Traditional Access Control

- The traditional way to control access to and traffic flows within a network is with fixed VLANs, IP addresses and Access Control Lists
- Users are expected to always connect to the same physical port where they are assigned an access VLAN and IP subnet
- Access Control Lists control traffic flows between IP subnets
- The configuration can get complex, and each device is configured individually
- The solution does not support user mobility

SD-Access Software Defined Access

- SD-Access is a newer method of network access control which solves the limitations of the traditional implementation
- Traffic flow security is based on user identity, not physical location and IP address
- Users log in from and can move to any physical location in the network

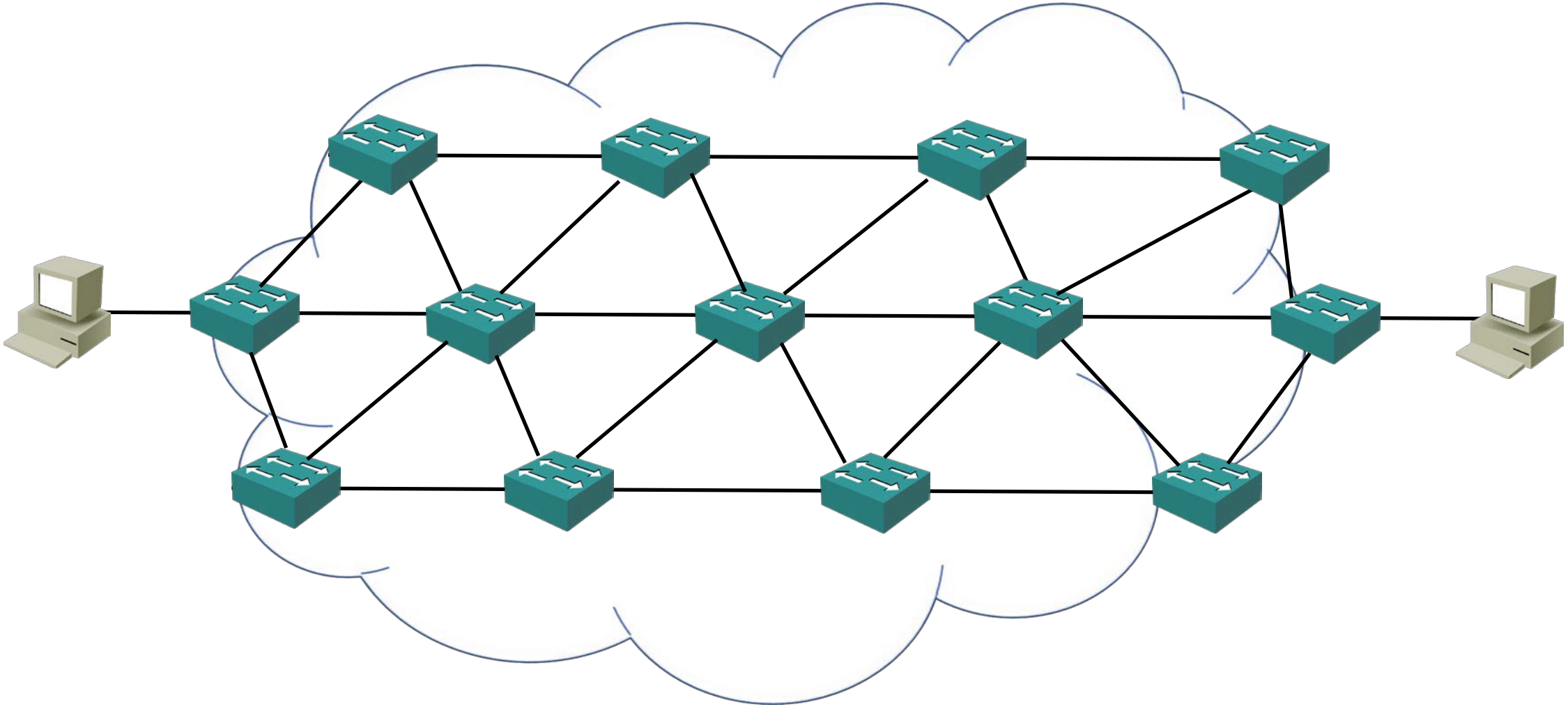
SD-Access Software Defined Access

- Two components are required for SD-Access:
- Users are authenticated by the ISE **Identity Services Engine**
- The security policy (permitted and denied communication between groups) is configured on the **DNA Center**

