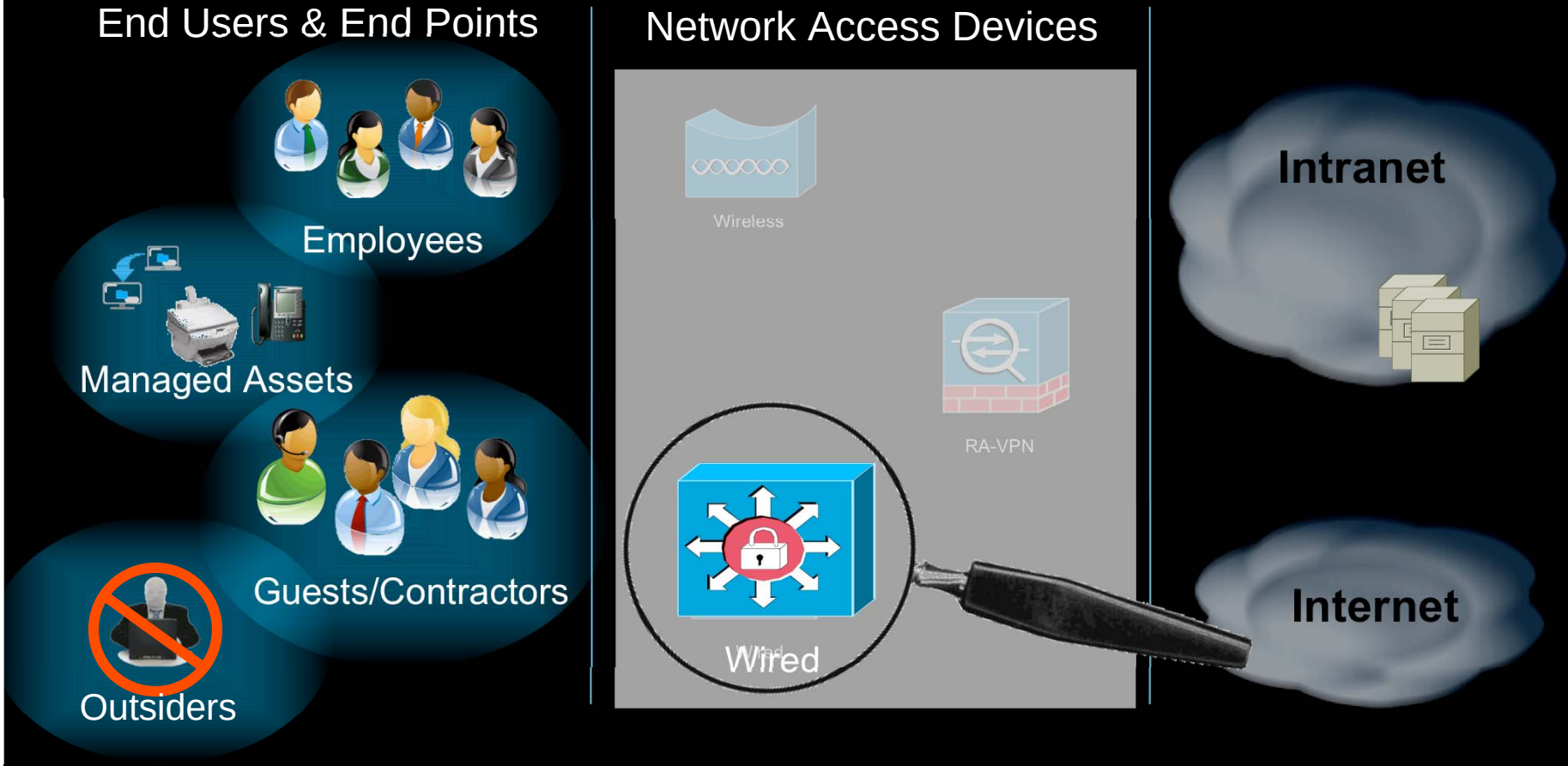
Identity Networking

Abstract

- Intro to Wired 802.1X – The Promise of Port-Based Access Control Deployment

- Common Challenges & Cisco Countermeasures
  - Clientless -- Profiler + MAB Deployment
  - Host Asset Management (PXE, GPO, etc) -- OpenMode
  - Operational Cost -- FlexAuth Deployment
  - IP Telephony Integration -- Multi-Domain Auth (MDA), EAPoL-Logoff, Inactivity, Violation handling, CDP 2nd Port

Identity for Today's Access Layer



Why is Identity Difficult in the Wired LAN?

- **WLANs**
  - Relatively New Technology
  - Required Client from the beginning
  - No legacy host issues to deal with
- **Remote Access VPN**
  - Relatively New Technology
  - Required a client from the beginning
  - No legacy host issues to deal with

- **Wired Ethernet Networks**
  - Ethernet Mature Technology Widely Deployed
  - Never really required authentication client
  - 20-Years of legacy protocols, devices, operating systems and applications
    - Most of which were built with the assumption of open connectivity
- **802.1X in Wired Environments**
  - Breaks all of this
  - Requires Prior Knowledge of device capabilities before configuring access port (Major Opex Challenge)

Identity 4.0 Delivers

- FlexAuth – Singe port configuration with flexible authentication technology (802.1X, MAB & WebAuth)
- 802.1X Open Mode - Enhance 802.1X Authenticator (i.e., wired switches) to ease *OS/protocol/mgmt app* issues
- IPT Integration Enhancements - Multi-Domain Auth (MDA)
- Simplification of MAB
  - NAC Profiler – To Provide Endpoint Discovery & Profiling
  - EASY - Simplification of Provisioning MAB

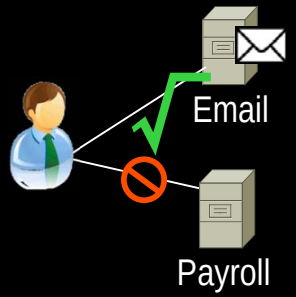
Why Is Identity Important in Wired LANs?

