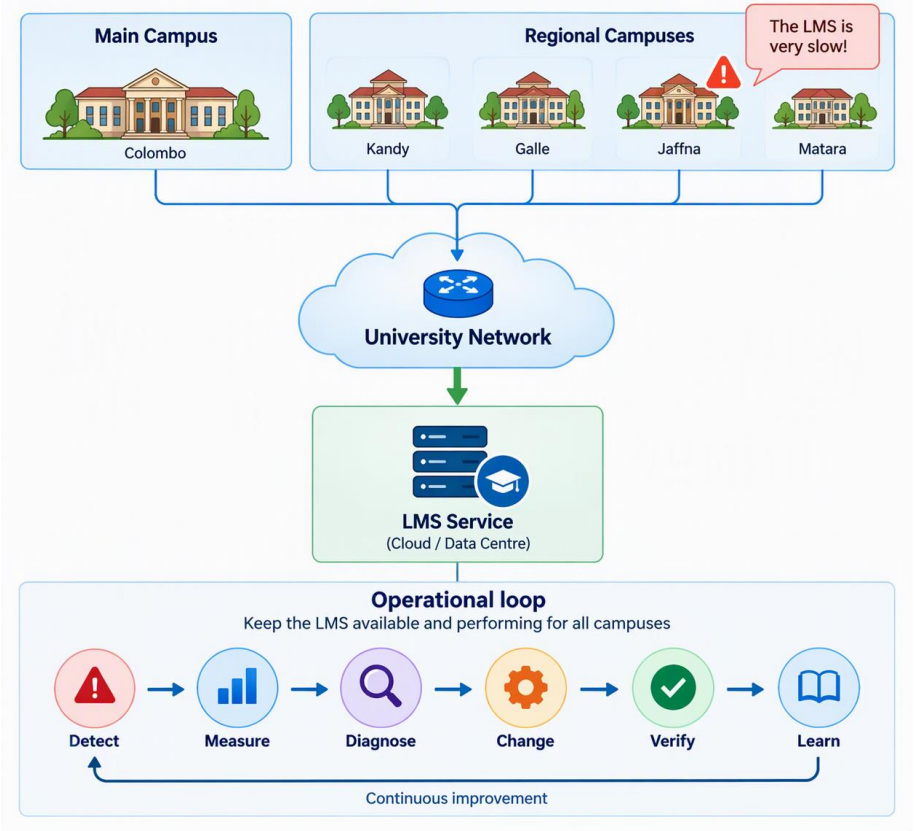
Network Management and Operations

ITN 4252 Advanced Topics in Networking

Partially based on PowerPoint slides for Computer Networking: A Top-Down Approach, 8th edition, Jim Kurose, Keith Ross, Pearson, 2020
and NOC Services and Applications by Sunday Folayan, Nishal Goburdhan, & Isatou Jah

How do we know what is happening?

- **… and what should we do next?**
- When a network service fails, operators must:
  - Detect the problem
  - Measure what is happening
  - Diagnose the likely cause
  - Change and verify safely
- **Keeping a network running requires visibility, control and operational judgement.**



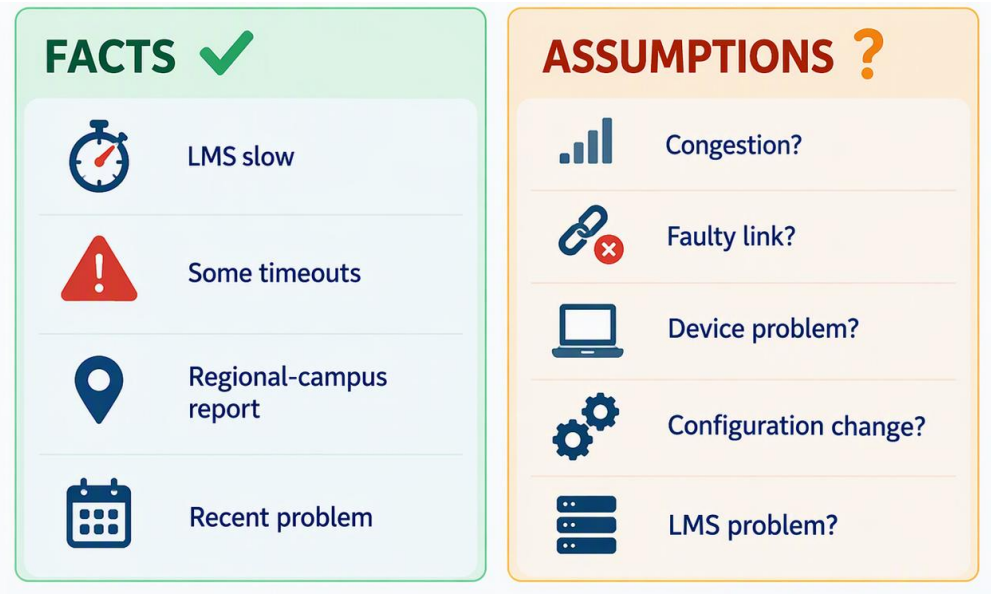
The LMS complaint

- ***“The LMS is suddenly very slow.”***
- A student at a regional campus reports:
  - Pages take much longer to load
  - Some requests appear to time out
  - Other Internet services seem normal
  - The problem started recently
- **Is this enough information to identify the network problem?**



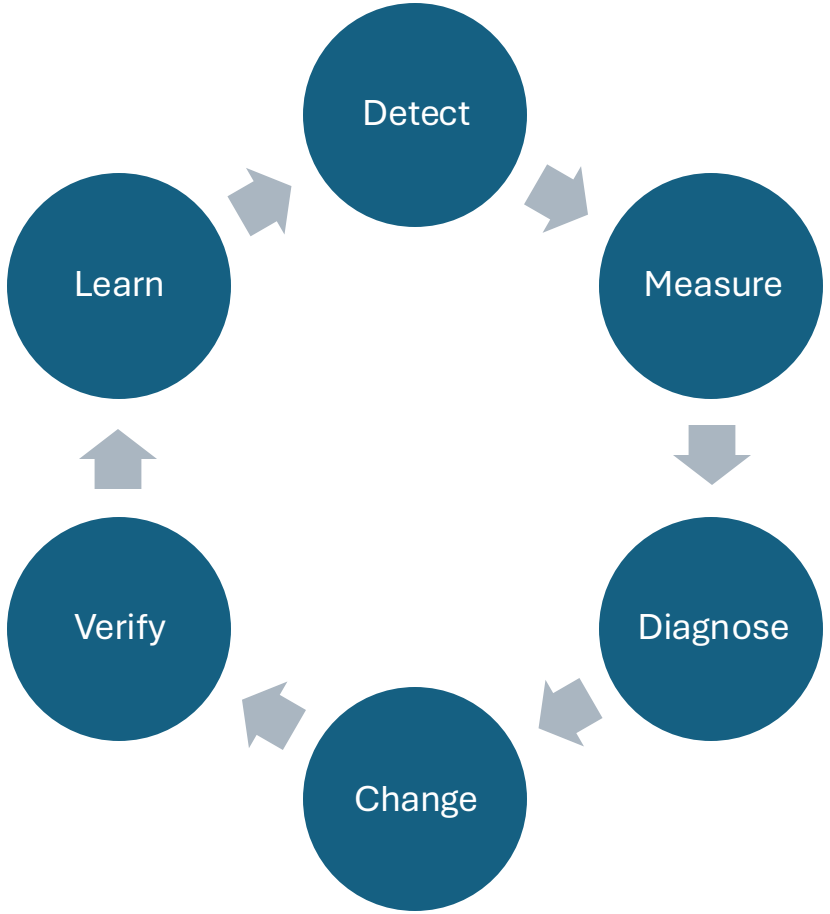
What do we know, and what are we assuming?