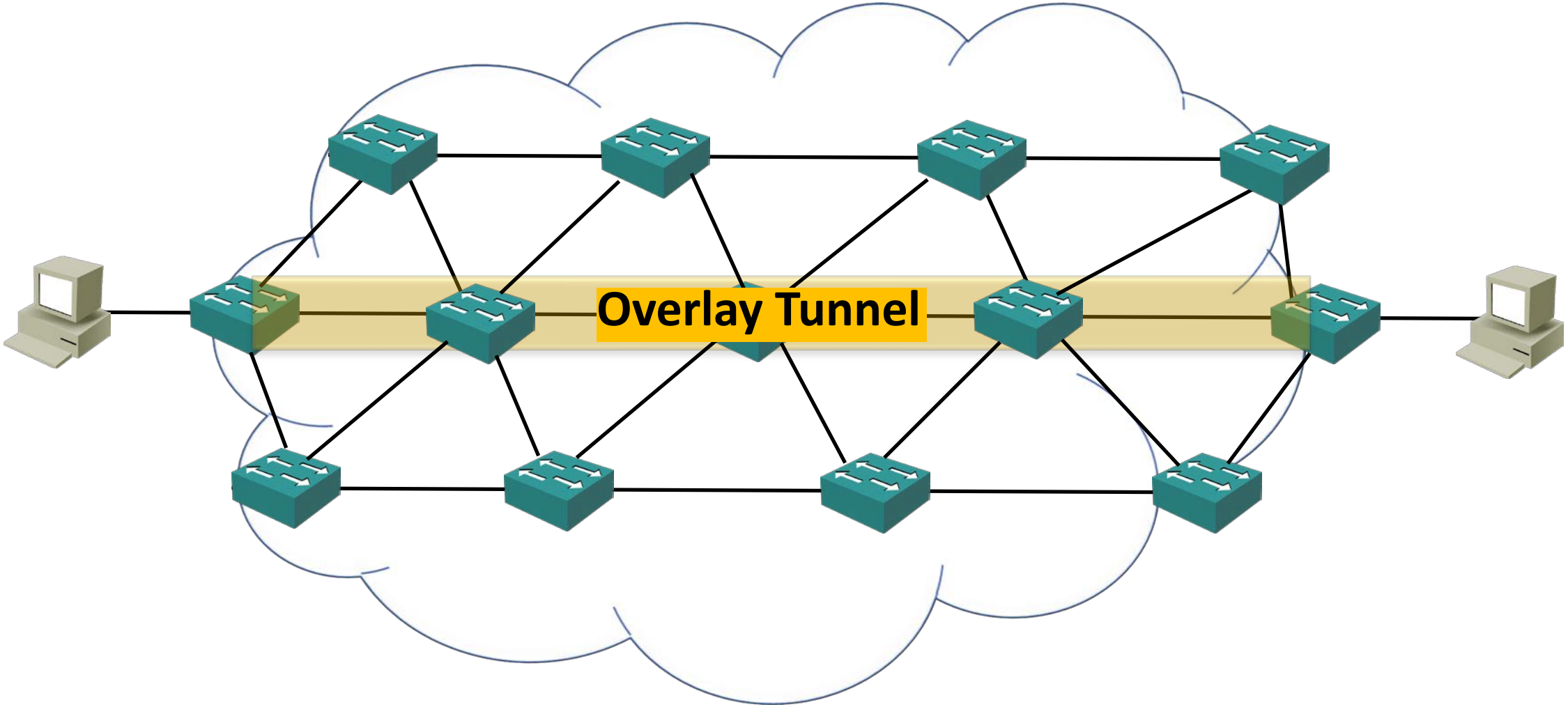
Underlay and Overlay Network

- SD-Access uses an underlay and overlay network
- An underlay network is the underlying physical network. It provides the underlying physical connections which the overlay network is built on top of.
- An overlay network is a logical topology used to virtually connect devices. It is built over the physical underlay network.
- The combination of underlay and overlay forms the SD-Access ‘network fabric’

