Wireless Without the Headache: Starting Out with the 9800 WLC

Keith Bogart

Cisco CCIE #4923

Key Concepts

- Understand the Role of the Cisco 9800 WLC
- Exposure to the Tag and Profile-Based Configuration Model
- Build and Broadcast a Simple WPA2/WPA3 WLAN

MAJOR TOPICS

- What the Cisco 9800 WLC Is and How It Fits into a Wireless Network
- Initial Setup and Access to the Web UI
- Configuration Model Based on Profiles and Tags
- Creating a Simple Corporate WLAN
- Flexibility and Scalability via Tags and VLAN Mapping

LEARNING OUTCOMES

+ Explain the basics of the Cisco 9800 WLC
+ Gain familiarity into the Initial 9800 Setup and Access to the Web UI
+ Understand the 9800 Configuration Model
+ Create a Simple Corporate WLAN
+ Scale WLANs with VLANs, Policy Profiles, and Tags

PREREQUISITES

- Familiarity with basic 802.11 WLAN terminology
- Experience with WPA2 & WPA3
- Understanding of DHCP
- Knowledge of Port Types (Console, Ethernet, etc)
- Familiarity with Basics of IOS-XE CLI

LET'S GO!

What is the Cisco Catalyst 9800?

Cisco 9800 Purpose

- A Wireless LAN Controller for Cisco access points
- Utilizes CAPWAP tunnels to;
  - Manage and configure lightweight access points
  - Place received WLAN client data onto the Distribution System
  - Forward data from Distribution System to WLAN clients
- Available in different form factors

Form Factors

- Physical Appliance
- Virtualized for Cloud
- Embedded

https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/nb-06-cat9800-ser-aag-ctp-en.html

Compatibility Matrix

- Not all Cisco access points are supported by the Cisco Catalyst 9800:
  - Some are only supported by Meraki controllers
  - Some are only supported by legacy AireOS Controllers

https://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html

Thank you for watching!!

Cisco 9800 Physical Interfaces

Thank you for watching!!

Connecting Your Lab to Our Lab

The Lab Environment

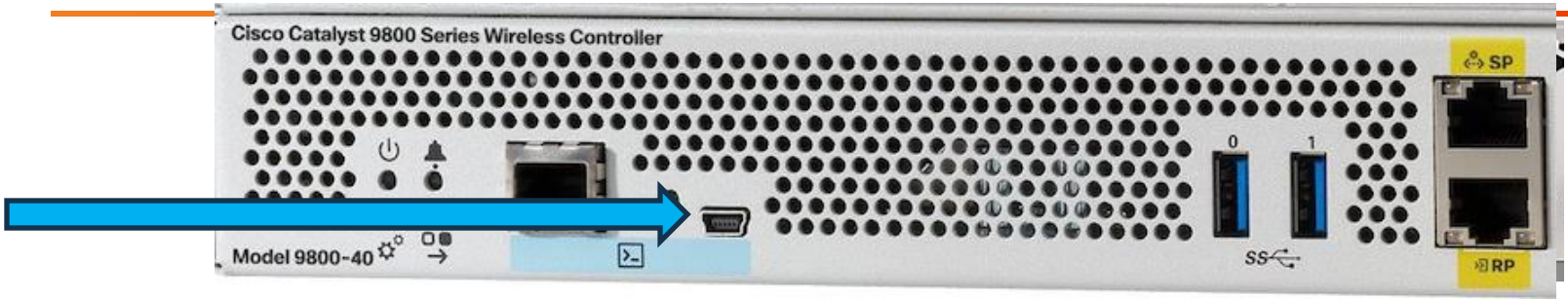
Initial Connection to the CLI

Connecting to the RJ-45 Console

- Requires USB-A to RJ-45 console cable for connecting to a standard laptop
- USB-C to RJ-45 cables also supported
- If laptop uses a FTDI or Prolific chipset, a driver install may be required.
- Start a terminal program (ie. Hyperterminal, PuTTY, etc)
- Console settings:

```
Baud Rate: 9600
Data Bits: 8
Stop Bits: 1
Parity: None
Flow Control: None
```

Connecting to the USB Console



- Requires appropriate USB cable/connector for your platform
  - 9800 H1/H2: 5-pin micro USB Type-B cable for connecting to a standard laptop
  - 9800-40/80: USB Type A to 5-pin mini USB Type-B cable
- Cable must not exceed 3-meters in length
- May require a Cisco Windows USB Console Driver
- Start a terminal program (ie. Hyperterminal, PuTTY, etc)
- Console settings:

```
Baud Rate: 9600
Data Bits: 8
Stop Bits: 1
Parity: None
Flow Control: None
```

The Management Interface

- Management interface location must be pre-determined
  - Service Port?
  - A Layer-3 switchport?
  - A VLAN Interface (SVI)?
- One must determine the following:
  - What will be the IP address and subnet mask?
  - How will 9800 route to non-local IP management traffic?

