Path Characteristics Verification and Attestation Services

Yutaka OIWA
IETF 120

Traditional Network Setting…

- L2 connectivity by physical switches/bridges
- L3 connectivity by physical routers
  - "physical" here means identifiable and locatable
- No tunneling/virtual networks/overlays

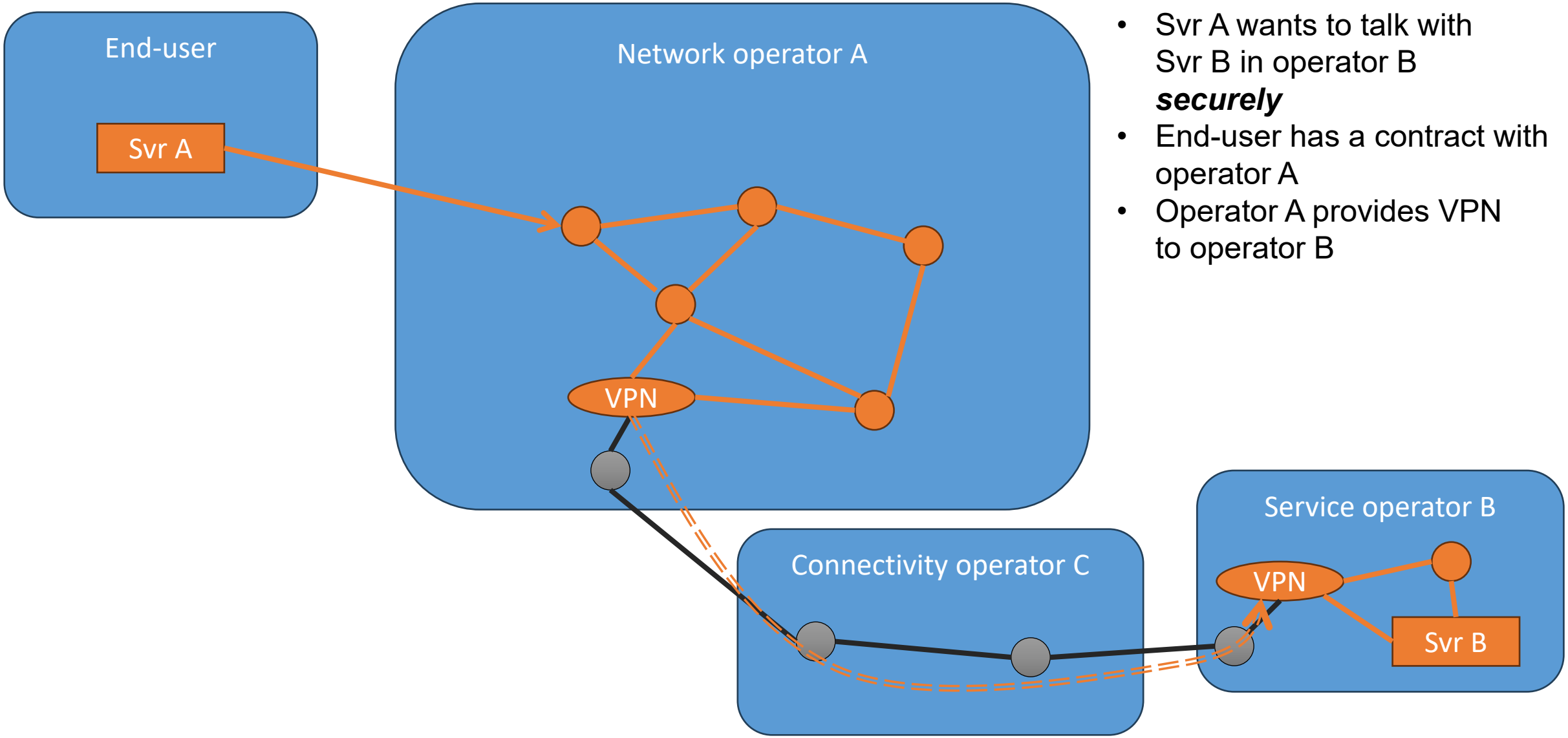
- Network Operators are local or "friends"
  - e.g. in small academic networks

- In this setting, tracing traffic routing is easy
  - "traceroute" will identify the actual path on L3
  - L2 will be traced via e.g. forwarding tables

In reality

- Overlays in various layers
  - L2 to L2 (e.g. VLAN/VXLAN)
  - L2 to L4 (e.g. L2TP)
  - L3 to L4 (VPN) etc.
- Software-defined networks and orchestrators
  - Virtualized L2 switches
  - Virtual Router Functions
  - Infrastructure as Code (IaC)

