Welcome

LA Networks
Michael Kim
mkim@la-networks.com

LAnet

Our Story

- Founded in 1997
- Started, Managed, and Led by Engineers
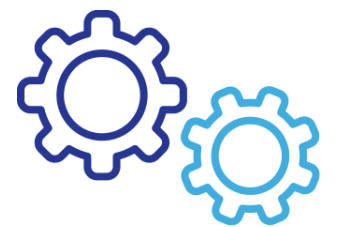- Known & Recognized for our Engineering

4 KEY INGREDIENTS

PASSION   PEOPLE   EXPERTISE   PROCESS

Core Technologies

5 VERTICALS

MANAGED SERVICES

COLLABORATION

DATA CENTER

NETWORK

SECURITY

- Dedicated teams for Each Vertical
- 75% of Our Staff Are Engineers
- Home Grown Engineers

Commitment

For over 20+ years, LA Networks has helped their clients leverage technology by linking their business needs with IT expertise.

Headquartered in Los Angeles – working on a national/global scale

Our organization is over 70% engineers with a quarter being CCIEs

90% of our engagements are repeat customers and referrals drive 80% of our new business

802.1X, RADIUS, and Cisco ISE

INTRODUCTION & DEMO

CISCO

Challenges in Networking

- Evolution of the network from Data and Voice to Data, Voice, Video, etc.

- Increase in BYOD and IOT devices

- Lack of visibility into the network –

  - Do you know every device that is on your network?

  - Do you know what each device can communicate with?

- Zero Trust architecture

What is 802.1X

- A method to authenticate devices connecting to LAN or WLAN

- IEEE 802.1X defines the encapsulation of EAP over IEEE 802 (EAPOL).

- EAP stands for Extensible Authentication Protocol

- IEEE defined framework for authentication over a wired or wireless LAN
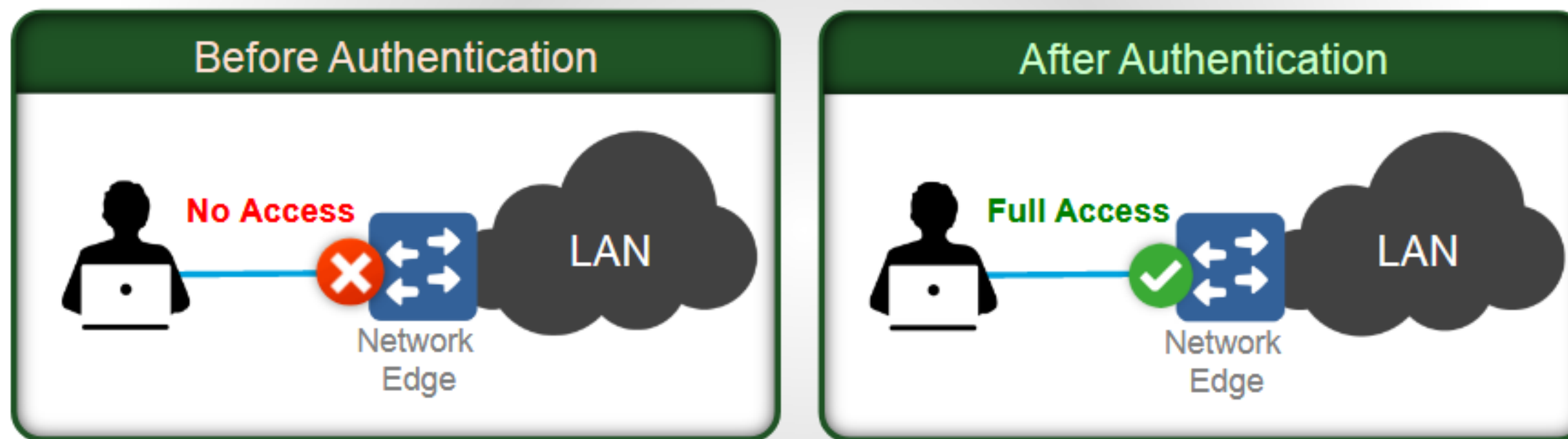
Components of 802.1X, RADIUS, and ISE

