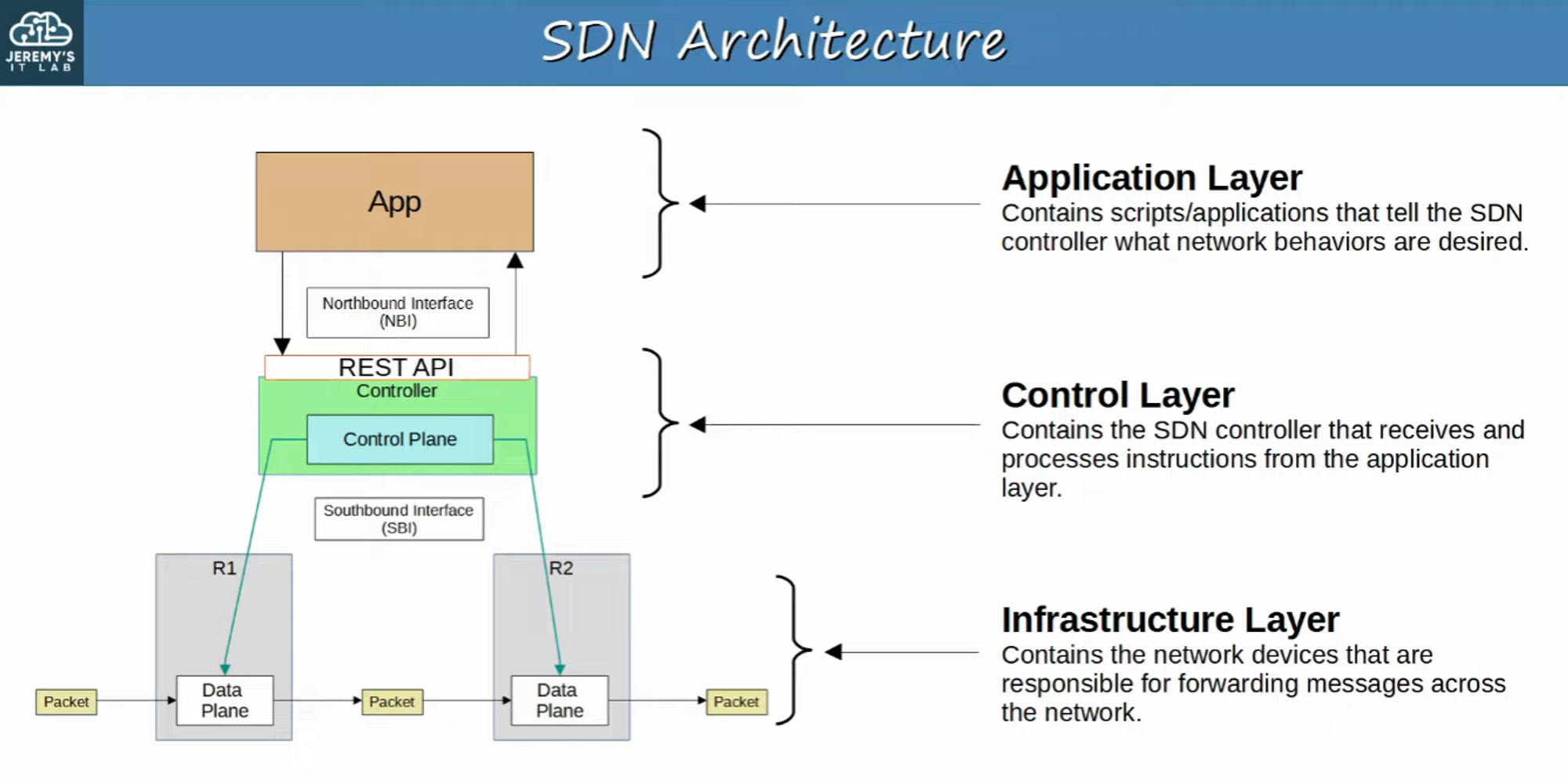
# **62. SOFTWARE DEFINED NETWORKING (SDN)**

