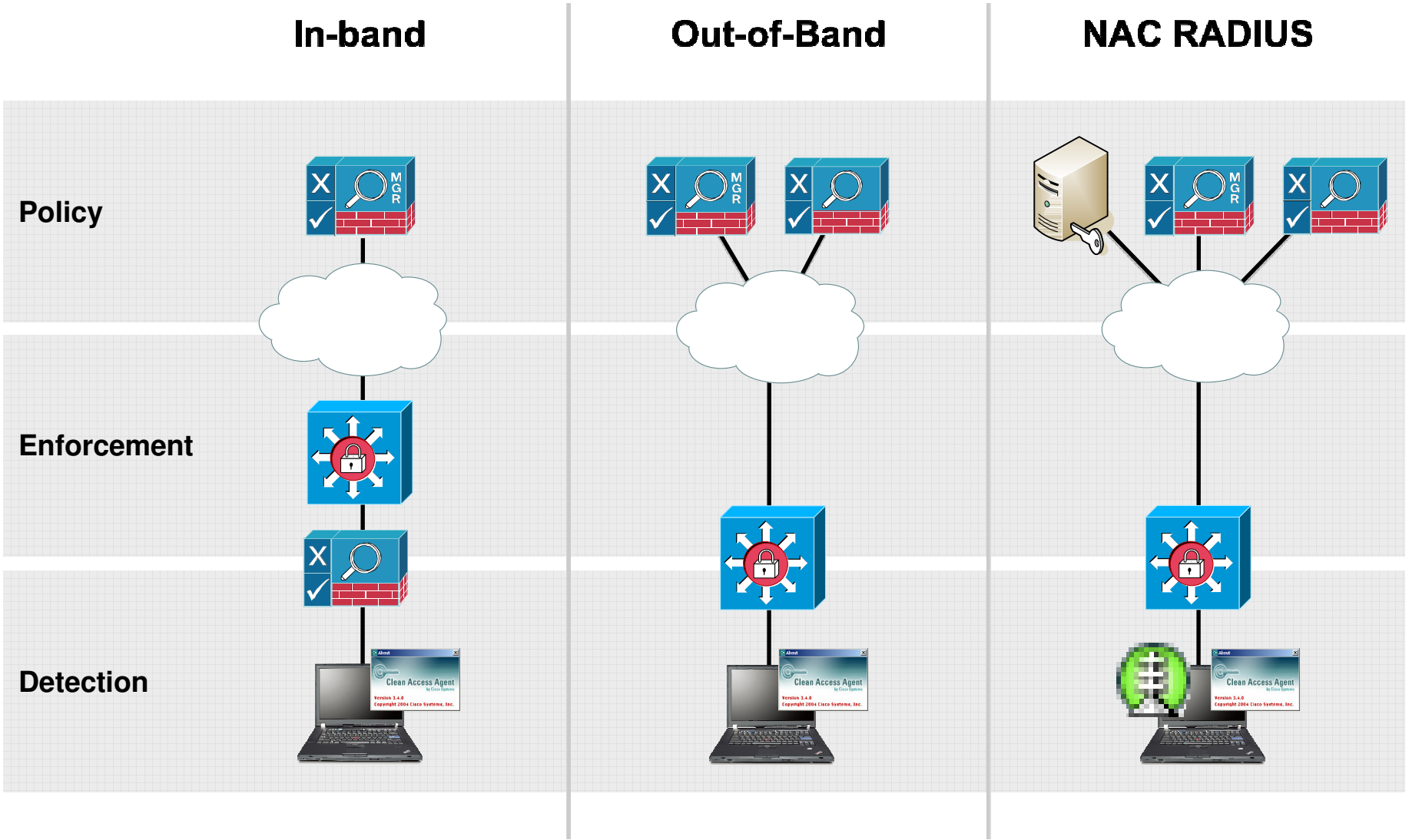
Network Admission Control – Part II (NAC RADIUS)