Example Setting

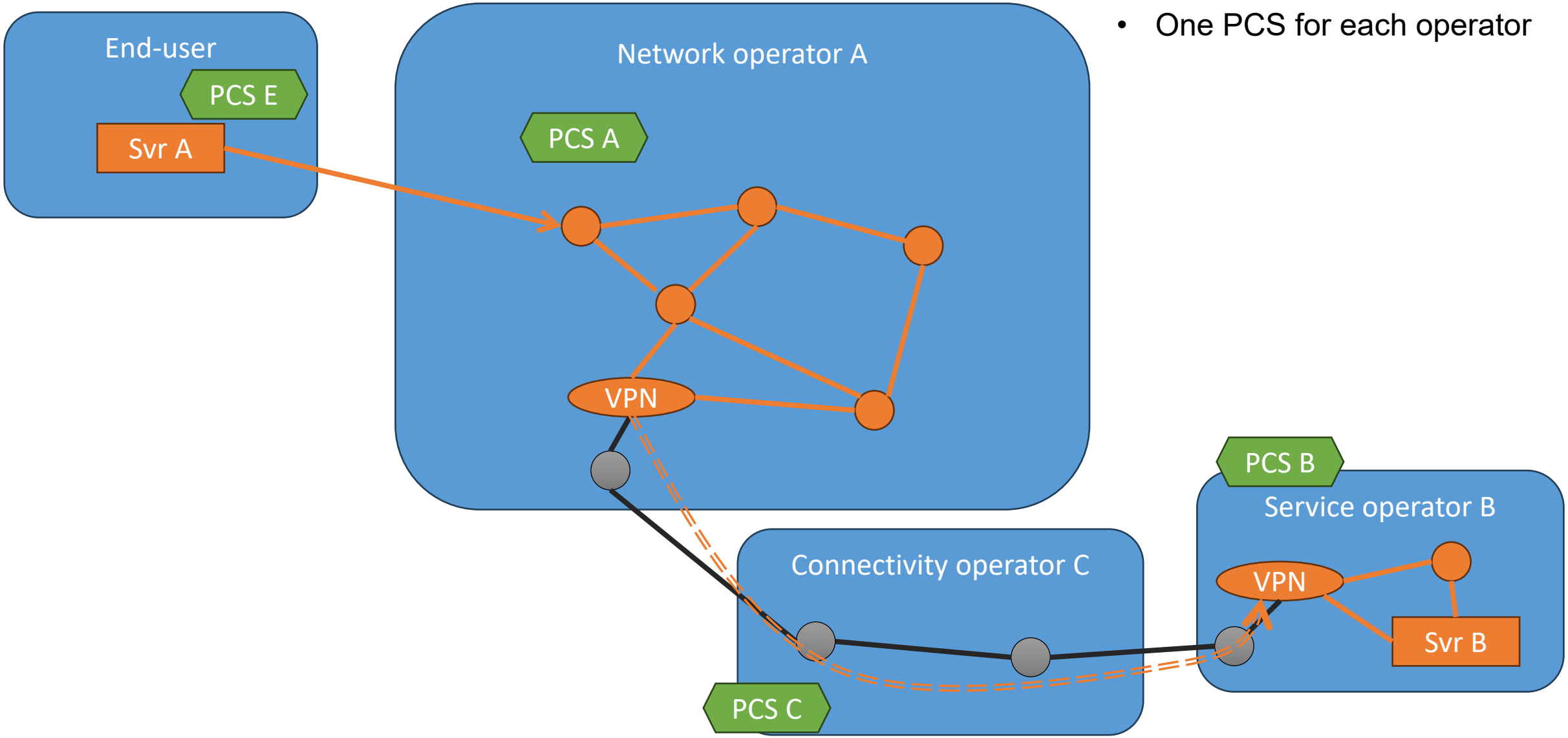


- Svr A wants to talk with Svr B in operator B ***securely***
- End-user has a contract with operator A
- Operator A provides VPN to operator B