- **Keep the outsiders out**

  Prevent unsecured individual gaining physical and logical access to a network

- **Keep the insiders honest**

  What can validated users do when they get network access?

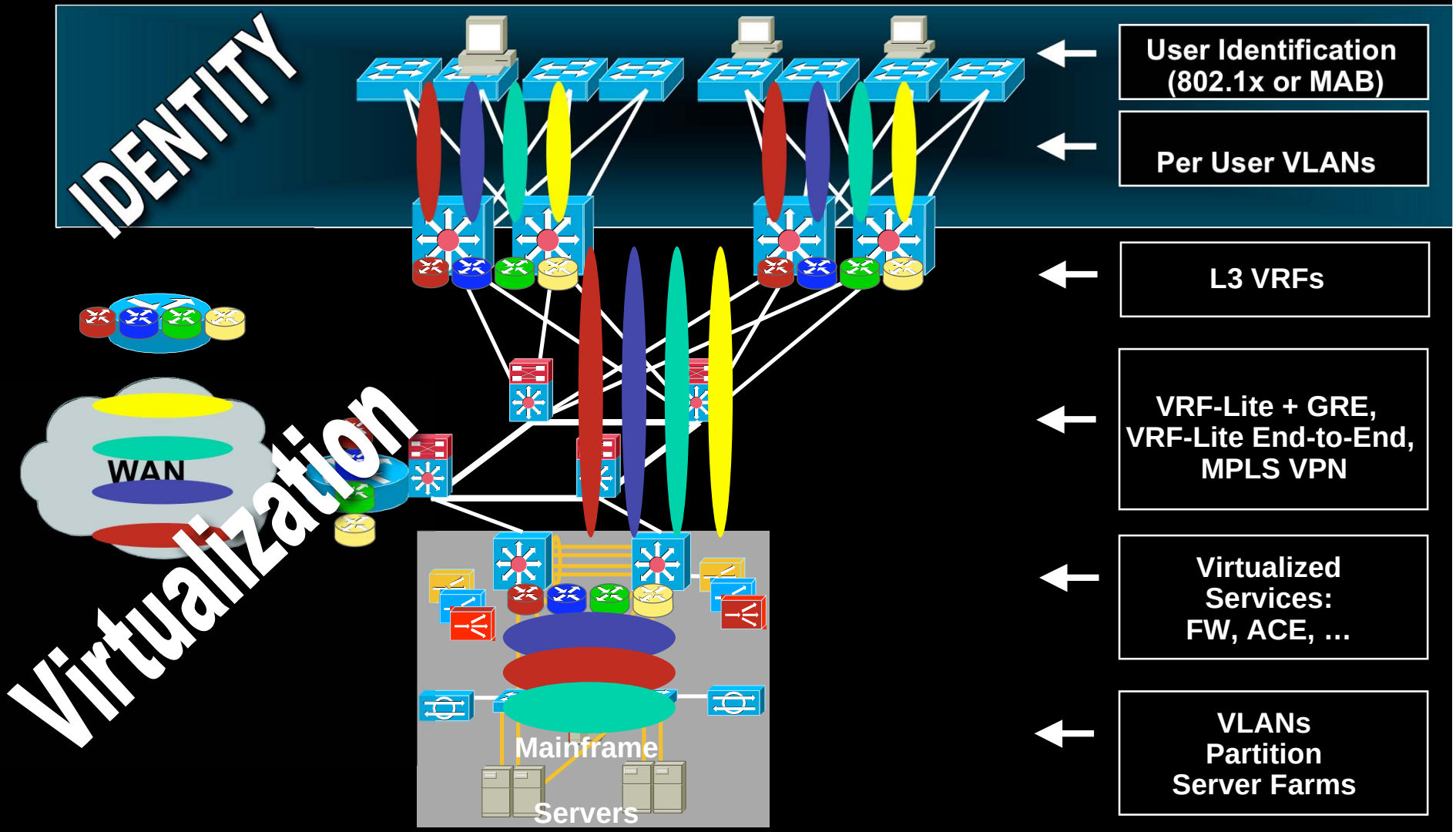


- **Increase network visibility**

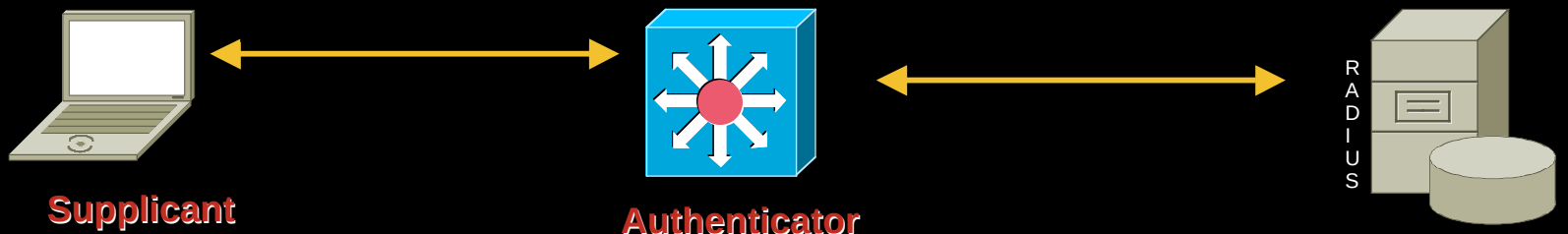
  Real-time and logged

  Enterprises need accountability

Laying the Groundwork



IEEE 802.1X: The Foundation of Identity



Supplicant
(802.1X Client)

