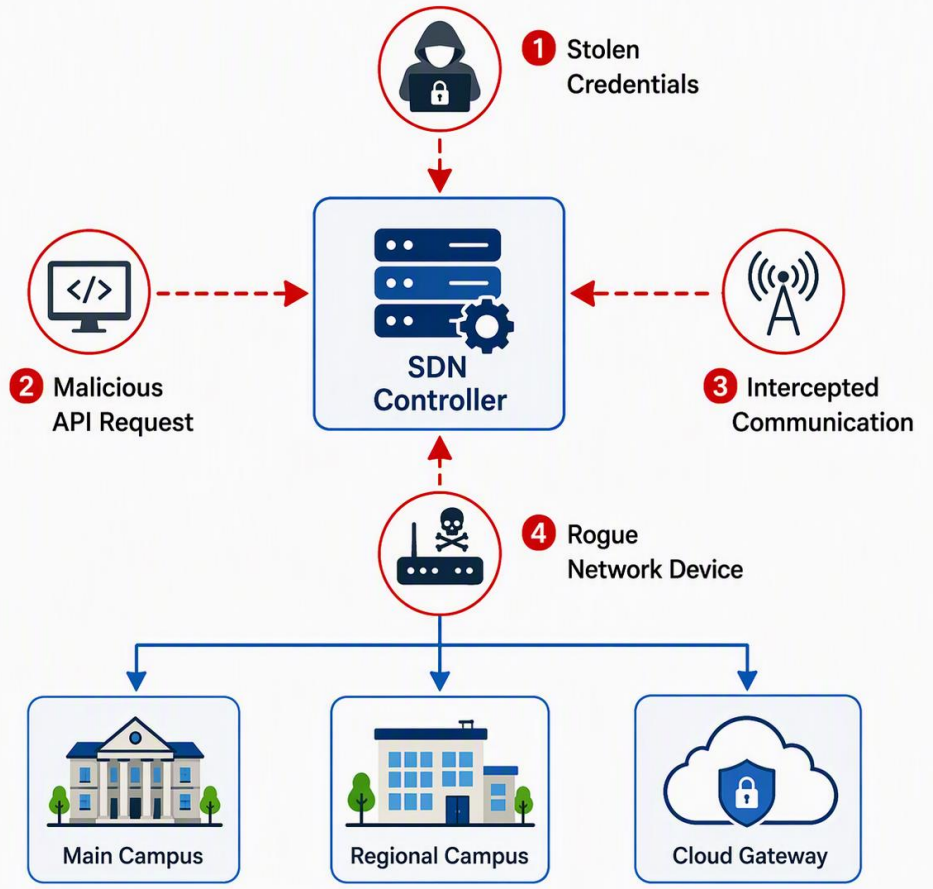
- SDN can improve
  - Consistent policy deployment
  - Network-wide automation and visibility
  - Rapid, repeatable configuration
  - Integration with orchestration platforms
- SDN does not eliminate
  - Architecture and engineering decisions
  - Legacy integration and interoperability issues
  - Testing, monitoring and troubleshooting
  - Security and operational risk

**Centralised control can distribute good decisions or bad decisions quickly.**

# Centralised control concentrates risk

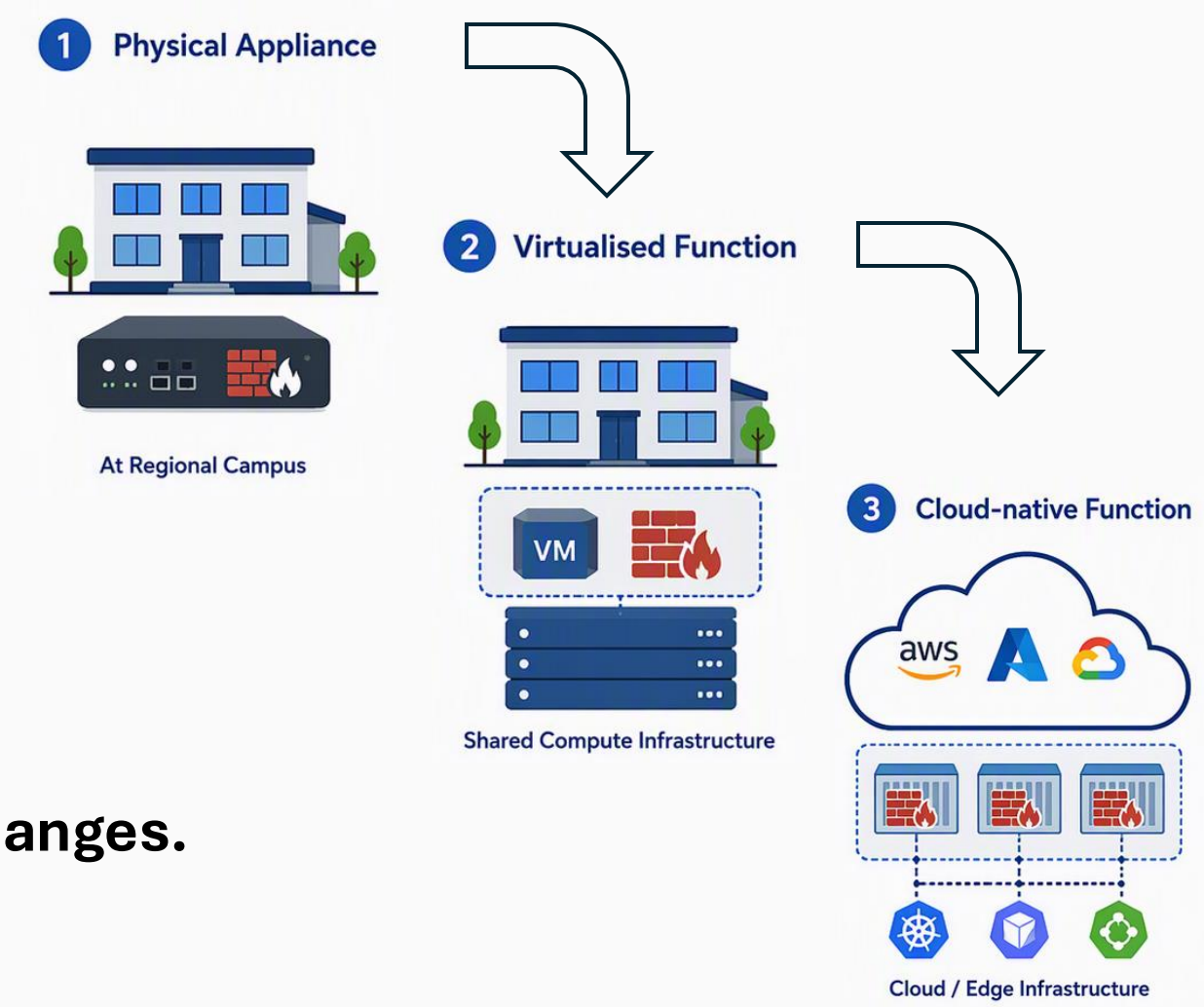
- Management access
  - Attackers may gain administrator-level control
- APIs
  - Compromised applications may request unsafe changes
- Controller communications
  - Intercepted or forged instructions may alter network behaviour
- Managed devices
  - Rogue devices may join or impersonate trusted components