Ricky Elias
Security Architect
Advanced Technology (Security)
relias@cisco.com

Agenda

- Identity-Based Access Control
- NAC RADIUS Overview
- Demo
- Q&A

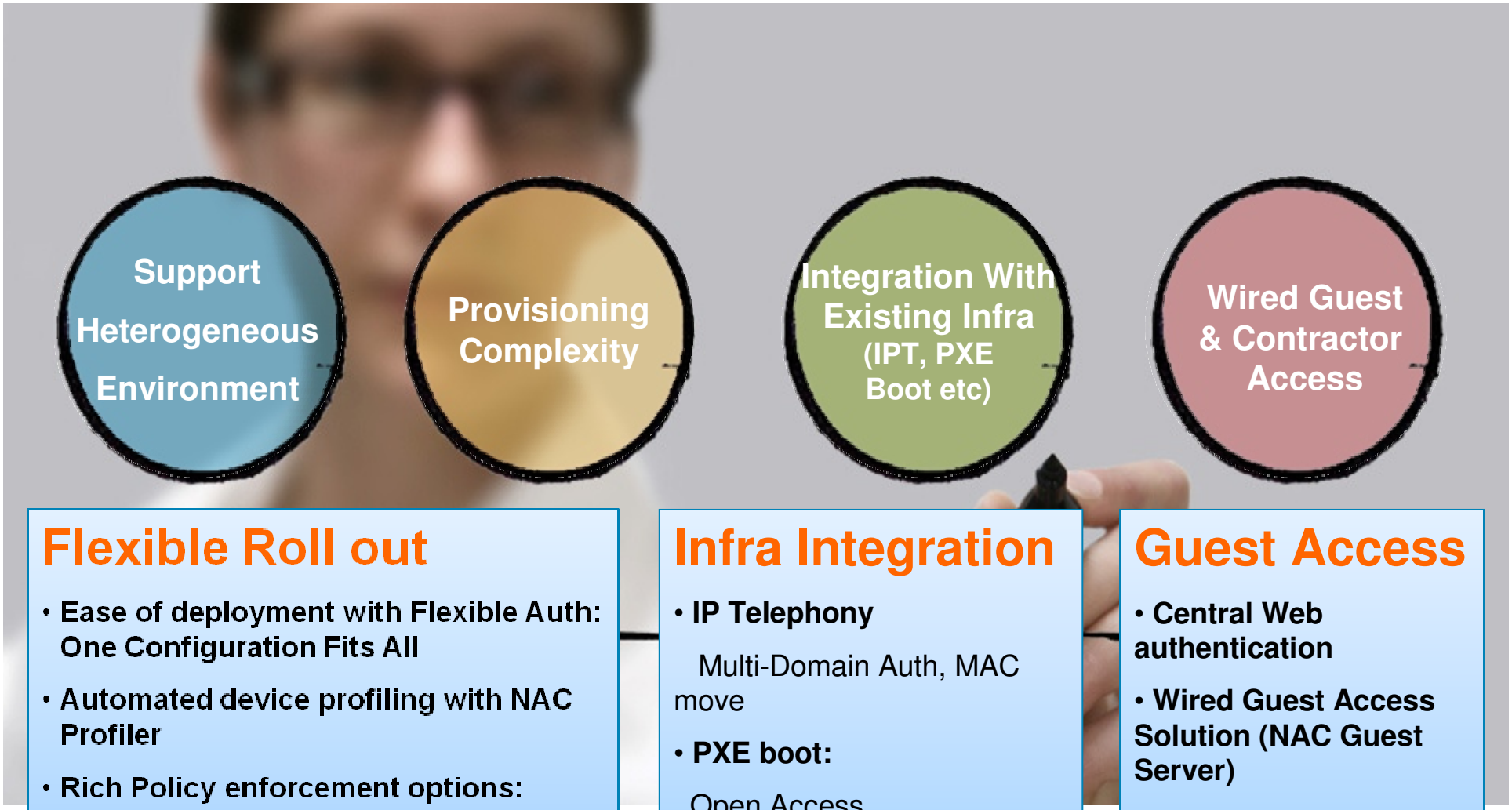
NAC Architectures



IEEE 802.1X

- Standard set by the IEEE 802.1 working group
- Is a framework designed to address and provide port-based access control using authentication
- 802.1X is primarily an encapsulation definition for EAP over IEEE 802 media—EAPOL (EAP over LAN) is the key protocol
- Layer 2 protocol for transporting authentication messages (EAP) between supplicant (user/PC) and authenticator (switch or access point)
- Assumes a secure connection
- Actual enforcement is via MAC-based filtering and port-state monitoring