Underlay Network



Overlay Network



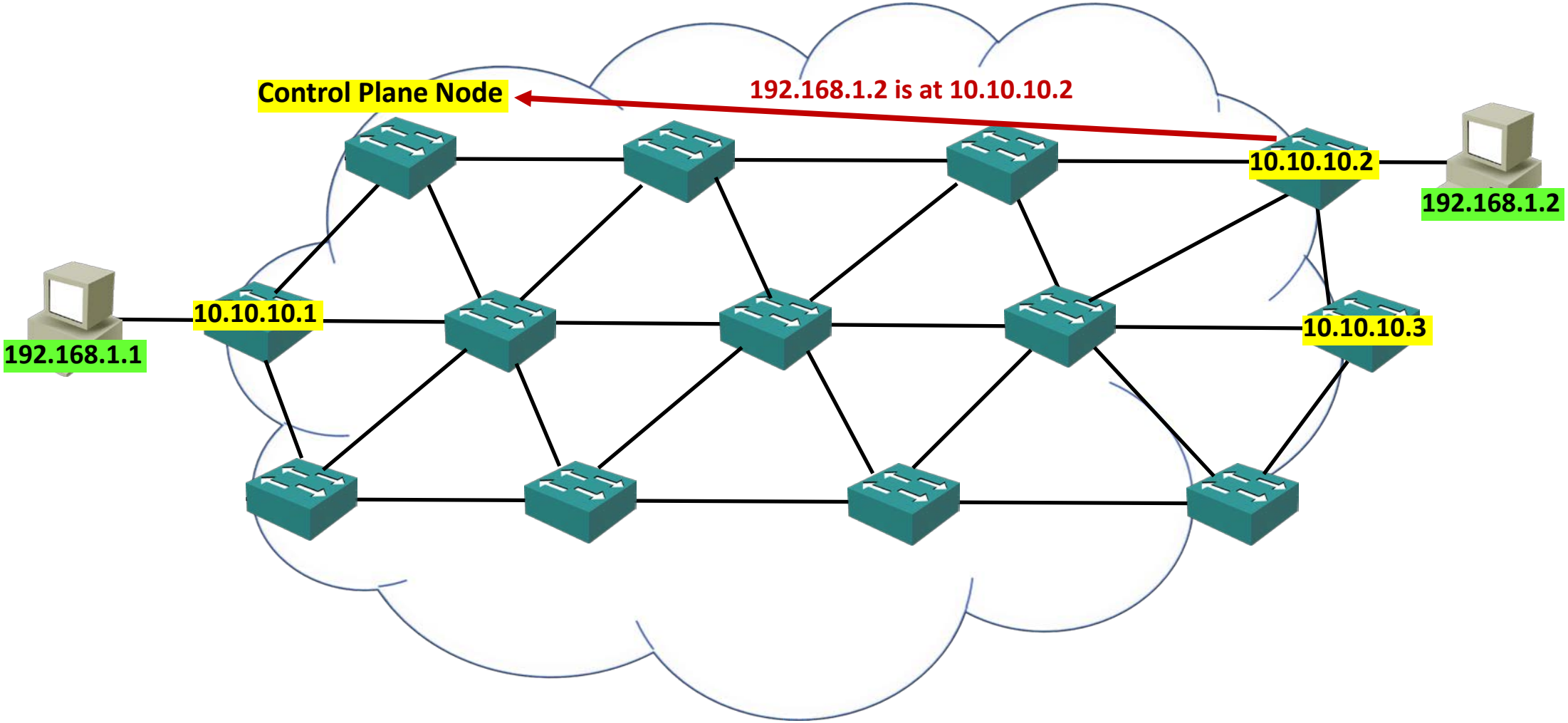
Underlay Network

- When SD-Access is deployed into an existing (‘brownfield’) network, any configuration can be used for the underlying physical network. Links between devices can be layer 2 or layer 3 and any routing protocol can be used
- DNA Center can be used to automatically provision the underlay network in new (‘greenfield’) sites. In this case layer 3 links are used between devices and IS-IS is used as the routing protocol