## **SD Review**

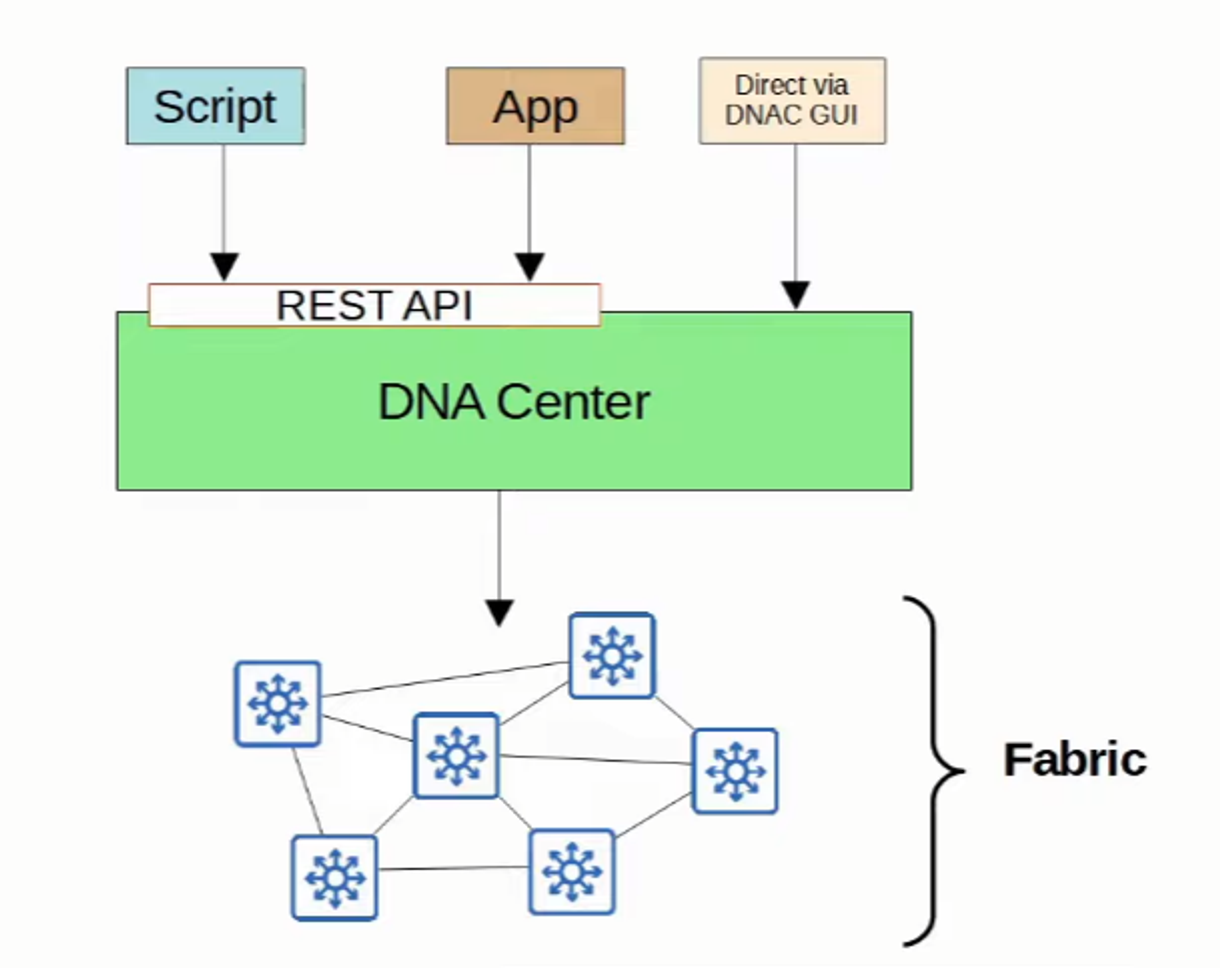
* **Software Defined Networking (SDN)** is an approach to networking that centralizes the control plane into an application called a *controller*.
* Traditional control planes use a distributed architecture.
* An SDN controller centralizes control plane functions like calculating routes.
* The controller can interact programmatically with network devices using APIs.
* The **South Bound Interface (SBI)** is used for communication between the controller and the network device it controls.
* The **North Bound Interface (NBI)** allows interaction with the controller using scripts and applications.

