



Connecting to Digital

Connect & Secure 2019

Welcome

14 maart 2019



Connecting to Digital

Connect & Secure 2019

Deepdive SD-Access

Jesse Schmidt
Systems Engineer Enterprise Networks

14 maart 2019

Cisco DNA Architecture

Intent-based networking



Cisco DNA Center™

Cisco DNA Automation

Cisco DNA Security

Cisco DNA Assurance



Cisco® Identity Service Engine



Wireless access point



Cisco® Catalyst® 2000, 3000



Cisco Catalyst 4000, 6000



Cisco Nexus® 7000



Wireless controller



ISR/ASR



Wireless 802.11 ac Wave 2 AP



Cisco Catalyst 3850



Cisco Catalyst 9000



Industrial Ethernet Catalyst



Wireless controller



4000 Series ISR



NFV-IS

Traditional Cisco and third-party networks

Cisco DNA-ready networks

A photograph of the Golden Gate Bridge in San Francisco, California, viewed from a low angle looking across the water towards the second tower. The bridge's iconic orange-red color is prominent against the grey, overcast sky and the dark water. The bridge's suspension cables and towers are clearly visible. In the background, the city of San Francisco is visible on the hills, with a prominent radio tower on a hillside.

Fabric

Underlay – Overlay

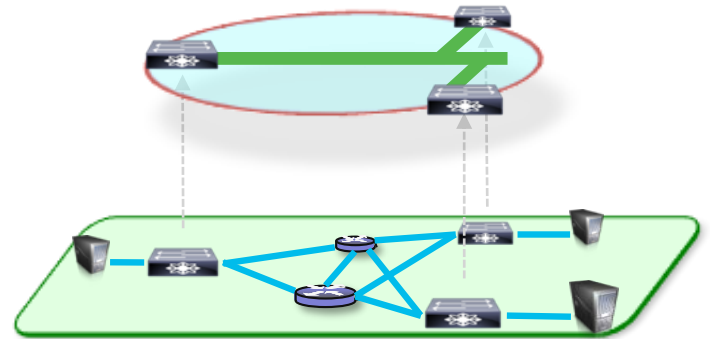
What exactly is a Fabric?

A **Fabric** is an **Overlay**

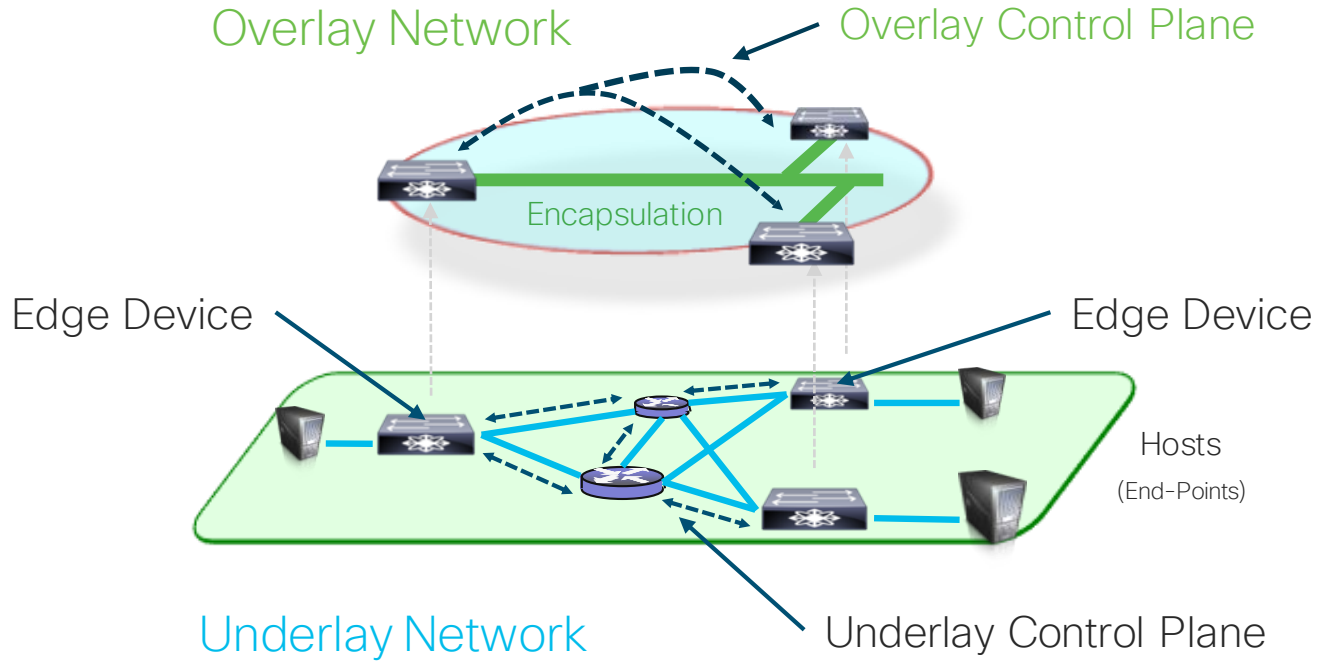
- An Overlay network is a logical topology used to virtually connect devices, built on top of some arbitrary physical Underlay topology.
- An Overlay network often uses alternate forwarding attributes to provide additional services, not provided by the Underlay.