Problems

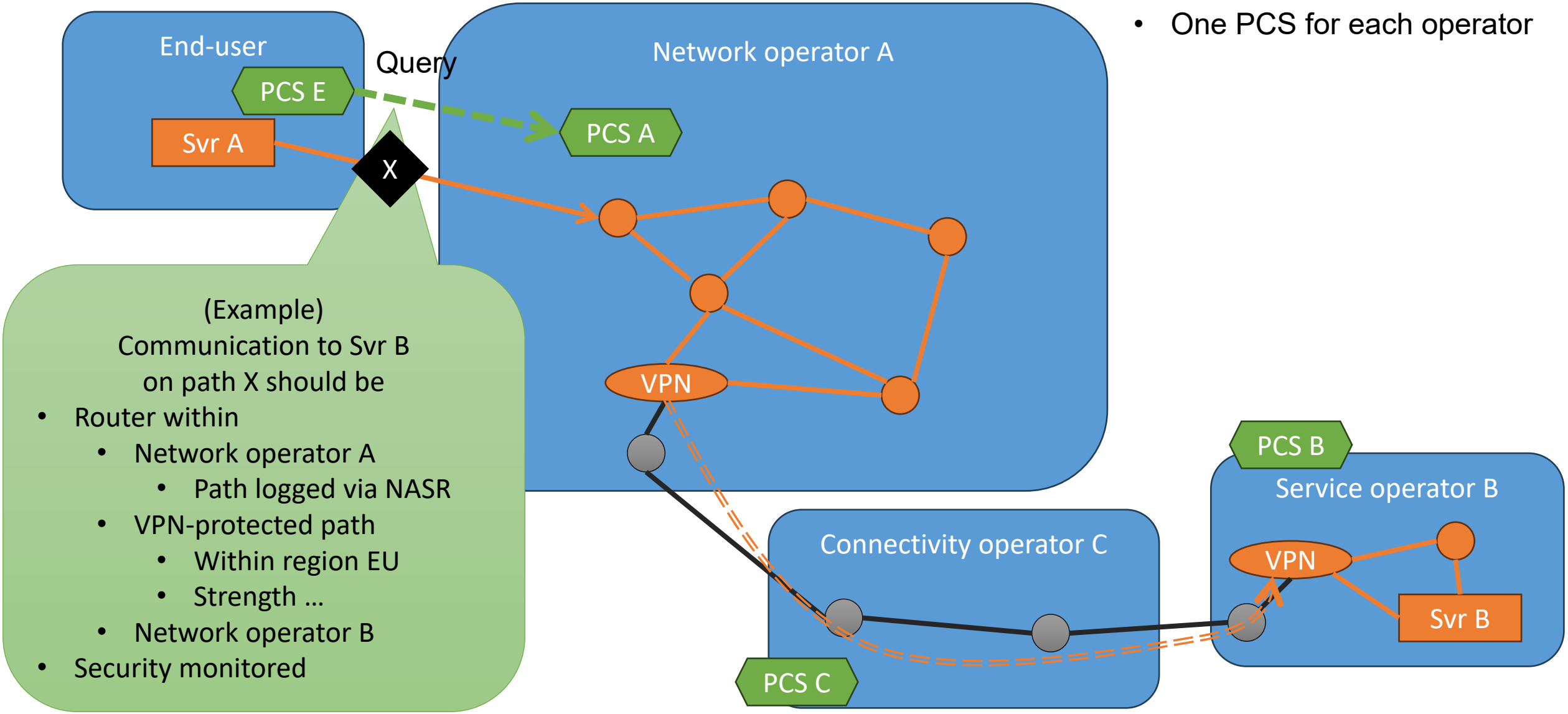
- The nature of multiple operators/stakeholders
- Determination of the "correct" states
- Shared infrastructure and information leakage
- Virtualized infrastructure
- Risks beyond network layers