Endpoint
(Supplicant)

Network Device
(Authenticator)

Cisco ISE
(Authentication Server)

What is RADIUS

- Remote Authentication Dial-In User Service

- Client-Server protocol usually with a NAD acting as the client and a RADIUS Server

- Authentication, Authorization, Accounting

- Authentication and Authorization are joined

What is Cisco ISE

- Next Generation RADIUS Server

- Define and group endpoints

- Connect to external authentication sources

- ISE can function as a Certificate Authority

- Port authentication using 802.1X, MAB (MAC Authentication Bypass), Central Web Authentication

- Create policies for authentication

- Authenticates devices connecting to the network

- Authorizes devices that have authenticated

What is Cisco ISE
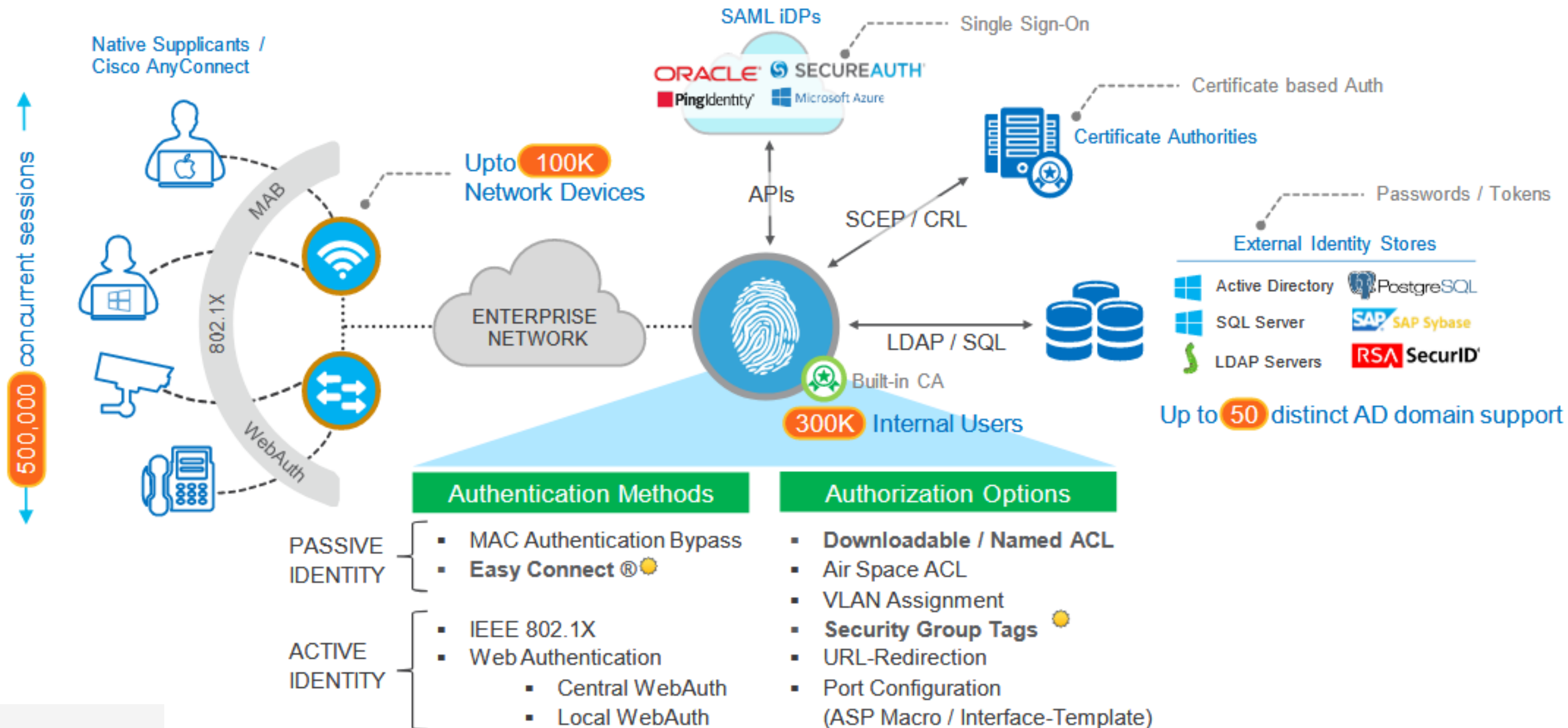
Why use 802.1X and ISE

