
cisco Live!
ALL IN

The bridge to possible

Segmentation Simplified

A Case Study of Meraki Adaptive Policy and Cisco TrustSec

Lee Sudduth, Customer Delivery Architect
Praveen Poojary, Customer Delivery Architect

BRKXAR-2005

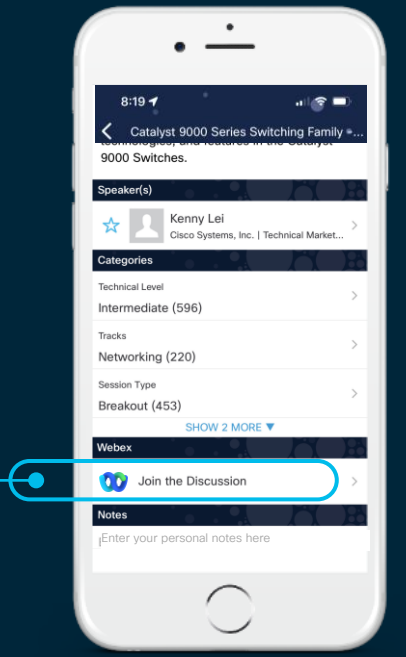
Cisco Webex App

Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKXAR-2005

Webex spaces will be moderated by the speaker until June 17, 2022.

About Us

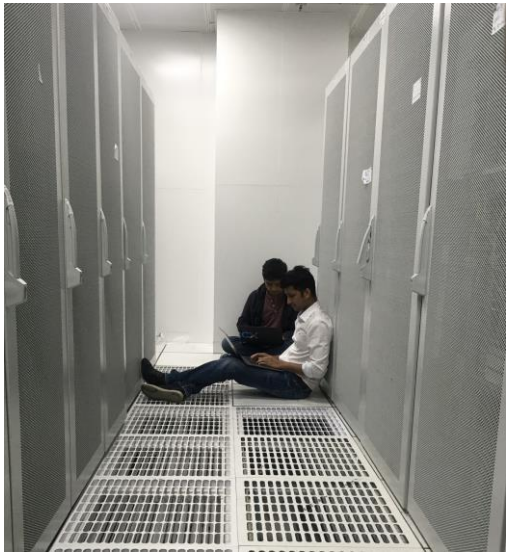
Praveen Poojary

Customer Delivery Architect

11 Years in Cisco

#3xCCIE

#CCDE



Lee Sudduth

Customer Delivery Architect

22 Years in Cisco

#CCIE

#CCDE

Introduction

Agenda

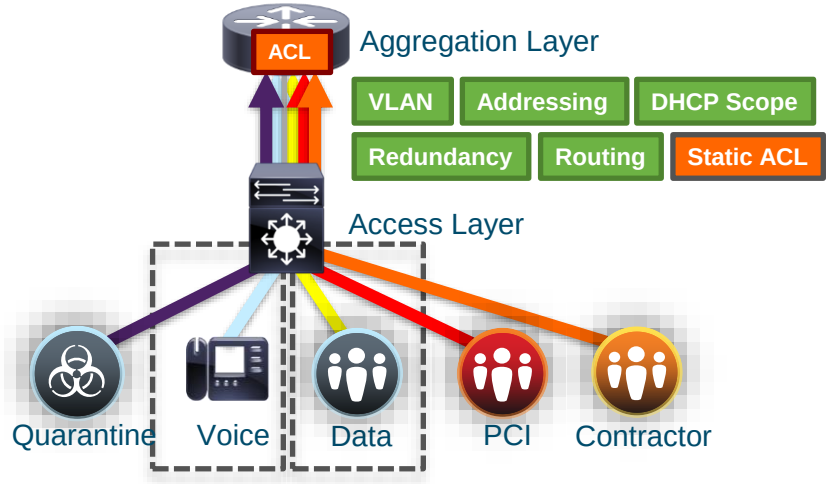
- Technology Overview
- Case Study
- Conclusion

Overview

Choosing the Right Tool

Traditional Segmentation

Design needs to be replicated for floors, buildings, offices, and other facilities. Cost could be extremely high



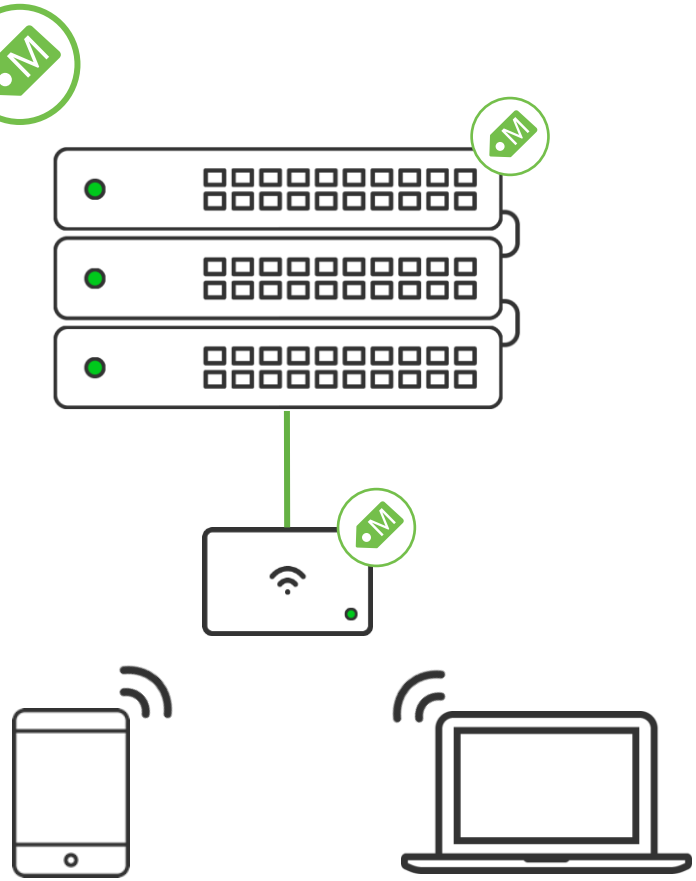
Simple Segmentation with 2 VLANs

More Policies using more VLANs

Meraki Adaptive Policy

- Identity and policy based on tags
- Uses inline SGTs
- Org-wide policy based on intent, not IP
- Provides micro-segmentation within VLANs
- Flexible tag assignment

- Supported platforms:
  - All Meraki 802.11ac wave 2 and Wi-FI 6 MR
    - Requires MR27 Firmware
  - All Meraki MS390 switching platforms
  - Requires MS390 & MR Advanced License