Examples of Network Overlays

- | | |
|------------------|--------|
| • GRE or mGRE | • LISP |
| • MPLS or VPLS | • OTV |
| • IPsec or DMVPN | • DFA |
| • CAPWAP | • ACI |



SD-Access Underlay / Overlay



SD-Access Underlay

Manual vs. Automated

Manual Underlay



You can reuse your existing IP network as the Fabric Underlay!

- **Key Requirements**

- IP reach from Edge to Edge/Border/CP
- Can be L2 or L3 – We recommend L3
- Can be any IGP – We recommend ISIS

- **Key Considerations**

- MTU (Fabric Header adds 50B)
- Latency (RTT of =/< 100ms)

Automated Underlay



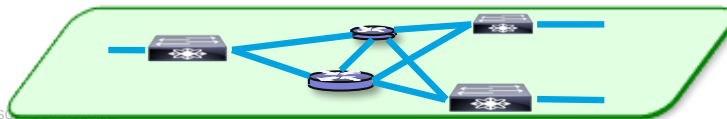
Prescriptive fully automated Global and IP Underlay Provisioning!

- **Key Requirements**

- Leverages standard PNP for Bootstrap
- Assumes New / Erased Configuration
- Uses a Global “Underlay” Address Pool

- **Key Considerations**

- PNP pre-setup is required
- 100% Prescriptive (No Custom)