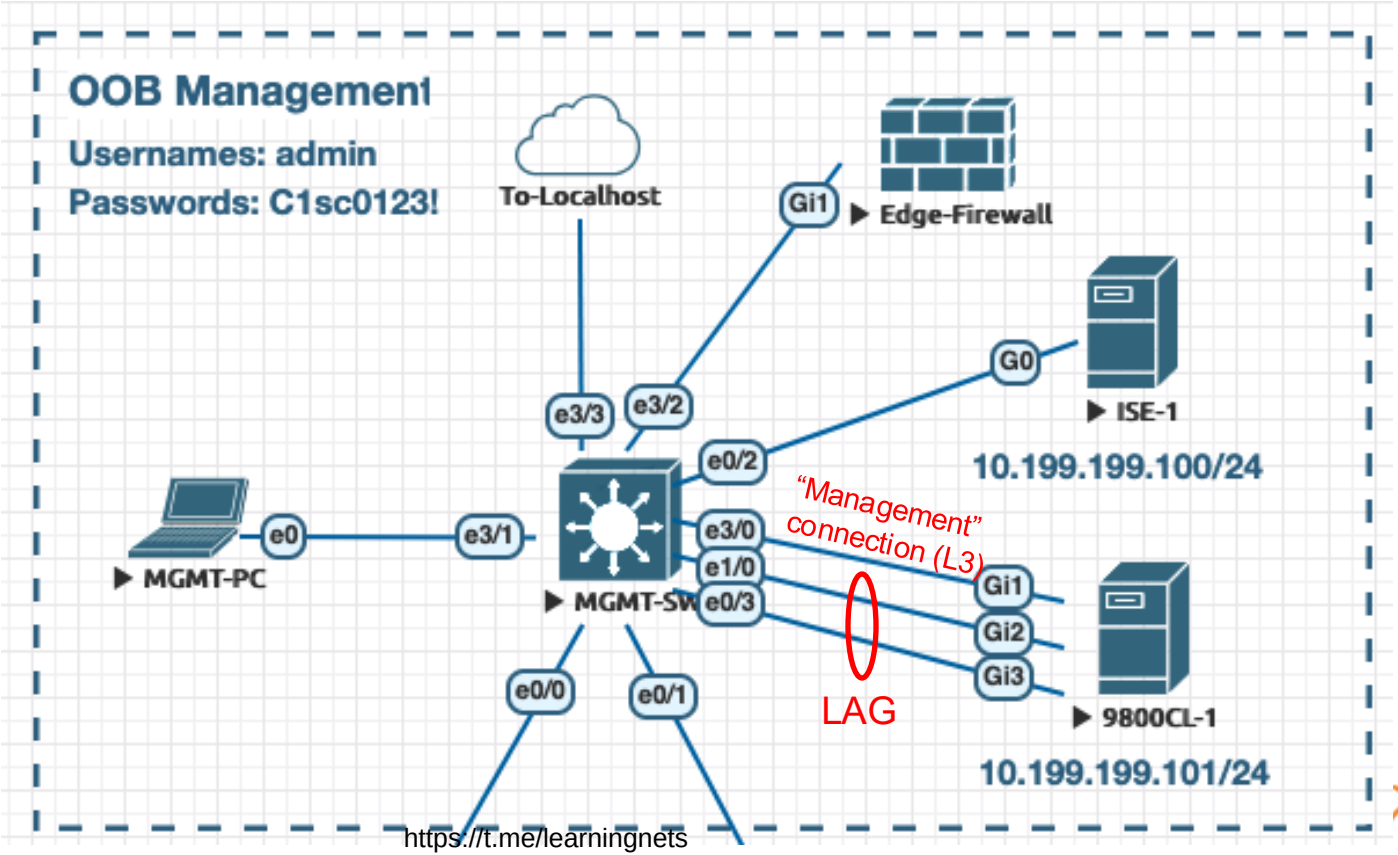
The Setup Command Facility

- If no configuration is present on the WLC you will be presented with an initial “Setup Command Facility” prompt.
- Only a few commands are needed to speedily work your way through these prompts.
  - Say “no” to the configuration dialogue prompt
  - Enable a 10-character “Enable Secret” (don’t worry, this will be deleted in the following step)
  - Enter “0” to “Go to the IOS command prompt without saving this config”

Minimum Required Configuration

- The following elements are the minimum required configuration to obtain Web GUI access to the WLC
  - Username and password
  - IP address and subnet mask on selected Management interface