Path characterics services



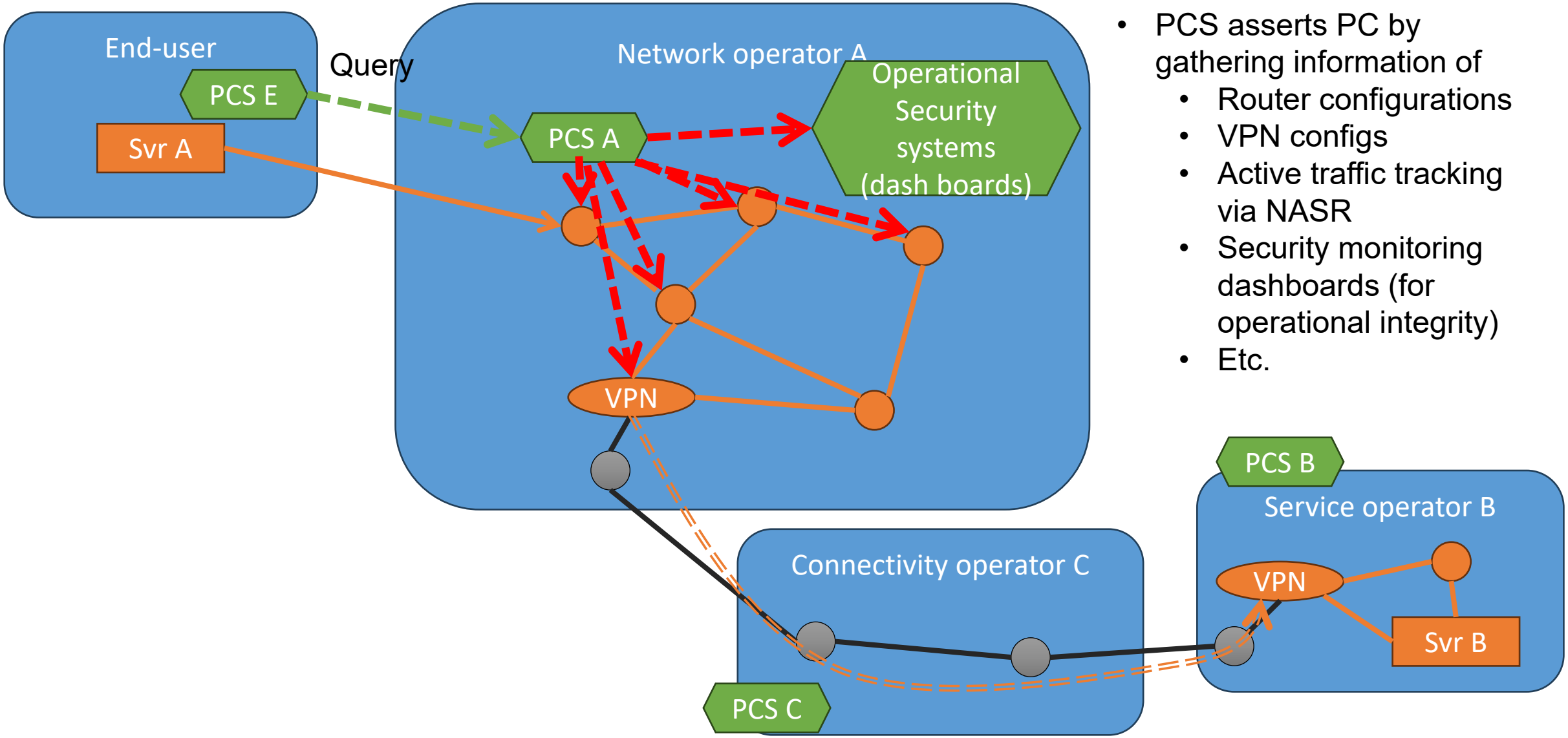
- One PCS for each operator

Path characterics services



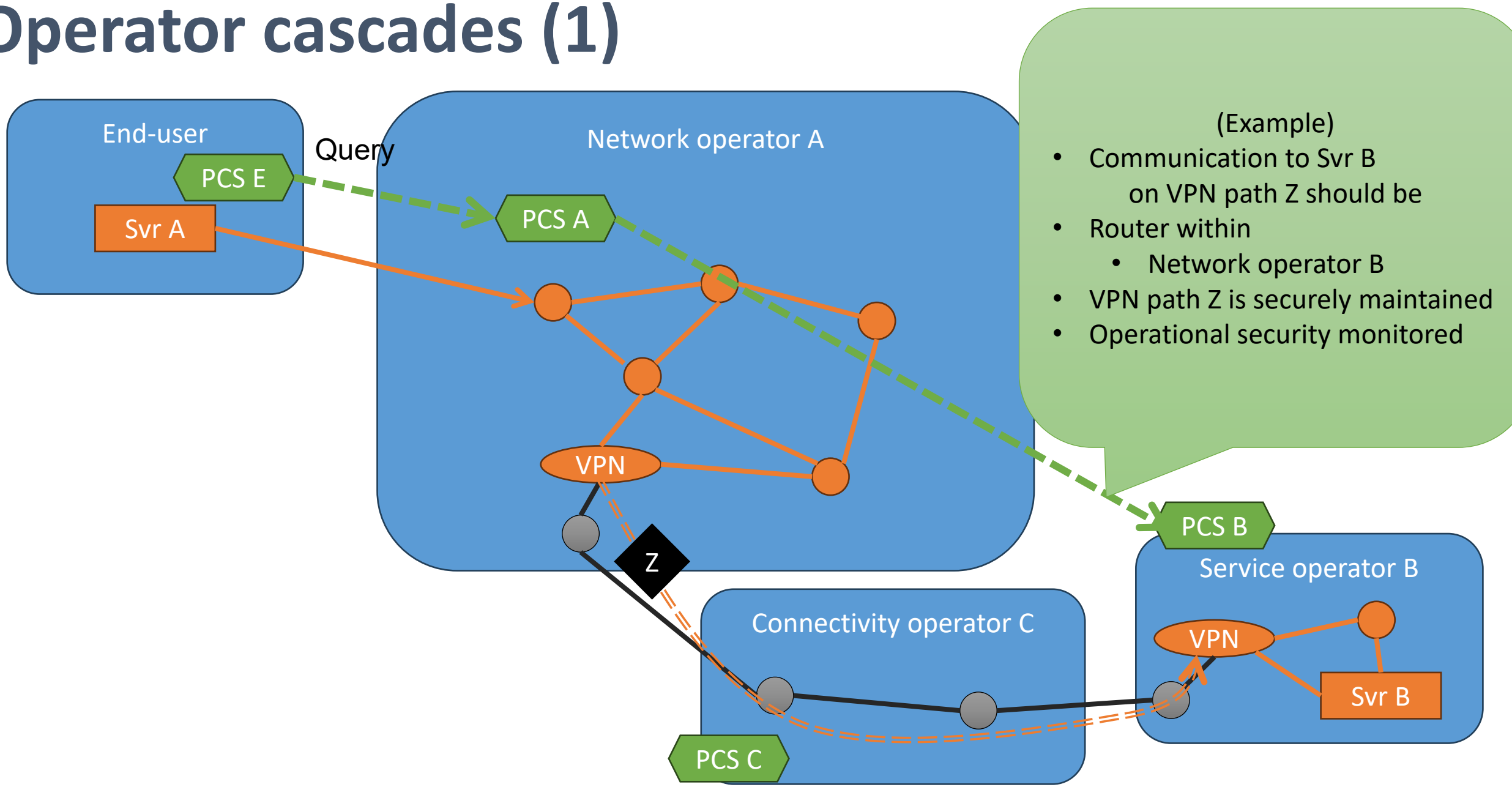
- One PCS for each operator

Characteristics verification within an operator