Flexible Tag Assignment

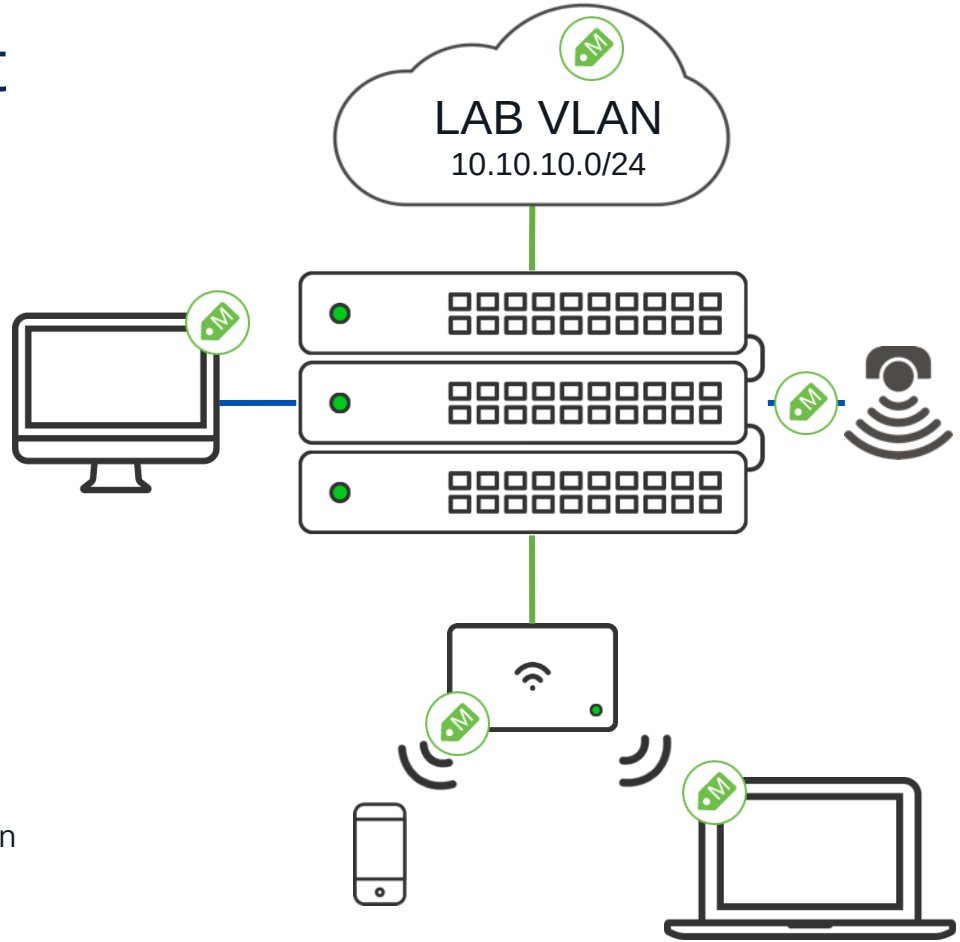
Tags can be applied in many different ways:

Statically assigned to a switch port
- Wired IOT Sensors

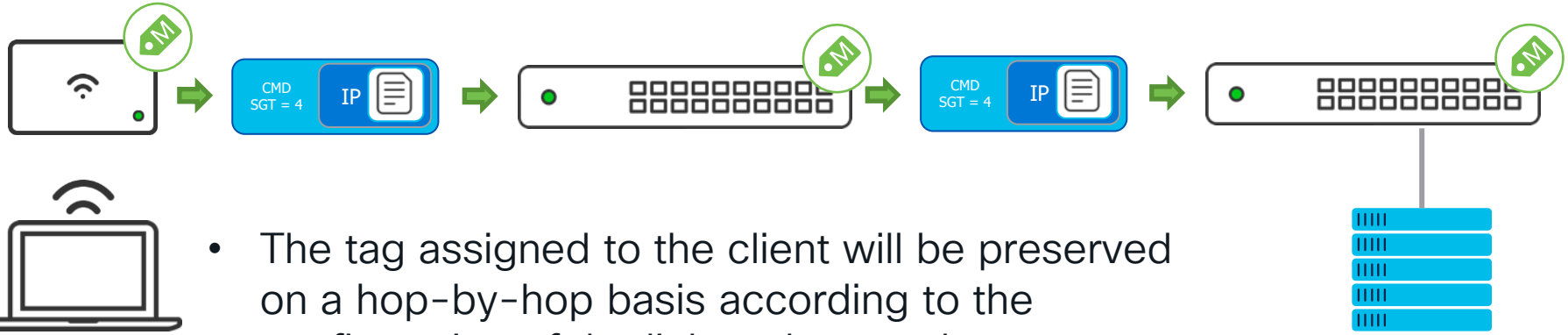
Static assignment per SSID
- Guest Users

Dynamic assignment via RADIUS
- Wired & Wireless 802.1x

Static IP to SGT Mapping
- Last resort to map traffic to an SGT
- Uses network objects as source for mapping
- Available w/ network object public beta – coming soon



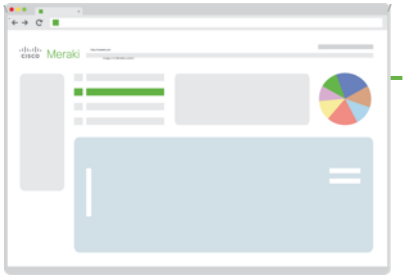
Tag Application and Preservation



- The tag assigned to the client will be preserved on a hop-by-hop basis according to the configuration of the link to the next hop
- Entire path must support inline SGTs
- The tag can be seen on the network device, not on the sending/receiving client