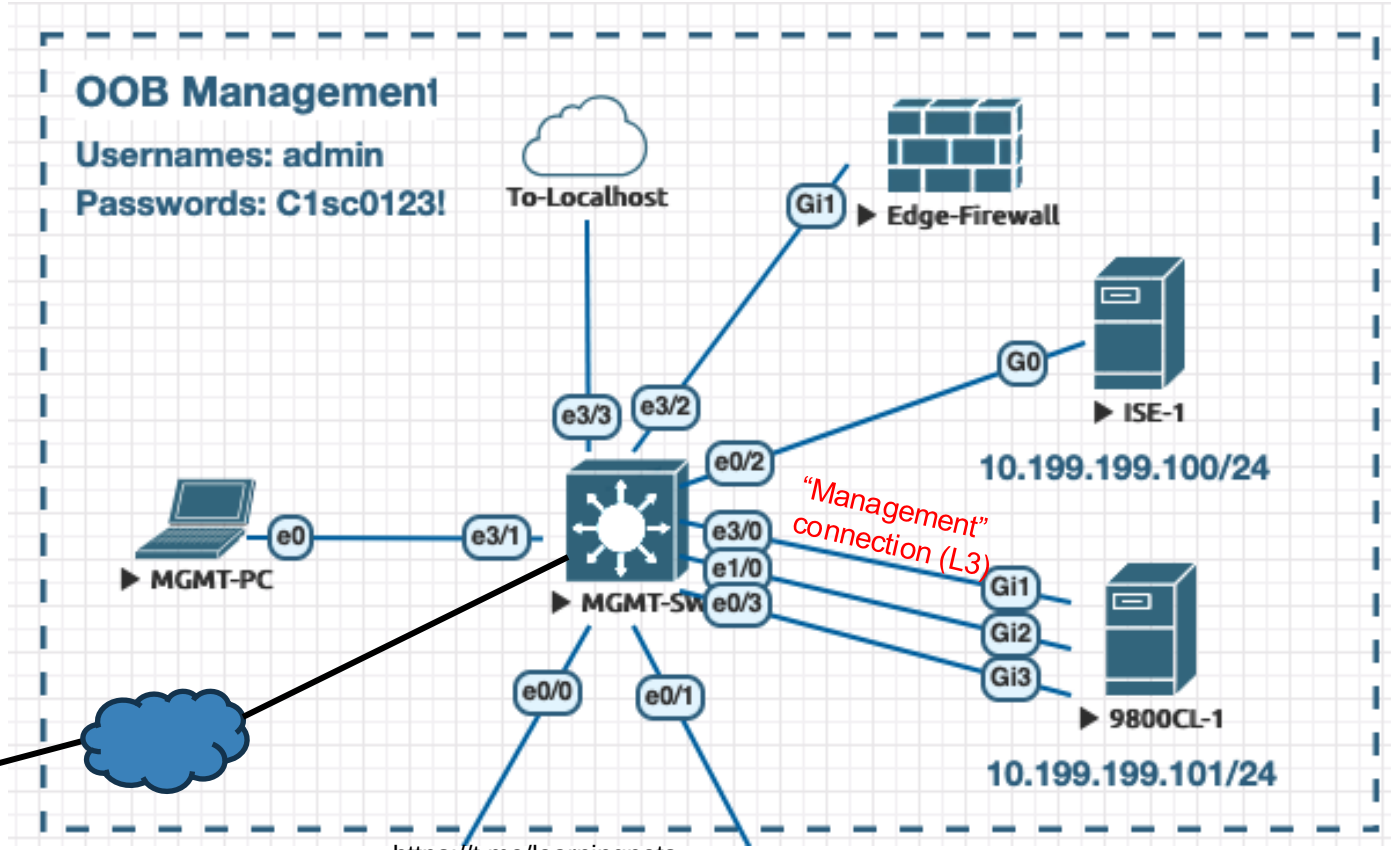
Configuration Steps



Thank you for watching!!

Working Through the Configuration Setup Wizard

Configuration Setup Wizard



Thank you for watching!!

Introduction to the Cisco 9800 Web UI

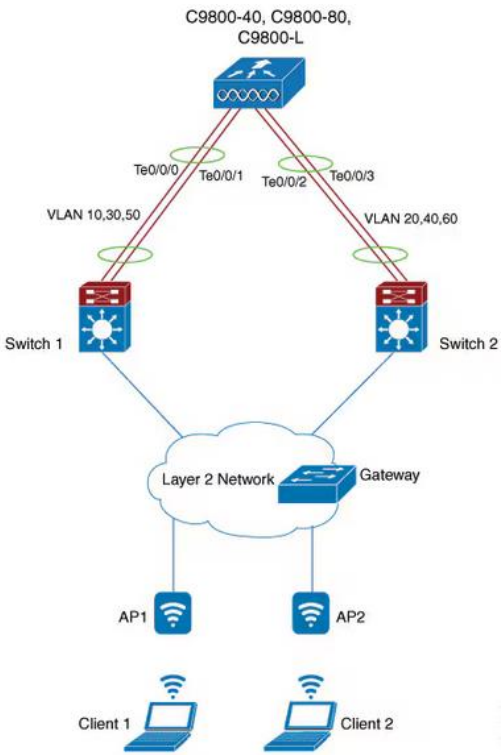
ine.com

Thank you for watching!!

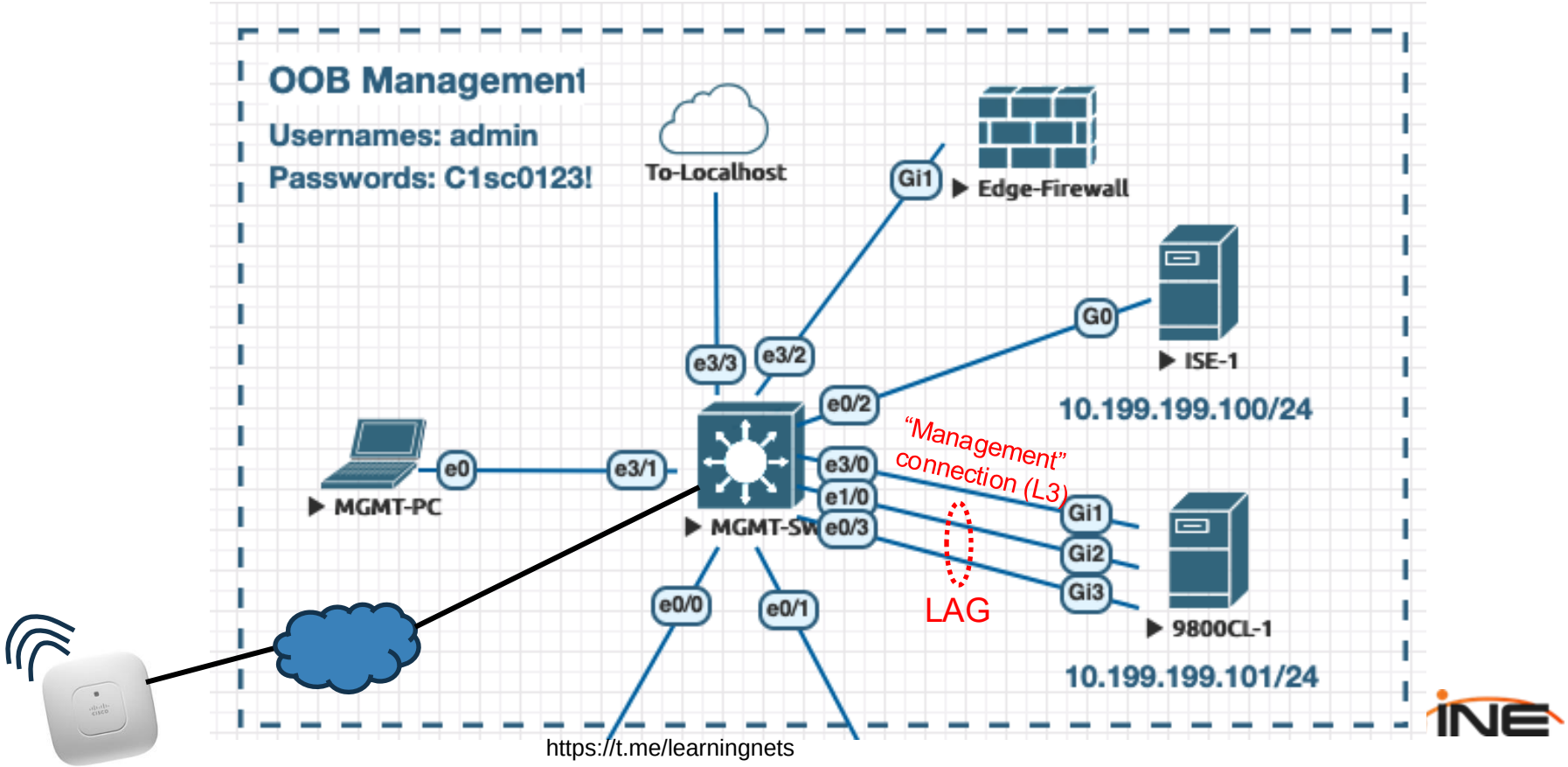
Creating Link Aggregation Groups (LAG)