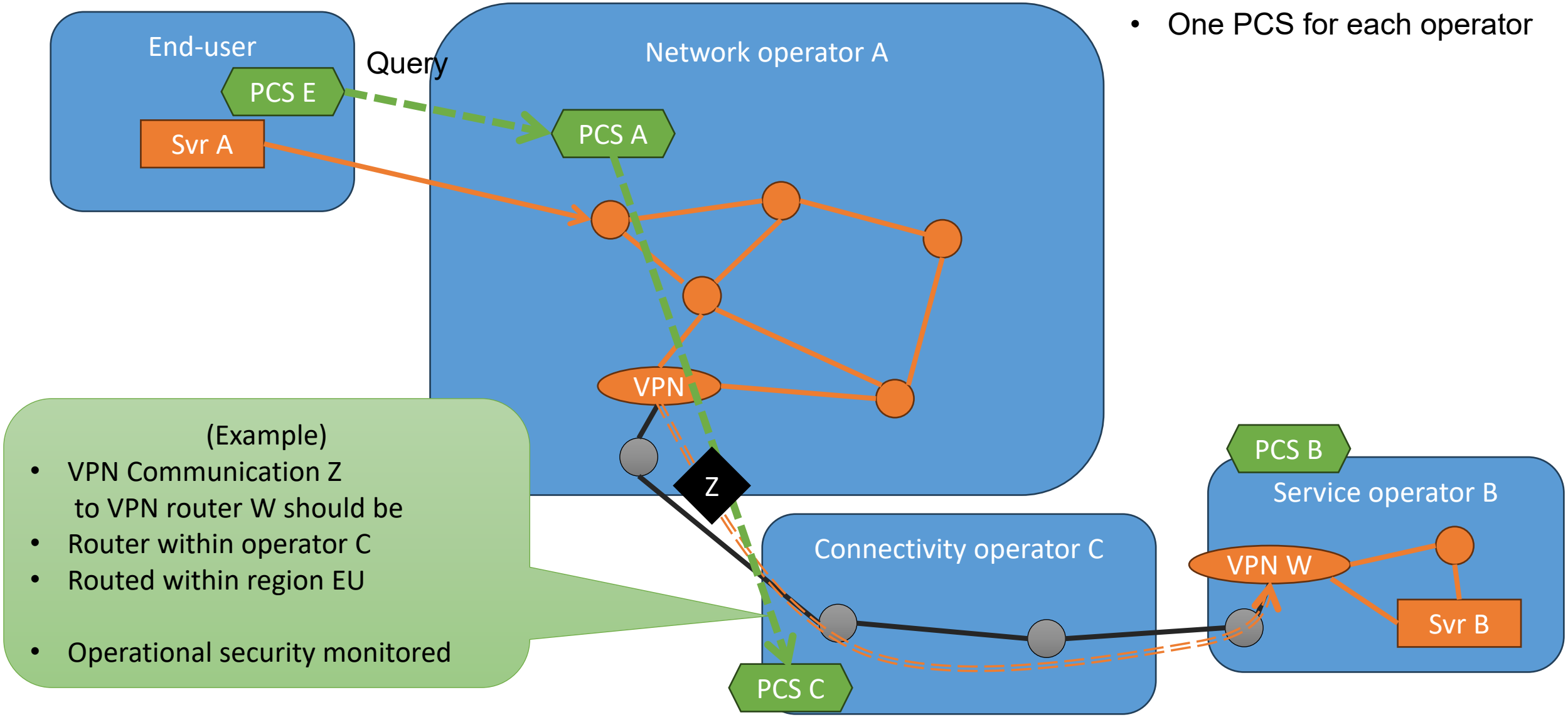


- PCS asserts PC by gathering information of
  - Router configurations
  - VPN configs
  - Active traffic tracking via NASR
  - Security monitoring dashboards (for operational integrity)
  - Etc.