- Start with evidence, not assumptions
- Known
  - A regional-campus student reports a slow LMS
  - Some requests appear to time out
  - Other Internet services appear normal
  - The problem started recently
- Unknown
  - Scope, location and cause of the problem
- **A symptom tells us what the user experiences, not why it is happening.**



What you should be able to do

- By the end of this lecture, you should be able to:
  - **Identify** useful network-management evidence
  - **Explain** SNMP, telemetry and model-driven management
  - **Diagnose** problems using multiple operational signals
  - **Plan** a controlled configuration change
  - **Verify** recovery and identify opportunities for automation
- **Good operations turns observations into evidence-based action.**



Network management vs. Network operations

- Management provides capability, operations uses it
- Network Management
  - Monitor network state and performance
  - Configure devices and services
  - Collect operational data
  - Control network resources
- Network Operations
  - Detect and troubleshoot problems
  - Respond and make changes
  - Verify service recovery
  - Maintain reliable service
- **Management provides the tools and visibility; operations turns them into action.**



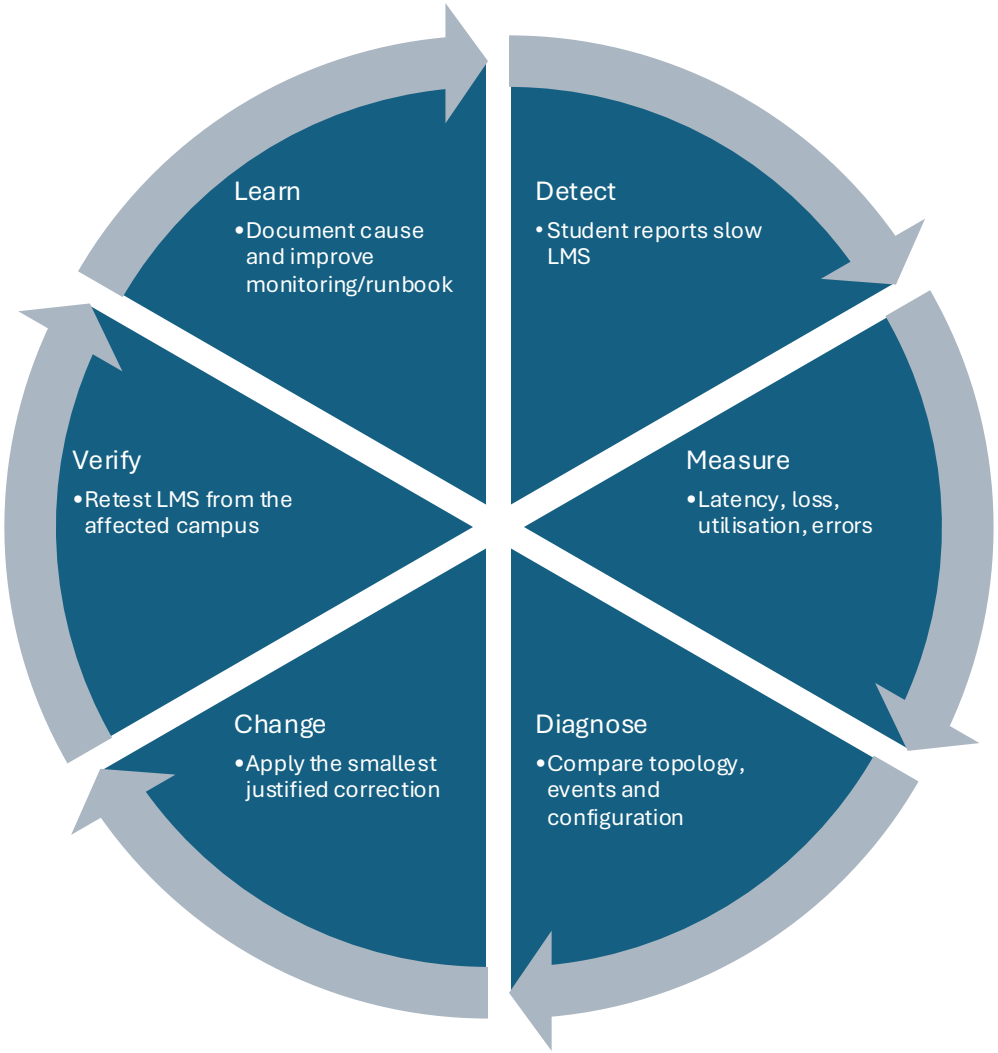
FCAPS: A lens for network management

- FCAPS organises network management into five areas
  - **Fault**: Detect, isolate and restore failures
  - **Configuration**: Manage and track network changes
  - **Accounting**: Measure resource and service usage
  - **Performance**: Monitor service quality and capacity
  - **Security**: Protect management and network resources
- **FCAPS classifies the work, it does not replace the operational workflow.**



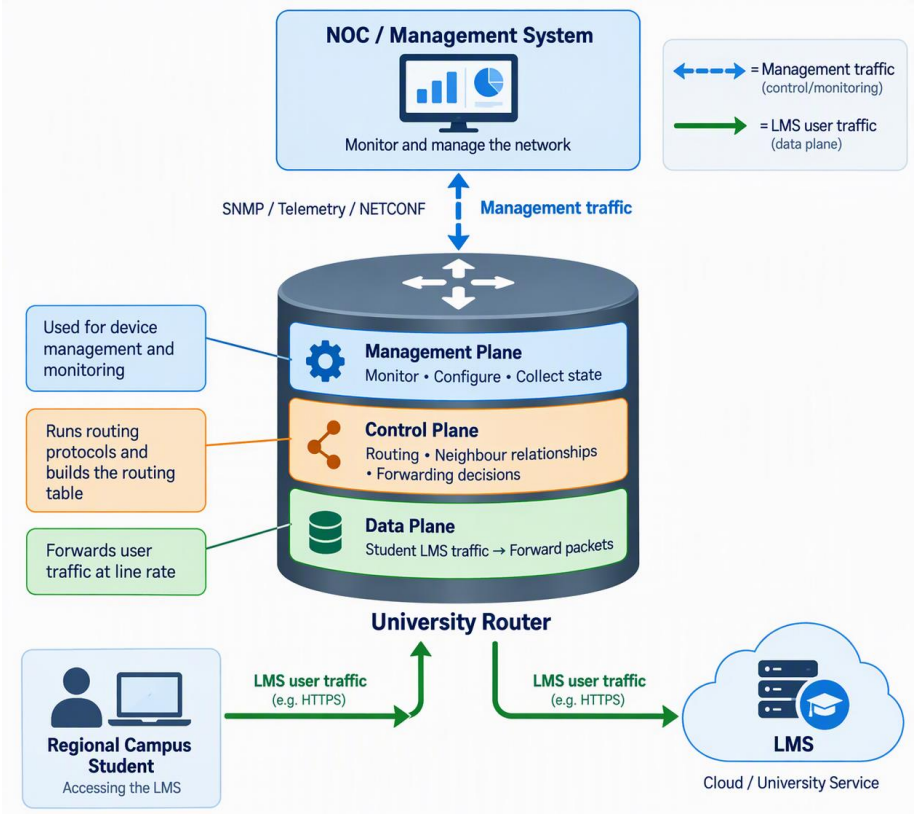
The operational lifecycle

- From problem report to verified recovery
  1. **Detect**: Identify service impact
  2. **Measure**: Collect relevant evidence
  3. **Diagnose**: Determine the likely cause
  4. **Change**: Apply a controlled correction
  5. **Verify**: Confirm service recovery
  6. **Learn**: Document and improve
- **Troubleshooting is a closed loop, not *“change something and hope”*.**