LAG Prerequisites

- Cisco 9800s support both LACP and PAgP
  - LACP is best practice
- All LAG members must be identical
- Multiple Link Aggregation Groups can be configured if desired
- LAG members should be configured a Layer-2 802.1q VLAN Trunks



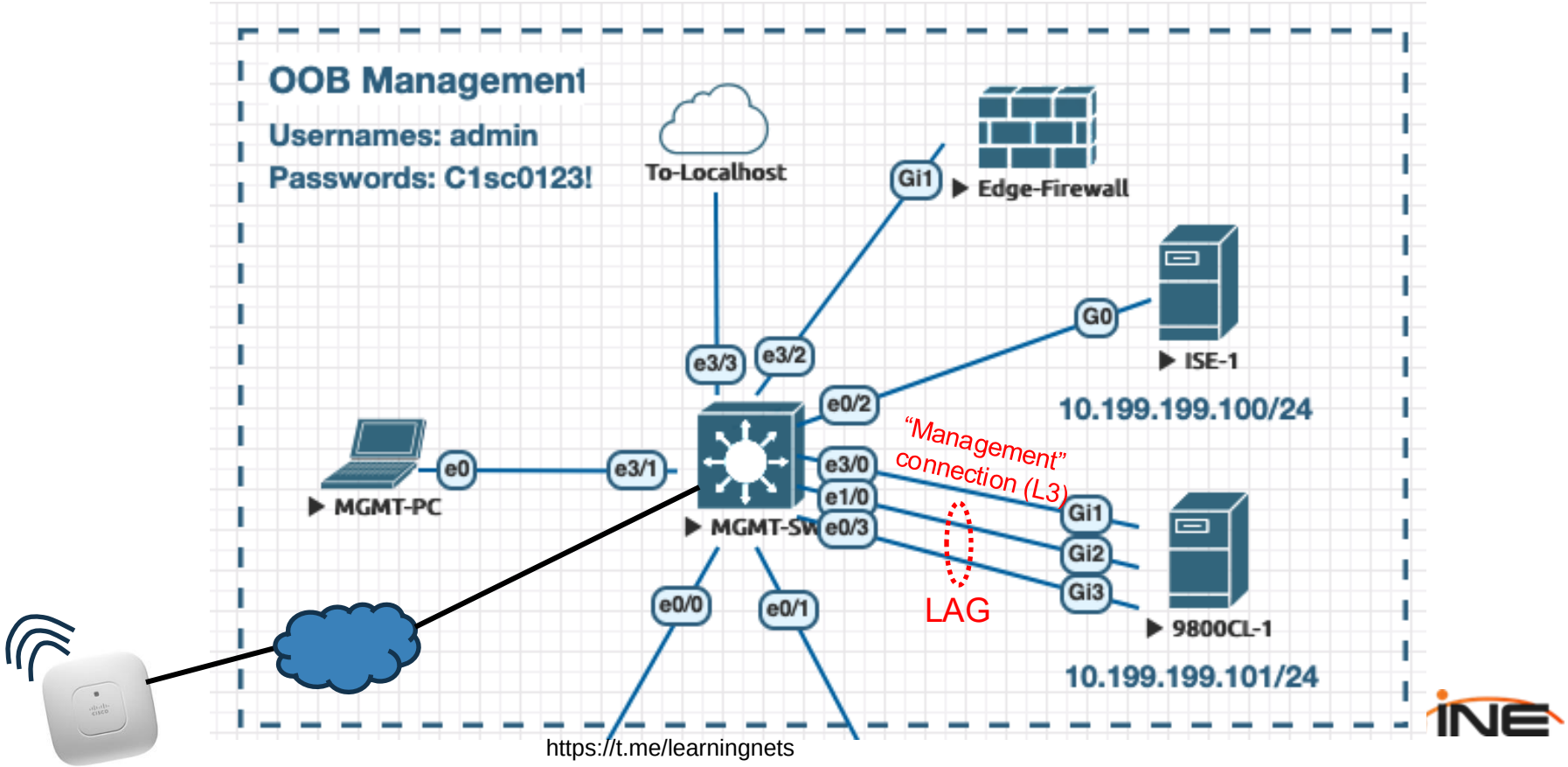
Configuring LAG



Thank you for watching!!

Configuring a Wireless Management Interface

Configuring LAG



Thank you for watching!!

Joining Access Points to your Cisco 9800 Controller

Show Me The Power!

- How will you be powering your access points?

PoE Type	Standard	Power Delivered	Typical Use
PoE (Type 1)	802.3af	up to 15.4W	Legacy/small APs
PoE+ (Type 2)	802.3at	up to 30W	Many mid-range Cisco APs
UPOE	Cisco proprietary	up to 60W	Higher-end Cisco APs
UPOE+ / PoE++ (Type 3/4)	802.3bt	up to 60W/100W	High-performance/multi-radio APs (like Wi-Fi 6/6E)

How is IP Learned?