Operator cascades (1)



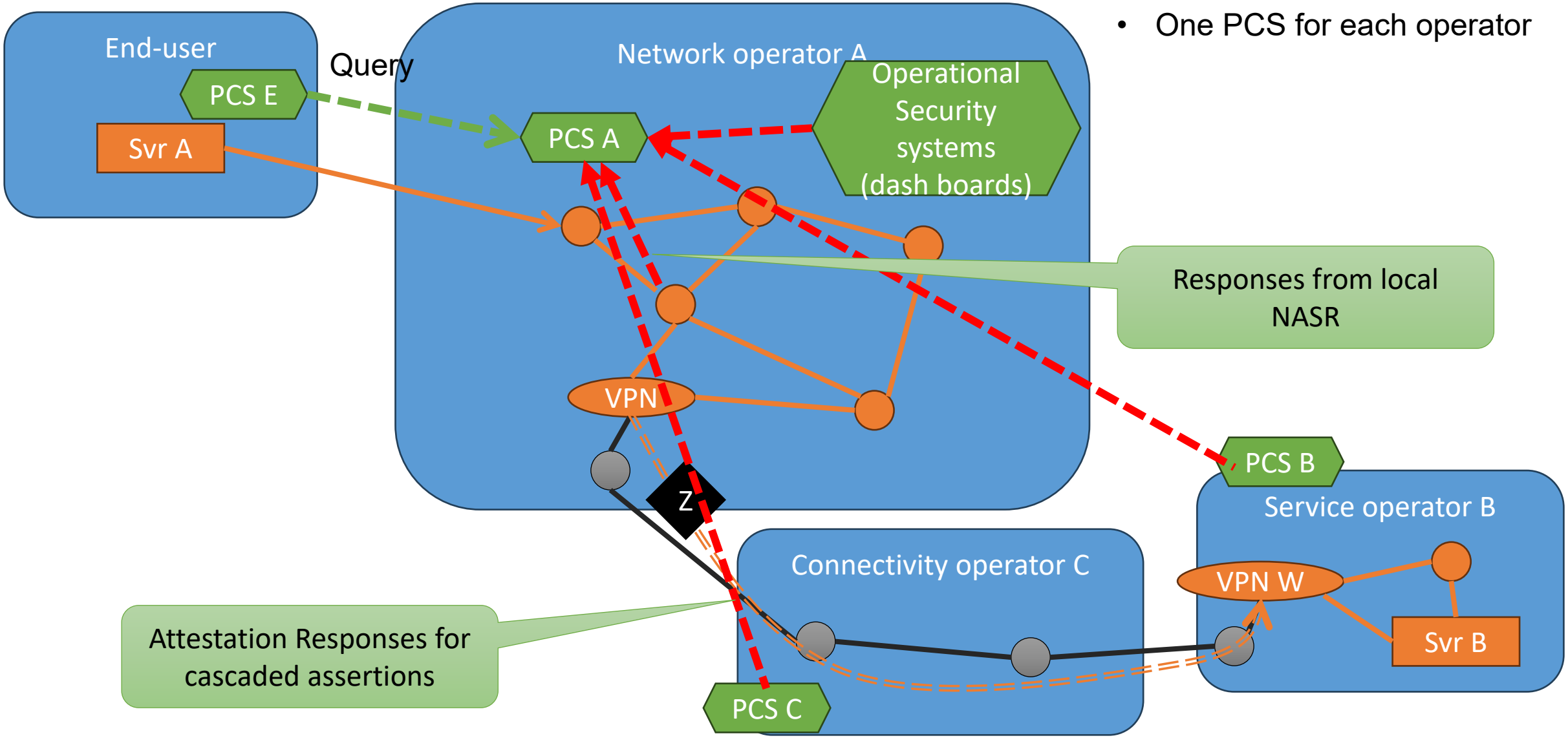
Operator cascades (2)