**Compromise the controller, and one intrusion may affect the entire network.**



# From dedicated appliance to software function

- Physical network function
  - Purpose-built hardware appliance
- Virtualised network function
  - Software running in a virtual machine
- Cloud-native network function
  - Containerised components designed for cloud environments

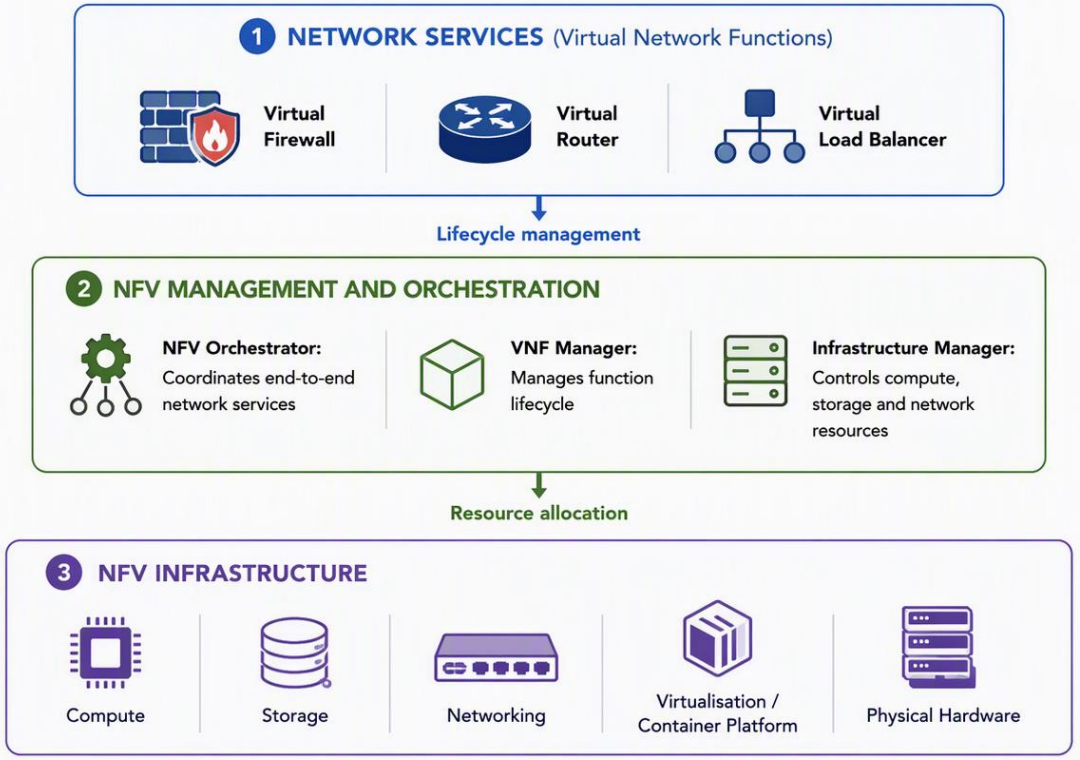



**The function remains.**
**How it is packaged and deployed changes.**

# NFV architecture

- Network functions
  - Software-based firewalls, routers and load balancers
- NFV infrastructure
  - Compute, storage, networking and virtualisation resources
- Management and orchestration
  - Deploys, scales, monitors and retires network services

**Software functions still require infrastructure and lifecycle management.**



# VNF lifecycle

- Instantiate
  - Deploy the function and allocate resources
- Scale
  - Adjust capacity as demand changes
- Heal
  - Recover or replace failed components
- Retire
  - Remove the function and release resources