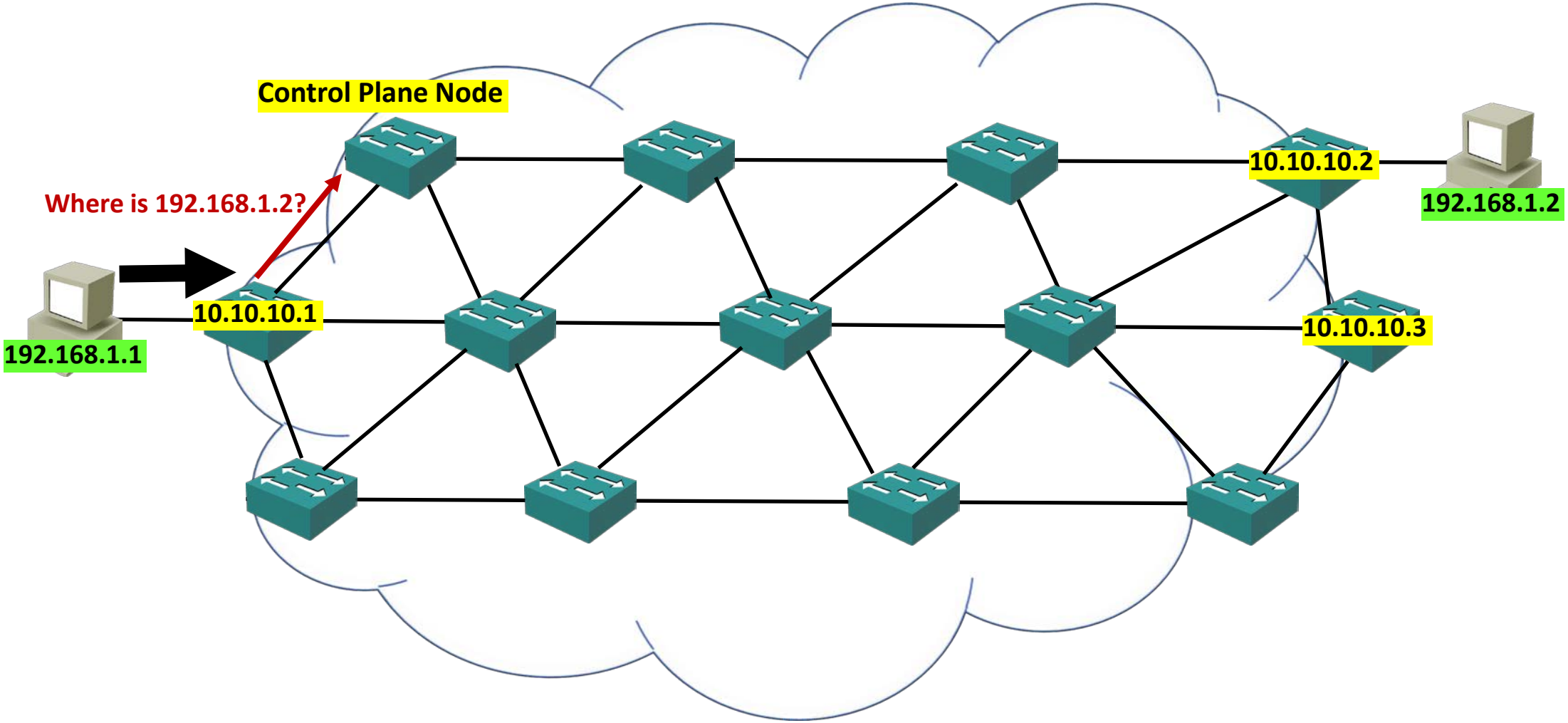
Overlay Network

- LISP is used for the Control Plane
- VXLAN is used for the Data Plane
- Cisco TrustSec CTS is used for the policy
- Each technology has been optimized for SD-Access

