White Paper

# Intent Based Campus Fabrics With Software Defined Access

forfusion

Transforming business, together
Visit www.forfusion.com

An Introduction

# What’s the difference between a traditional campus LAN and Cisco’s Software-Defined Access (SD-Access)?

Following on from an article that we wrote regarding the differences between Catalyst IOS and NX-OS, this is the first in a series that seeks to simplify the differences between traditional networking and SDN (software defined networking).

## Automation and Orchestration

### The first and most significant difference is automation and orchestration.

Traditionally a LAN implementation, for example, would require low-level configuration of each and every device that comprises the LAN, which can be a laborious process, and it also means that any subsequent changes need to be made to each device. With SD-Access, network configuration is automatic and based upon a single policy that governs how the network will behave. Changes and additions are also automatic, with the changes to the policy being passed down to the devices by a controller.

> SD-Access unifies both wired and wireless access together

Another important point is that SD-Access unifies both wired and wireless access together, whereby the same policies are propagated to both wired and wireless access networks at the same time.

A network policy controller (3rd party provisioning tools notwithstanding) is not a brand new concept in networking; however, the way that it's implemented for Cisco SD-Access is. The main principles of SD-Access operation are as follows:

- SD-Access uses Cisco DNA Center to manage, monitor and implement network policies, the policies themselves are used to generate configurational changes, and then pass these changes to each of the devices either by direct SSH access or by a Restful API call.
- SD-Access uses an automatically built underlay network using IS-IS as its control plane, the network automatically builds the underlay based on the initial policy.
- Fabric border nodes are analogous to distribution / core switches, they allow the end hosts to talk to IP networks outside of the fabric, such as a data centre or the internet.
- Fabric edge nodes are analogous to access layer switches, they allow the end hosts to connect to the network.
- Security policies for the end hosts are defined in Active Directory (AD) or a combination of AD and Cisco Identity Services Engine (ISE). 802.1X is then used to authenticate devices wishing to join the network.
- Both wired and wireless access can utilise the same policies and be controlled by the same instance of DNA Center, allowing the two technologies to be controlled in the same way, with the same policies.

## SD-Access Diagram

### A diagram detailing the components of SD-Access is shown on the next page, the main points to note are:

- Communication between hosts and outside networks is implemented by the use of overlays. When traffic from a source is permitted to talk to a destination an overlay is built to carry this traffic.
- The overlays are implemented using LISP encapsulated into VXLAN. LISP and VXLAN function to tunnel the traffic between fabric edge nodes and from edge nodes to border nodes.
- There are two types of overlays used, a layer 3 overlay when traffic needs to be routed and a layer 2 overlay when traffic needs to stay within the same broadcast domain.
- A layer 3 overlay is used to send traffic outside of the fabric, such as the internet or a data centre.
- A layer 2 overlay is used to send traffic between two hosts and is roughly analogous to a VLAN.

Get the White Paper

# Want to keep on reading?

To get access to this white paper and the full series, head to:

www.forfusion.com/white-papers