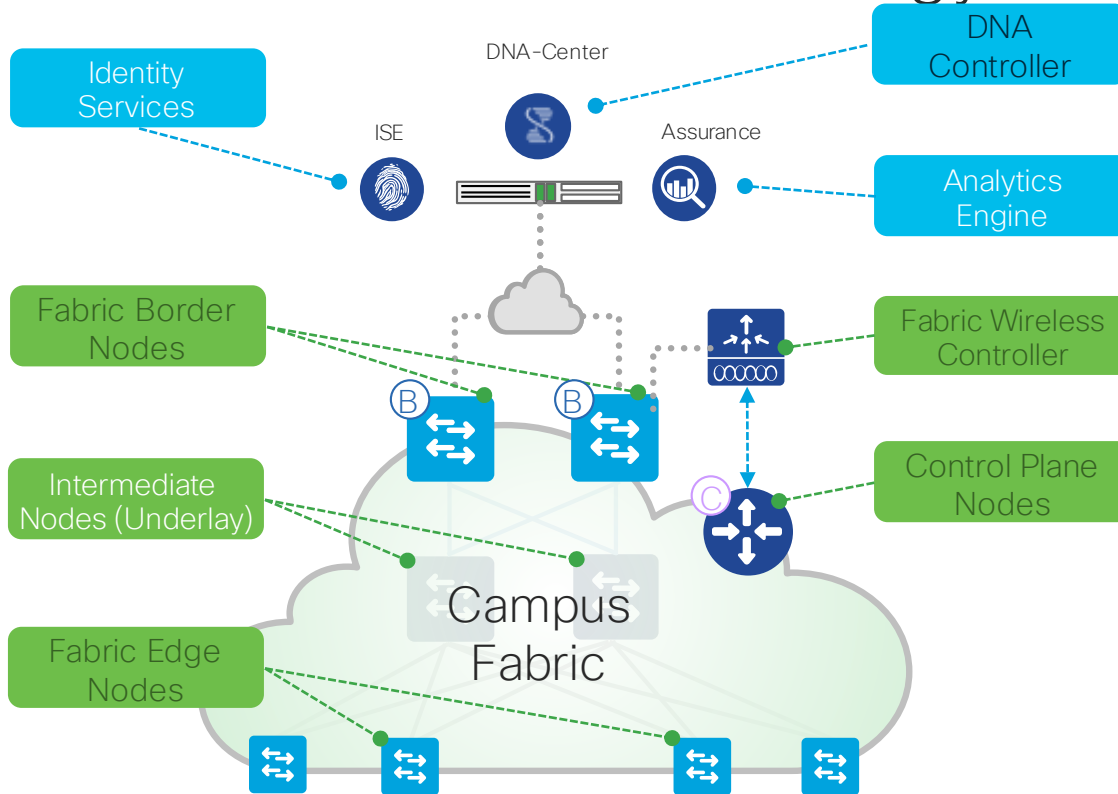


A photograph of the Golden Gate Bridge in San Francisco, California, viewed from a low angle looking across the water towards the second tower. The bridge's iconic orange-red color is prominent against the grey, overcast sky and the dark water. The text "SD-Access Roles" is overlaid in white on the left side of the bridge.

SD-Access Roles



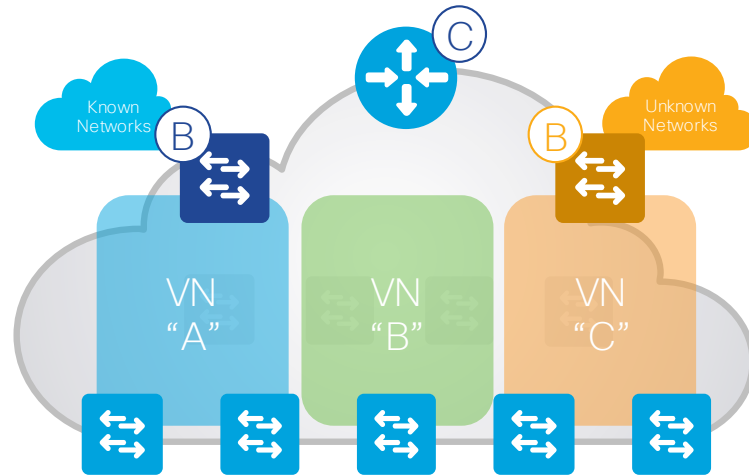
Fabric Roles & Terminology



- **DNA Controller** – Enterprise SDN Controller (e.g. DNA Center) provides GUI management and abstraction via Apps that share context
- **Identity Services** – External ID System(s) (e.g. ISE) are leveraged for dynamic Endpoint to Group mapping and Policy definition
- **Analytics Engine** – External Data Collector(s) are leveraged to analyze Endpoint to App flows and monitor fabric status
- **Control Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A Fabric device (e.g. Core) that connects External L3 network(s) to the SD-Access Fabric
- **Fabric Edge Nodes** – A Fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SD-Access Fabric
- **Fabric Wireless Controller** – A Fabric device (WLC) that connects Wireless Endpoints to the SD-Access Fabric

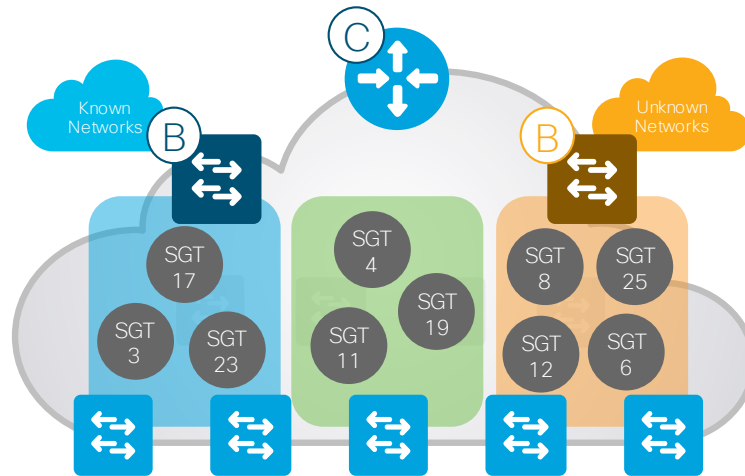
SD-Access Virtual Network

Virtual Network maintains a separate Routing & Switching instance for the devices within it.