Authenticator
(e.g. Switch, Access Point)

Authentication Server
(e.g., ACS)

- ✓ IEEE 802.1 working group standard
- ✓ Provides port-based access control using authentication

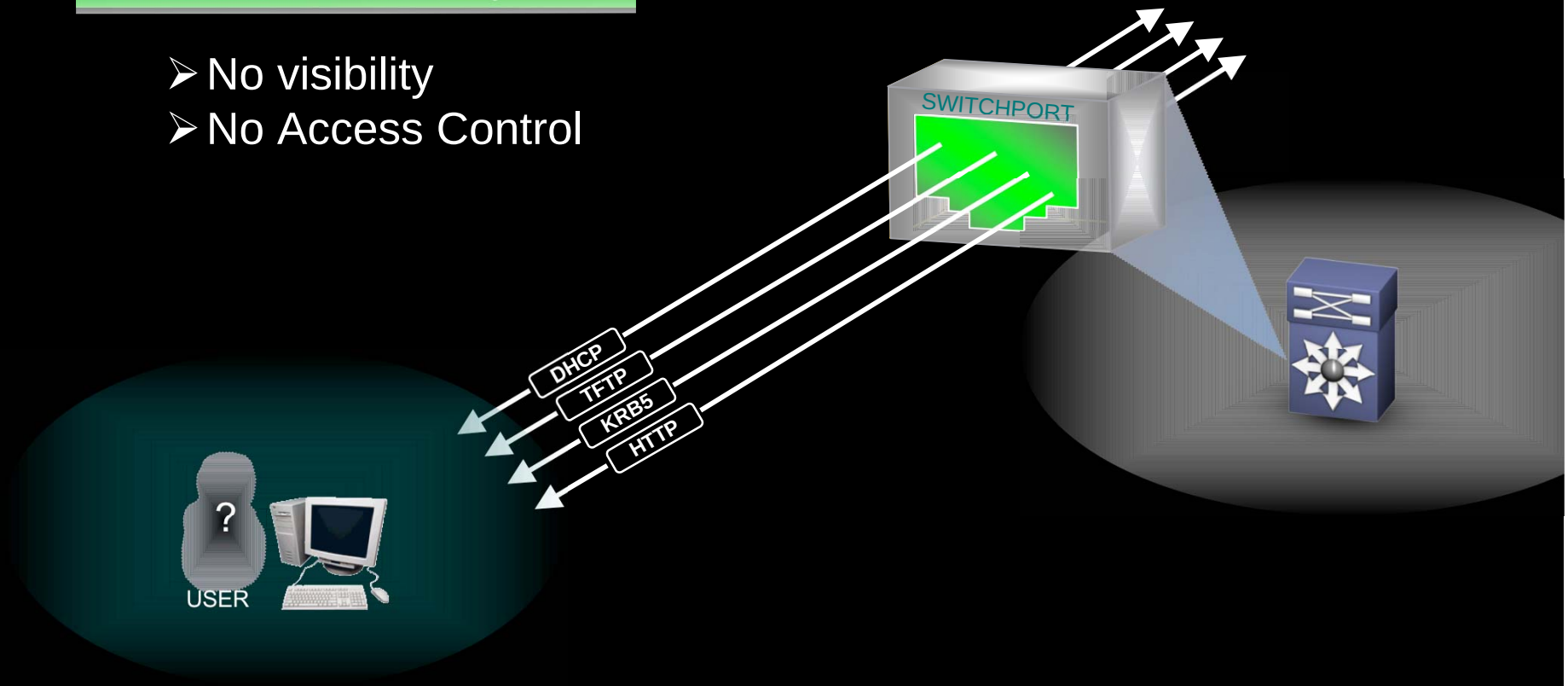
Enforcement via MAC-based filtering and port-state monitoring

Defines encapsulation for Extensible Authentication Protocol (EAP) over IEEE 802 media— “EAPoL”