- One PCS for each operator

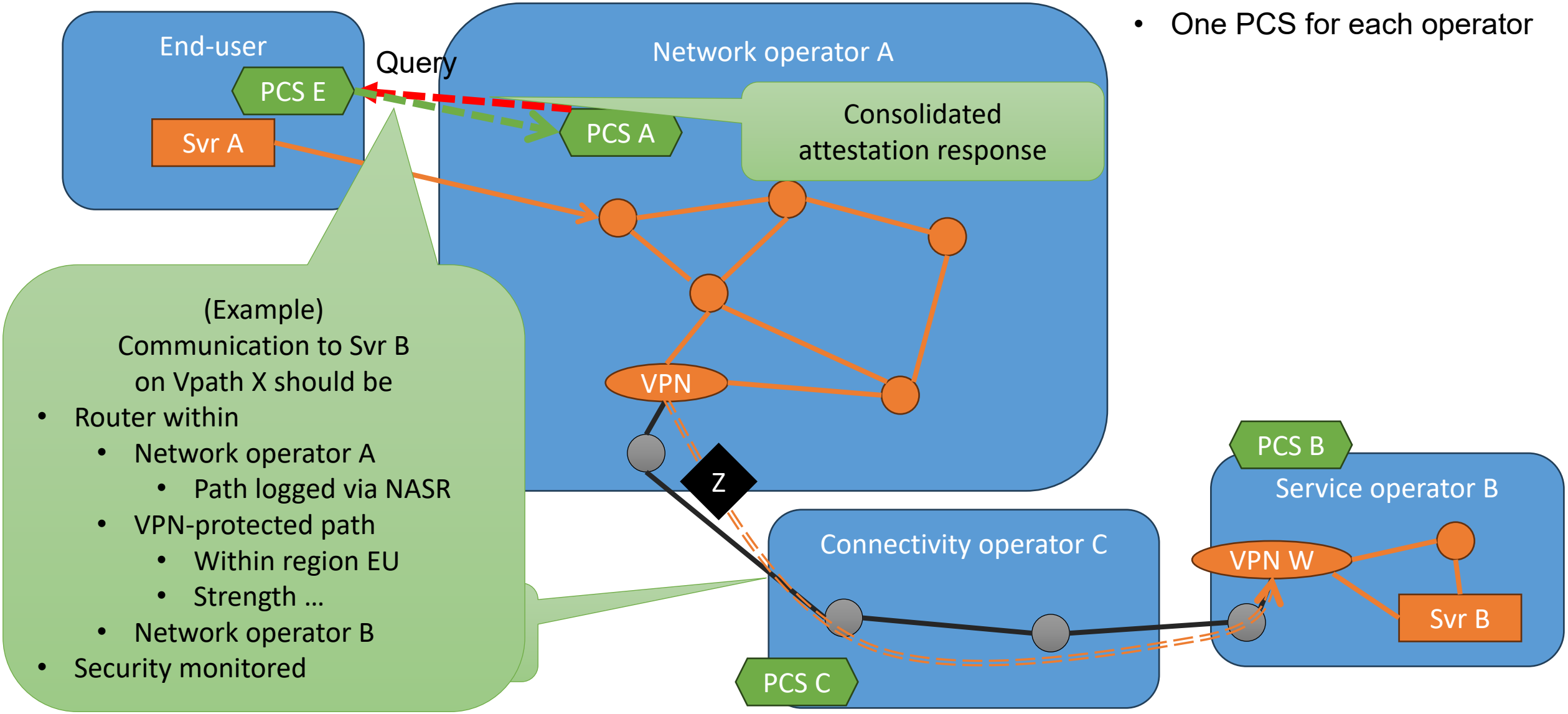
Gathering responses

- One PCS for each operator



Returning consolidated path characteristics

- One PCS for each operator



(Example)
Communication to Svr B on Vpath X should be

- Router within
  - Network operator A
    - Path logged via NASR
  - VPN-protected path
    - Within region EU
    - Strength …
  - Network operator B
- Security monitored

Levels of queries

- Intensiveness of validation
  - Checks just for normal operations
  - Checks for pre-flight configurations
    - Routing tables etc.
  - Checks for pre- and post-flight status
    - NASR, packet monitoring etc.
- Depth of validation
  - Whether to check underlying networks for VPN, overlays
  - VLAN, MPLS etc.
- Strength of validation
  - Via specific pre-known routers
  - Within specific operators (e.g. AS numbers)
  - Within specific jurisdicial regions (e.g. within European Union jurisdiction)
  - Etc.

Levels of results

- Temporal validity
  - Periodical checking
  - Dynamic updates
- Assertion opacity
  - Discloses all collected cascaded information
  - Asserts the verifier's characteristics (e.g. software versions)
  - Just say "yes, believe me"
    - Possibly with digital signature schemes

Targets for verification

- Network (IP) routing
  - L3 routing directions
  - L2 integrity (incl. end-point attestations)
    - Overlay configurations
      - Label-based (VLAN, MPLS)
      - Crypto-based (VPN)
  - L1 characteristics and status
- Application-level routing
  - DNS
- Operational integrity
  - Assertion from security dashboards (e.g. CDM and SOC)

Summary

- Endpoint can ask the direct-connected network operator for
  - Whether some future communication will flow over some characteristics-assured path or not
    - Characteristics include routing paths, operators' integrity, geo fenses, overlay networks etc.
- The asked network operator will gather information from
  - Inner information sources such as NASR mechanism
  - Their own configuration/operation systems
  - Cascading queries to next-hop operators
- The asked network operator will answer to the query, either transparently or opaquely

To be designed and implemented

- Query languages for PCS
- Verifier implementations, including logical derivation engines
- Interface APIs to existing/tbd mechanisms
  - NASR
  - VPN or overlay network
  - Internally-used SDN
  - CDM and other security dashboards