Identity-Based Access Control
Deployment Considerations



Flexible Roll out

- **Ease of deployment with Flexible Auth: One Configuration Fits All**
- **Automated device profiling with NAC Profiler**
- **Rich Policy enforcement options:** VLAN (PVLAN, Guest, Auth Fail), Per-user ACL, QoS, ACS 5.0
- **x-Catalyst consistency**

Infra Integration

- **IP Telephony**

  Multi-Domain Auth, MAC move
- **PXE boot:**

  Open Access
- **Shared Media Access**

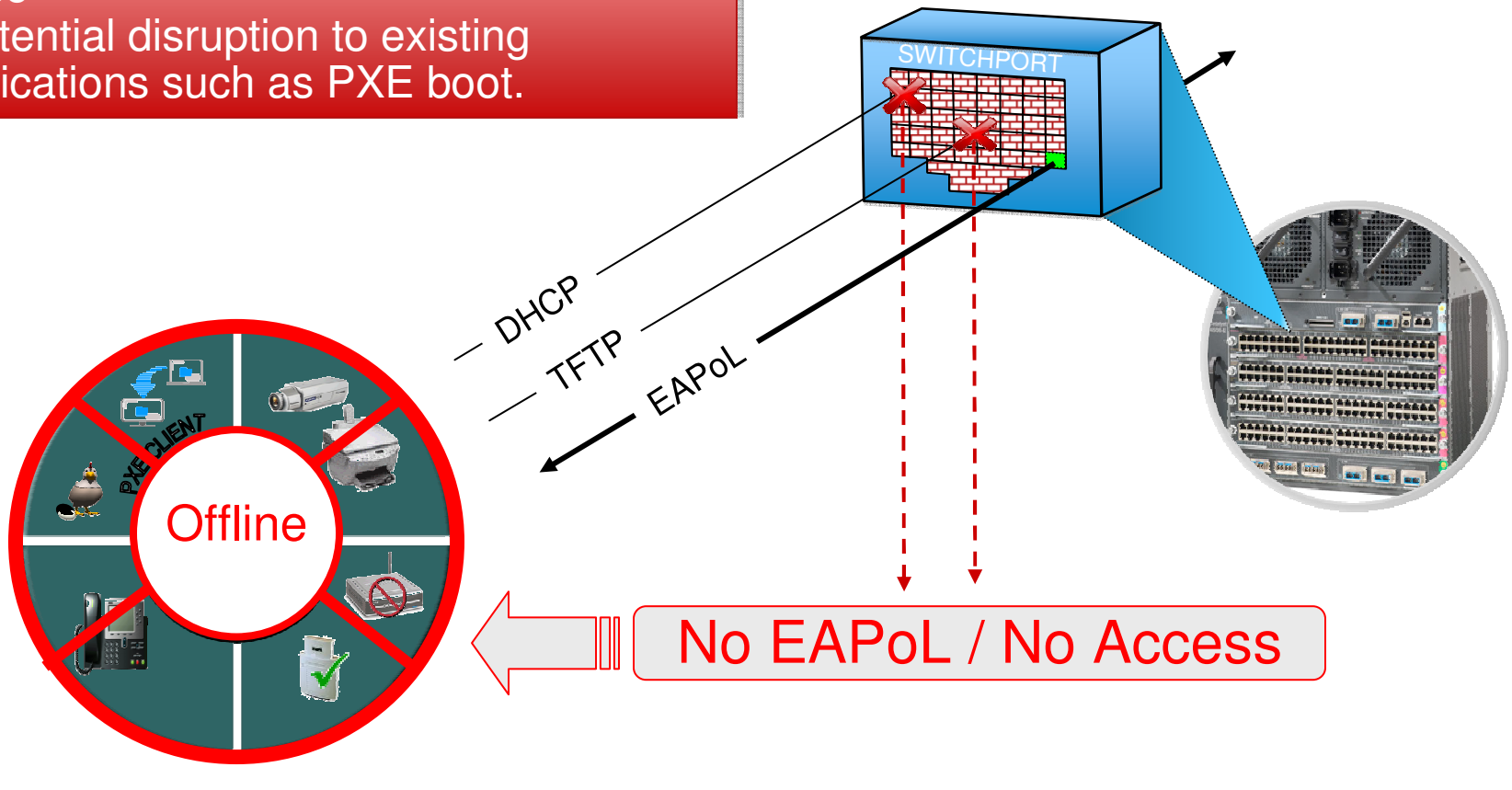
  Multi-auth

Guest Access

- **Central Web authentication**
- **Wired Guest Access Solution (NAC Guest Server)**