Benefits

- Network Access Control

- Network Segmentation

- Simplified Policy Management and logging

- Policy based on authentication and authorization

- Security is moving quickly towards the Zero Trust model as IOT and internal threats become more prevalent

Authentication vs Authorization

Authentication

user name

******

LOGIN

Who are you?
Validate a system is accessing by the right person

Authorization

Are you allowed to do that?
Check users' permissions to access data

Authentication Process

Credentials (Certificate / Password / Token) → Endpoint (Supplicant) → Network Device (Authenticator) → Cisco ISE (Authentication Server) → Active Directory (Identity Store)

EAP
EAP 802.1X
EAP RADIUS
EAP

RADIUS: ACCESS-REQUEST
RADIUS SERVICE-TYPE: FRAMED
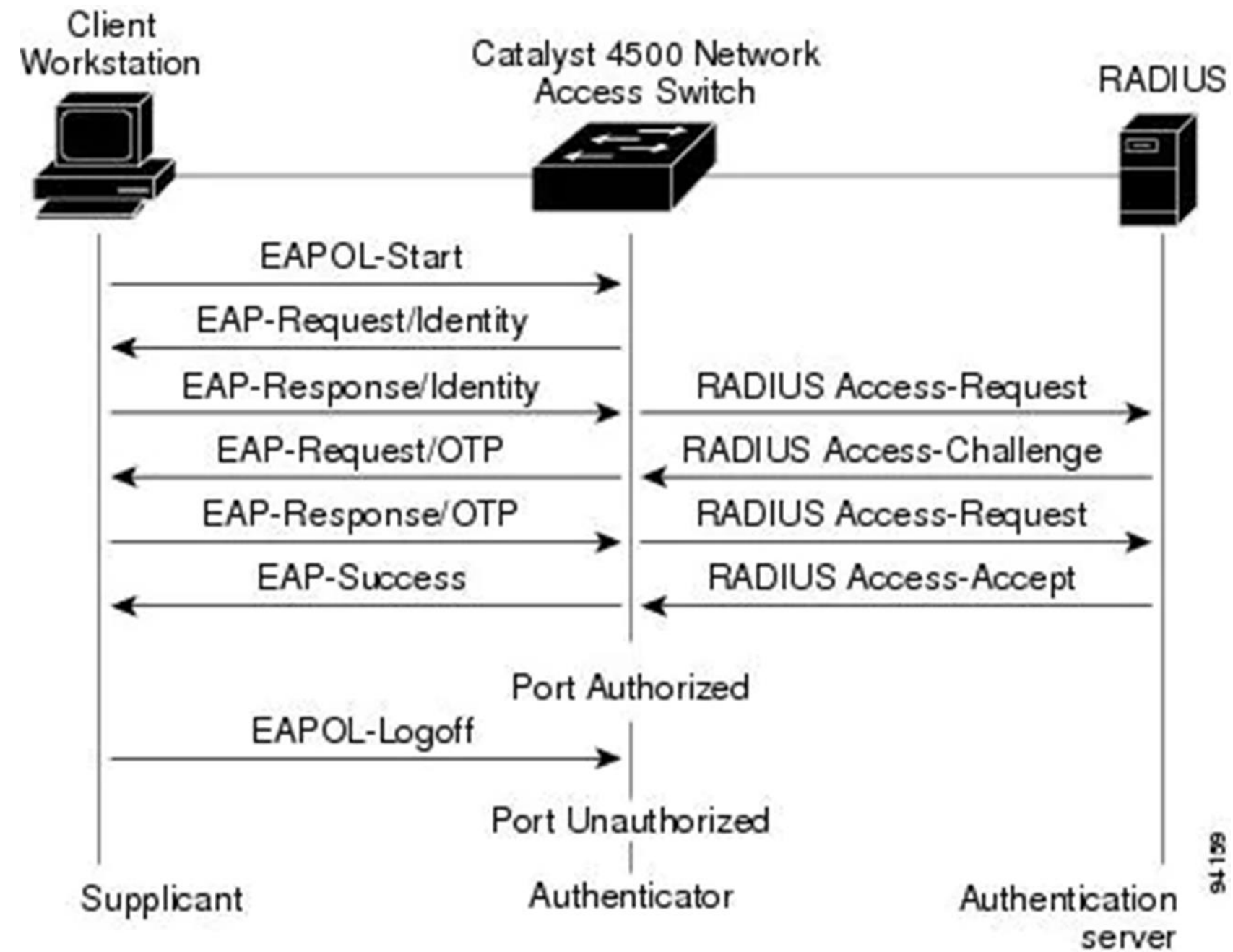EAP: EAP-RESPONSE-IDENTITY
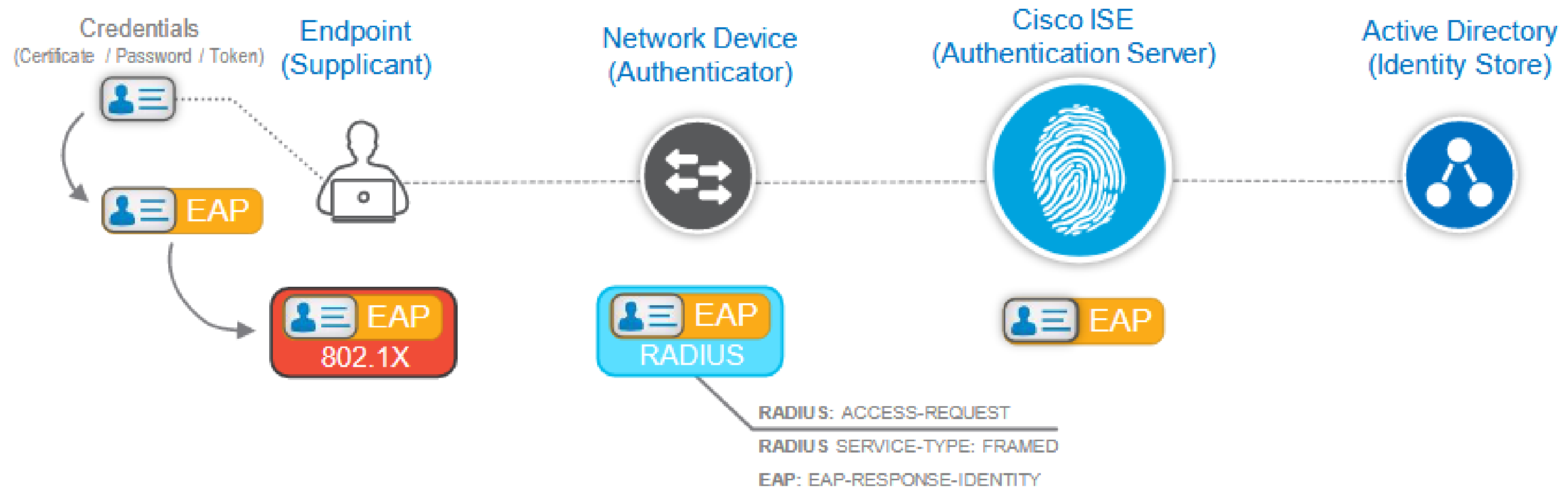
EAP: Extensible Authentication Protocol