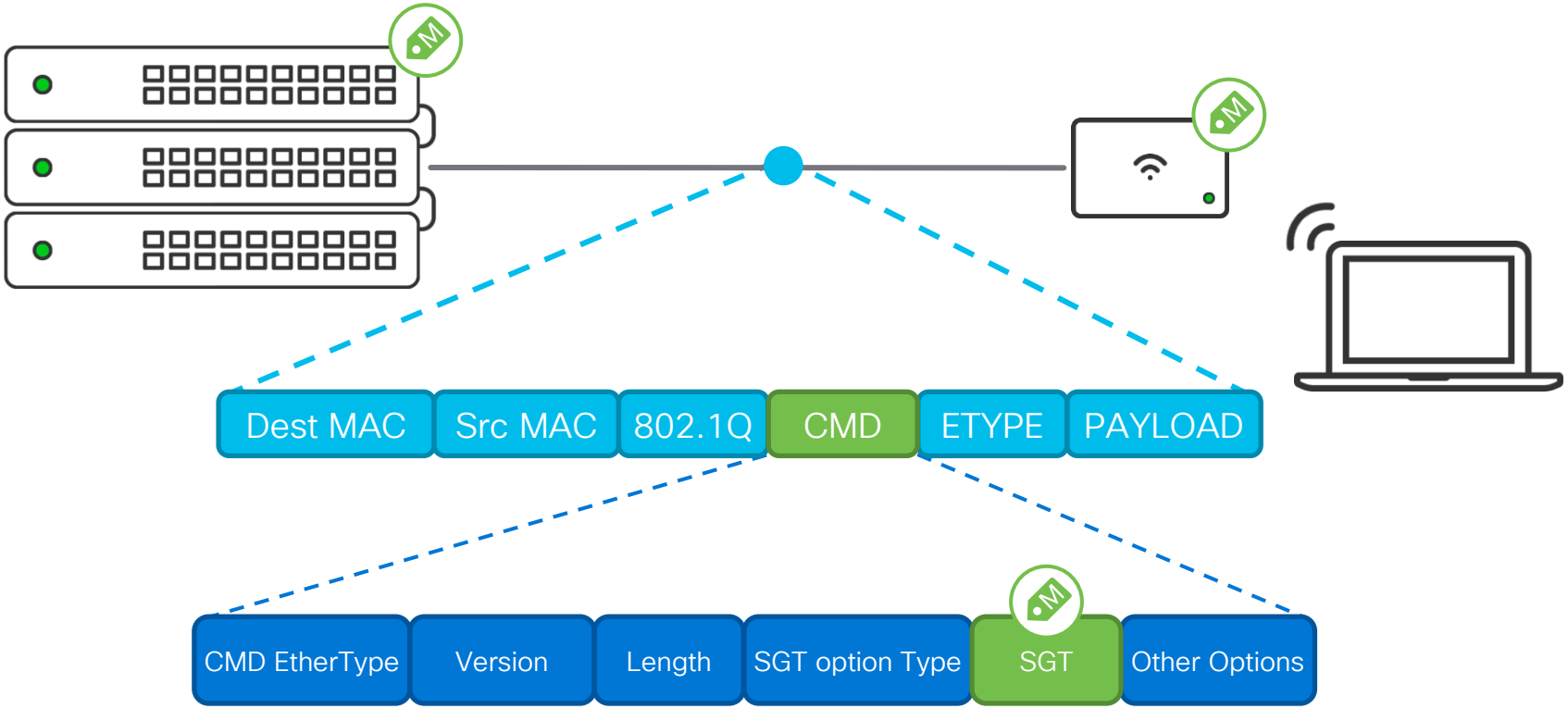
One Consistent Policy Across All Sites

SRC | DST	Employee	IoT	IoT Server
Employee	✔	✘	✔
IoT	✘	✘	✔
IoT Server	✔	✔	✔



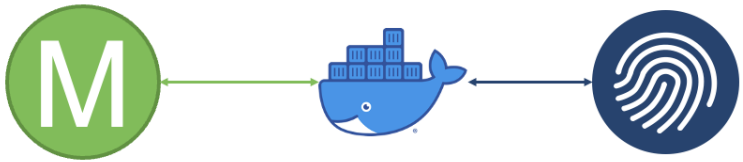
Policy & Groups are configured in dashboard and pushed to Adaptive Policy nodes like any other Meraki configuration change

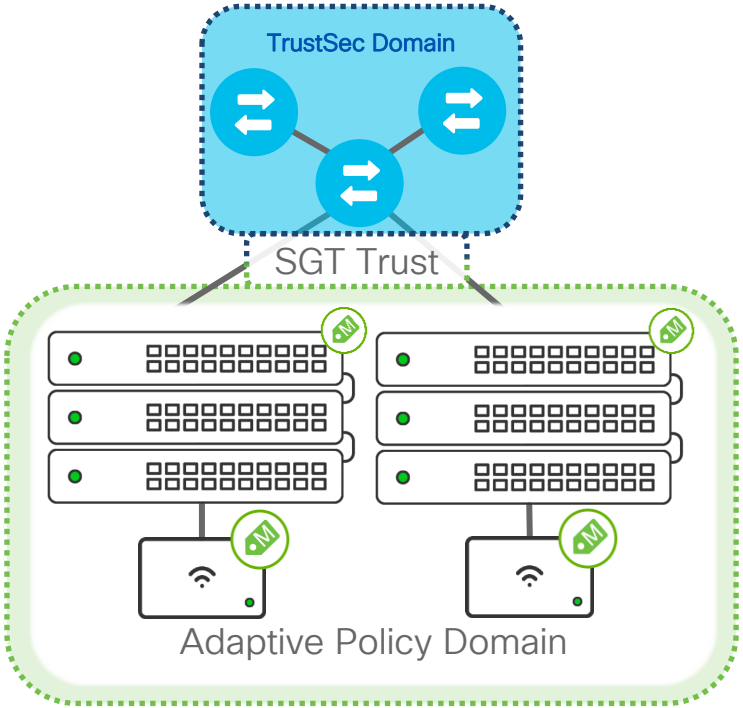
What are SGTs?



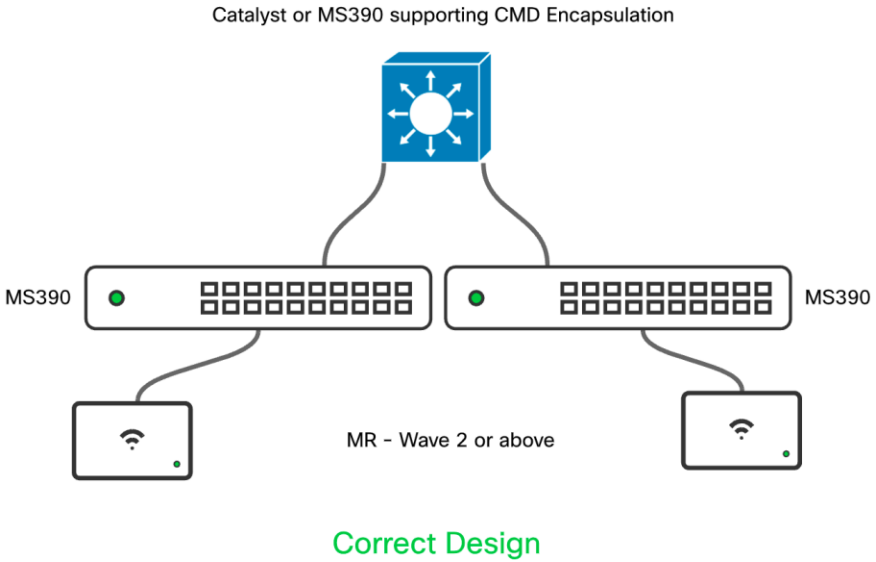
Adaptive Policy and TrustSec

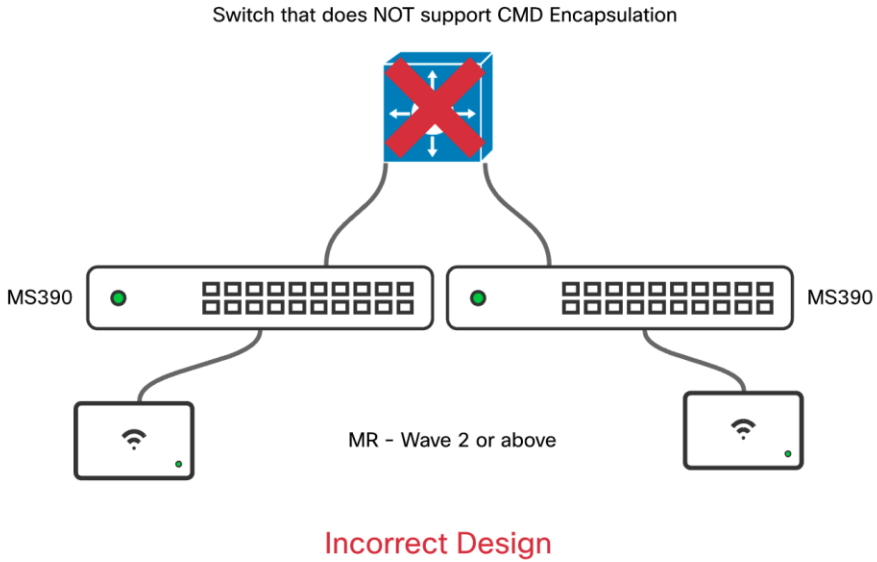
- Tag propagation between domains
- ISE as the central policy source of truth
- Use container for policy sync *(Optional)*
- <= 60 tags in deployment