IEEE 802.1X Default Security Behavior

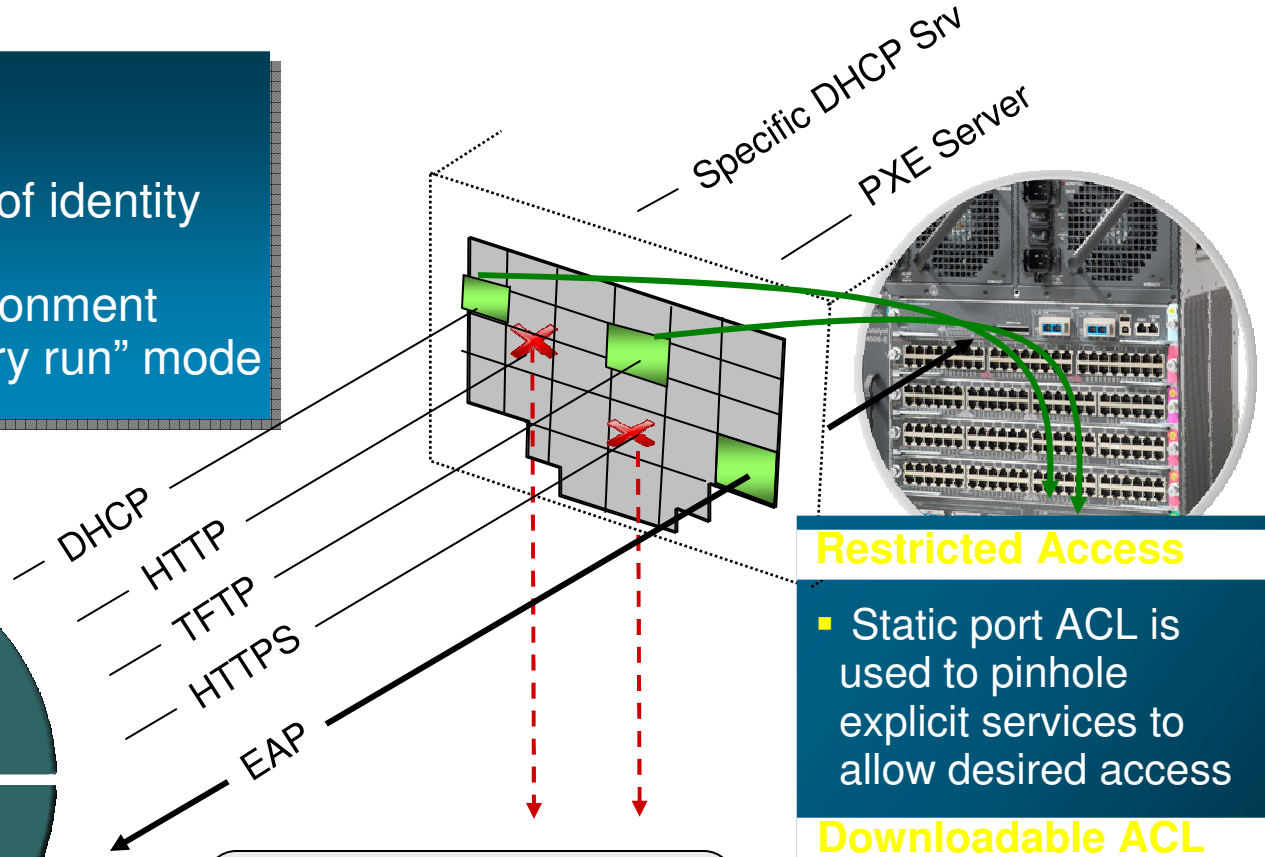
IEEE 802.1x Challenges
- Switch port changes from open → Close
- Potential disruption to existing applications such as PXE boot.