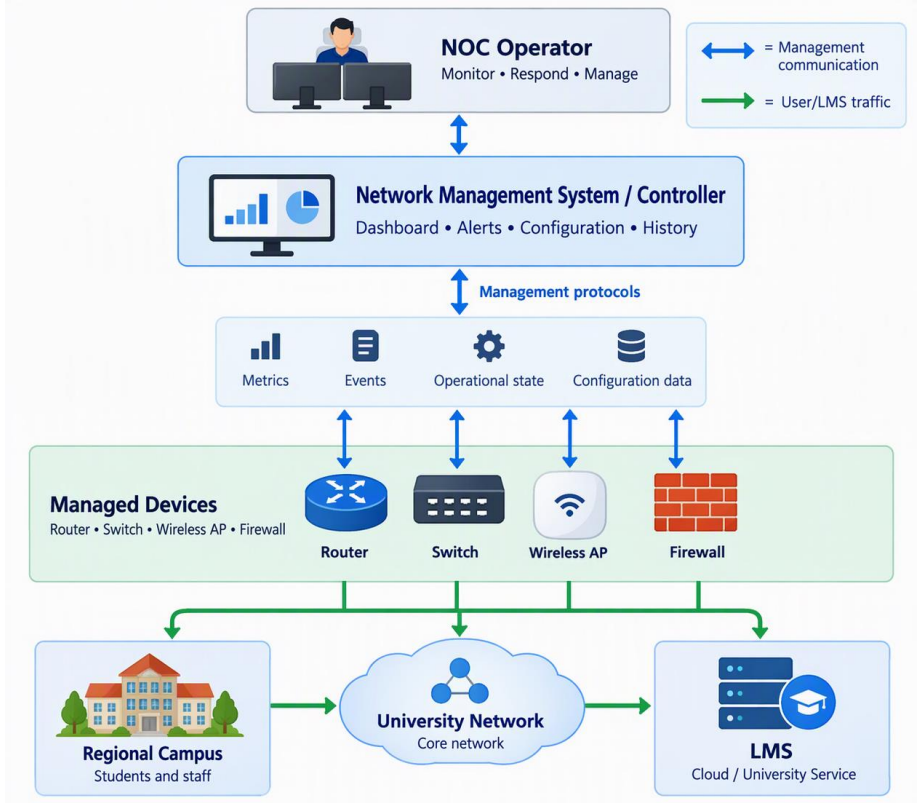
The management plane

- The management plane observes and controls the network
  - **Data plane**: Forwards user traffic
  - **Control plane**: Determines network paths and forwarding state
  - **Management plane**: Monitors, configures and administers devices
  - Management traffic should remain separate from normal user activity where practical
- **The LMS uses the network; the management plane helps operators understand and control it.**



The network management architecture

- Management connects devices, data and people
  - **Managed devices**: Routers, switches, wireless APs and other infrastructure
  - **Management system**: Collects, stores and presents network information
  - **Management data**: Metrics, events, configuration and operational state
  - **Operators**: Interpret evidence and decide what action to take
- **Devices provide evidence; management systems organise it; people make operational decisions.**



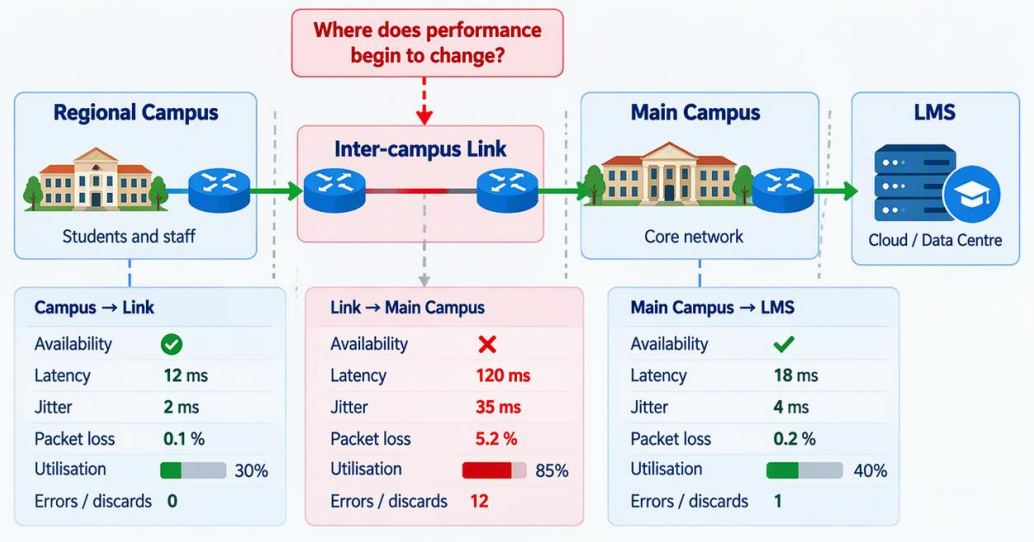
Symptoms, causes and evidence

- A symptom is not the root cause
  - **Symptom**: What the user or service experiences
  - **Hypothesis**: A possible explanation to test
  - **Evidence**: Measurements and state that support or reject it
  - **Diagnosis**: The explanation best supported by the evidence
- **Do not change the network until the evidence supports the hypothesis.**



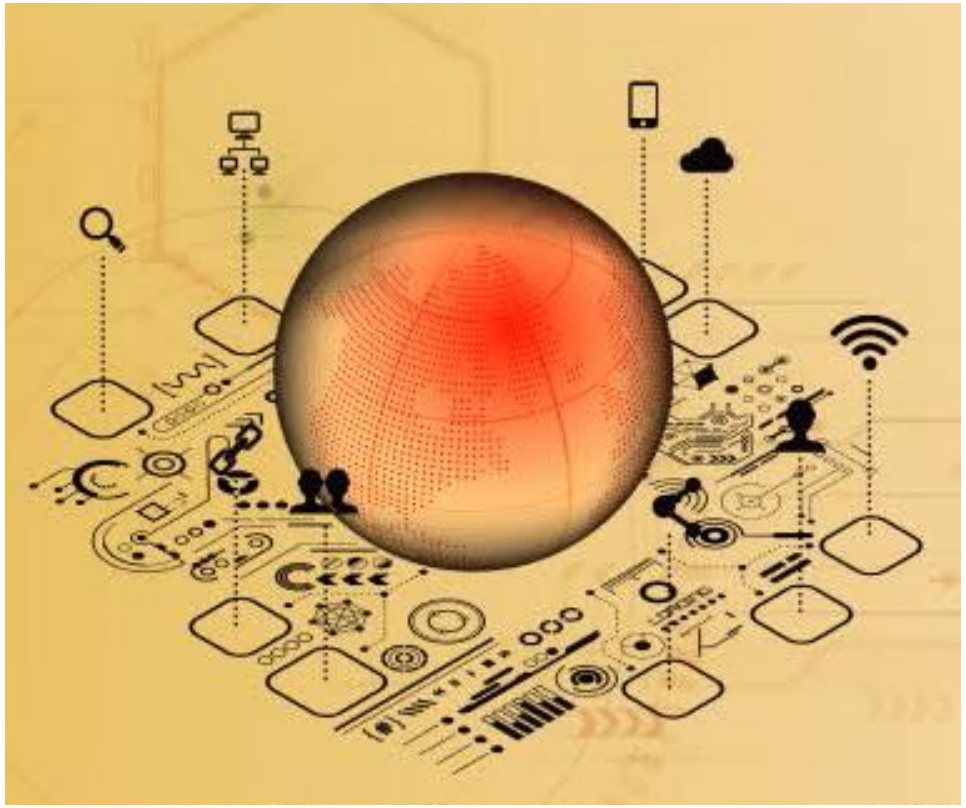
Operational metrics that matter

- Measure the network from the user's perspective
  - **Availability**: Is the service reachable?
  - **Latency & jitter**: How long does traffic take, and how consistent is it?
  - **Packet loss**: How much traffic fails to arrive?
  - **Throughput & utilisation**: How much capacity is being used?
  - **Errors & discards**: Is traffic being lost inside the network?
- **Choose metrics that help explain the symptom.**