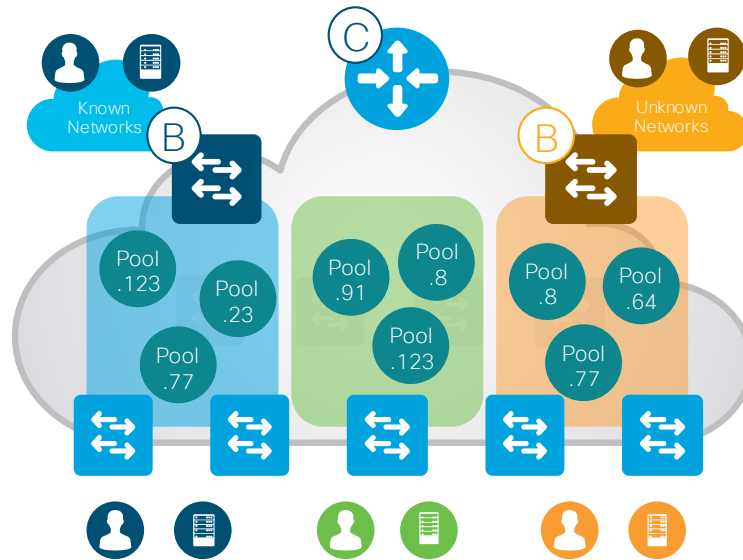
SD-Access Scalable Group

Scalable Group is a logical ID object to “group” Users and/or Devices.