## **SDN Architecture**

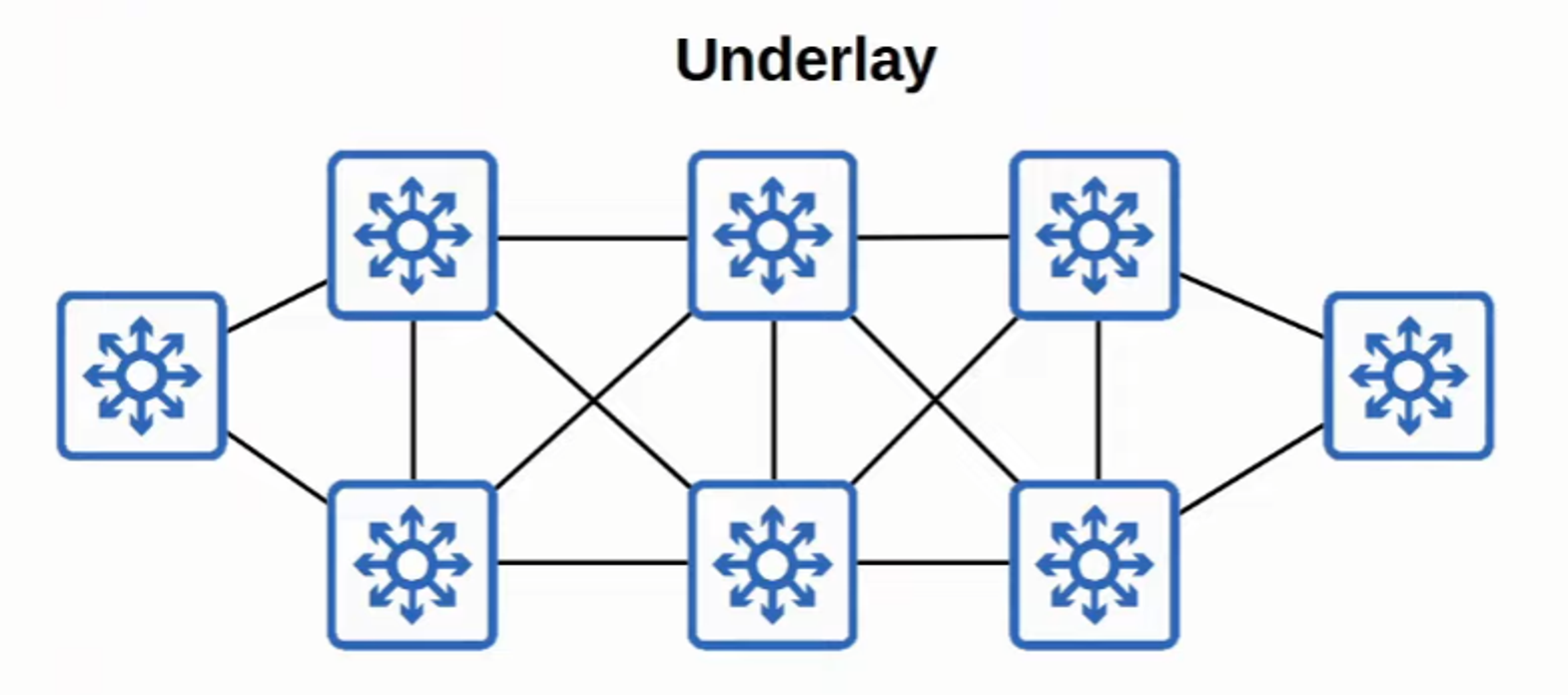