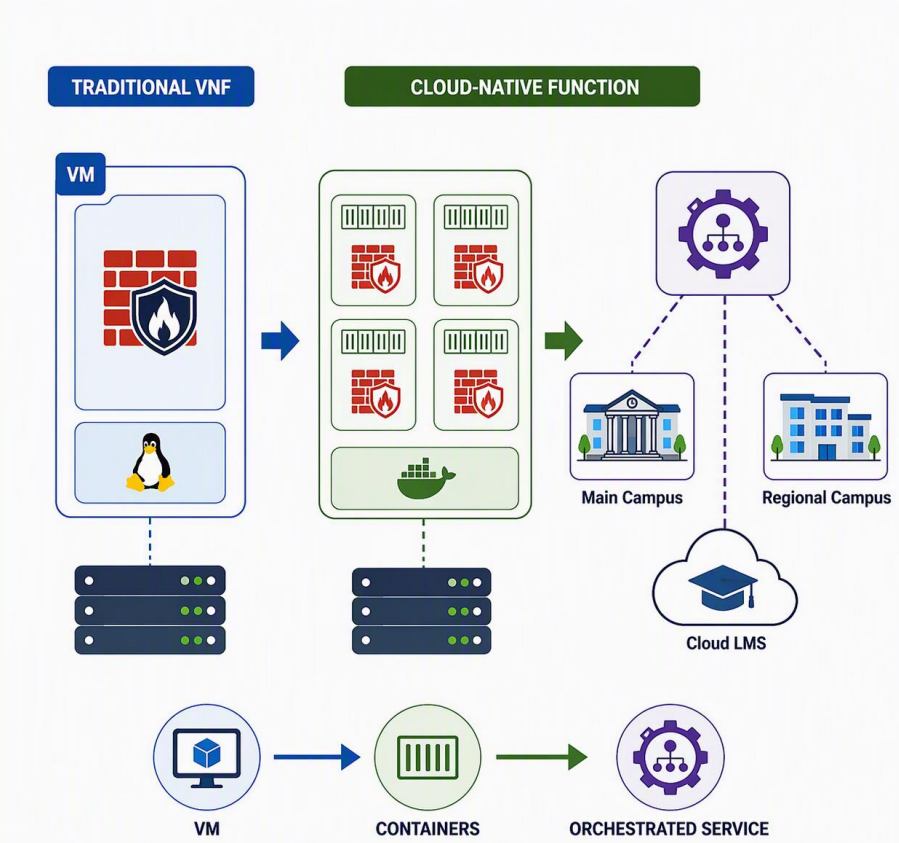
**Virtualisation enables flexibility. Orchestration makes it operational.**



# Network functions are becoming cloud-native

- Modular
  - Functions can be divided into smaller components
- Containerised
  - Workloads run on shared container infrastructure
- Scalable
  - Components can scale independently with demand
- Automated
  - APIs and CI/CD support faster lifecycle changes

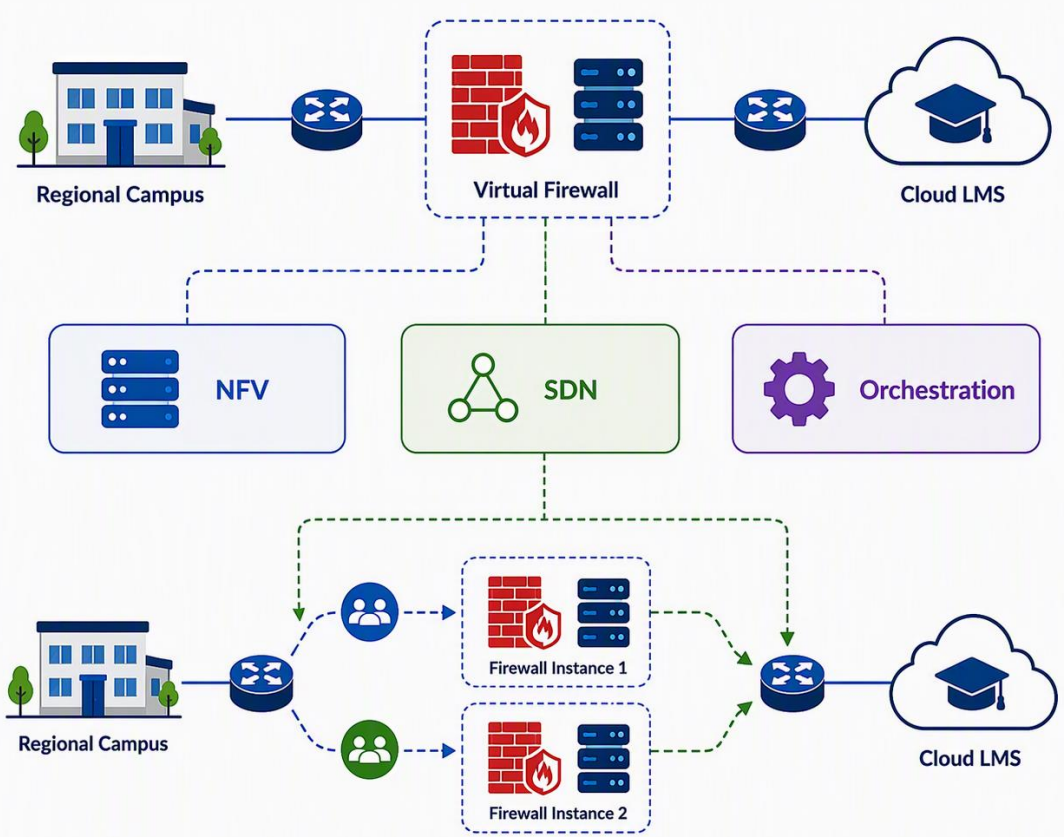
**Cloud-native is a design approach, not simply a different packaging format.**