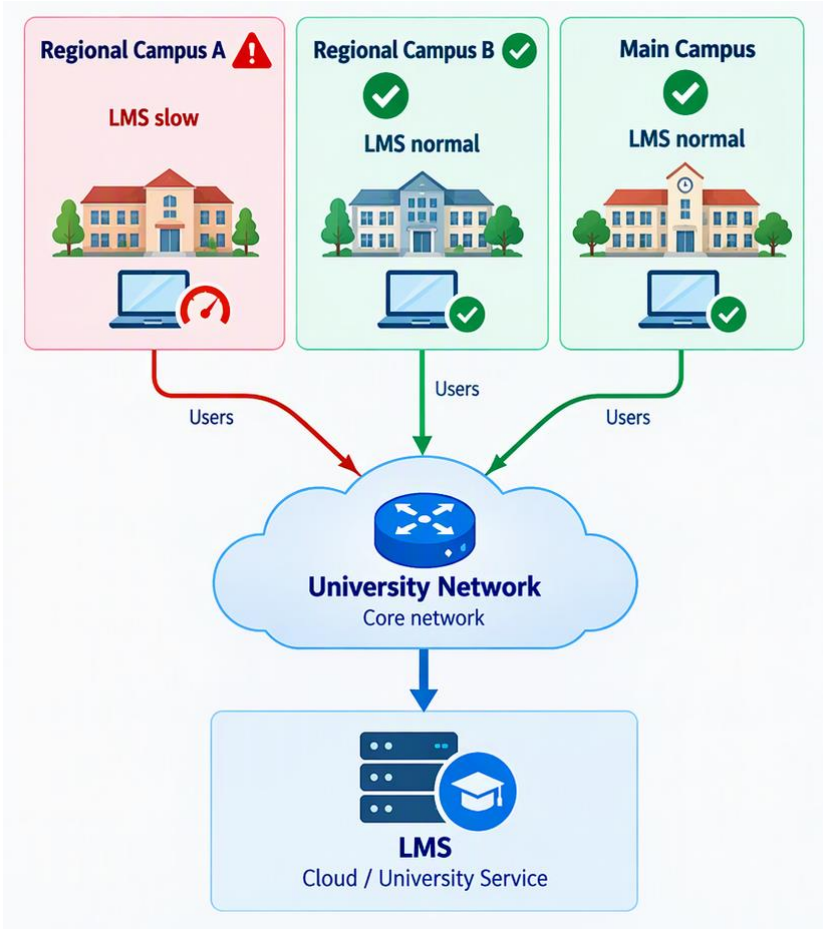
Observability: build the complete picture

- No single signal tells the whole story
- Combine different sources of evidence:
  - **Metrics**: Performance and device health
  - **Logs & events**: What happened and when
  - **Traffic flows**: Who is communicating and how much
  - **Topology & configuration**: How the network is built and configured
  - **Active tests**: Test reachability and the network path
- **Observability comes from connecting evidence, not watching one dashboard.**



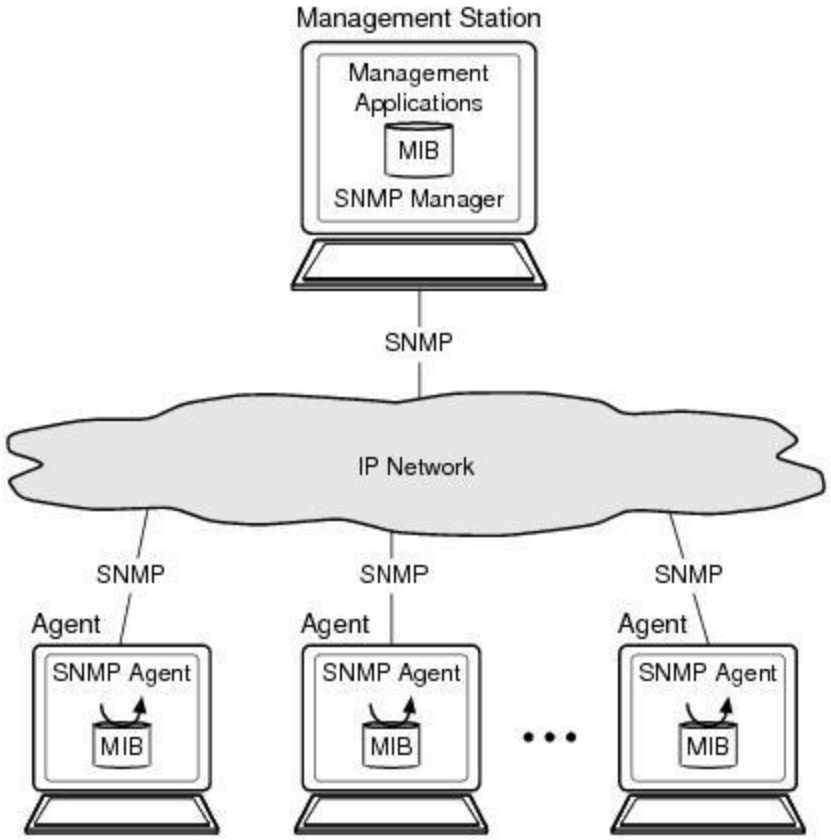
Which evidence would you collect first?

- The first measurement should test the scope.
- The LMS is slow at one regional campus.
- What should we check first?
  - **Compare** affected and unaffected campuses
  - **Test** LMS reachability, latency and packet loss
  - **Check** the network path and interface health
  - **Review** recent events and configuration changes
- **Start broad enough to locate the problem, then narrow the investigation.**



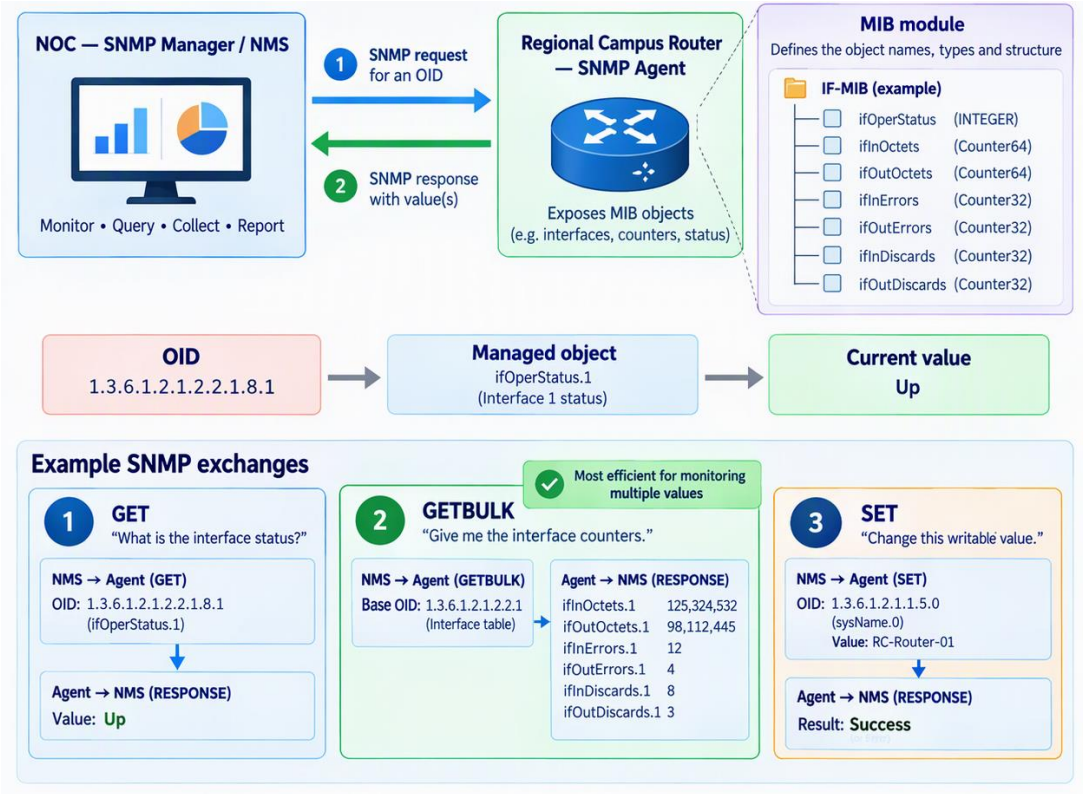
Simple Network Management Protocol (SNMP)

- SNMP retrieves structured management data
  - **Manager / NMS**: Requests and receives management information
  - **Agent**: Exposes management data on the managed device
  - **MIB module**: Defines related managed objects and their structure
  - **OID**: Uniquely identifies a managed object
  - **Object value**: Reports the device's current state or counter
- **The manager requests an OID; the agent returns its current value.**