Open Mode With Restricted Access
Balancing Act

Open Mode Benefits:

- Reduce Network impact of identity deployment
- Supports PXE boot environment
- Provides customers a “dry run” mode



Block General Access Until Successful 802.1X, MAB or WebAuth

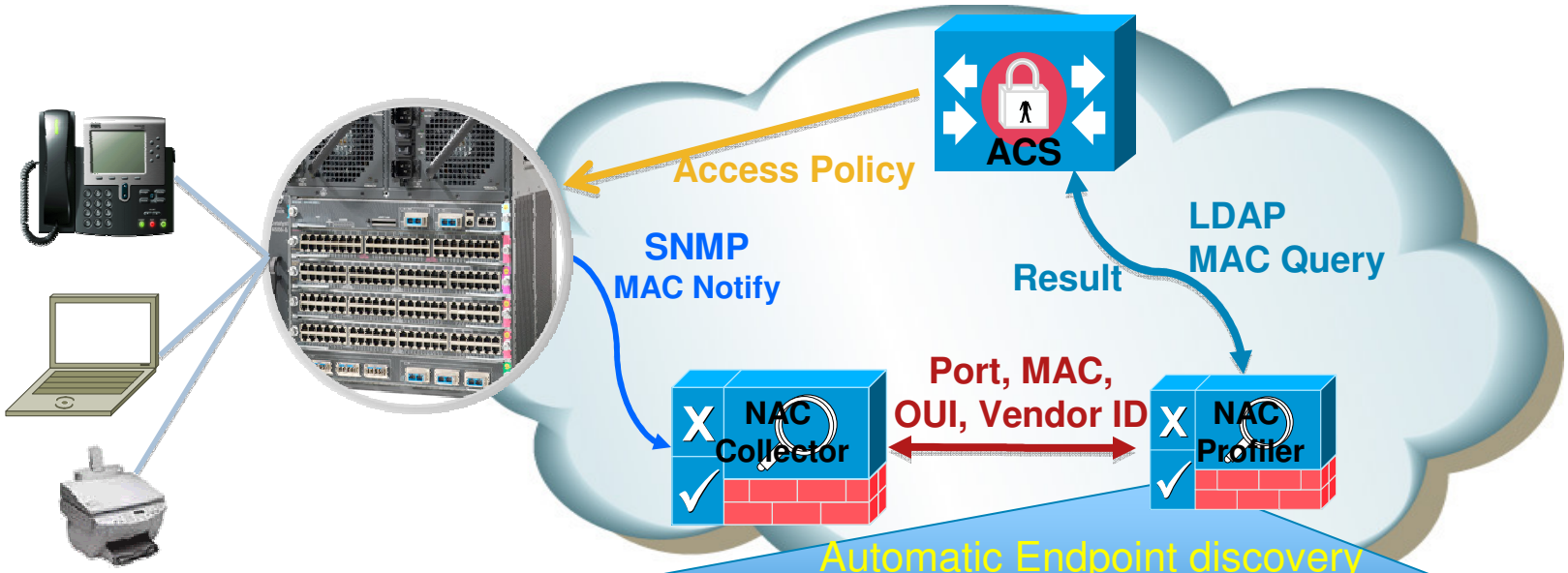
Restricted Access

- Static port ACL is used to pinhole explicit services to allow desired access

Downloadable ACL

- ACS downloadable ACL provides more granular per-user access control after authentication