# SDN and NFV solve different problems

- SDN controls the traffic
  - Creates connectivity, paths and forwarding policy
- NFV delivers the service
  - Deploys firewalls, routers and other functions as software
- Orchestration coordinates both
  - Connects functions, allocates resources and manages lifecycle

**NFV creates the function.**
**SDN steers traffic through it.**

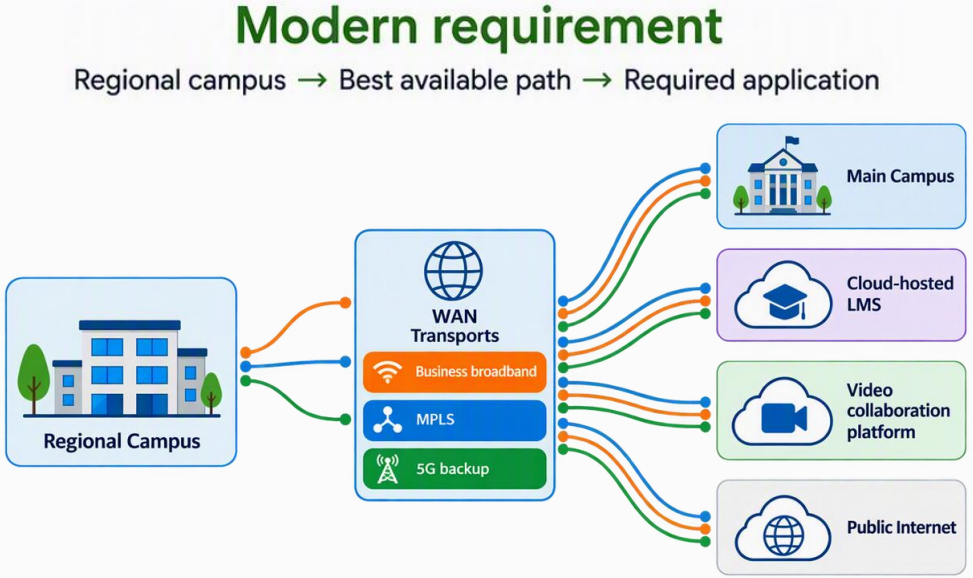


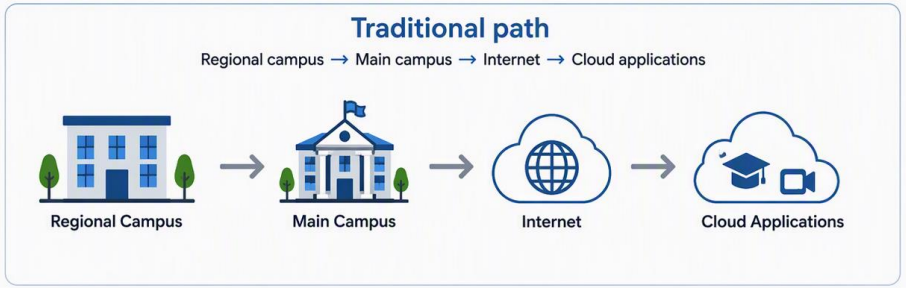

Peek Demand:
Second firewall instance added

# The regional campus needs cloud connectivity

- The LMS and collaboration tools are cloud-hosted
- Users need direct, reliable application access
- One WAN link may not provide sufficient resilience
- Different applications have different performance needs