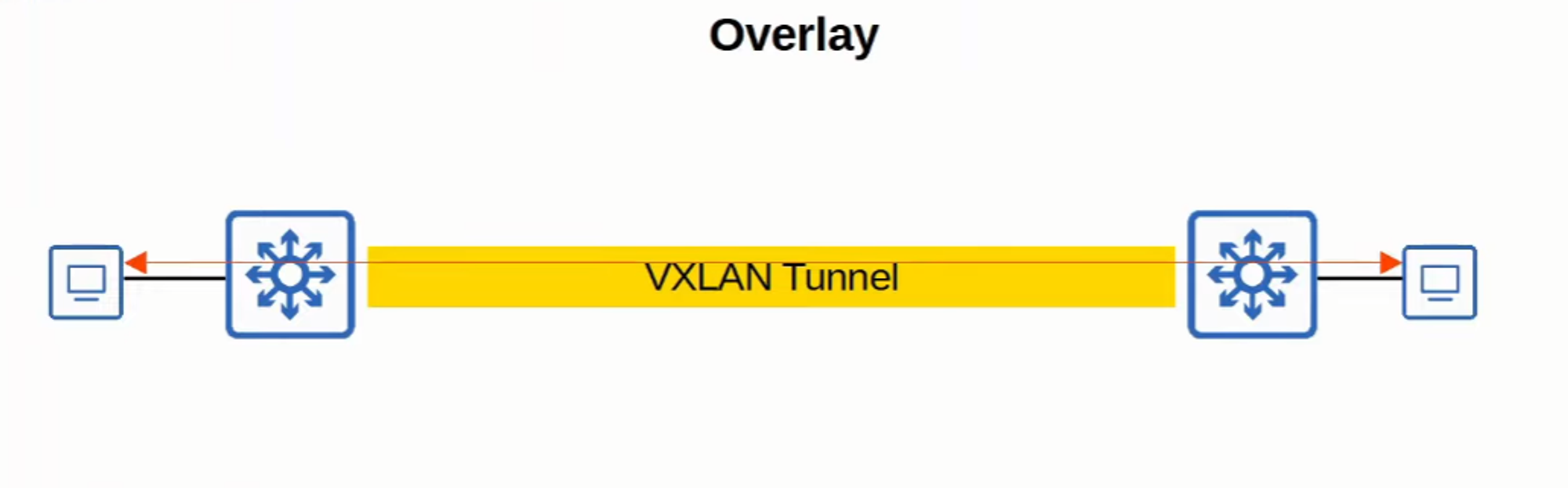
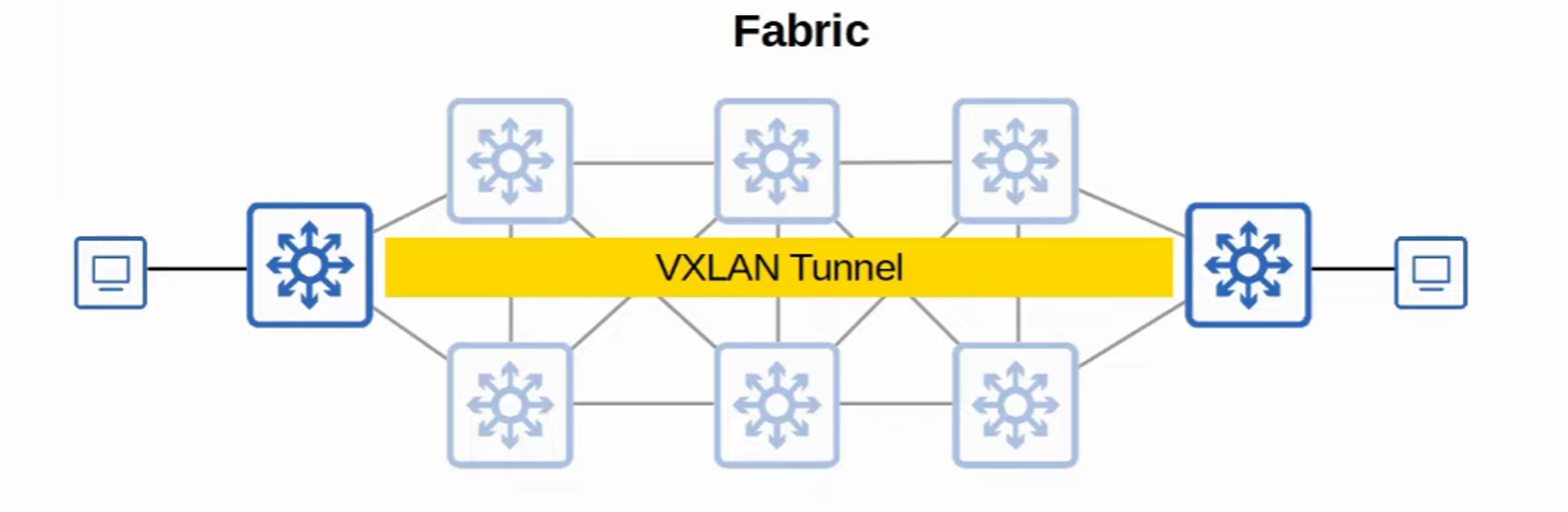
****