Device Profiling With NAC Profiler

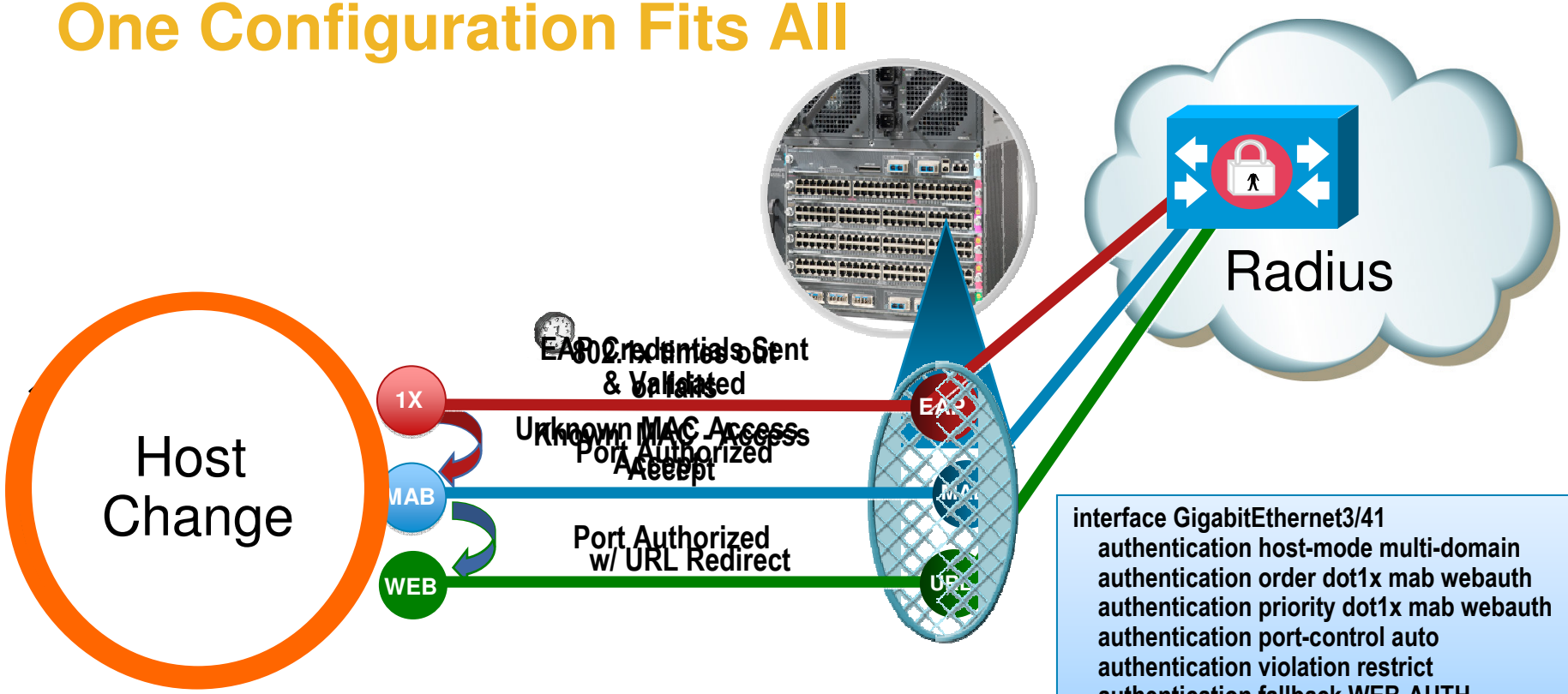


Automatic Endpoint discovery
Reduce identity deployment time
Real-time and historic visibility for all endpoints

Table of Windows OS
Total Profiles 9 Summary

MAC	IP	Certainty	Switch IP port	Link	VLAN
00:1c:c4:03:b0:2d (Hewlett Packard)	10.100.10.122	60%	6506 Distribution Gi1/23	Up	1
00:18:f8:09:cf:d7 (Cisco-Linksys LLC)	10.100.30.201	60%	4506-2 Gi1/0/5	Up	30