**The WAN must connect locations, users and clouds, not just buildings.**

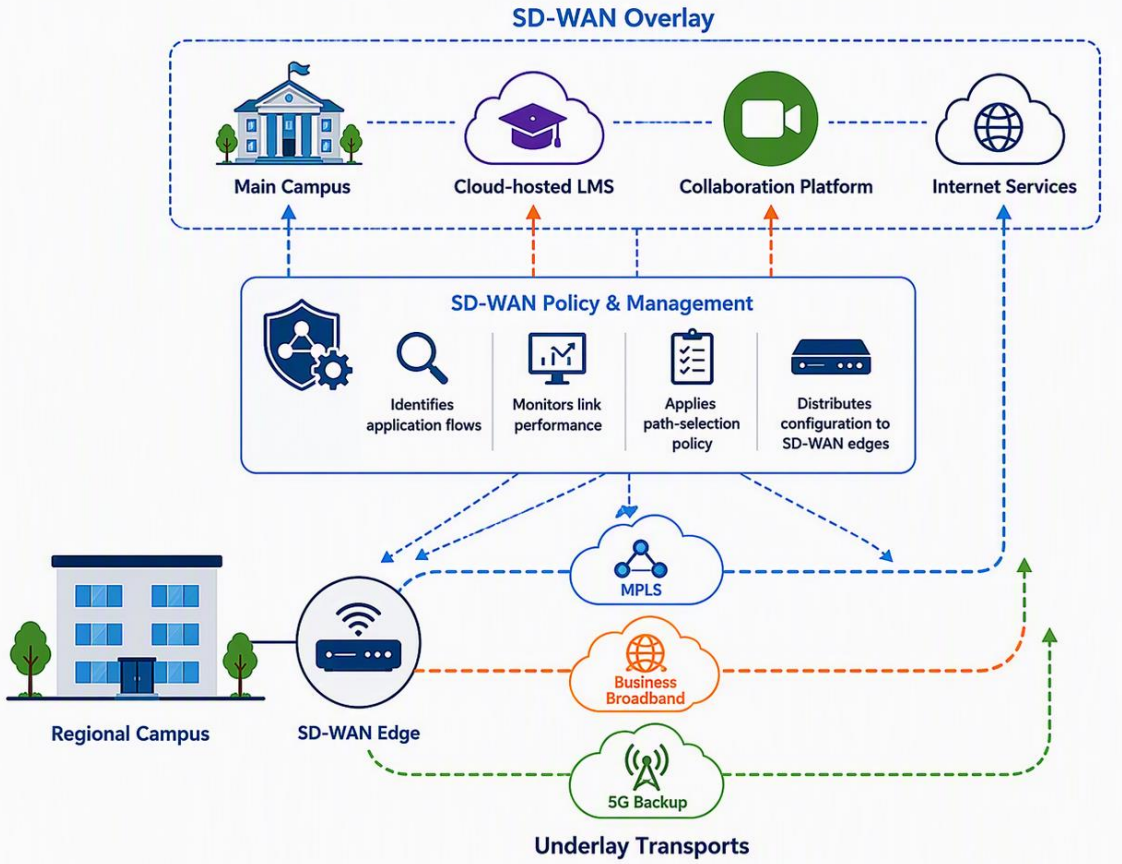


# SD-WAN, policy across multiple connections

- Underlays
  - Broadband, MPLS and 5G provide physical connectivity
- Overlay
  - Secure logical connections link sites and cloud services
- Policy
  - Applications receive different path, priority and security treatment
- Visibility
  - Path performance is continuously measured

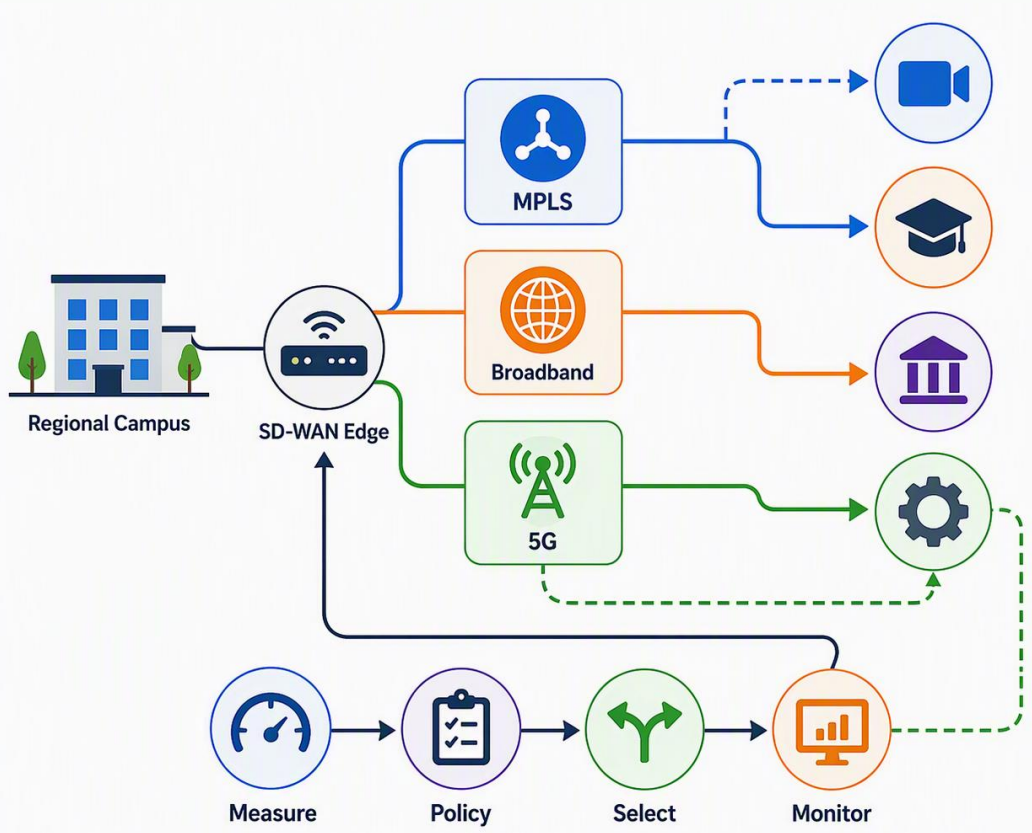
**The underlay provides connectivity. SD-WAN decides how to use it.**



# Different applications need different paths

- Identify
  - Recognise the application flow
- Measure
  - Monitor latency, loss, jitter and availability
- Match
  - Compare each path against application requirements
- Steer
  - Use the best policy-compliant available path