## **Cisco SD-Access**

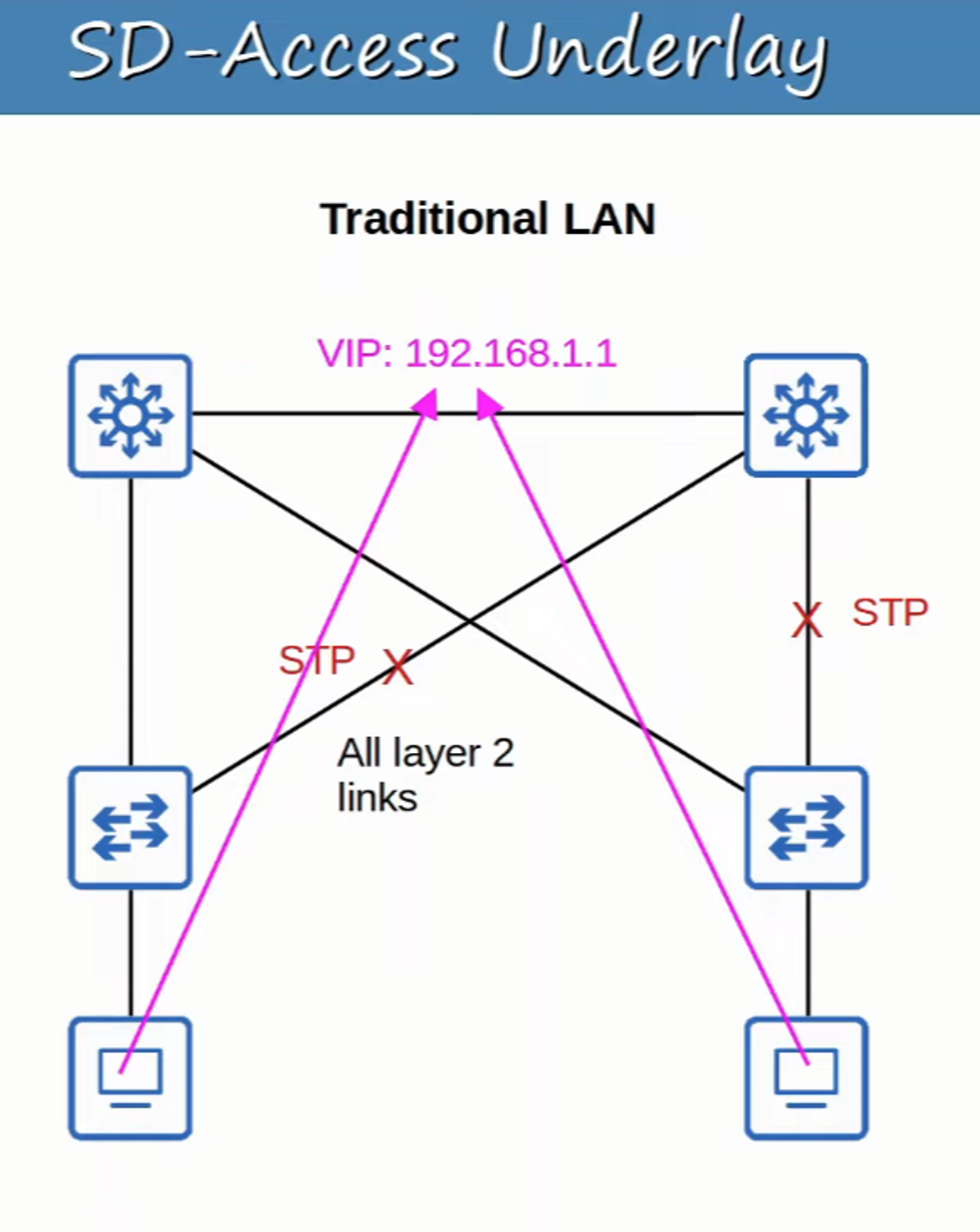
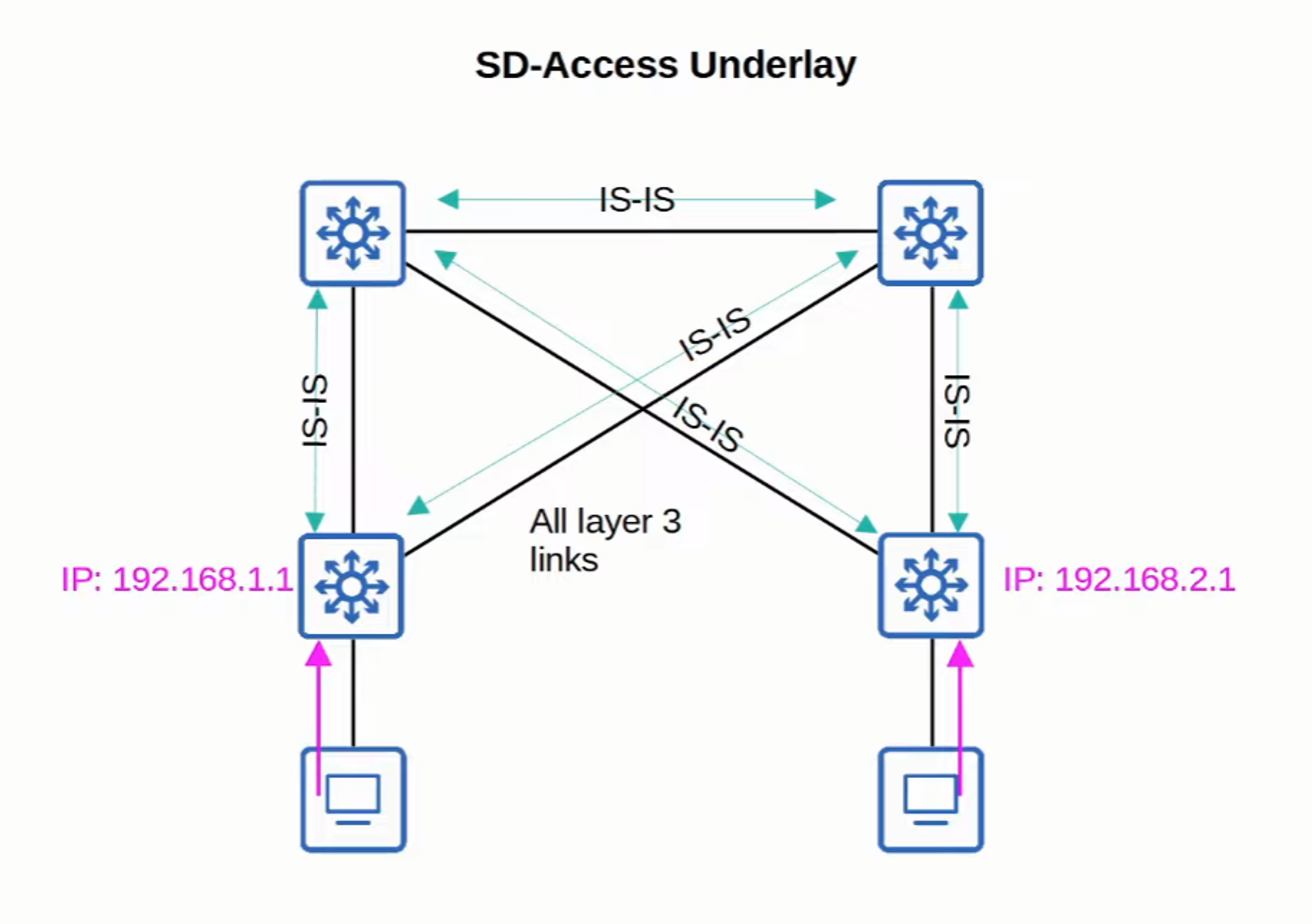
* **Cisco SD-Access** is Cisco’s SDN solution for automating campus LANs.
  + **ACI (Application Centric Infrastructure)** automates data center networks.
  + **SD-WAN** automates WANs.
* **Cisco DNA (Digital Network Architecture) Center** is the controller at the center of SD-Access.