Flexible Authentication
One Configuration Fits All



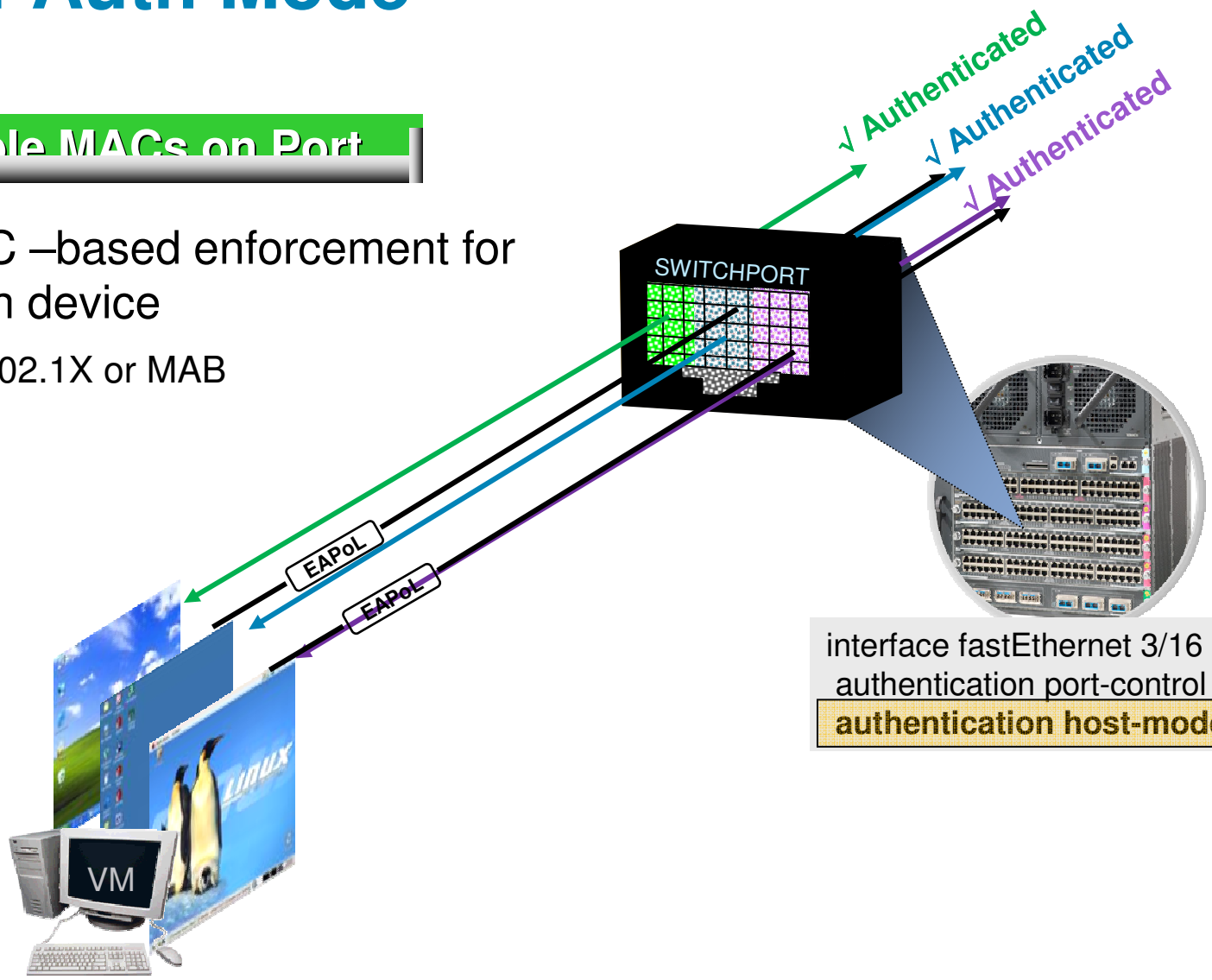

```
interface GigabitEthernet3/41
    authentication host-mode multi-domain
    authentication order dot1x mab webauth
    authentication priority dot1x mab webauth
    authentication port-control auto
    authentication violation restrict
    authentication fallback WEB-AUTH
    mab
```

- One configuration addresses all use cases, all host modes
- Controllable sequence of access control mechanisms, with flexible failure and fallback authorization
- Choice of policy enforcement mechanisms: VLAN, downloadable per-user ACL, URL
- Support single-host and multi-auth scenarios

Multi-Auth Mode

Multiple MACs on Port

- MAC –based enforcement for each device
  - 802.1X or MAB




```
interface fastEthernet 3/16
 authentication port-control auto
 authentication host-mode multi-auth
```

Multi-Domain Authentication (MDA)