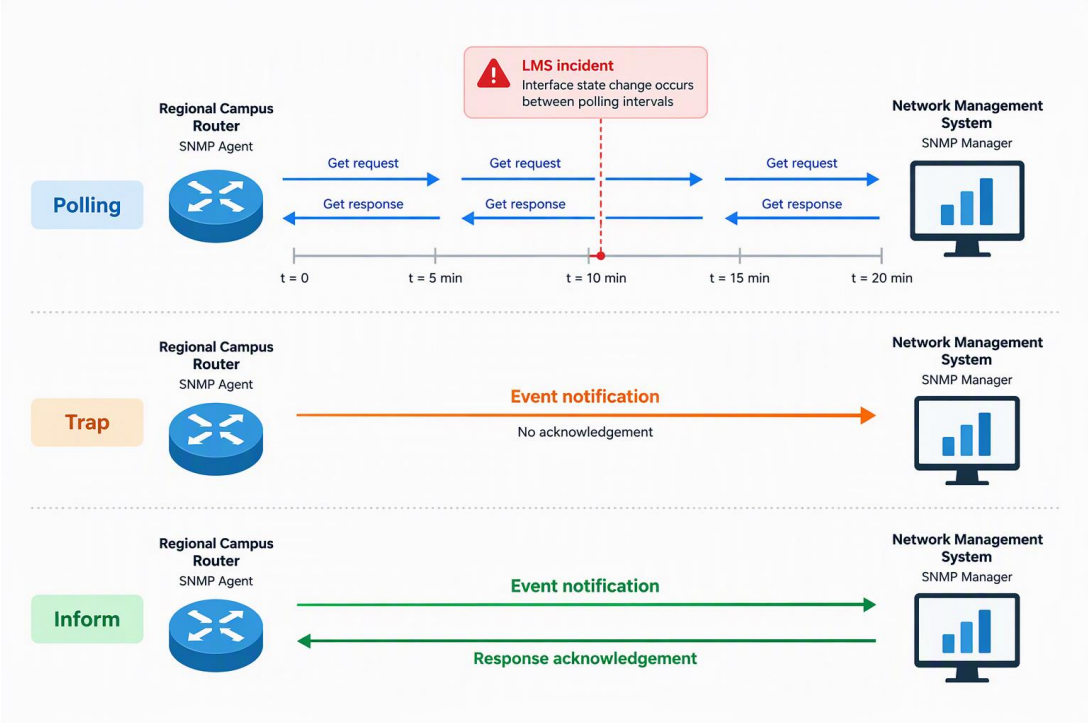
SNMP operations: retrieve and change values

- SNMP uses simple operations on managed objects
  - GET: Retrieve a specific object value
  - GETNEXT / GETBULK: Retrieve multiple related values efficiently
  - SET: Request a change to a writable object
  - RESPONSE: Return values or the result of a request
- **SNMP identifies the object by OID, the operation determines what happens to it.**



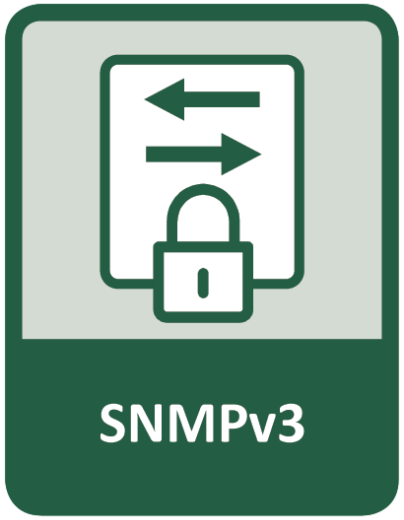
Polling, traps and informs

- SNMP learns about change in two ways
  - **Polling**: Manager requests values at regular intervals
  - **Trap**: Device sends an event notification with no acknowledgement
  - **Inform**: Device sends a notification and expects a response
- **Polling shows ongoing state; notifications highlight events. Use them together.**



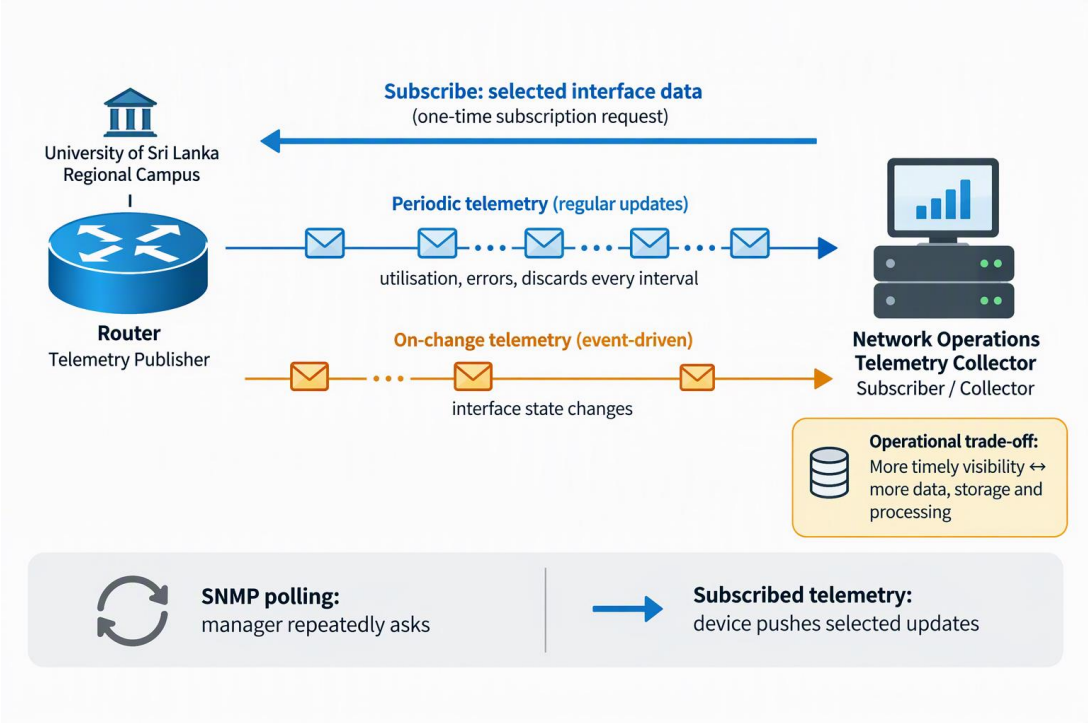
SNMPv3 security and practical limits

- Management data and access must be protected
  - **SNMPv1/v2c**: Community-based access; limited security
  - **noAuthNoPriv**: No authentication or privacy
  - **authNoPriv**: Authentication and integrity; no privacy
  - **authPriv**: Authentication, integrity and privacy
  - **Access control**: Restricts which objects may be read or changed
- **SNMPv3 adds security, but monitoring still requires careful design.**



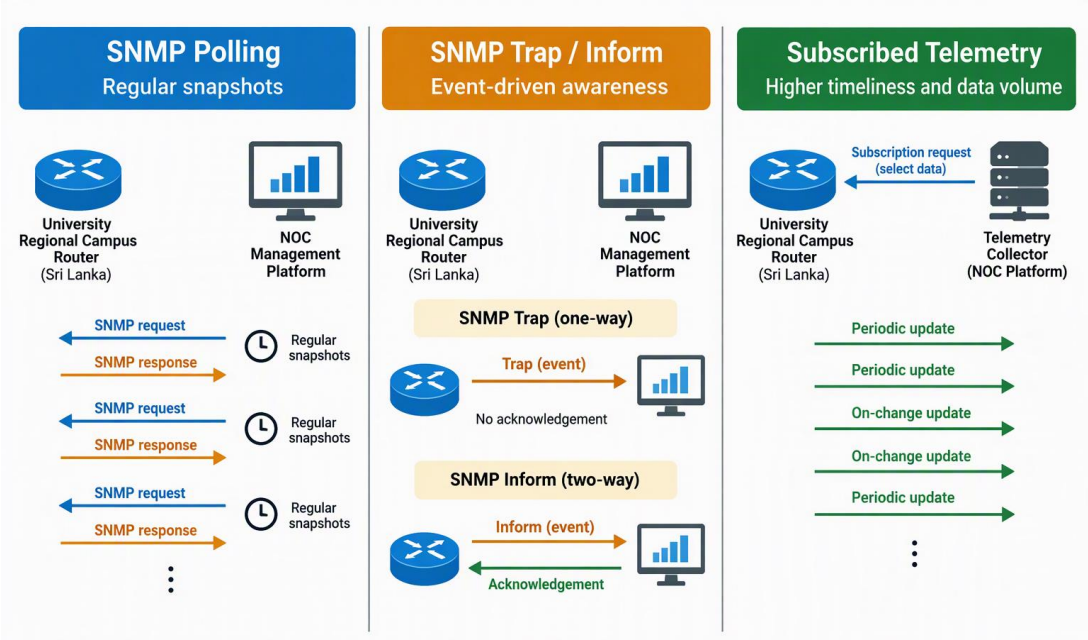
Subscribed telemetry: push selected updates