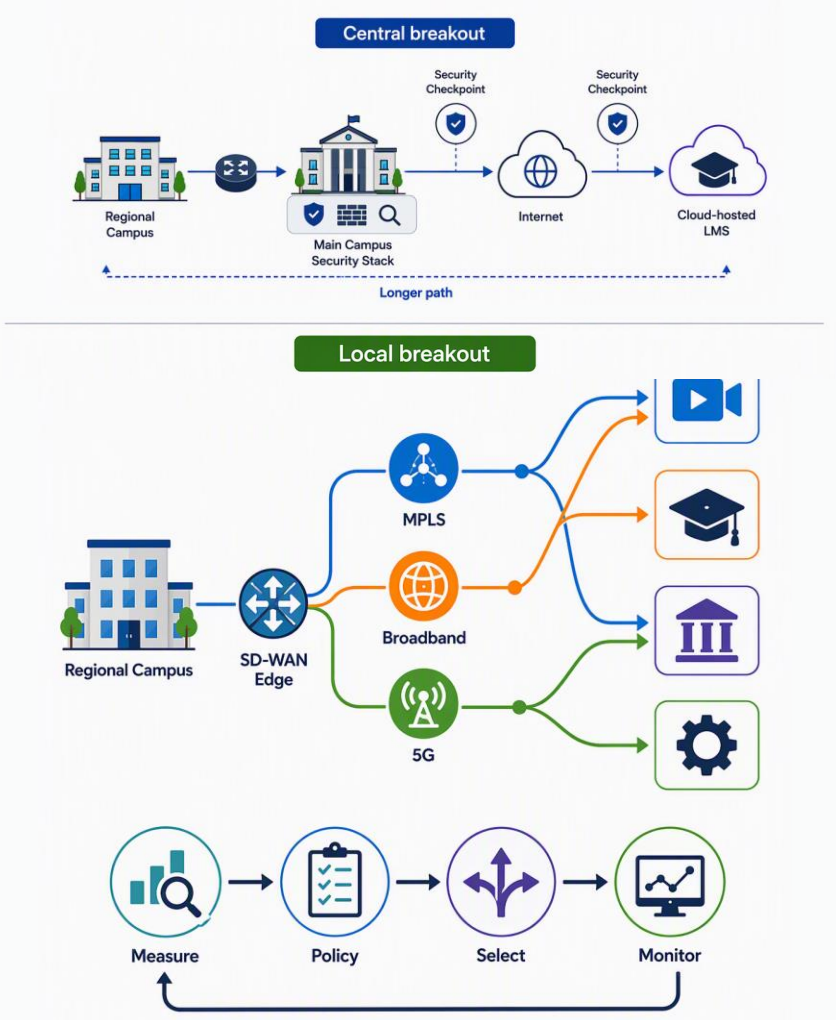
**The shortest path is not always the best application path.**



# Direct cloud access changes the security path

- Central breakout
  - Traffic passes through central security controls
- Local breakout
  - Traffic exits directly from the regional campus
- Benefit
  - Reduced backhaul and improved cloud access
- Trade-off
  - Security controls must follow the traffic

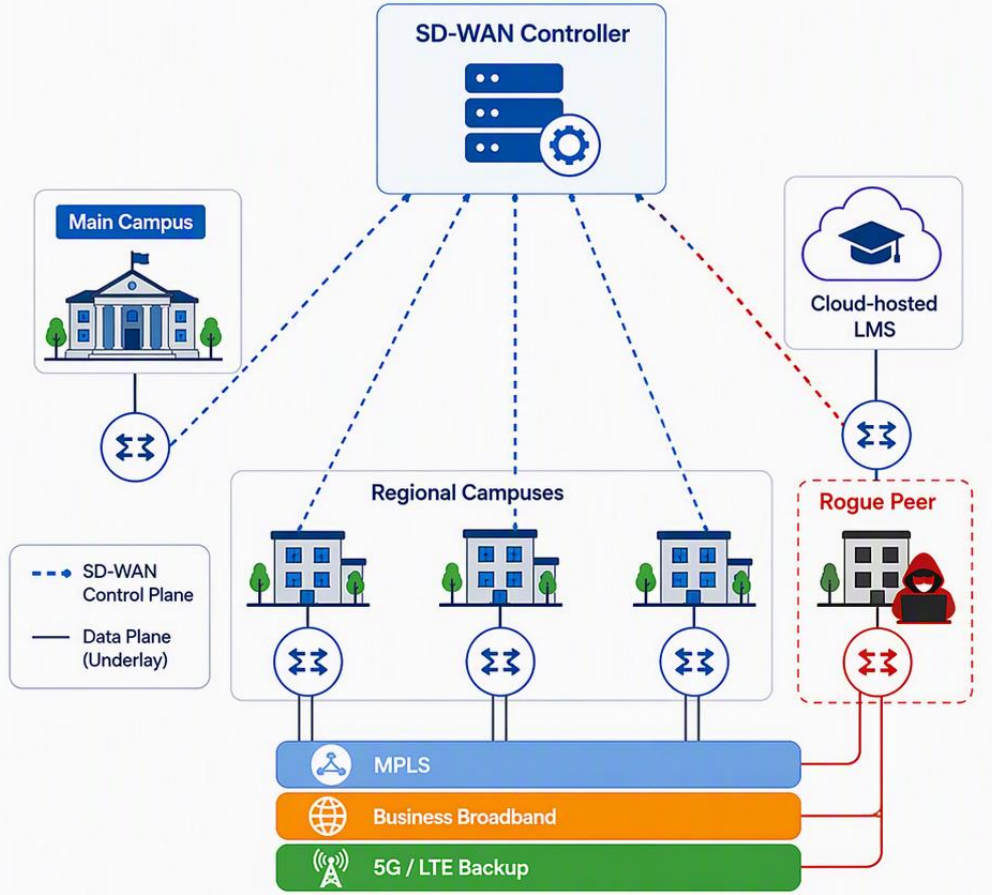
**A shorter path must still be a secure path.**