Additional/Spare slides

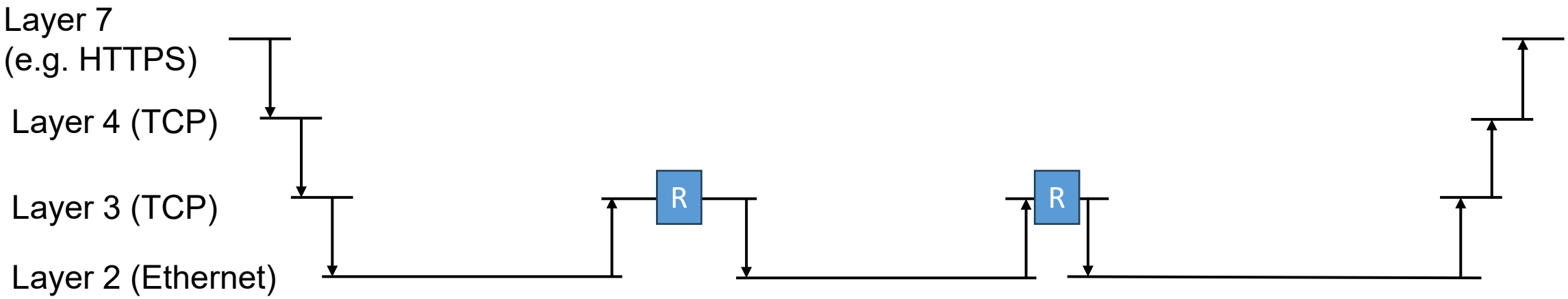
What we need to trace

- Trust chain for secure routing is not a “one-dimensional chain”

- We need to address (at least) three dimensional tree of chains
  - Dimension 1: along communication path
  - Dimension 2: stacks of protocol stacks
  - Dimension 3: operational layers

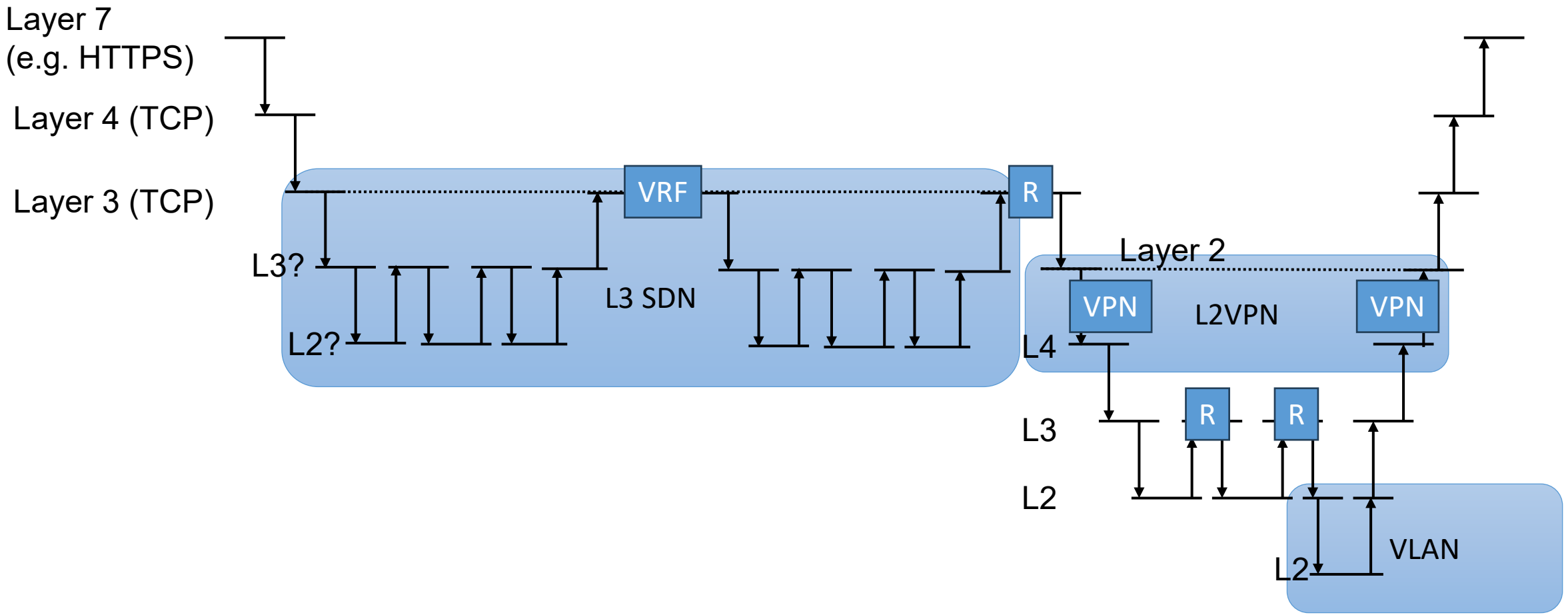
Dimensions 1 and 2

- Protocol stacks are further stacked by virtualization/overlays



Dimensions 1 and 2

- Protocol stacks are further stacked by virtualization/overlays



Dimensions 3

- Config is viable for security of virtualization