Default Port State without 802.1X

No Authentication Required

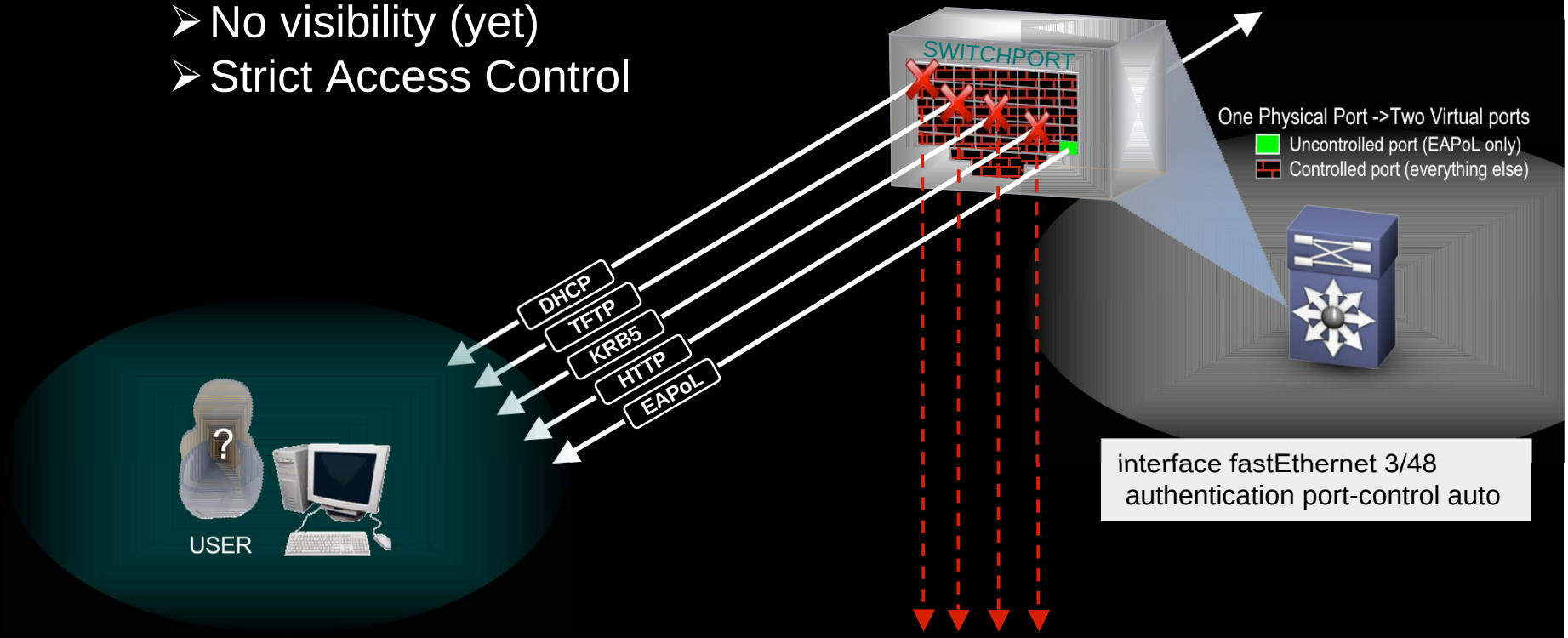
- No visibility
- No Access Control



Default Security with 802.1X

Before Authentication

- No visibility (yet)
- Strict Access Control