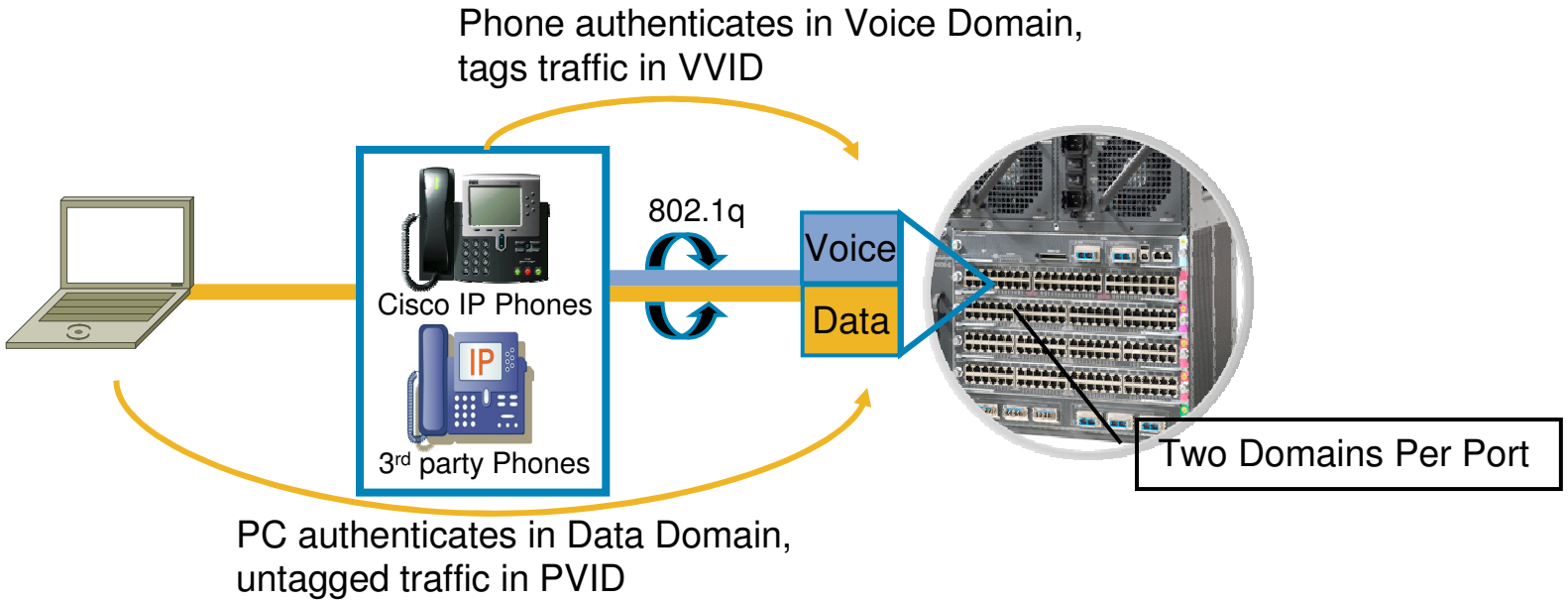
Solving the two-devices-per-port problem

IEEE 802.1X

Single device per port

MDA

Single device *per domain* per port



- MDA replaces CDP Bypass
- Supports Cisco IP Phones and 3rd Party IP Phones
- Phones *and* PCs use 802.1X or MAB

Addressing MAC Moves Issues
Options and Enhancements

Proxy EAPoL-Logoff

Session cleared immediately by proxy EAPoL-Logoff

Only works for 802.1X devices behind logoff-capable phones

802.1x/MAB Inactivity Timeout

Vulnerability until the Inactivity Timer expires, and session is cleared

Quiet devices may have to re-authenticate. Vulnerability within timer time

CDP Host Disconnect TLV

Session cleared immediately by CDP Link Down

- ✓ **Works for MAB, 802.1X, and Webauth.**
- ✓ **No configuration needed**

Evolution of Network Access Control

Topology Aware to Role Aware

Cisco Trusted Security (CTS)

- Network-wide role-based access control
- Network device access control
- Consistent policies for wired, wireless and remote access

Network Admission Control (NAC)

- Posture validation endpoint policy compliance

Identity-Based Access Control

- Flexible authentication options:
  802.1x, MAB, WebAuth, FlexAuth
- Comprehensive post-admission control options:
  dACL, VLAN assignment, URL redirect, QoS…

Network Address-based Access Control

- ACL, VACL, PACL, PBACL etc