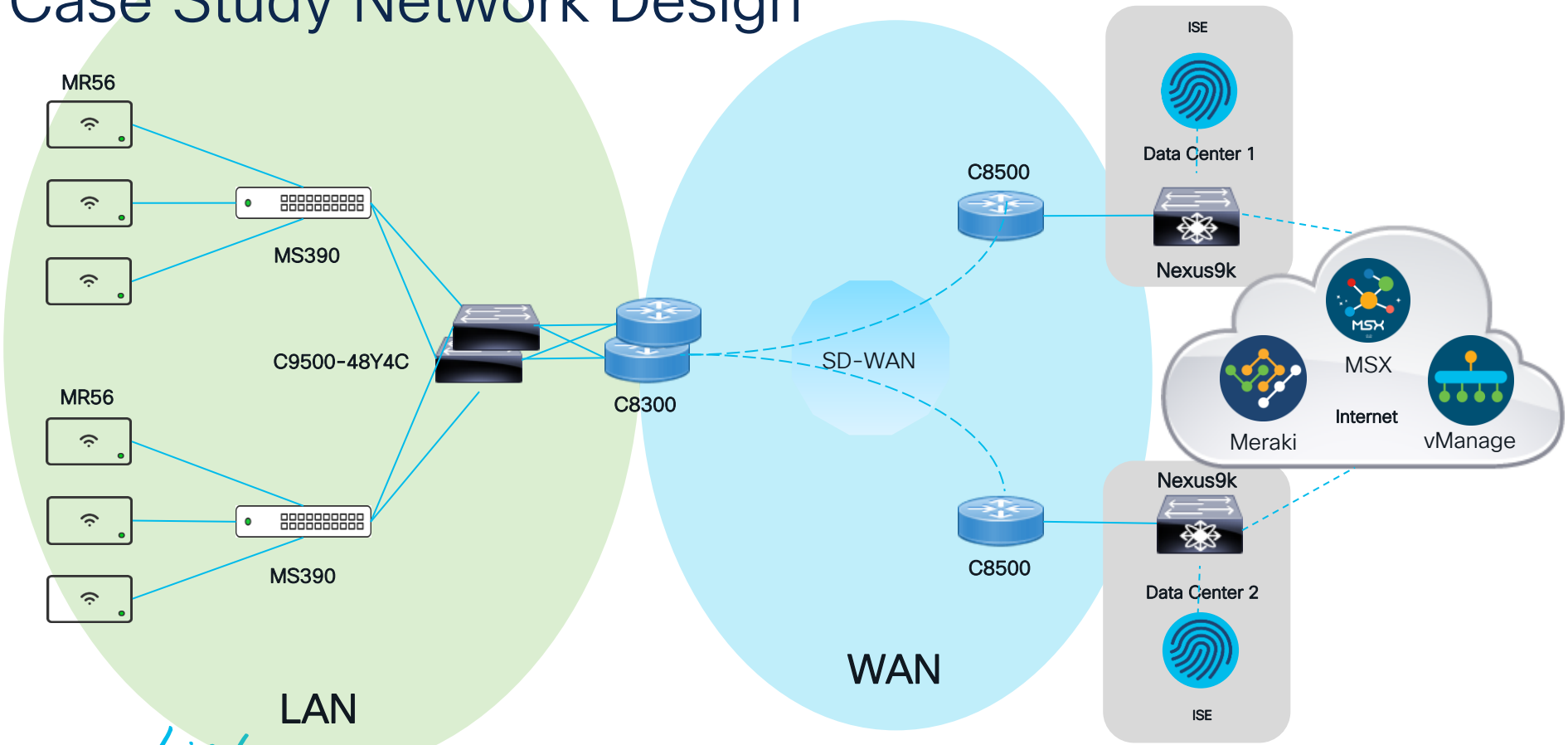
Integrating with Catalyst





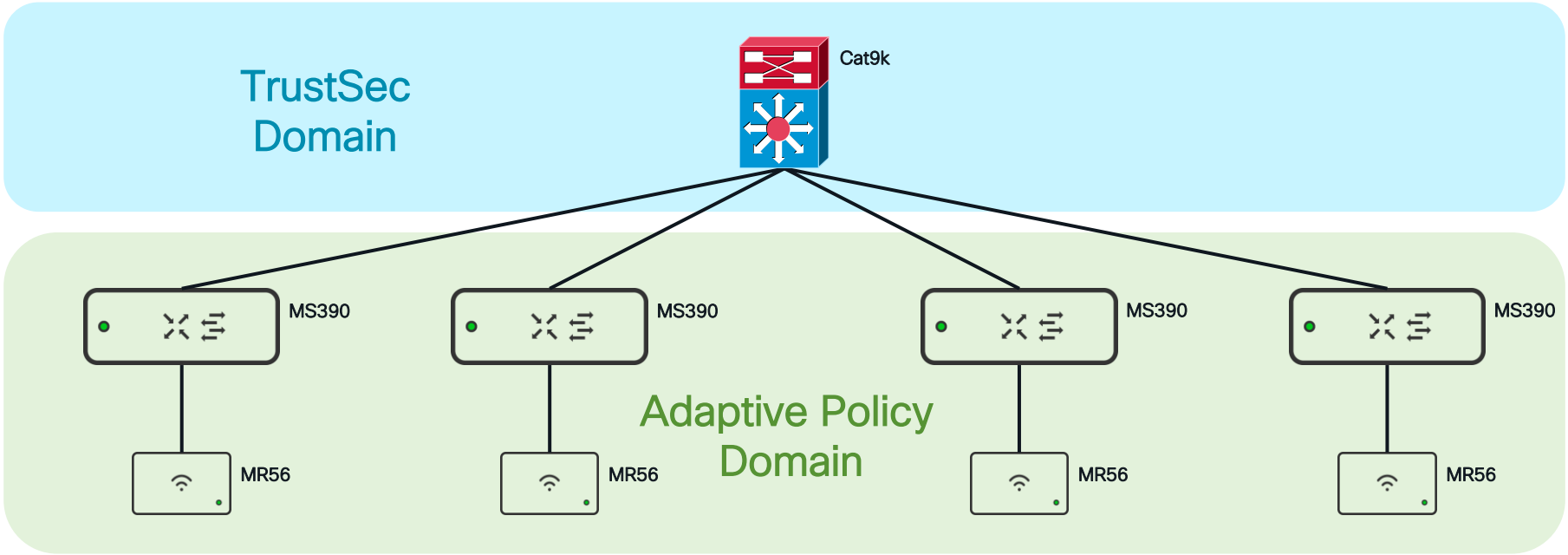
Case Study

Case Study Network Design



Meraki Access / Catalyst Core

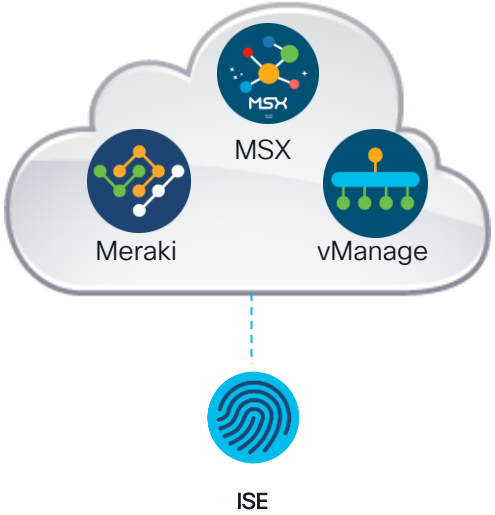
Core: SGT Propagate and Enforce



Case Study Orchestration Design

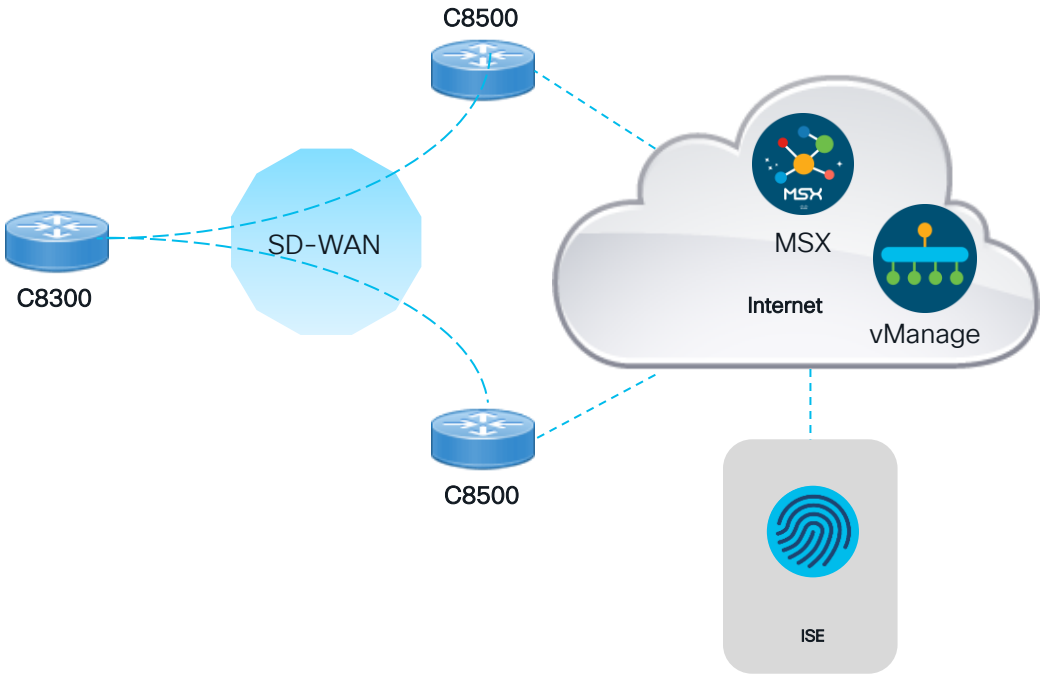
MSX Orchestrator

- Meraki Dashboard