- Access points need the following information to operate:
  - IP address and subnet mask
  - Default gateway IP address
  - IP address of the Wireless LAN Controller
  - NTP Server IP address
- Most common method is to utilize DHCP for these variables

```
ip dhcp pool Wireless
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.1
 dns-server 1.1.1.1 8.8.8.8
 option 43 hex f104.0ac7.6365
 option 42 ip 10.10.10.1
```

WLC address

NTP Server address

When IP Isn't Learned

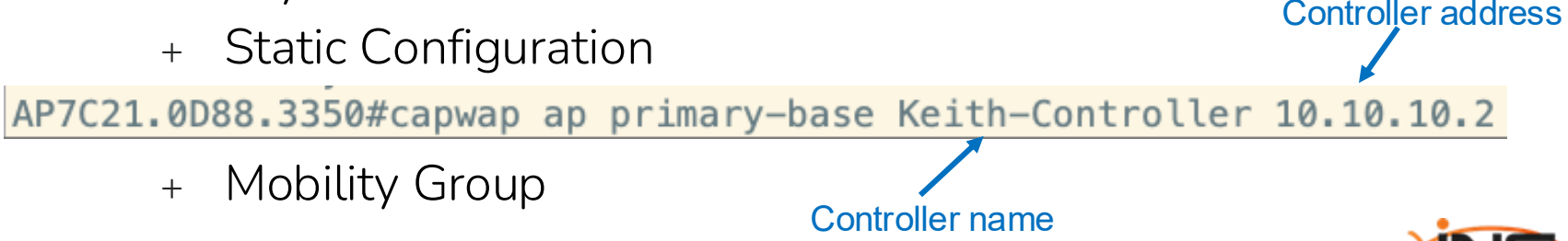
- CLI on access point will display the following if DHCP is unreachable/unresponsive

```
[*08/11/2024 05:14:32.1597] ethernet_port wired0, ip 0.0.0.0, netmask 0.0.0.0, gw 0.0.0.0, mtu 0, bcast 0.0.0.0, dns1 0.0.
0.0, vid 0, static_ip_failover false, dhcp_vlan_failover false
[*08/11/2024 05:14:32.3196] Check whether client_ip_table entry need to be cleared 0
[*08/11/2024 05:14:32.3196] Clearing client entry
```

```
[*08/11/2024 05:14:43.4961] CAPWAP State: Discovery
[*08/11/2024 05:14:43.4961] Not sending discovery request, AP does not have an IP!!
```

Learning of the WLC

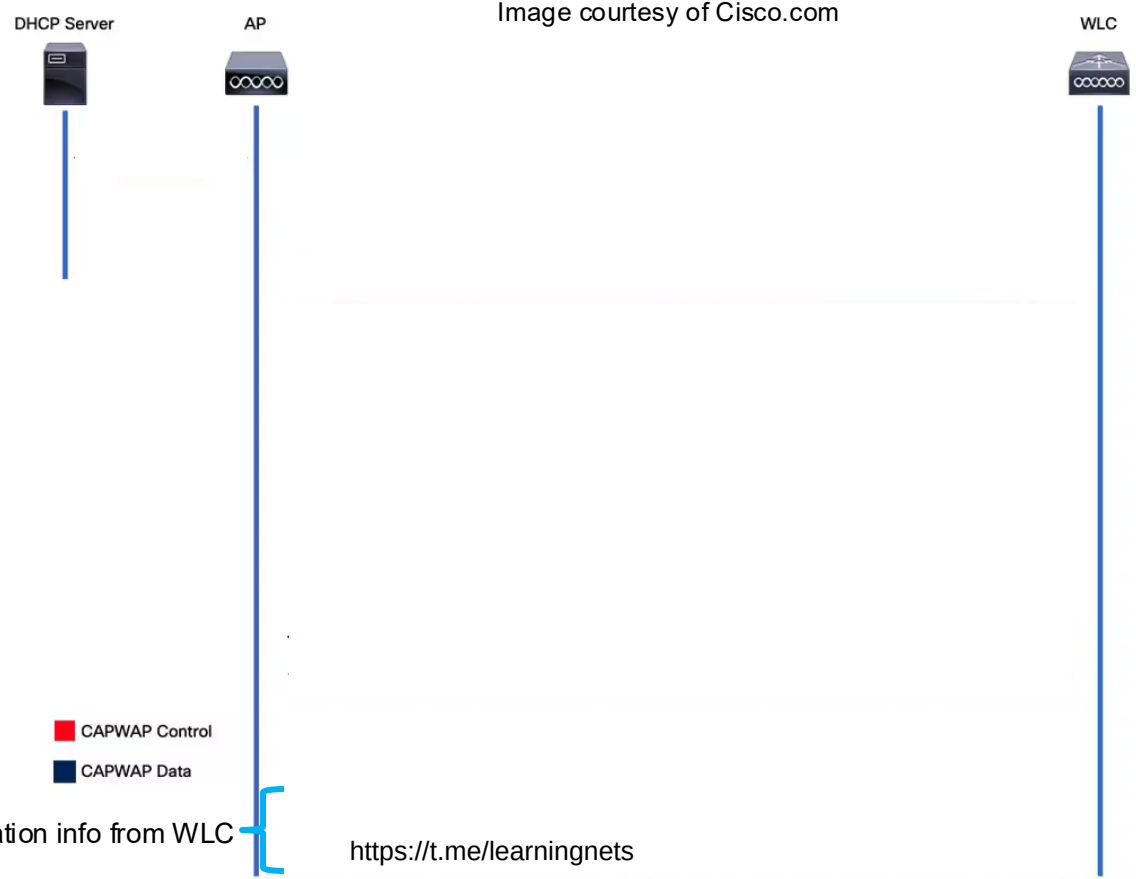
- As previously mentioned, DHCP is a very easy way to push the IP of the WLC to your APs
- Other methods also exist:
  - DHCP Option 56 (for IPv6 networking)
  - DNS Discovery (APs queries the domain name *CISCO-CAPWAP-CONTROLLER.localdomain*)
  - Layer-3 Broadcast to 255.255.255.255
  - Static Configuration



  - Mobility Group

Joining the Controller

Image courtesy of Cisco.com



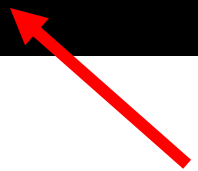
AP receives configuration info from WLC

Verify CA_Server Functionality

- Cisco 9800s must create & distribute Digital Certificates to access points
- These are used to:
  - Authenticate to the AP
  - Distribute Public Key to AP
- By default, the WLC_CA server functionality in 9800 is shutdown
- 9800 can’t create certs for AP’s unless this is enabled.