- Devices can stream the data operators need
  - **Subscribe**: Select operational data to receive
  - **Periodic**: Push current values at configured intervals
  - **On-change**: Push supported values when they change
  - **Collector**: Receives, stores and analyses the updates
  - **Complementary**: Extends visibility beyond traditional polling
- **More timely visibility brings more data to process and store.**



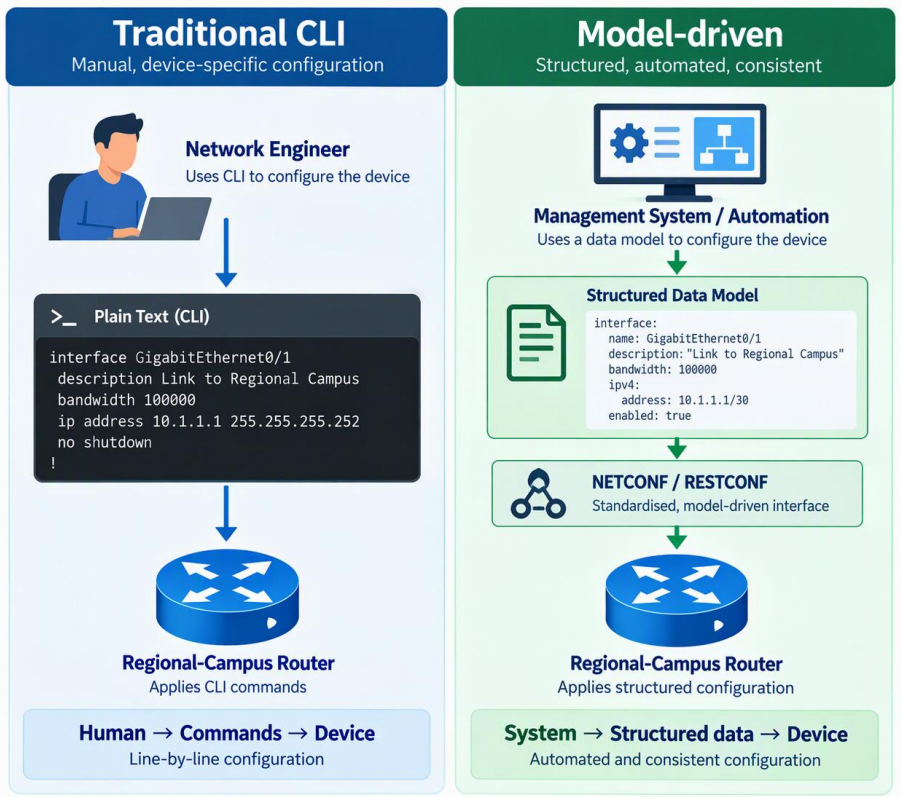
Polling, notifications and streaming telemetry

- Different mechanisms provide different visibility
  - **Polling**: Regular snapshots and historical trends
  - **Trap / Inform**: Event-driven awareness when something happens
  - **Subscribed telemetry**: Selected periodic or on-change updates
  - **Combined visibility**: Use each where it provides operational value
- **Choose by timeliness, data volume, reliability and device support.**



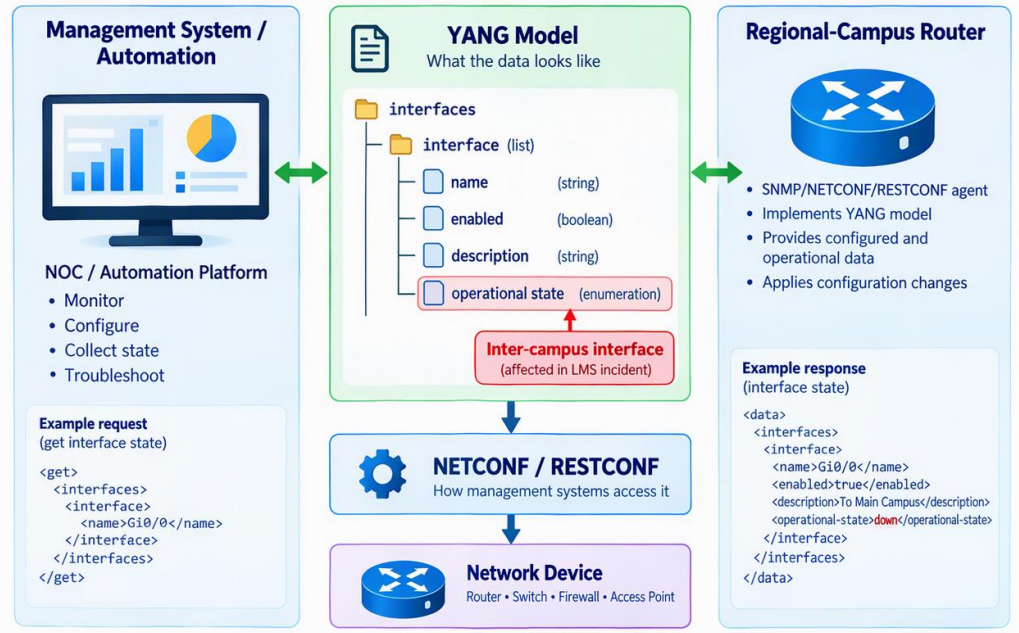
From CLI to model-driven management

- CLI works well, but structured management scales better
- CLI
  - Human-readable commands
  - Flexible for troubleshooting and one-off changes
  - Can vary across platforms and software versions
- Model-driven management
  - Uses structured, machine-readable data
  - Supports consistent validation and automation
  - Separates the data model from the management interface
- **The shift is from configuring commands to managing structured network state.**



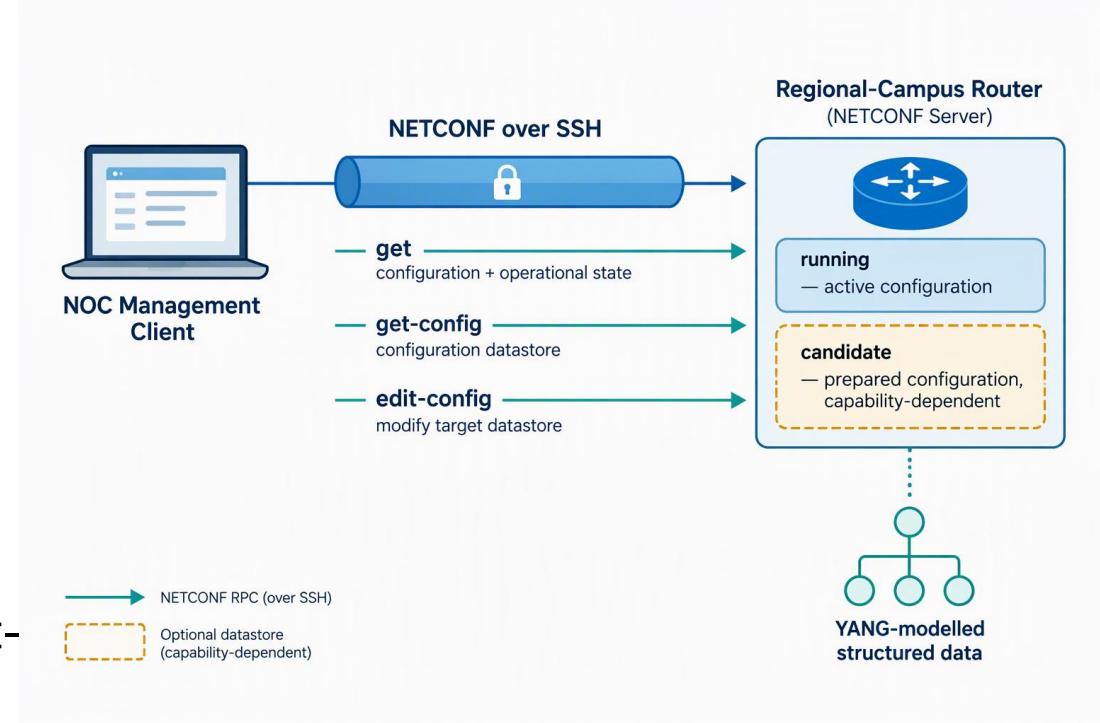
YANG: The shared data model

- YANG defines how network data is structured
  - **Configuration**: What we want the device to use
  - **Operational state**: What the device is currently reporting
  - **Actions / RPCs**: Operations a system can request
  - **Notifications**: Events a device can report
- **YANG defines the data, NETCONF and RESTCONF provide ways to access it.**