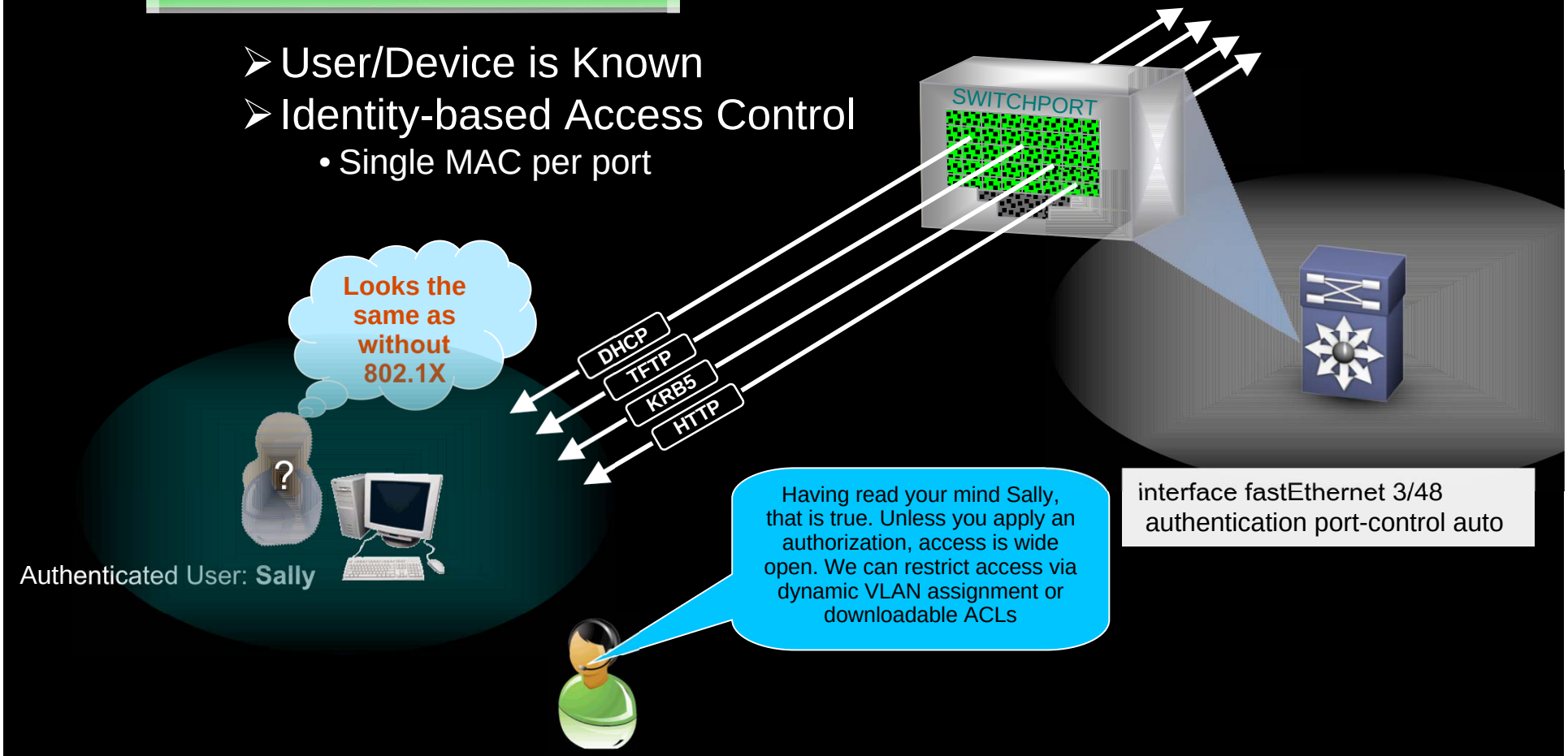


ALL traffic *except* EAPoL is dropped

Default Security with 802.1X

After Authentication

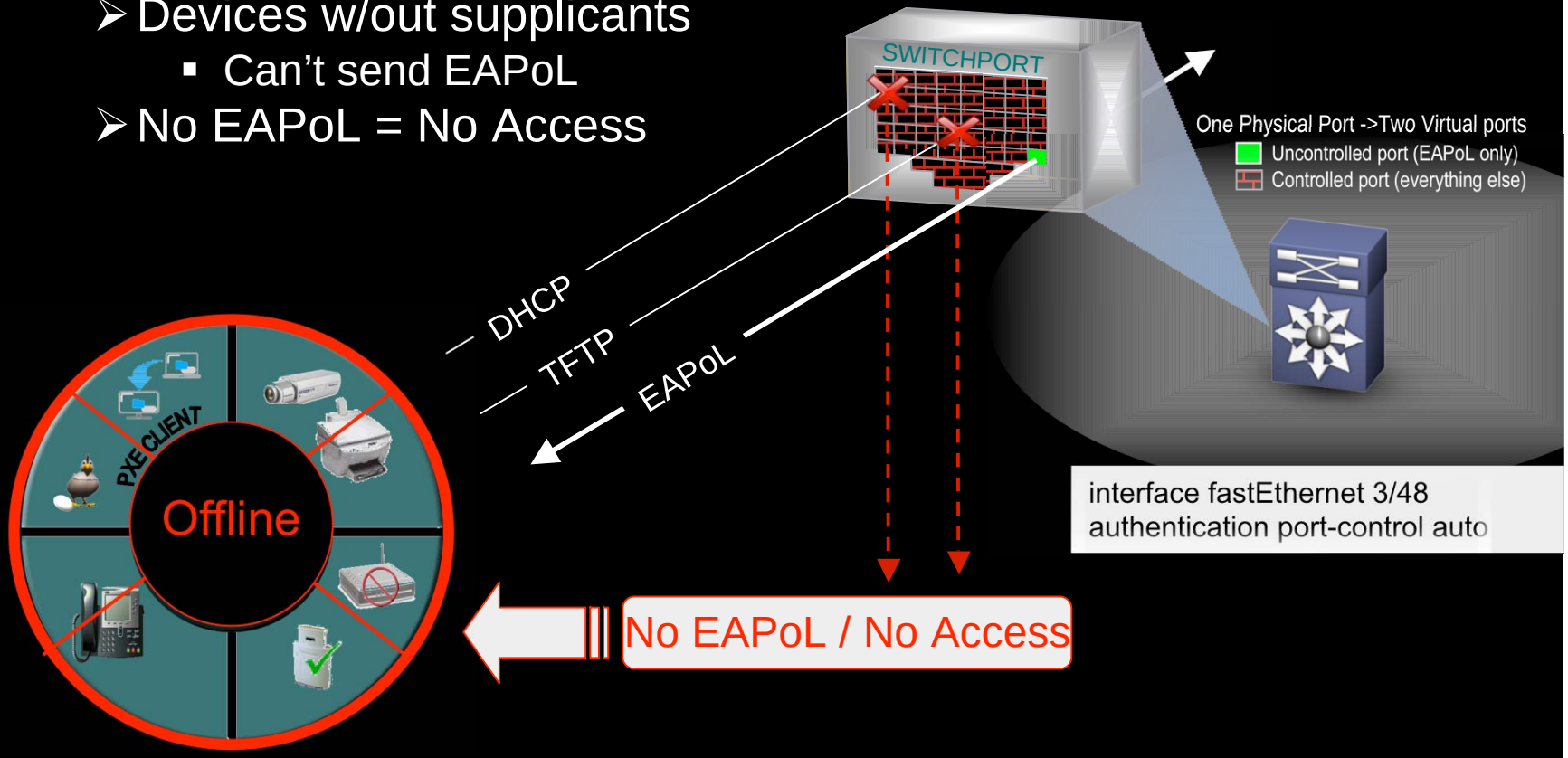
- User/Device is Known
- Identity-based Access Control
  - Single MAC per port