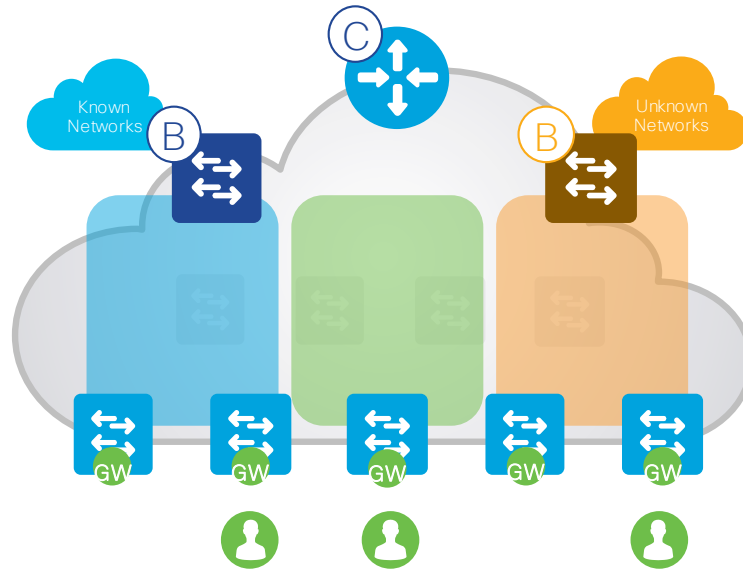
SD-Access Host Pool

Host Pool provides basic IP functions necessary for attached Endpoints



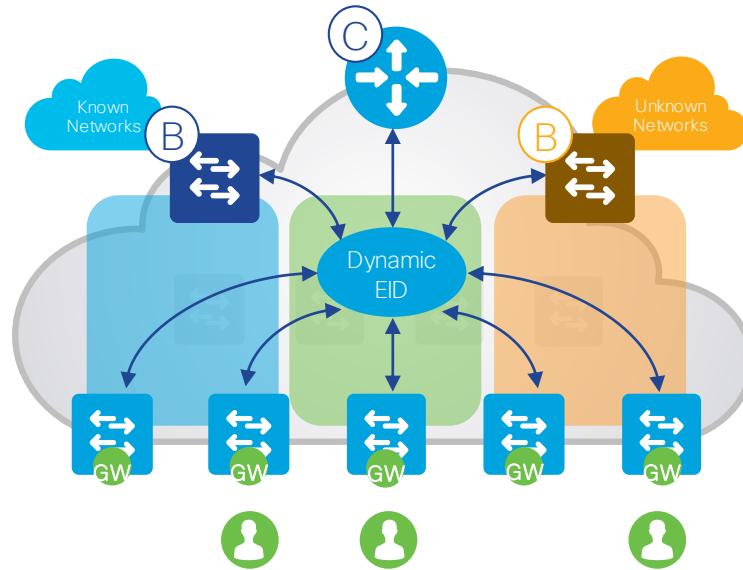
SD-Access Anycast Gateway

Anycast GW provides a single L3 Default Gateway for IP capable endpoints



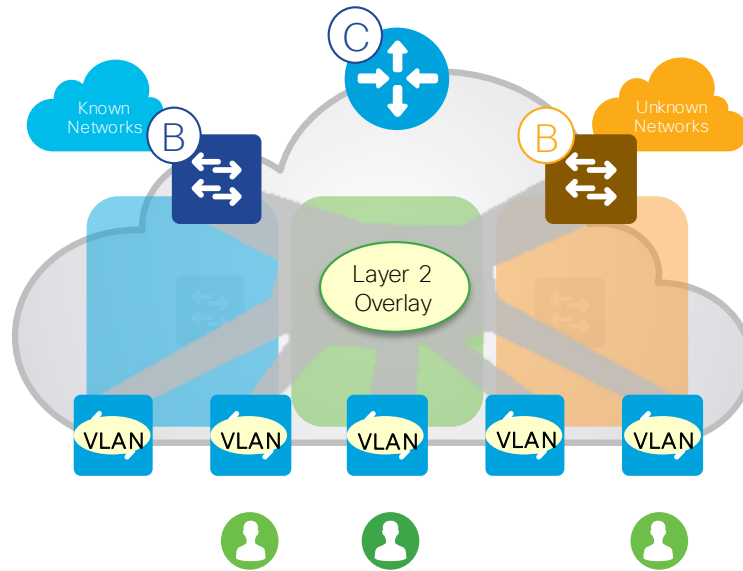
SD-Access Stretched Subnets

Stretched Subnets allow an IP subnet to be “stretched” via the overlay



SD-Access Layer2 Overlays

Layer2 Overlays allows Non-IP hosts to connect
Broadcast & Multicast



A photograph of the Golden Gate Bridge in San Francisco, California, viewed from a low angle looking across the water towards the second tower. The bridge's iconic orange-red color is prominent against the grey, overcast sky and the dark water. The bridge's suspension cables and towers are clearly visible. The text "SD-Access Key Components" is overlaid in white on the left side of the image.

SD-Access Key Components

Key Components of SD-Access

1. Control Plane based on LISP
2. Data-Plane based on VXLAN
3. Policy-Plane based on TrustSec

Key Differences

- L2 + L3 Overlay -vs- L2 or L3 Only
- Host Mobility with Anycast Gateway
- Adds VRF + SGT into Data-Plane
- Virtual Tunnel Endpoints (No Static)
- No Topology Limitations (Basic IP)

Locator / ID Separation Protocol LISP Mapping System

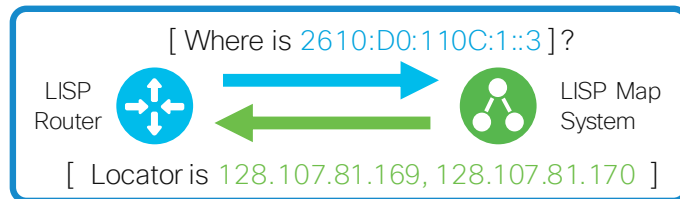
LISP “Mapping System” is analogous to a DNS lookup

- DNS resolves [IP Addresses](#) for queried [Name](#) Answers the “WHO IS” question



DNS
Name -to- IP
URL Resolution

- LISP resolves [Locators](#) for queried [Identities](#) Answers the “WHERE IS” question