# One compromised controller affects every site

- Initial access
  - Exploit the SD-WAN control system
- Trusted presence
  - Add a rogue peer that appears legitimate
- Privilege
  - Gain elevated access and persistence
- Network-wide impact
  - Manipulate connectivity, configuration and visibility

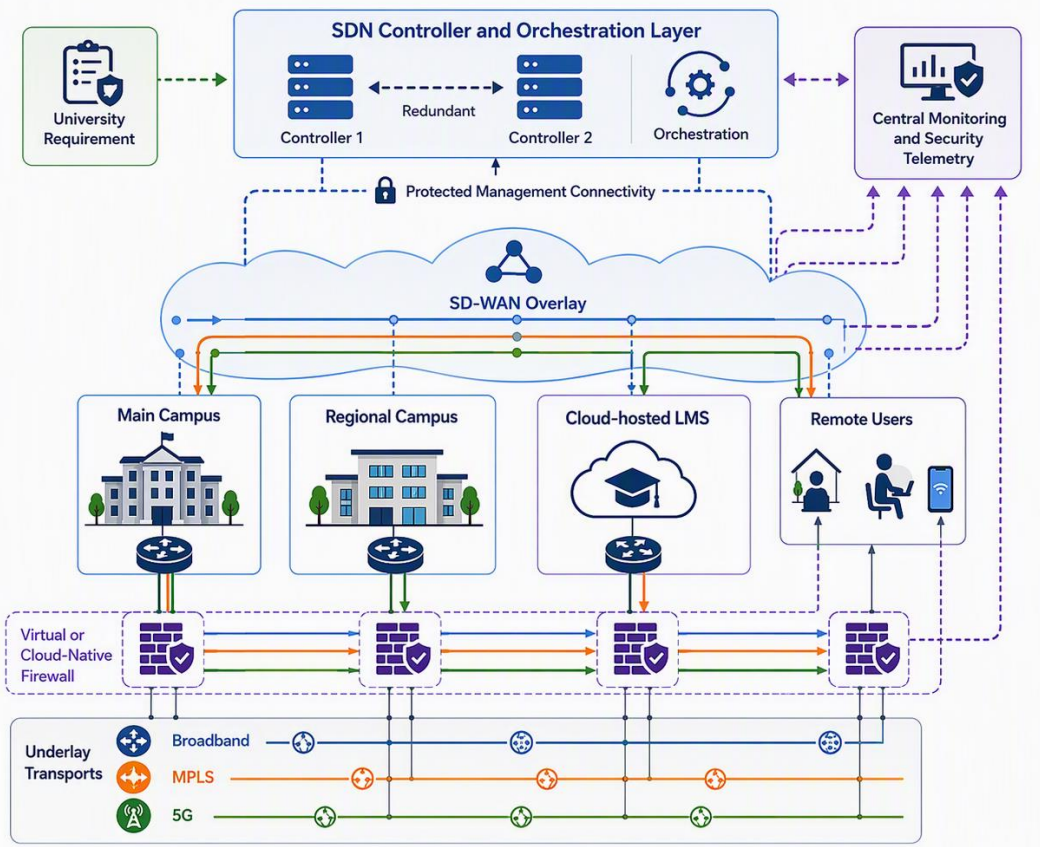
**Centralised control creates centralised trust.**



# Bring the paradigms together

- SDN
  - Apply consistent network and segmentation policy
- NFV
  - Deliver security and network functions as software
- SD-WAN
  - Connect campuses and cloud services across resilient paths
- Operations and security
  - Monitor, validate, protect and recover the complete service

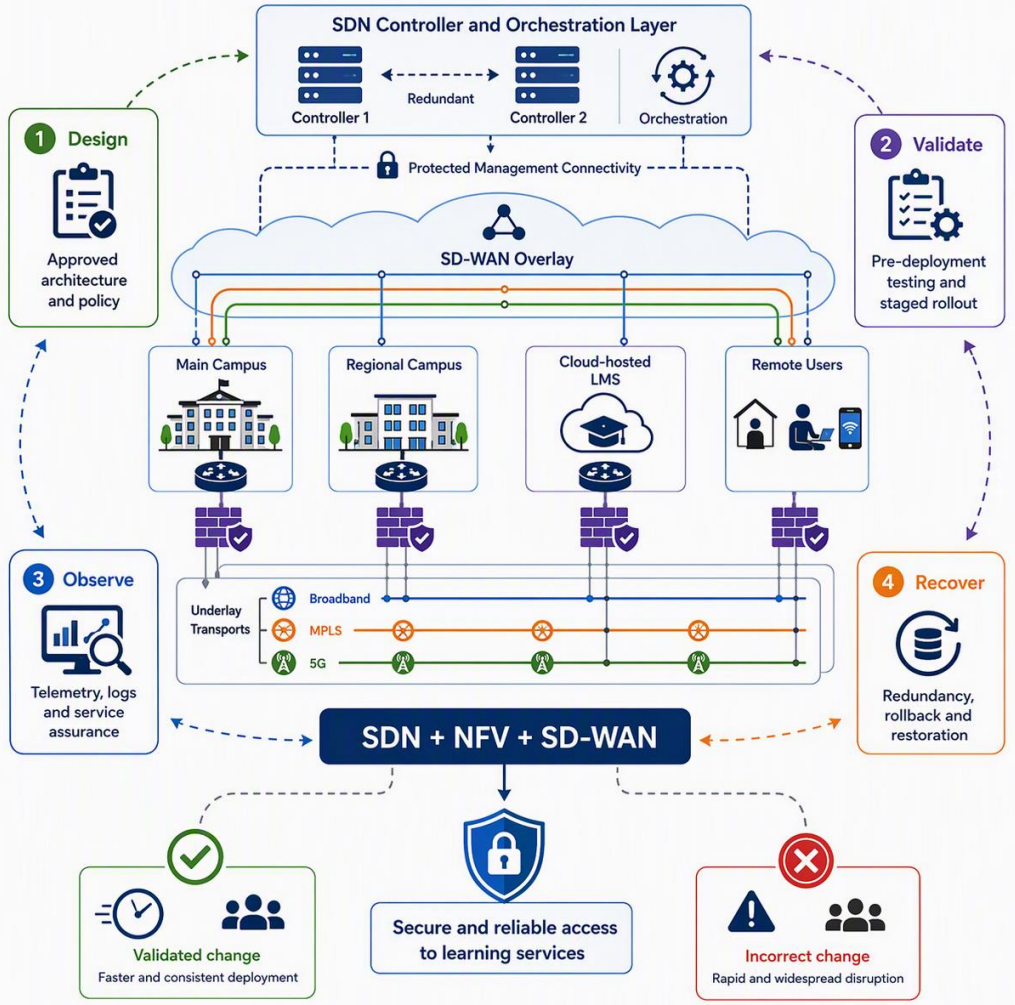
**A successful design coordinates control, functions and connectivity.**