### **SD-Access Components**

* **Underlay**: The underlying physical network providing IP connectivity (e.g., using IS-IS).  
  + Multilayer switches and their connections.
* 
* **Overlay**: The virtual network built on top of the physical underlay.  
    
   
* **Fabric**: The combination of the overlay and underlay (physical and virtual network as a whole).  
    
   

## **SD-Access Underlay**

* The **underlay** supports the **VXLAN tunnels** of the overlay.
* **Three roles for switches in SD-Access:**
  + **Edge Nodes**: Connect to end hosts.
  + **Border Nodes**: Connect to devices outside of the SD-Access domain (e.g., WAN routers).
  + **Control Nodes**: Use **LISP (Locator ID Separation Protocol)** for control plane functions.
* **Deployment Types:**
  + **Brownfield deployment**: Adds SD-Access on top of an existing network (if hardware/software supports it).
  + **Greenfield deployment**: DNA Center configures an optimal SD-Access underlay.
    - All switches are **Layer 3** and use **IS-IS** as the routing protocol.
    - All links between switches are **routed ports** (no STP required).
    - Edge nodes (access switches) act as **default gateways** for end hosts.
*   
    
   

# **SD-ACCESS OVERLAY**

## **LISP (Locator ID Separation Protocol)**

LISP provides the control plane of SD-ACCESS:

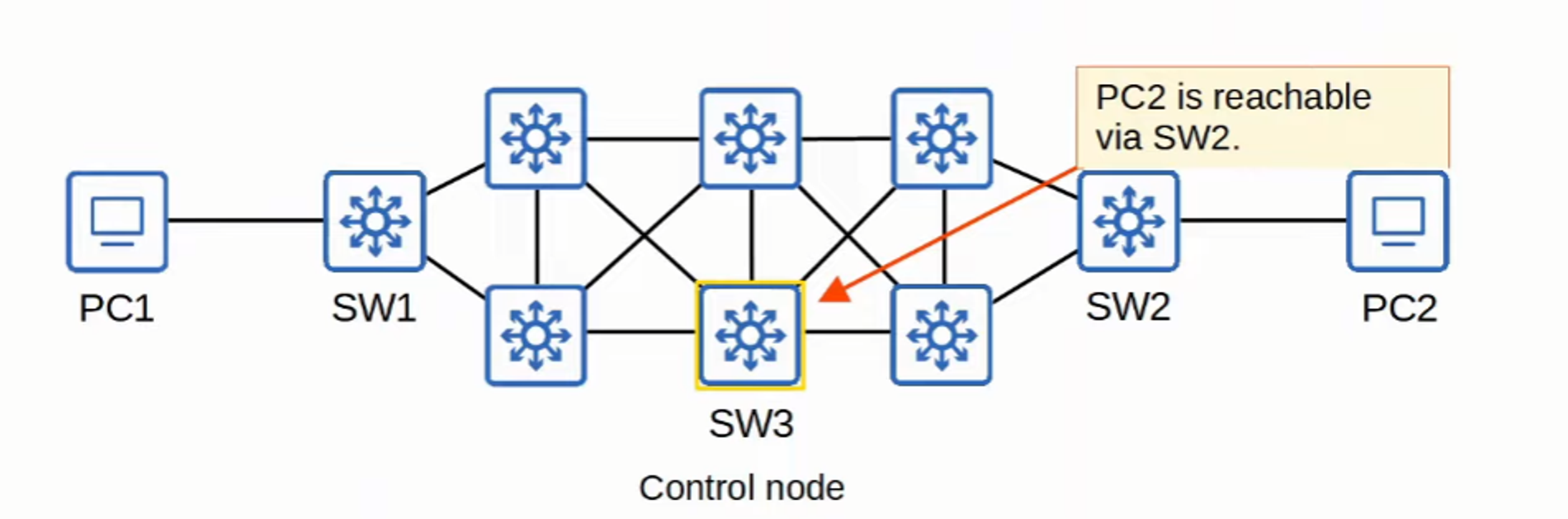
* Maintains a mapping of **EIDs (Endpoint Identifiers)** to **RLOCs (Routing Locators)**.
* **EIDs** identify **end hosts** connected to **edge switches**.
* **RLOCs** identify the **edge switch** used to reach the end host.
* LISP significantly differs from traditional control planes by decoupling location and identity.