LISP
ID -to- Locator
Map Resolution

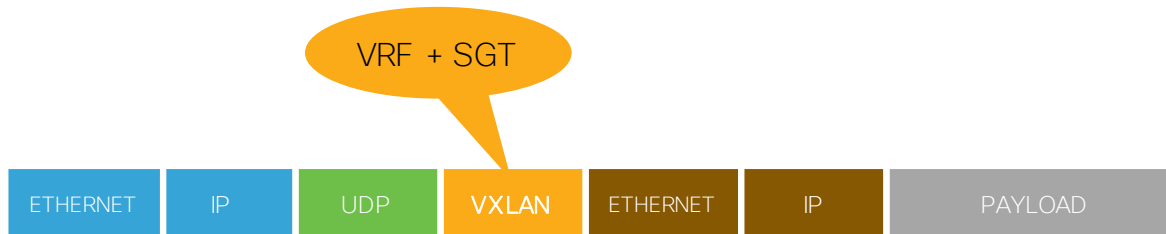
SD-Access Key Components – VXLAN

1. Control Plane based on LISP
2. Data-Plane based on VXLAN



SD-Access Key Components – TrustSec

1. Control Plane based on LISP
2. Data-Plane based on VXLAN
3. Policy-Plane based on TrustSec



Virtual Routing & Forwarding
Scalable Group Tagging

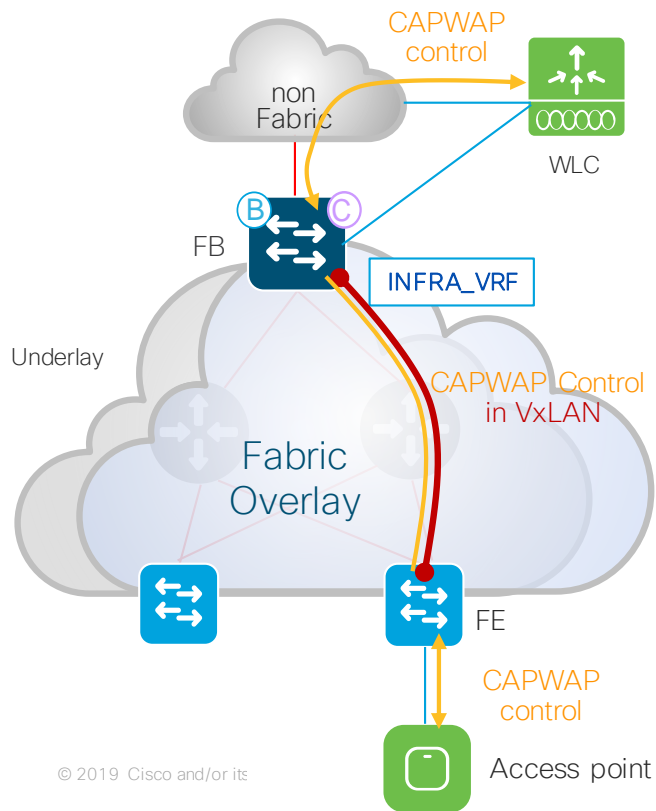


A photograph of the Golden Gate Bridge in San Francisco, California, viewed from a low angle looking across the water towards the second tower. The bridge's iconic orange-red color is prominent. The sky is overcast and grey, and the water is dark. The text "SD-Access Wireless Integration" is overlaid in white on the left side of the image.

SD-Access Wireless Integration

Wireless Integration

Where to connect APs and WLC?



Access Points

- AP is directly connected to FE
- AP is part of Fabric overlay
- AP belongs to the INFRA_VRF which is mapped to the global routing table (new in DNAC 1.1)
- AP joins the WLC in Local mode

WLC

- WLC is connected outside Fabric (optionally directly to Border)
- WLC needs to reside in global routing table
- No need for inter-VRF leaking for AP to join the WLC
- WLC can only belong to one FD. WLC talks to one CP (two for HA)

Design Notes:

- 1) Fabric AP is in local mode, need < 20ms latency between AP & WLC
- 2) If WLC is used also for non-Fabric (mixed mode), considered MAC and ARP table scale of the directly-connected Border device

A wide-angle, low-angle shot of the Golden Gate Bridge in San Francisco, California, taken during the "blue hour" of dusk. The bridge's iconic orange-red towers and suspension cables are silhouetted against a pale, overcast sky. The bridge deck is visible, with several cars driving across it. The water of the San Francisco Bay is dark and calm, reflecting the ambient light. In the background, the city's hills and a prominent radio tower are visible under the twilight sky. The overall mood is serene and atmospheric.

Demo

A photograph of the Golden Gate Bridge in San Francisco, viewed from a low angle looking up at the tower and across the water. The bridge's red-orange color is prominent against the grey sky and water.

Key takeaways

- Plan your personal demo: <https://cs.co/sdademo>
- Contact your Cisco AM to schedule a design session
- Pick up your SD-Access book