  - Wireless Access
- Meraki Dashboard
  - Wired Access
- MSX (NSO)
  - Cat9k Core Switches
- vManage
  - SD-WAN
- ISE/ Meraki Dashboard
  - Adaptive Policy



SD-WAN Overlay Design

- C8300 cEdge Router
- C8500 cEdge Router
- Routing to Data Center via C8500
- TrustSec Security Policy



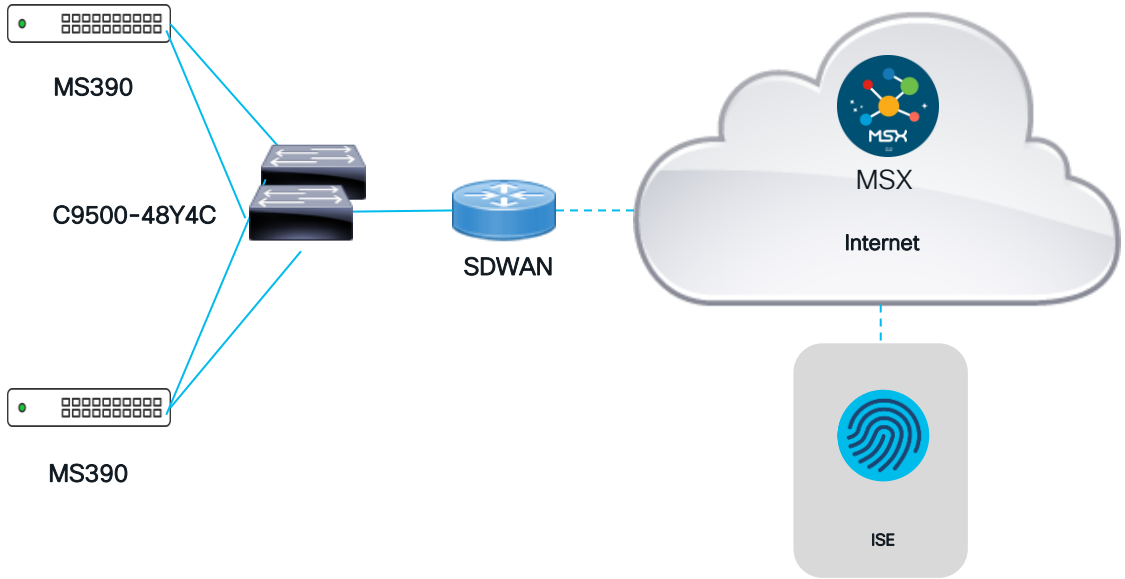
Catalyst 9500 LAN Routing and Switching Core