# Software-driven networking needs engineering

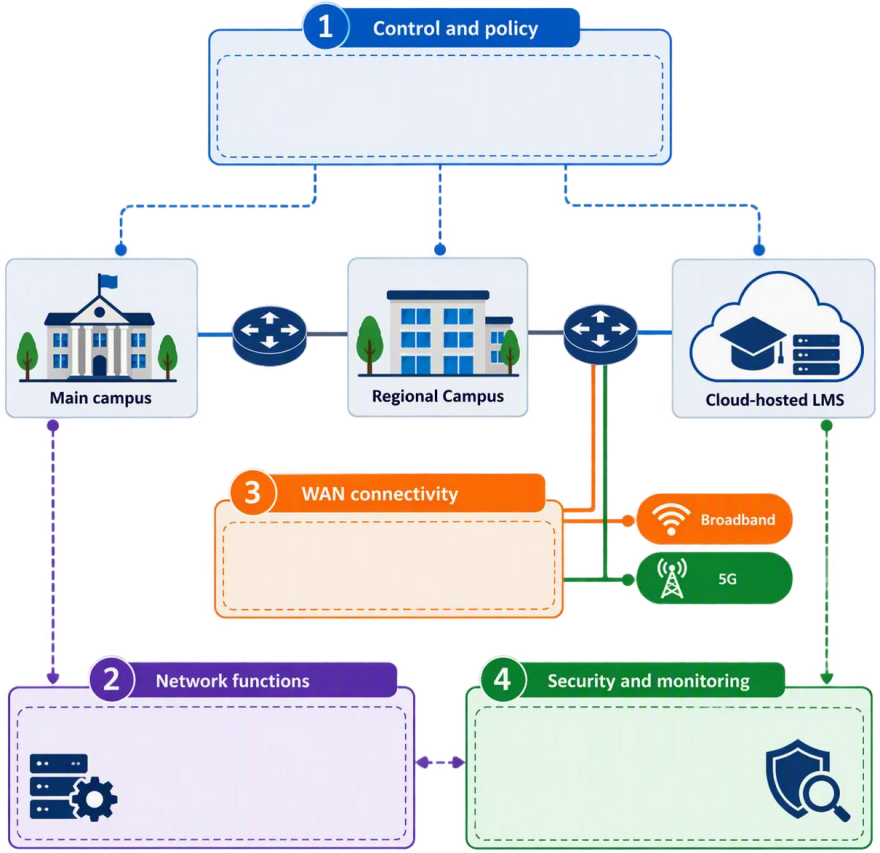
- Design
  - Define clear architecture, policy and service outcomes
- Validate
  - Test changes before broad deployment
- Observe
  - Monitor performance, security and policy compliance
- Recover
  - Maintain redundancy, rollback and incident-response capability

**Automation increases speed.**
**Engineering provides control.**



# Take-Home Group Design Assignment:
## Design the University's New Regional Campus Network

- Design a secure, resilient network using:
  - SDN for policy and network control
  - NFV for software-based network functions
  - SD-WAN for campus and cloud connectivity
  - Monitoring and security for assurance and recovery
- In groups, you will deliver a 3-min presentation
  - Explain your design, justify your choices and identify the main trade-off.



# Assignment Groups

- Group design constraints:
  - Group 1: Limited budget
    - Minimise dedicated hardware and recurring connectivity costs.
  - Group 2: High availability
    - Live teaching must continue if the primary WAN link fails.
  - Group 3: Sensitive information
    - Administrative traffic requires stronger security and monitoring.
  - Group 4: Rapid expansion
    - The design must support five additional learning centres.
  - Group 5: Limited technical support
    - The regional centre has no permanent on-site network engineer.

- Group allocation formula
  - Sort the NT student list by Index Number.
  - Take your position in the list, calculate position MOD 5, then add 1 to get your group number.

*Group number = (your position in the NT student list, sorted by Index Number, modulo 5) + 1*

# Questions?