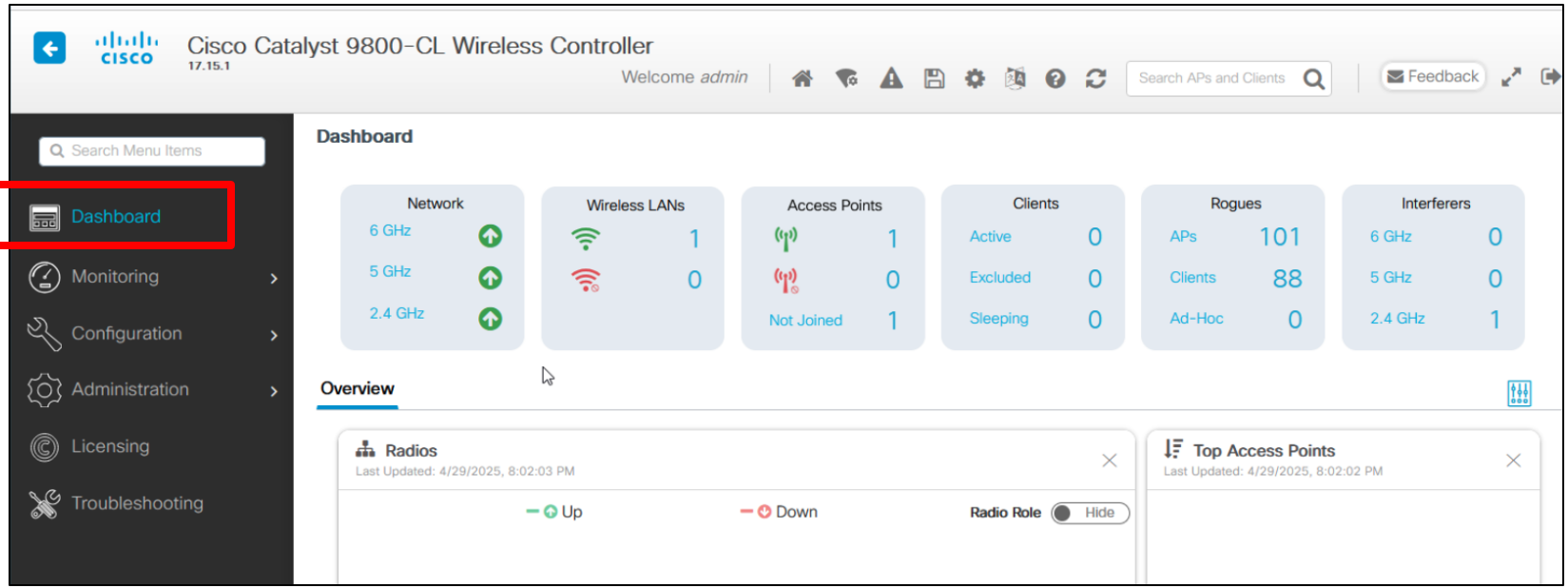
Enabling 9800 Certificate Authority

```
!
crypto pki server WLC_CA
 database archive pkcs12 password 7 15315A1F077A7A767B72
 issuer-name O=Cisco Virtual Wireless LAN Controller, CN=CA-vWLC_WLC
 grant auto
 hash sha1
 lifetime certificate 3652
 lifetime ca-certificate 3652
 shutdown
!
```



Issue “no shutdown” here in CLI

Essential AP Monitoring



Thank you for watching!!

Troubleshooting AP Join Issues

Common Problems

- AP didn’t receive IP information via DHCP
- AP wasn’t able to resolve IP address of Controller
- Wireless Management interface on Controller:
  - Doesn’t exist
  - Is down
  - Is unreachable
- AP model is not supported by the 9800 Controller
- Other problems

Thank you for watching!!

Introduction to FlexConnect

Definition of Terms

AP in “FlexConnect Mode”

Image courtesy of: https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213945-understand-flexconnect-on-9800-wireless.html

What is FlexConnect

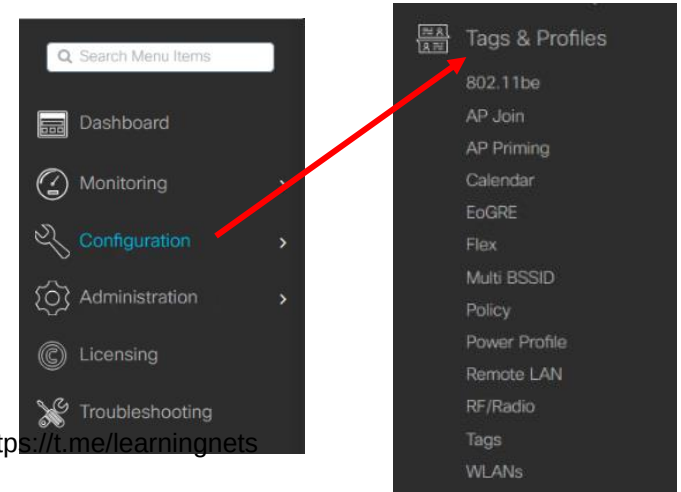
- FlexConnect AP's utilize *Local Switching*
  - No CAPWAP Data tunnel is created
  - Wireless authentication still controlled by WLC
  - APs can locally enforce authentication if connection is lost to WLC
- ACLs configured on the WLC can be pushed to APs for local enforcement of client traffic

Thank you for watching!!