Catalyst 9500-48Y4C
- Stackwise Virtual

Layer 2
- VLAN Segmentation
- SGT Propagation

Layer 3
- IP Segmentation
- Local Routing
- WAN Routing

Security Policy
- TrustSec



Meraki LAN Access

- MR56 Wireless Access
- MS390 Wired Access

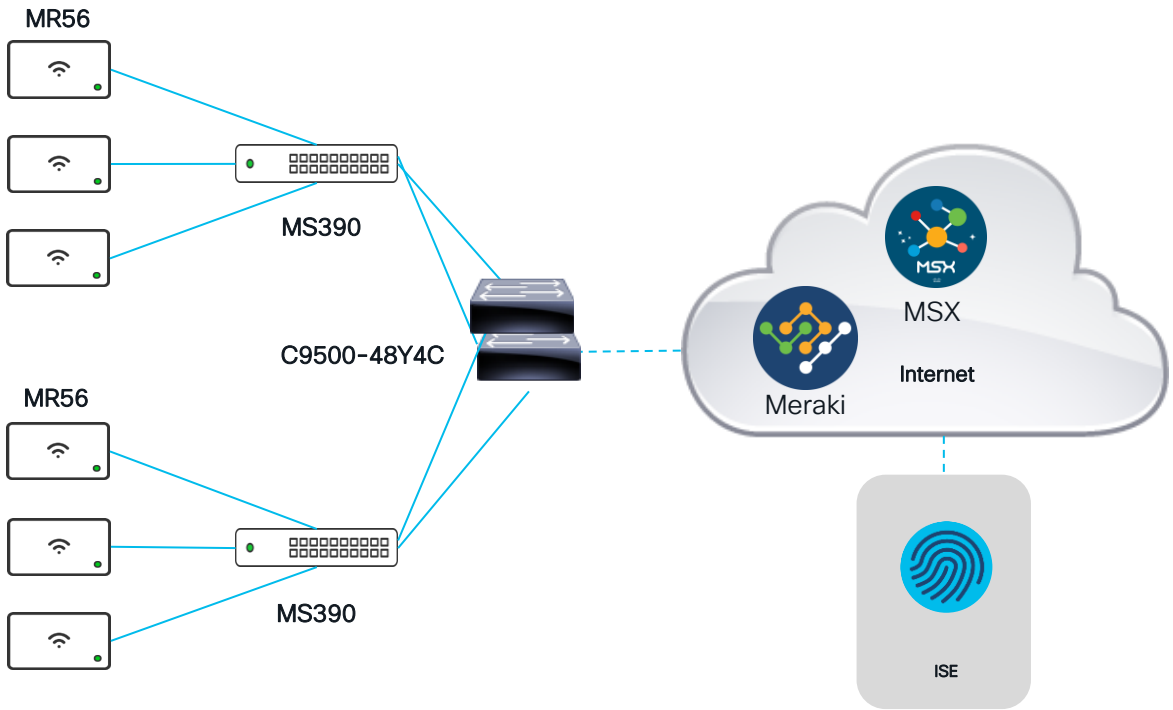
- Security Policy

Statically assigned to a switch port

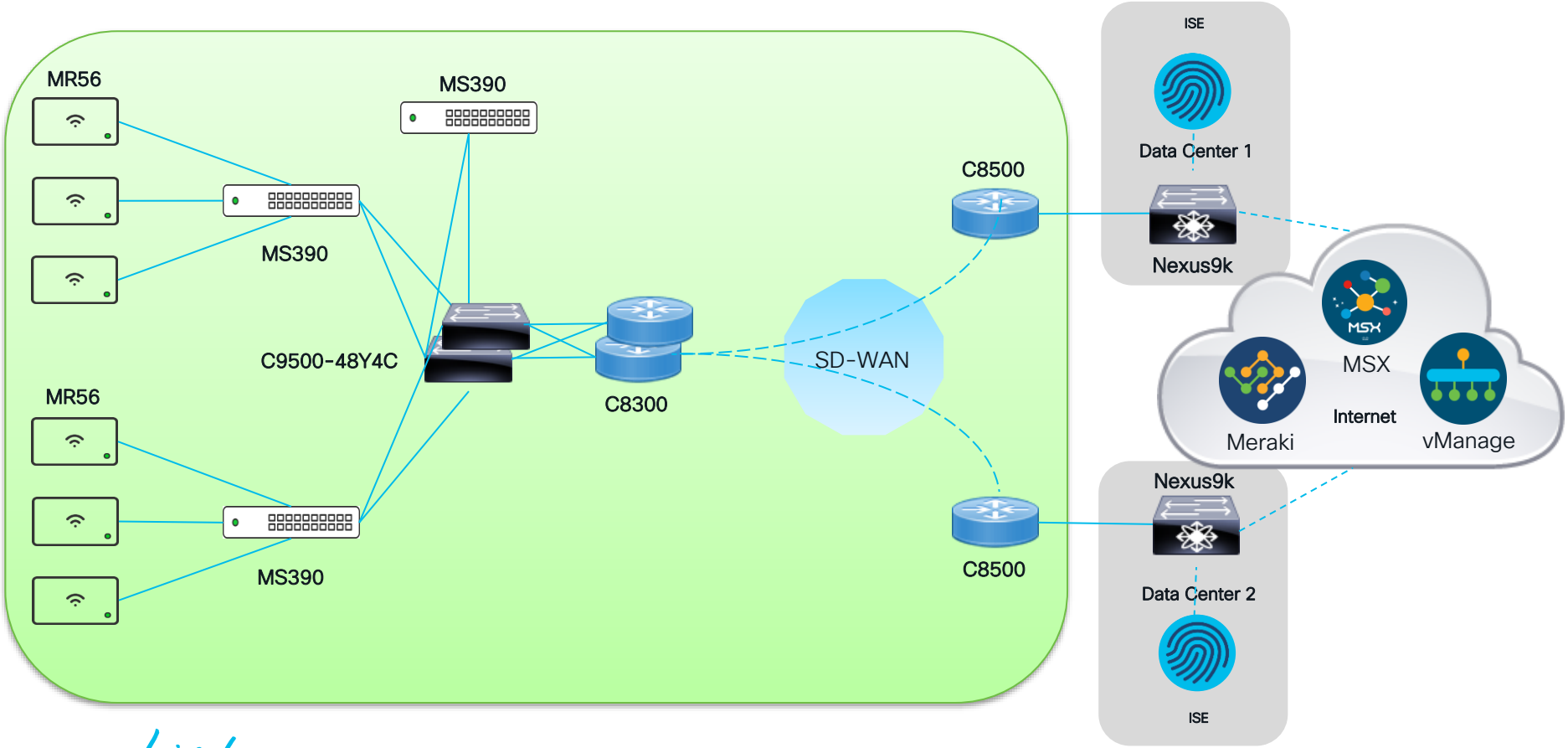
Static assignment per SSID

Dynamic assignment via RADIUS
Wired & Wireless 802.1x

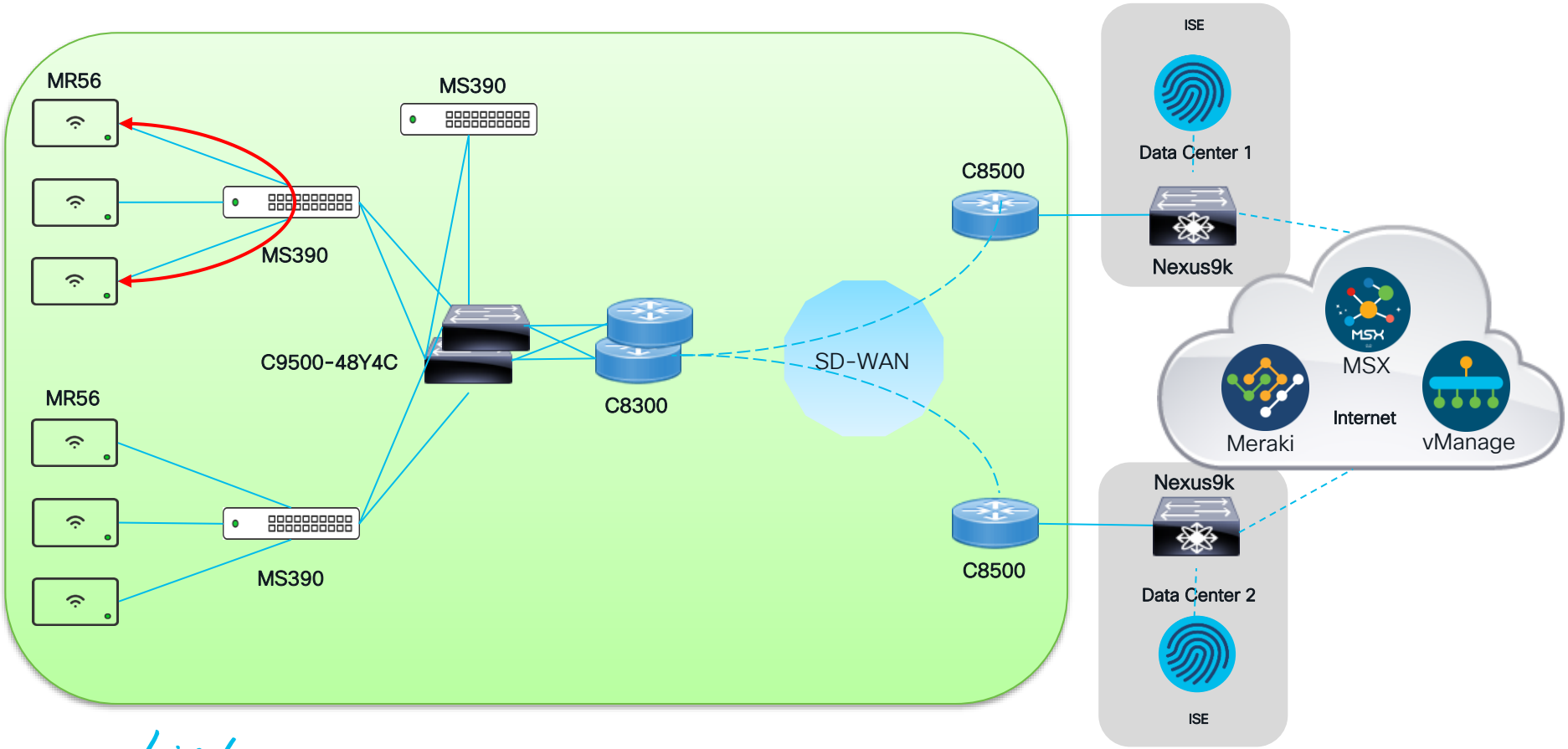
Static IP to SGT Mapping
Uses network objects