Default Security: Consequences

Default 802.1x Challenge

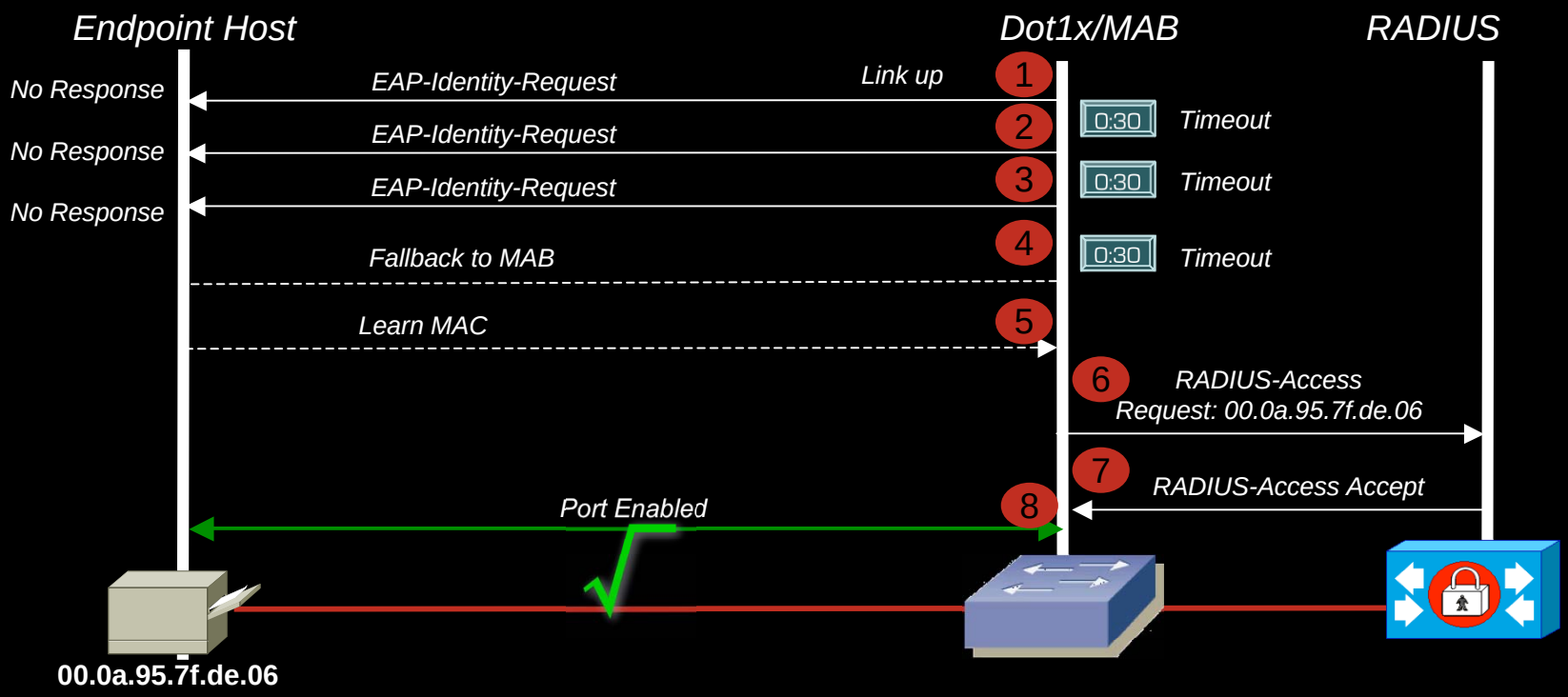
- Devices w/out supplicants
  - Can't send EAPoL
- No EAPoL = No Access



Simplifying 802.1X Deployments

Challenge	Cisco IOS Enhancement
Clientless Device	IOS MAB + Profiler / EEM
Host Asset Management	IOS 802.1X OpenMode
Operation Cost	IOS Flexible Authentication (FlexAuth)
IPT Integration	IOS Multi-Domain Auth (MDA) IOS EAPoL-Logoff, MAB Inactivity IOS CDP 2nd Port Notification

Authenticating Clientless Devices
MAC Authentication Bypass (MAB)



- **Same authorizations as 802.1X (VLAN or ACL)**
- **Requires current database of known MACs**

```
interface fastEthernet 3/48
 authentication port-control auto
 mab
```

MAB Limitations & Challenges

- MAB requires creating and maintaining MAC database
- Default 802.1X timeout = 90 seconds
  - 90 sec > default MSFT DHCP timeout
  - 90 sec > default PXE timeout
  - Current Workaround: Timer tuning (always requires testing)
    - max-reauth-req: maximum number of times (default: 2) that the switch retransmits an EAP-Identity-Request frame on the wire
    - tx-period: number of seconds (default: 30) that the switch waits for a response to an EAP-Identity-Request frame before retransmitting
    - 802.1X Timeout == (max-reauth-req + 1) * tx-period

Simplifying MAB Deployments: NAC Profiler Build MAC Database Before Deploying 802.1X

```
interface range gigE 1/0/1 - 24
  switchport access vlan 30
  switchport voice vlan 31
snmp-server host 10.100.10.215 RO
snmp-server enable traps mac-notification
snmp-server enable traps snmp linkup linkdown
```