Overview of the Cisco 9800 Configuration Model

Configuration Flexibility

- Cisco 9800 WLCs provide configuration flexibility and scalability
- Definition and implementation of wireless features, and control policy, are dictated by two constructs:
  - Profiles
  - Tags



Overview of Profiles & Tags

- Profiles *group a set of features and functionalities*
  - Think of Cisco IOS “route-maps” or “policy-maps”
  - Both are named constructs that group features
  - Both must be applied against something
- Tags allow you to *assign these features and functionalities to the access points* (APs).
  - Think of Cisco IOS “distribute-lists” (that reference route-maps”) or Service-Policies (that reference named “Policy-Maps”)

Cisco 9800 Configuration Profiles

- Five types of profiles
  - AP Join Profile (CAPWAP settings, SSH/Telnet settings)
  - Policy Profile (Client VLAN, AAA, ACLs)
  - FlexConnect Profile
  - RF Profile
  - WLAN Profile (Define SSID, security settings)
- Defaults exist for all of these EXCEPT WLAN Profiles
- Let's look at some of these defaults...

Cisco 9800 Configuration Tags

- Tags are applied to access points
- Tags apply policies to access points
- Three types of tags
  - Policy Tag (Ties together Policy Profile and WLAN Profile)
  - Site Tag (Determines local site settings and ties with AP Join Profile)
  - RF Tag (binds the 6GHz, 5GHz, and 2.4GHz RF profiles to APs)

Putting it all Together

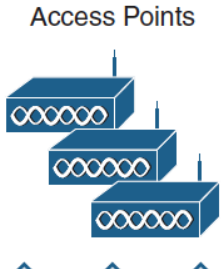


Image courtesy of, "Understanding & Troubleshooting Cisco 9800 Wireless LAN Controllers" https://t.me/learningnets

Minimum Configurations

- For a simple goal of creating a WLAN utilizing WPA2 PSK one only needs to create a new WLAN Profile
- One can then use the default Policy Tag to;
  - Bind the WLAN Profile and default Policy-Profile together
  - Apply Policy Tag to the appropriate access point(s)

Thank you for watching!!

Preparing the Infrastructure

Preliminary Tasks

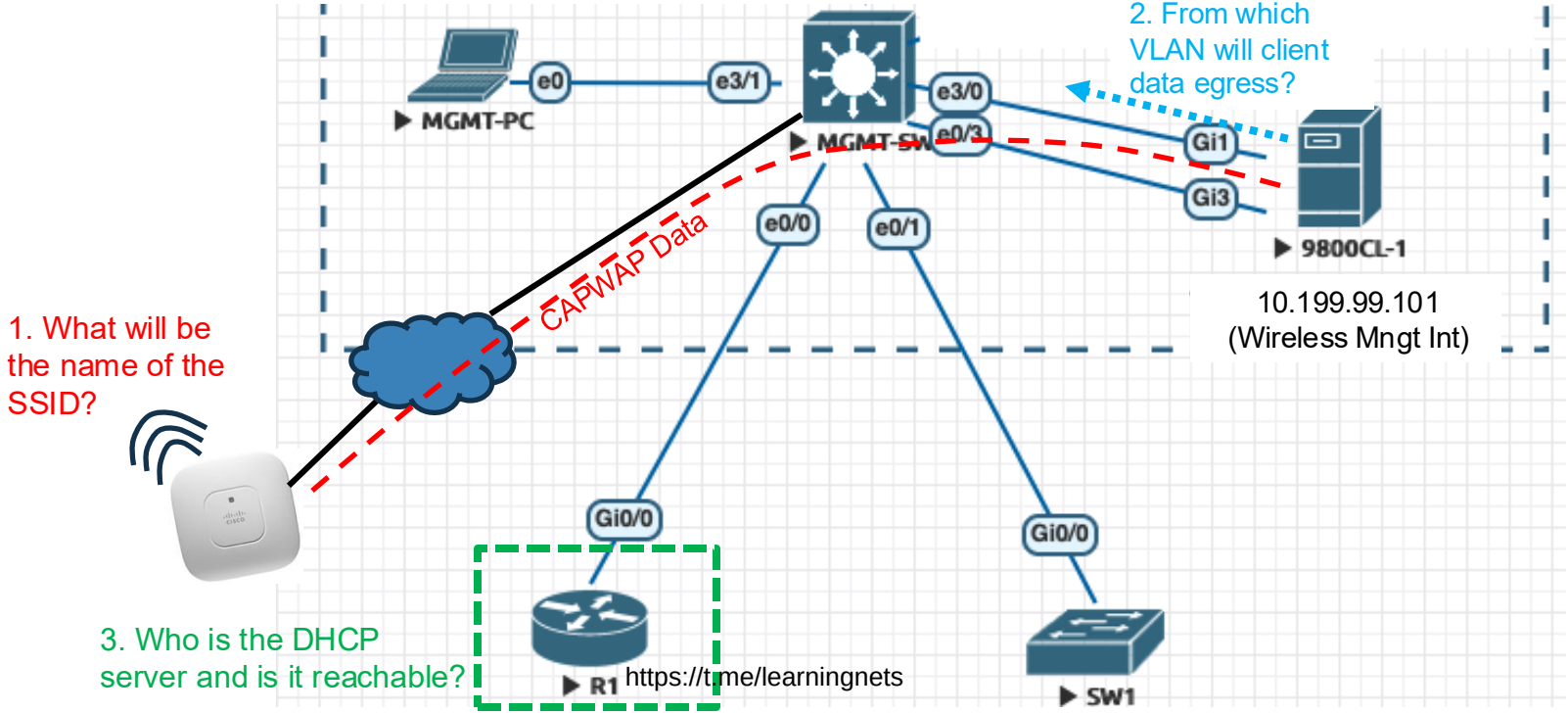
- Even after the physical infrastructure is in place, additional network configuration tasks will be needed prior to WLAN implementation.
- Network devices (and servers) will need to be configured with things such as:
  - VLANs
  - Routing
  - DHCP
  - Security Features

The WLAN Objectives

- Create a Corporate WLAN that:
  - Will be advertised by access points
  - Will utilize CAPWAP Data and Control tunnels
  - Will enforce WPA2/PSK as well as WPA3/SAE authentication
  - Will ensure WLAN Clients are placed onto VLAN-3 of the Distribution System
    - *NOTE: Best practices recommend that the VLANs mapped to the Wireless Management and Management interfaces be unique from WLAN client traffic VLANs*

Planning & Designing

- Prior to any Cisco 9800 WLC configuration the following plans and designs must be established:



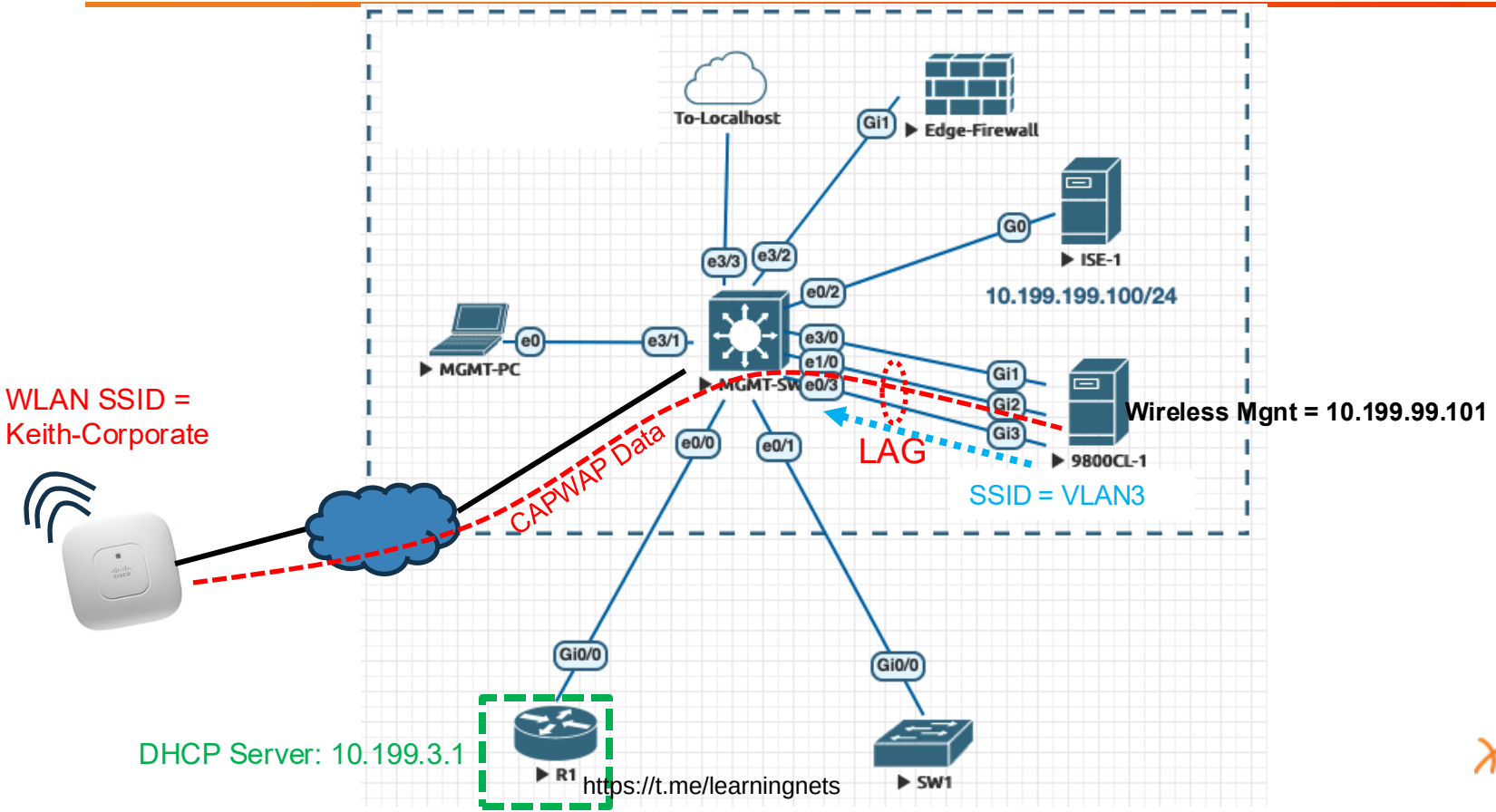
Thank you for watching!!

Configuring Your First WLAN

The WLAN Objectives

- A quick recap:
- Create a Corporate WLAN that:
  - Will be advertised by access points
  - Will utilize CAPWAP Data and Control tunnels
  - Will enforce WPA2/PSK as well as WPA3/SAE authentication
  - Will ensure WLAN Clients are placed onto VLAN-3 of the Distribution System
    - *NOTE: Best practices recommend that the VLANs mapped to the Wireless Management and Management interfaces be unique from WLAN client traffic VLANs*

Our Topology



The Steps

1. Create a new VLAN on the Cisco 9800
2. Create WLAN Profile with essential configurations
3. Update default Policy Profile with VLAN information
4. Update default Policy Tag
   - ✓ Pair Policy Profile and WLAN Profile
   - ✓ Apply tag to access point
5. Test with WLAN Client

Thank you for watching!!

Simple Scaling Across the Enterprise

Same SSID for Everyone!

The Steps

1. Create a new Policy Profile for each subnet/building
2. Assign a different VLAN to each new Policy Profile
3. Create a new Policy Tag for each subnet/building
   - ✓ Bind same WLAN across different Policy Profiles
   - ✓ Assign Policy Tag to appropriate access points

Thank you for watching!!

Wireless Without the Headache: Starting Out with the 9800 WLC - Summary

Key Concepts - Recap

- Understand the Role of the Cisco 9800 WLC
- Exposure to the Tag and Profile-Based Configuration Model
- Build and Broadcast a Simple WPA2/WPA3 WLAN

Learning Outcomes Recap

+ Explain the basics of the Cisco 9800 WLC
+ Gain familiarity into the Initial 9800 Setup and Access to the Web UI
+ Understand the 9800 Configuration Model
+ Create a Simple Corporate WLAN
+ Scale WLANs with VLANs, Policy Profiles, and Tags

Next Steps

- Purchase your own access points and practice concepts you learned in the course.
- Start learning about 802.1x for WLANs
- Review all INE courses in the Learning Path, “Wireless Enterprise Networking”

THANKS FOR WATCHING!