Authentication Process
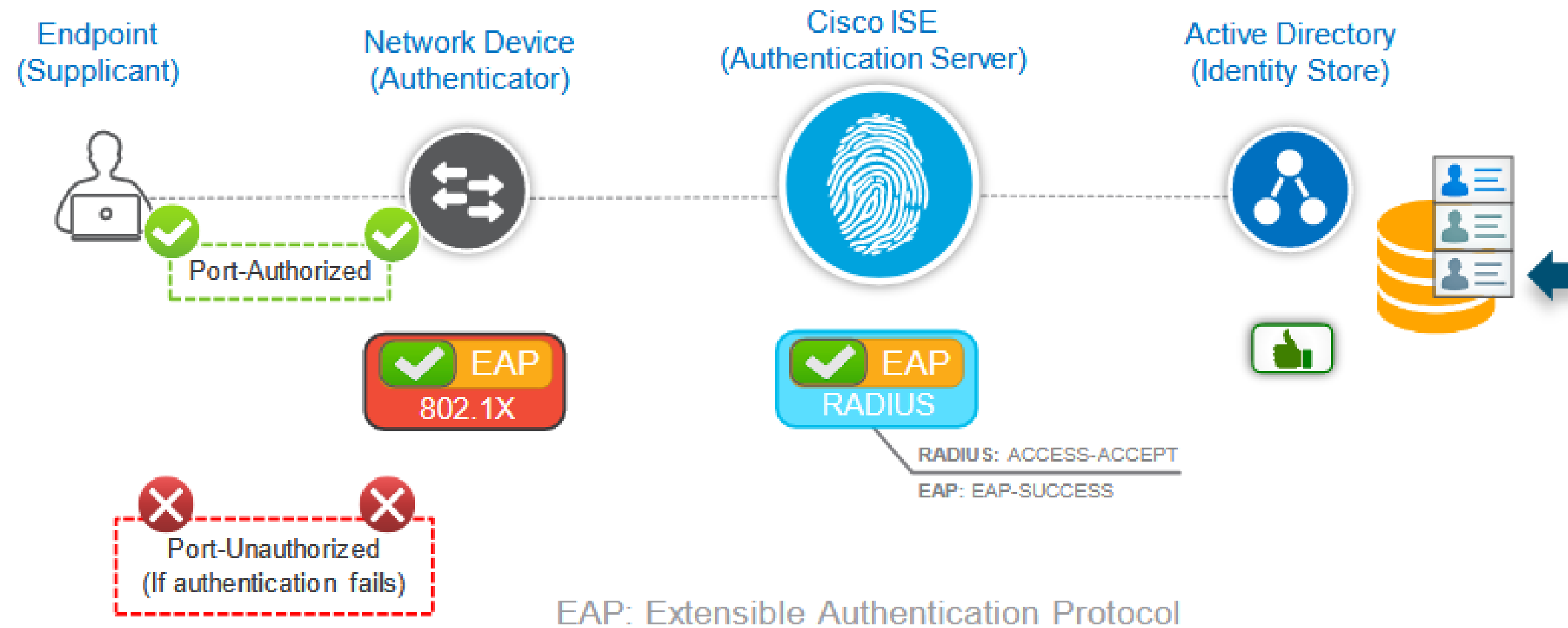
Authentication Process

Authorization Options

Authorization Options

- **Downloadable / Named ACL**
- Air Space ACL
- VLAN Assignment
- **Security Group Tags**
- URL-Redirection
- Port Configuration
  (ASP Macro / Interface-Template)

Authorization

✅ Tier1 Wired Access	AND	📖 Wired_802.1X 📖 is_Tier1_AD_Group	× TIER1_WIRED_ACCESS ➕

Authorization Profiles > **TIER1_WIRED_ACCESS**
Authorization Profile

* Name	TIER1_WIRED_ACCESS
Description	
* Access Type	ACCESS_ACCEPT ▼
Network Device Profile	cisco Cisco ▼ ⊕
Service Template	☐
Track Movement	☐ ⓘ
Passive Identity Tracking	☐ ⓘ

▼ **Common Tasks**

☑ DACL Name   TIER1_ACCESS 🔽

☐ IPv6 DACL Name

☐ ACL (Filter-ID)

☐ ACL IPv6 (Filter-ID)

DEMO

Fin

Thank you for your time!

LAnet