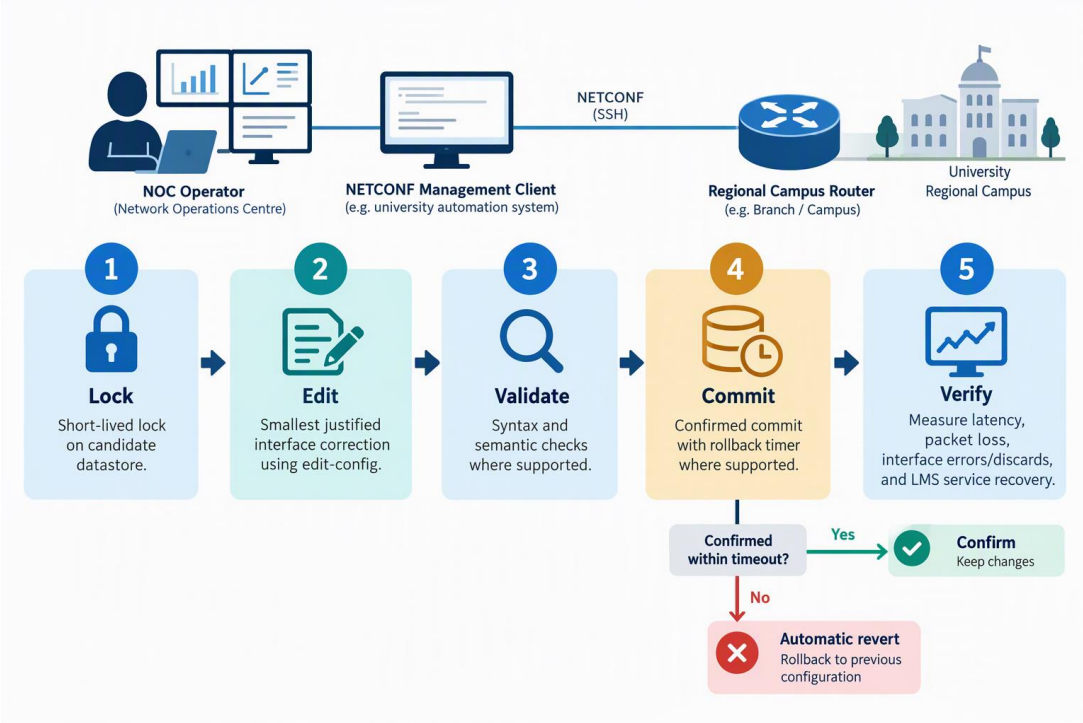
NETCONF: Structured configuration over SSH

- NETCONF retrieves and changes structured network data
  - **RPC-based**: Client requests operations from the network device
  - **SSH**: Mandatory-to-implement secure transport
  - **`running`**: Configuration currently active on the device
  - **`candidate`**: Optional workspace for preparing changes
  - **Core operations**: get, get-config and edit-config
- **YANG defines the data; NETCONF securely operates on it.**



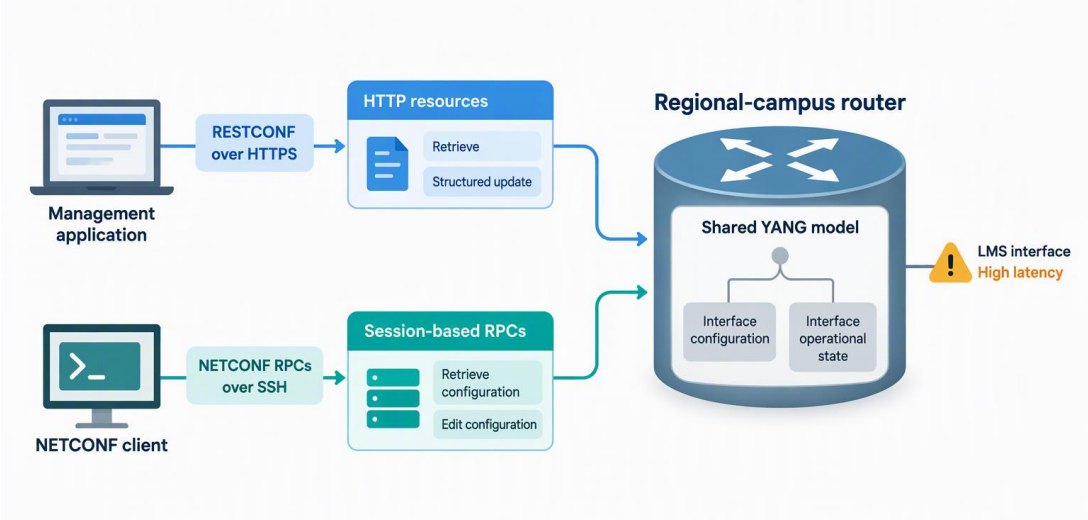
Safe NETCONF change

- Change safely, not simply quickly
  - **Lock**: Prevent competing changes
  - **Edit**: Apply the smallest justified correction
  - **Validate**: Check the configuration where supported
  - **Commit**: Activate the change with a rollback safeguard
  - **Verify**: Confirm recovery or revert
- **A successful commit is not proof that the service has recovered.**



RESTCONF: YANG data over HTTPS

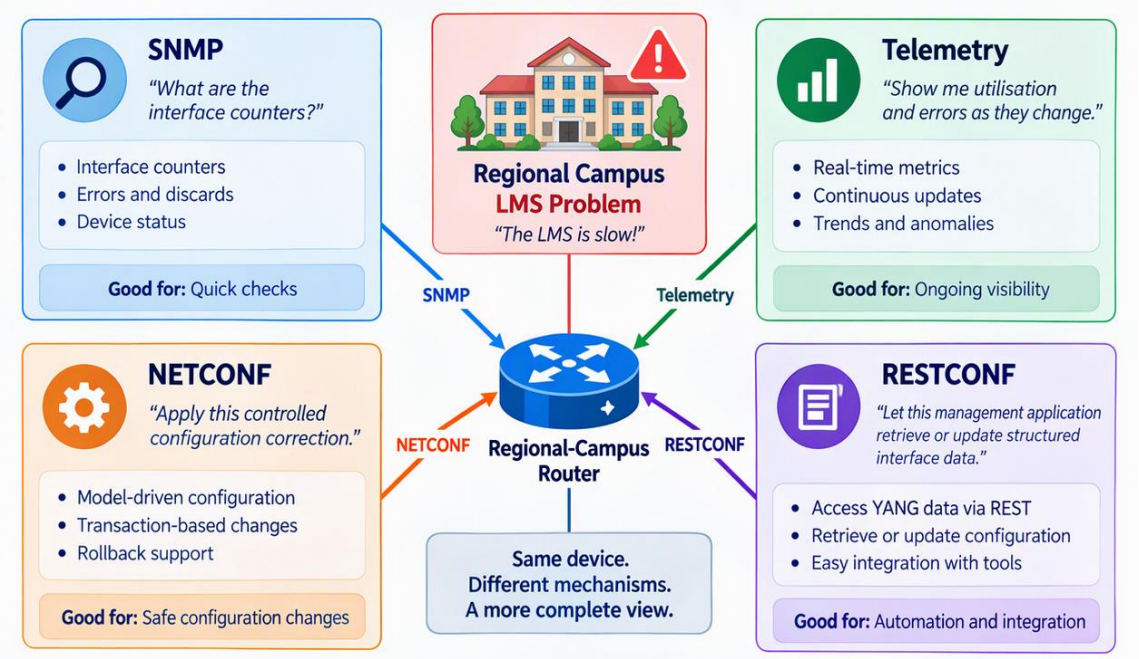
- RESTCONF exposes YANG-modelled data through HTTPS
  - **HTTP-based:** Access network data as resources
  - **YANG-modelled:** Uses structured configuration and operational data
  - **HTTPS / TLS:** Protects management communication
  - **XML or JSON:** Machine-readable request and response data
  - **Web operations:** Retrieve or update selected resources
- **Same YANG model, different management interface.**