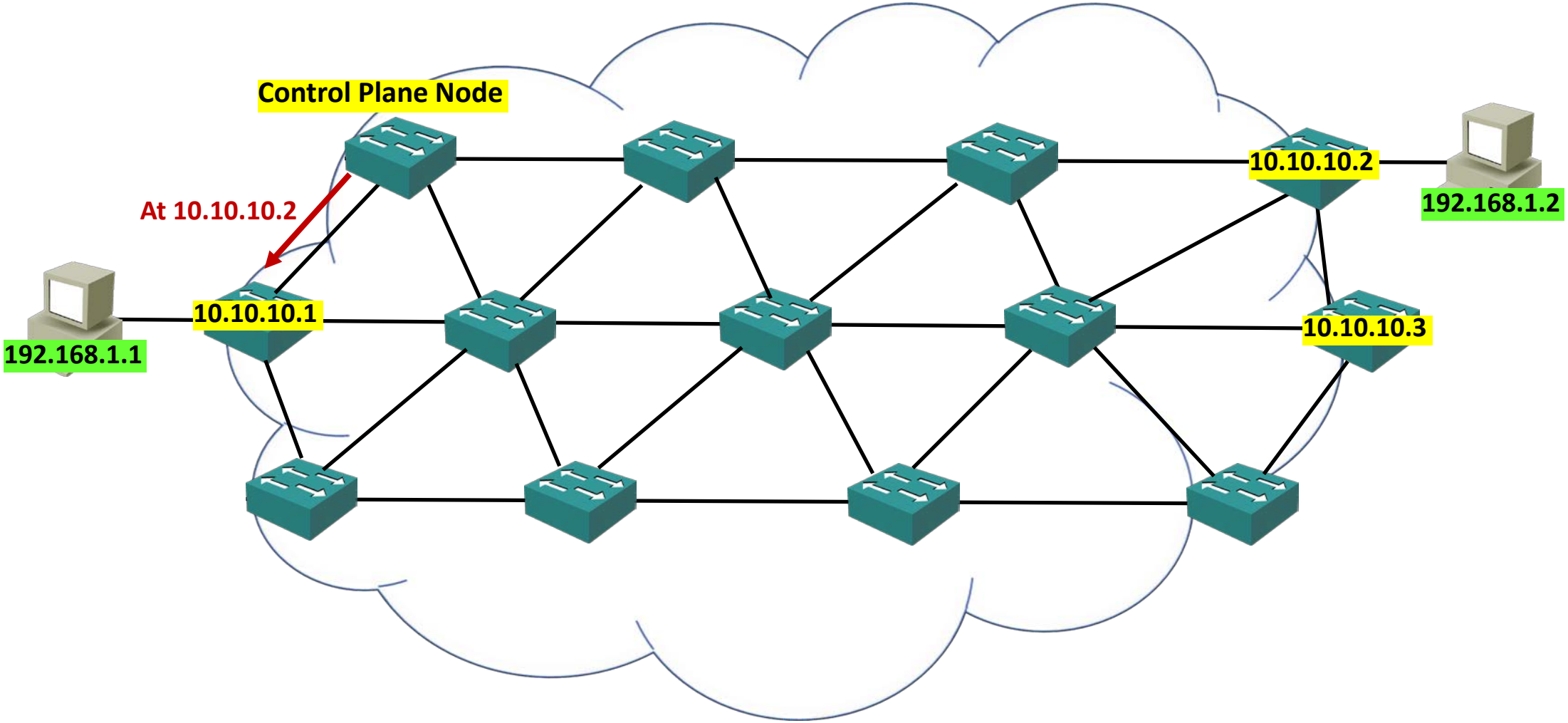
Control Plane - LISP



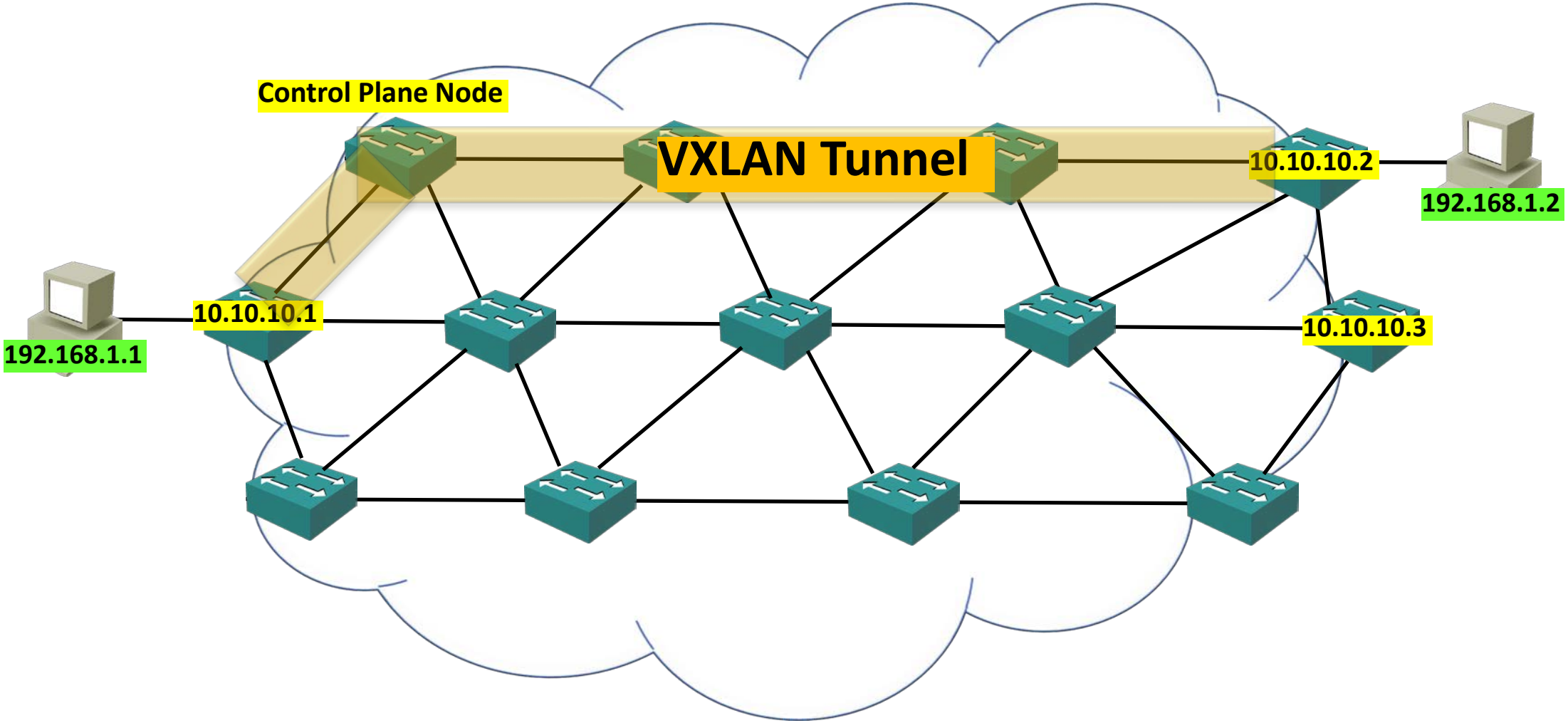
Control Plane - LISP



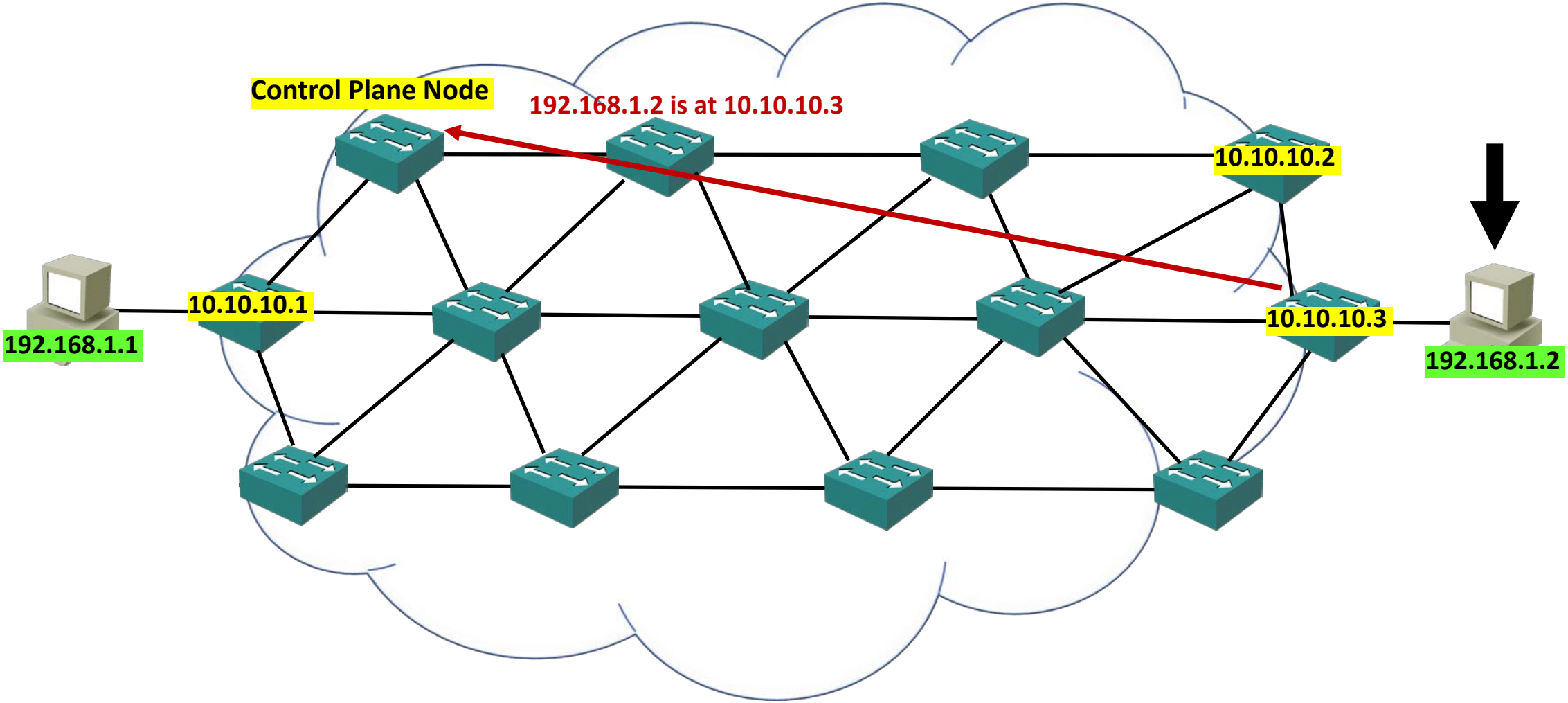
Control Plane - LISP



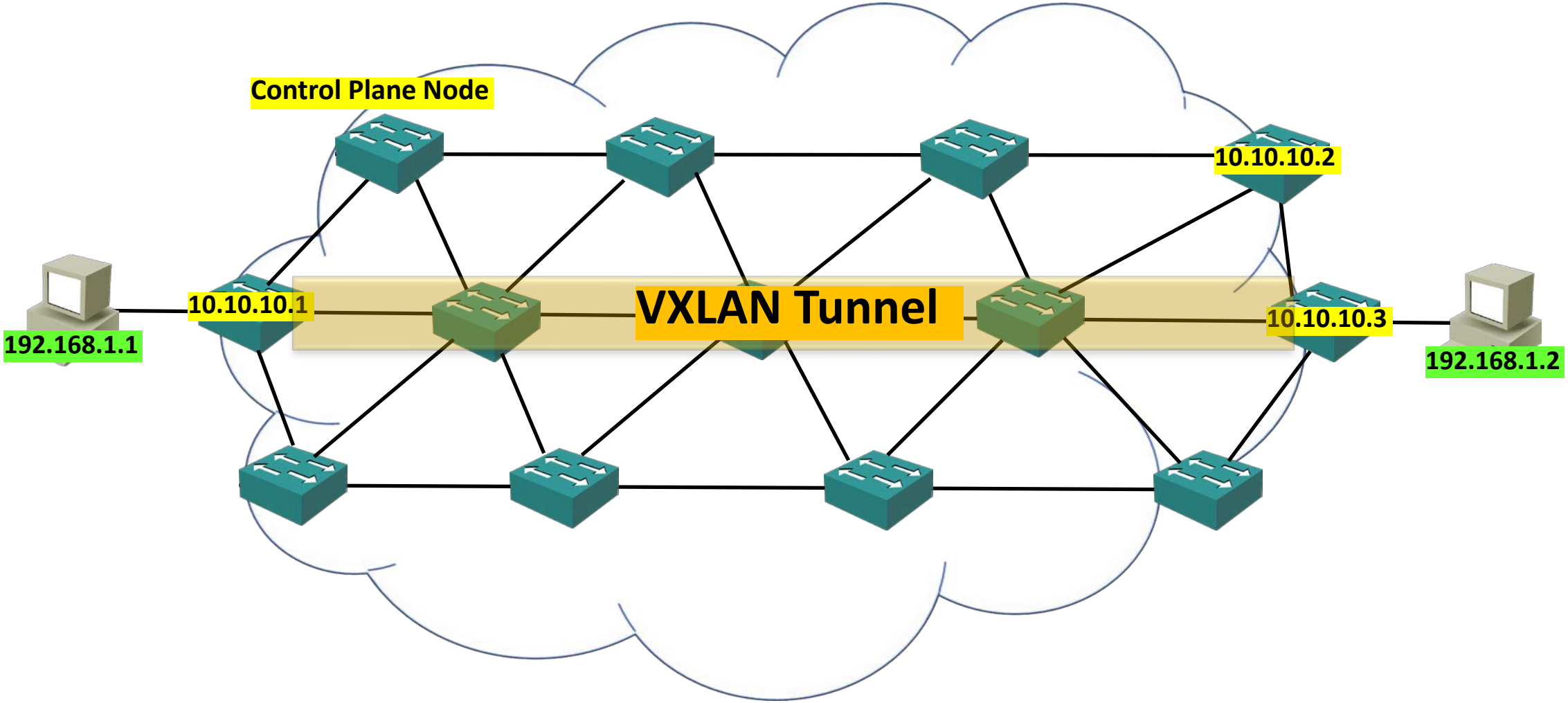
Data Plane - VXLAN



Mobility


Control Plane Node
192.168.1.2 is at 10.10.10.3
10.10.10.2
10.10.10.1
10.10.10.3
192.168.1.1
192.168.1.2

Mobility


Control Plane Node
10.10.10.2
10.10.10.1
VXLAN Tunnel
10.10.10.3
192.168.1.1
192.168.1.2

Policy Plane – Cisco TrustSec CTS

- Users are authenticated by the ISE Identity Services Engine
- The security policy is configured on DNA Center
- Users are allocated an SGT Scalable Group Tag
- Cisco TrustSec secures traffic flows based on the security policy and SGTs
- Standard TrustSec needs end-to-end TrustSec devices, SD-Access uses overlay tunnels so can work with other devices