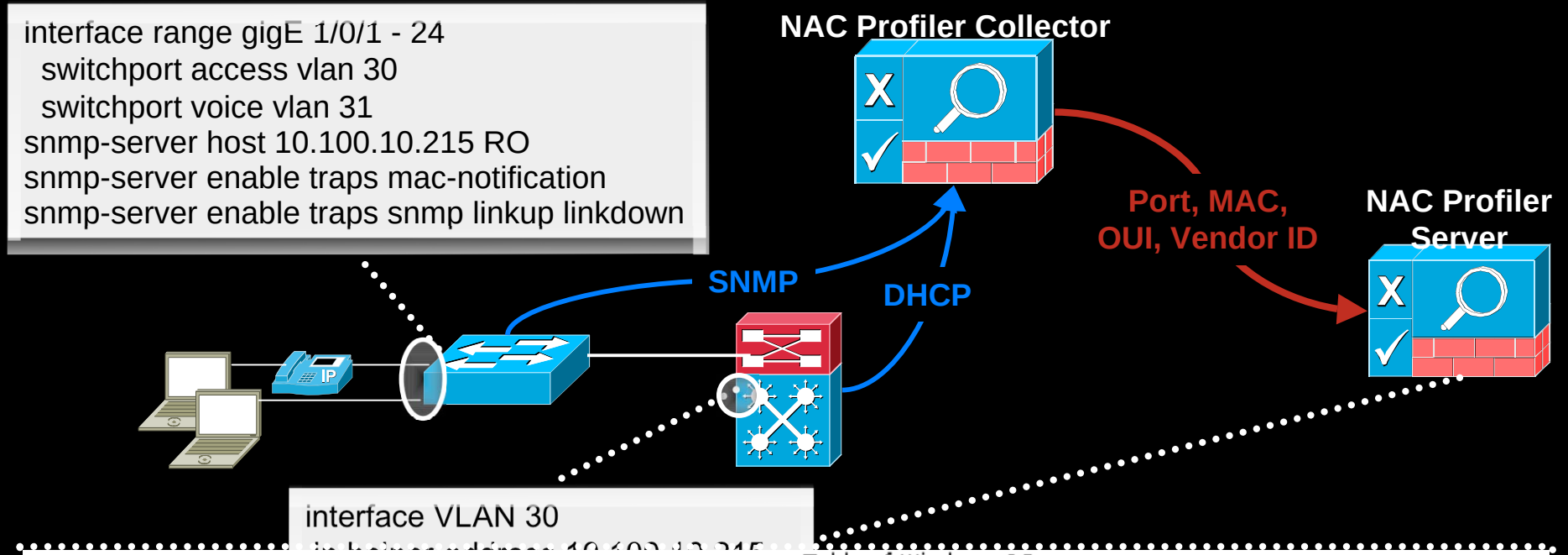
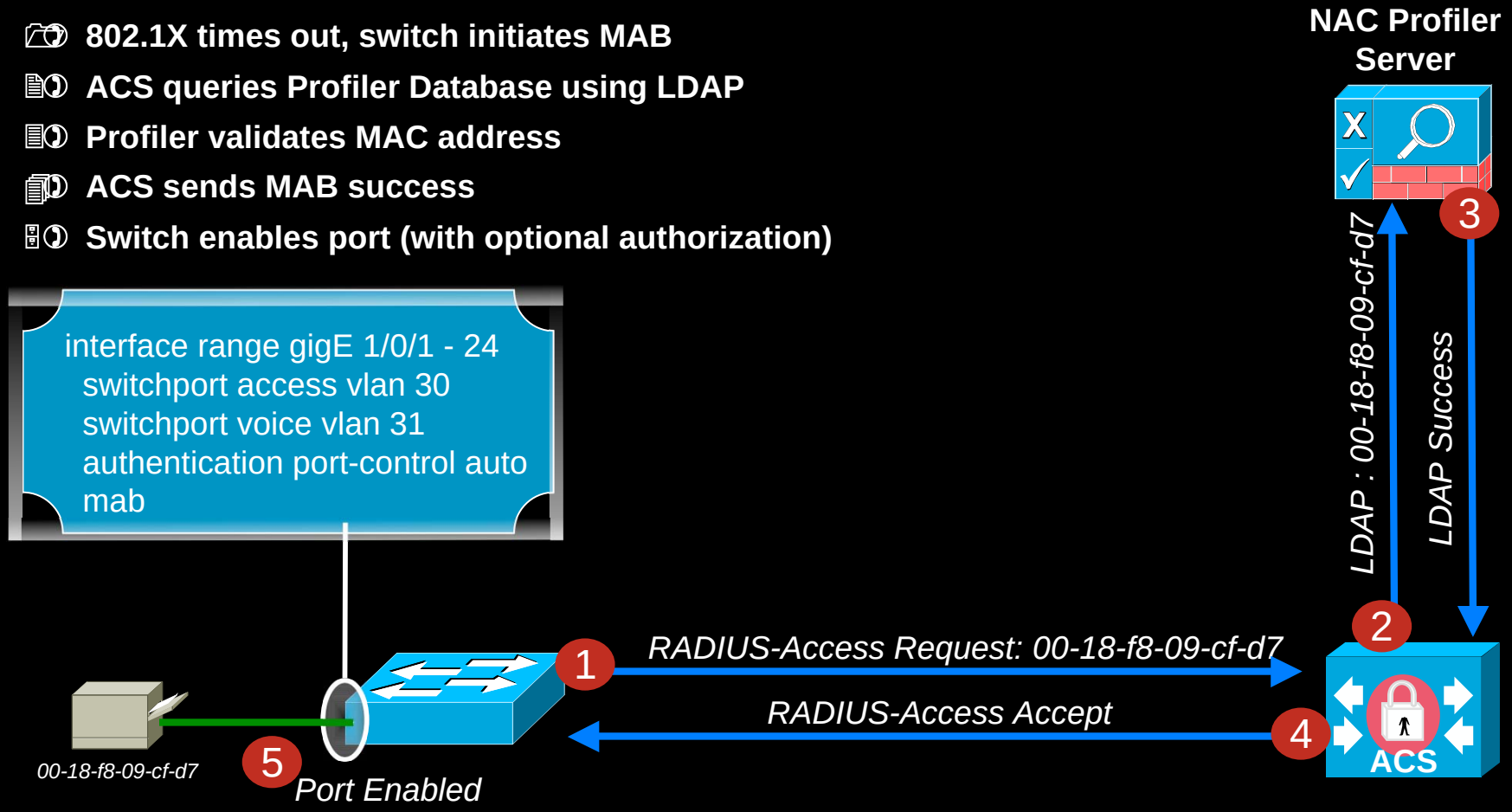