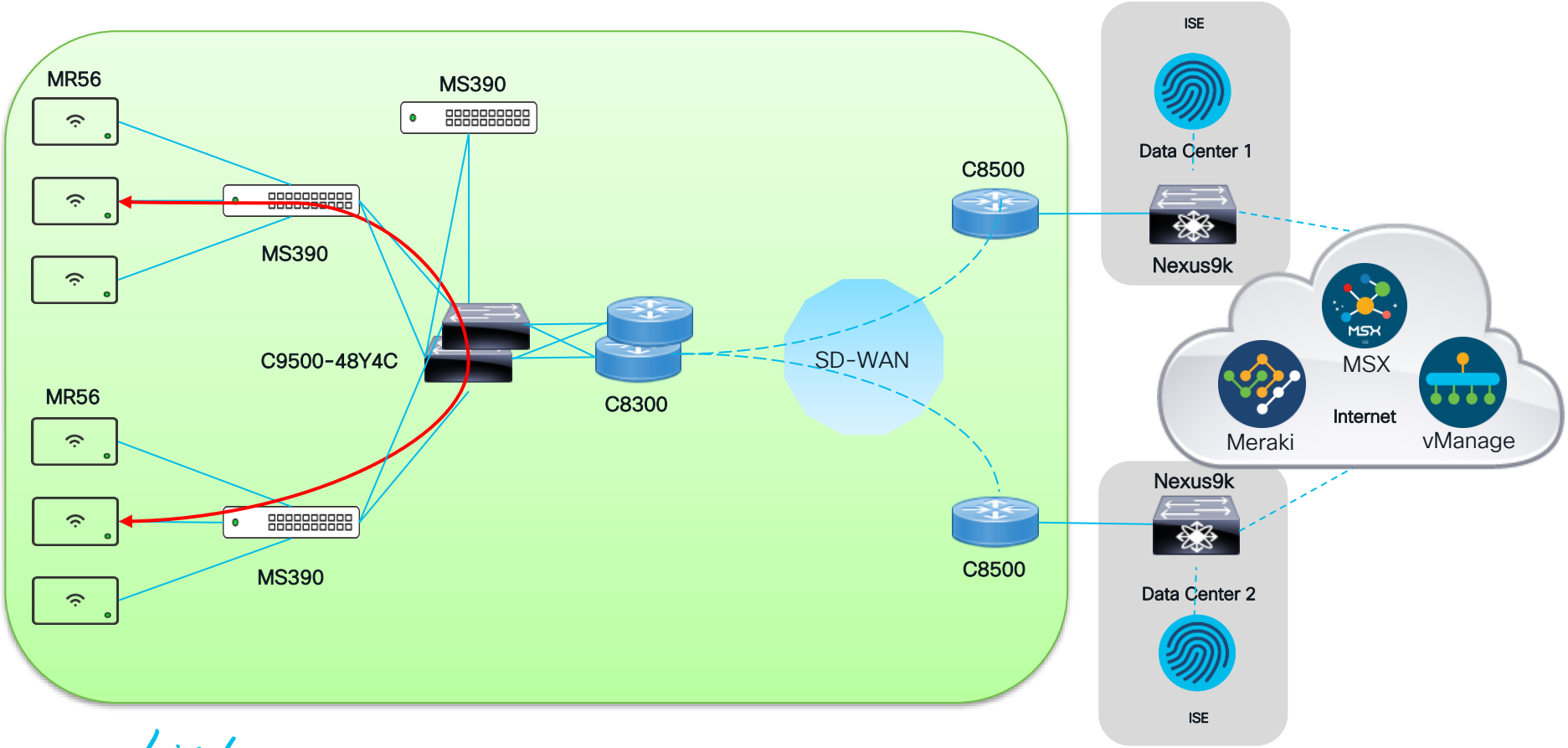
Adaptive Policy Applications



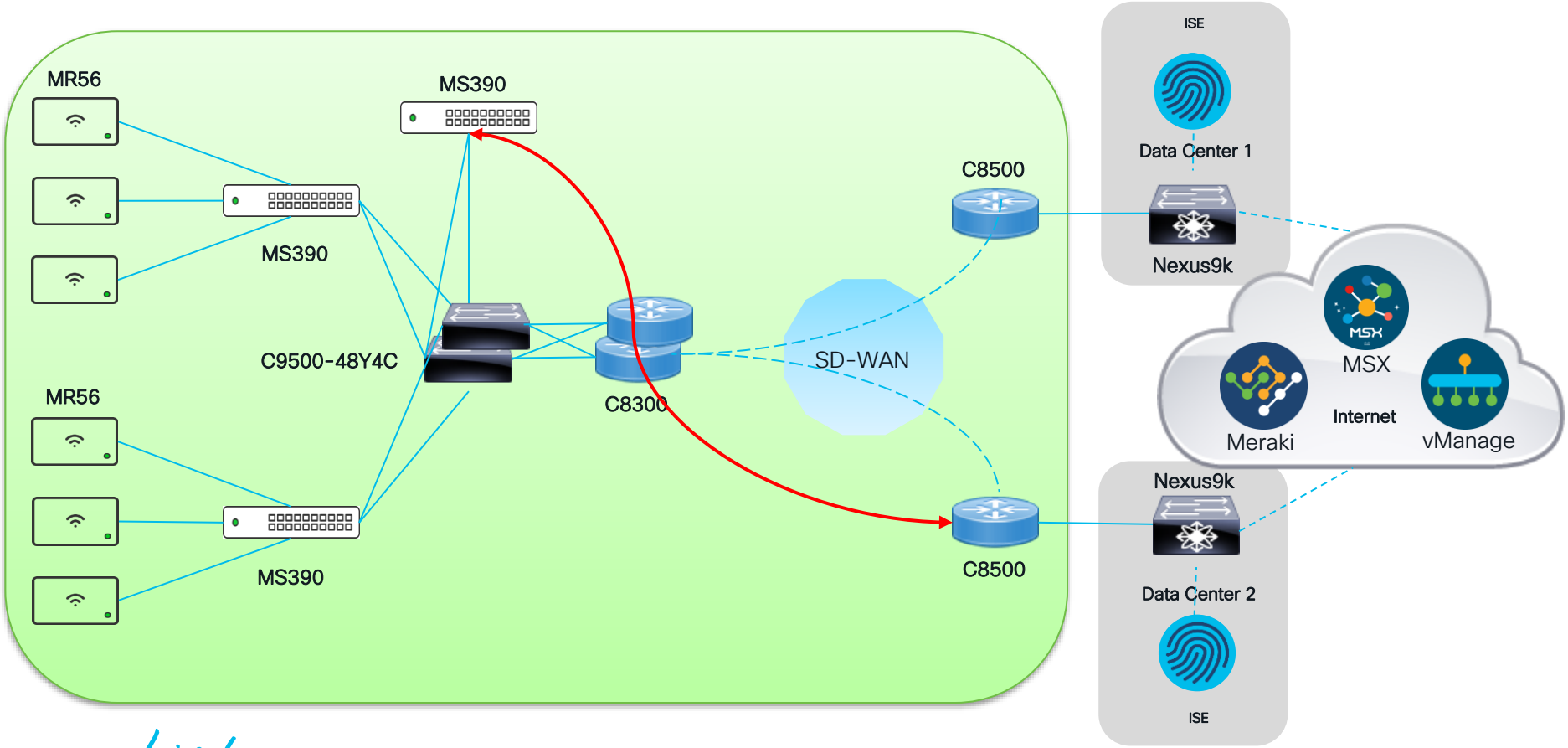
Adaptive Policy with MS390 and MR56



Adaptive Policy with TrustSec on Catalyst 9500



Adaptive Policy with TrustSec on SD-WAN

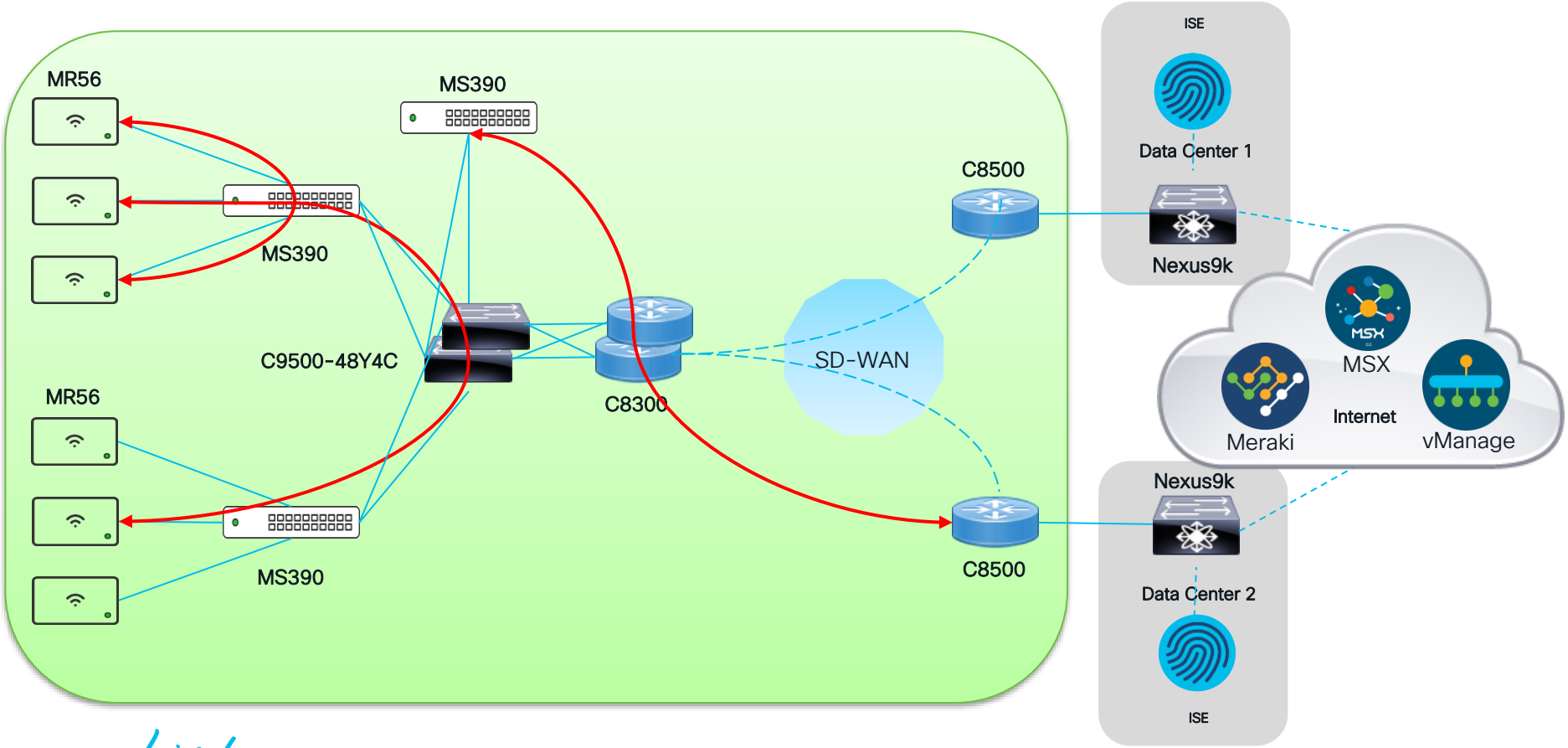


CMD Packet Structure

```
> Frame 310: 1325 bytes on wire (10600 bits), 1325 bytes captured (10600 bits)
> Ethernet II, Src: CiscoMer_75:65:00 (38:84:79:75:65:00), Dst: Cisco_9c:44:bf (70:b3:17:9c:44:bf)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1
v Cisco MetaData
    Version: 1
    Length: 1
    Options: 0x0001
    SGT: 2
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src:                 Dst: 209.206.51.215
> User Datagram Protocol, Src Port: 40152, Dst Port: 7351
> Data (1271 bytes)
```

MS390 Cat9k

Multiple Technologies--Multiple Applications



Conclusion

Generalized Tools to Specialized Tools

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

cisco Live!

Thank you


cisco Live!
ALL IN