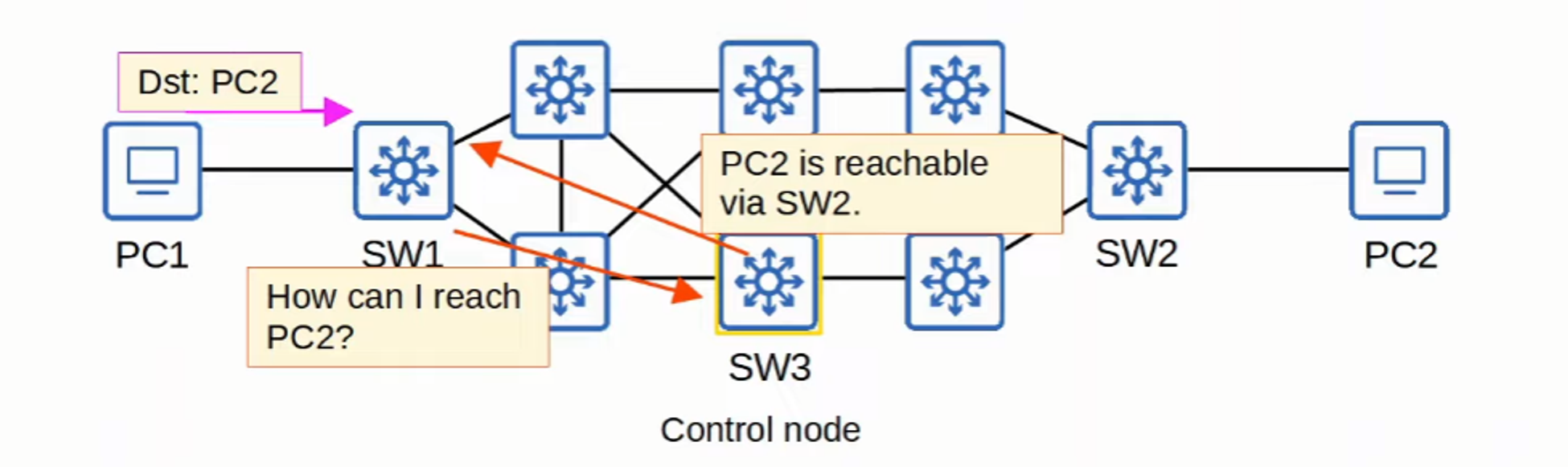
## **Cisco TrustSec (CTS)**

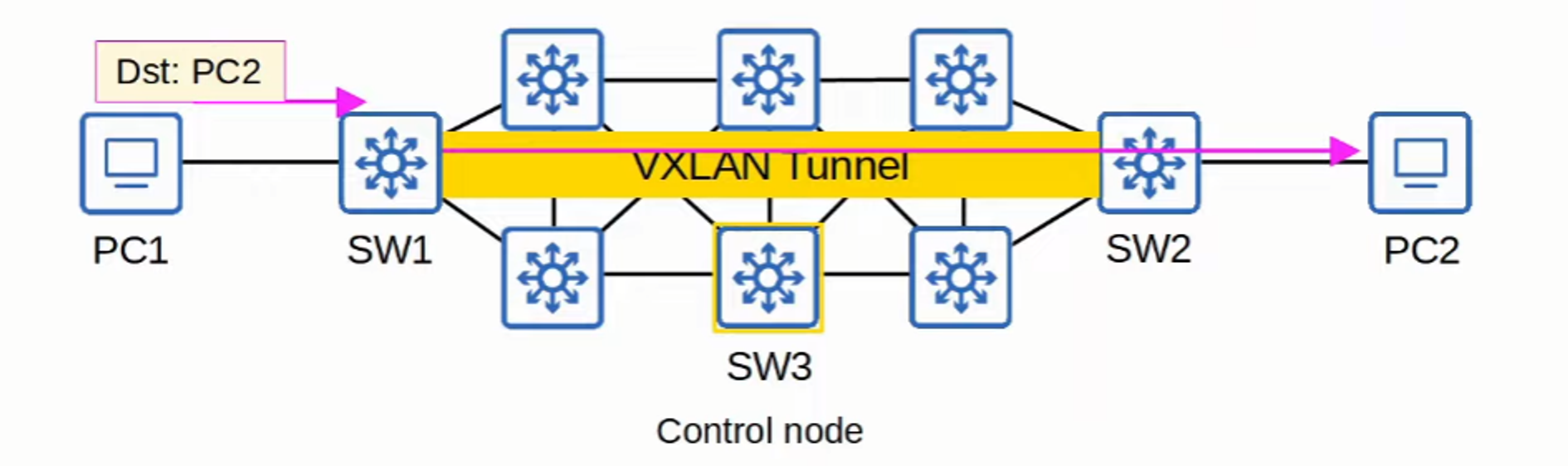
* Provides **policy control** (e.g., QoS, security policy enforcement).

## **VXLAN**

* Provides the **data plane** of SD-ACCESS.







# **CISCO DNA CENTER**

## **Main Roles of DNA Center**

1. **SDN Controller** in SD-ACCESS.
2. **Network Manager** in traditional networks (non-SD-ACCESS).

## **Key Features**

* Runs as an **application on Cisco UCS server hardware**.
* Offers a **REST API** for automation and integration.
* Supports **Southbound Interfaces (SBI)** such as:
  + **NETCONF, RESTCONF**
  + Traditional protocols (**Telnet, SSH, SNMP**)
* Enables **Intent-Based Networking (IBN)**:
  + Engineers specify the desired network behavior, and DNA Center configures devices accordingly.

## **Policy Management**

* Traditional **ACL-based security policies** can be **cumbersome**:
  + ACLs can contain **thousands of entries**.
  + The intent behind ACL entries may be lost over time.
* **DNA Center simplifies policy management**:
  + Example policies:
    - *"This group of users cannot communicate with that group."*
    - *"This group can access this server but not that one."*
  + DNA Center automates the implementation of these policies.



### **Additional Resources**

For more details, visit: [sandboxdnac.cisco.com](http://sandboxdnac.cisco.com/) **Credentials:** User: devnetuser, Password: Cisco123!

# **DNA CENTER NETWORK MANAGEMENT VS. TRADITIONAL**

| **Feature** | **Traditional Management** | **DNA Center-based Management** |
| --- | --- | --- |
| **Device Configuration** | Configured **one-by-one** via SSH/Console | Centrally managed via **DNA Center GUI/REST API** |
| **Deployment Process** | Manual configuration before deployment | Devices receive configurations **automatically** |
| **Policy Management** | Managed **per device** | Centrally managed across all devices |
| **Software Updates** | Manual updates required | DNA Center **monitors and updates** devices centrally |
| **Deployment Time** | **Slow**, requires manual effort | **Faster**, automated configuration deployment |
| **Error Handling** | **Higher risk** due to manual input | **Reduced risk** through automation |