Choosing the Right Management Interface

- Different management tasks need different mechanisms

Need	Best fit
Regular device counters and status	**SNMP**
Frequent or on-change operational updates	**Telemetry**
Structured configuration with transaction controls	**NETCONF**
Application-friendly access to YANG data	**RESTCONF**



- **Choose the interface for the operational task, not because one technology is newer.**

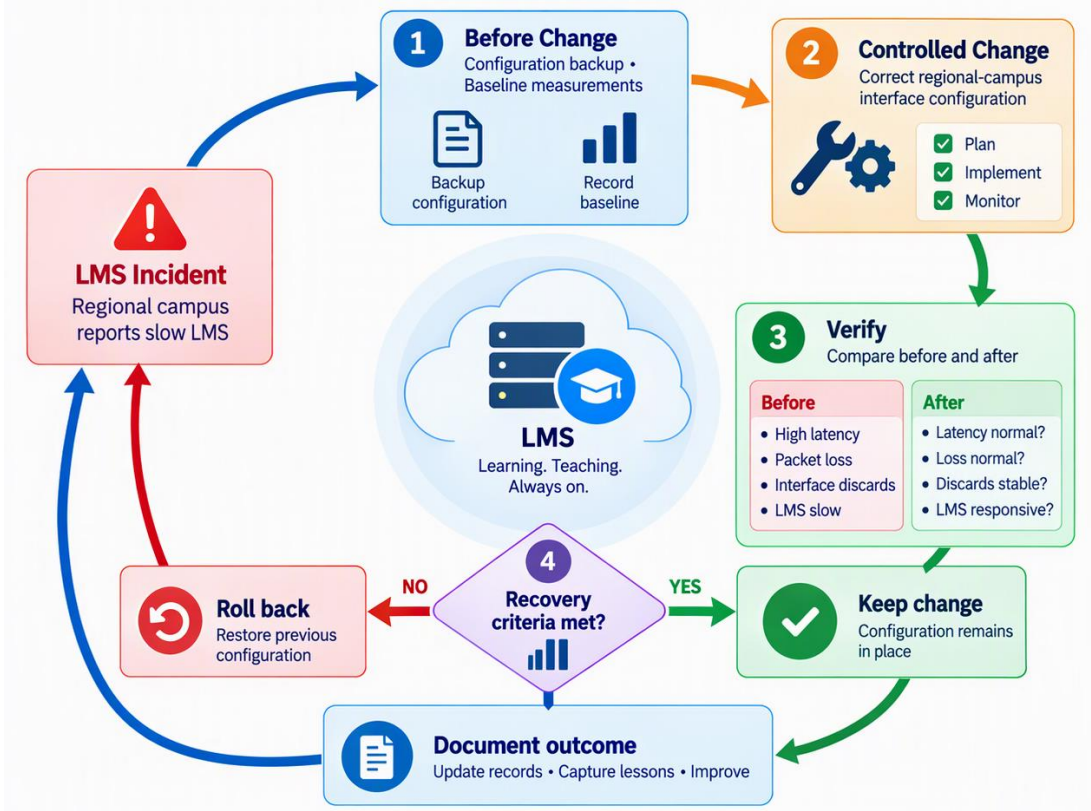
NOC workflow: from alert to ownership

- The NOC coordinates the operational response
  - **Triage**: Confirm impact and gather initial evidence
  - **Prioritise**: Assess severity and service impact
  - **Escalate**: Involve the right technical expertise
  - **Communicate**: Keep affected users and teams informed
  - **Own**: Track the incident through recovery and verification
- **The NOC does not just watch dashboards; it coordinates restoration of service.**



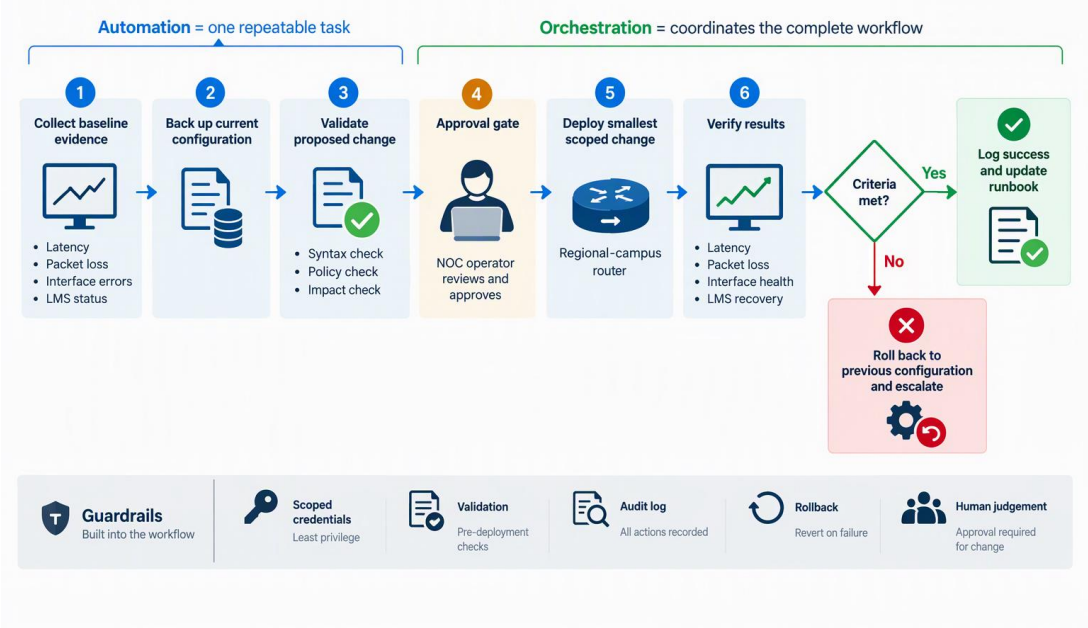
Controlled change: verify and ready to roll back

- A change is not complete until it is verified
- Before changing the network:
  - **Record**: Capture the current state and configuration
  - **Plan**: Define the change, expected result and rollback trigger
  - **Apply**: Make the smallest justified correction
  - **Verify**: Repeat the measurements that identified the problem
  - **Rollback**: Restore the previous state if recovery criteria are not met
- **“The command succeeded” is not the same as “the service recovered.”**



Automation and orchestration: repeat safely

- Automate the task, orchestrate the workflow
  - **Automation**: Performs one repeatable task consistently
  - **Orchestration**: Coordinates tasks, dependencies and approvals
  - **Guardrails**: Validate, limit access, log actions and retain rollback
  - **Verification**: Confirm the network and LMS meet recovery criteria
  - **Human judgement**: Required when diagnosis or impact is uncertain
- **Automate validated decisions, not uncertain assumptions.**



Next: Network Operations Centre

- We have seen what network operations must achieve.
- Next week, we focus on how a NOC delivers it:
  - **Monitor** network and service health
  - **Triage** alerts and user-reported issues
  - **Escalate** and coordinate technical response
  - **Communicate** service impact and recovery
  - **Learn** from incidents and improve operations
- **From managing the network → to operating the NOC.**