Table of Windows OS
Total Profiles: 9 Summary

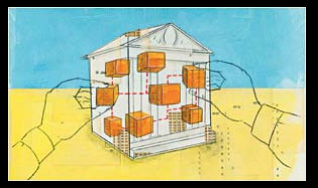
MAC	IP Address	Certainty	Switch IP Port	Link	VLAN
00:1c:c4:f3:b0:2d (Hewlett Packard)	10.100.10.122	60%	6506 Distribution Gi1/23 (23)	Up	1
00:18:f8:09:cf:d7 (Cisco-Linksys LLC)	10.100.30.201	60%	3750-2 Gi1/0/5 (10105)	Up	30

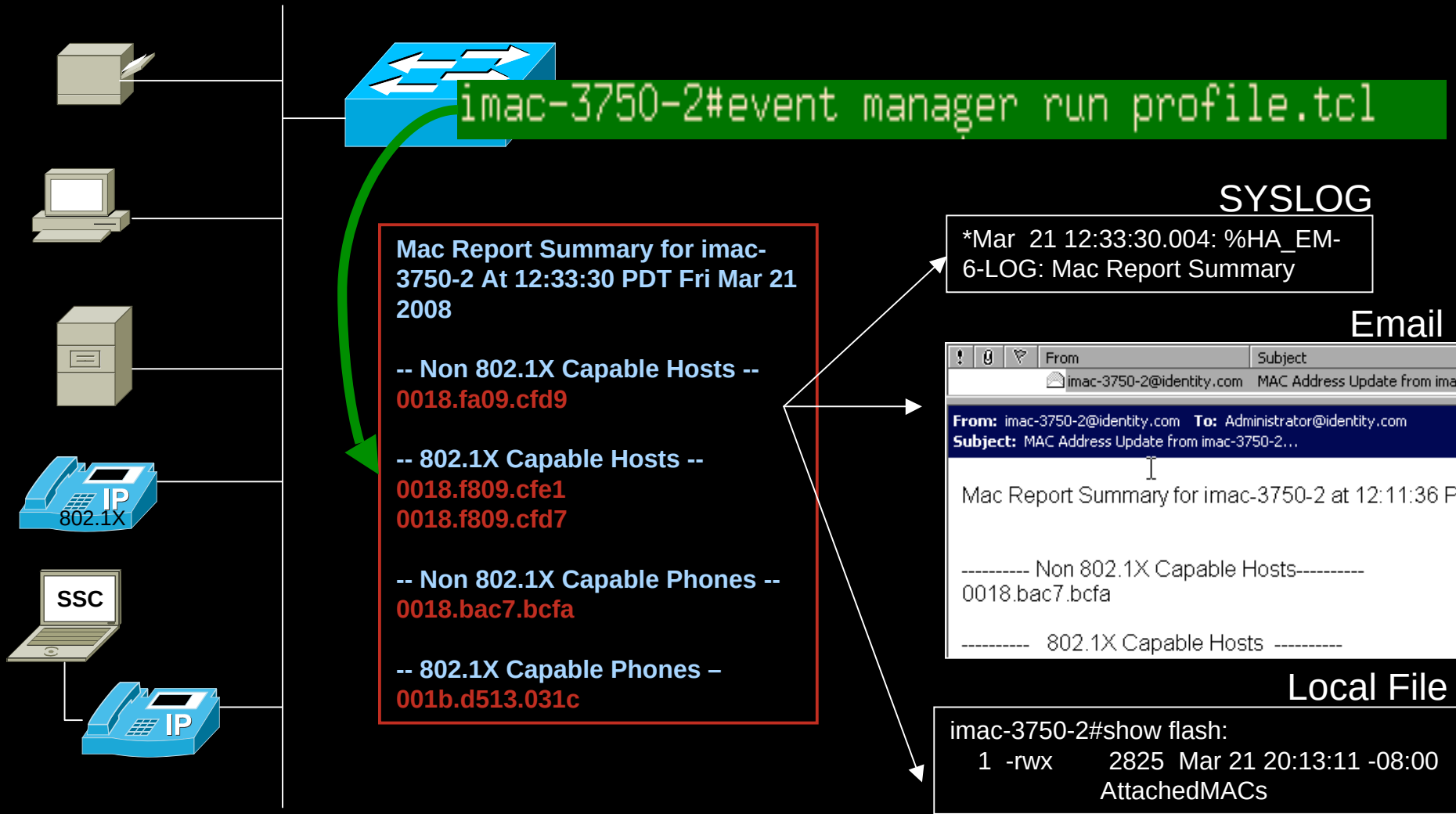
NAC Profiler
Query MAC Database After Deploying 802.1X

- 802.1X times out, switch initiates MAB
- ACS queries Profiler Database using LDAP
- Profiler validates MAC address
- ACS sends MAB success
- Switch enables port (with optional authorization)

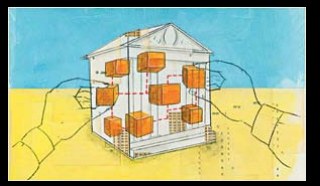


Using EEM to Prepare for 802.1X





EEM Profile.tcl Sample Script



```
imac-3750-2#show run | include event manager
event manager environment _email_from imac-3750-2@identity.com
event manager environment _email_to Administrator@identity.com
event manager environment _email_server 10.100.10.116
event manager environment fs f
event manager environment _log
event manager directory user p
event manager policy profile.t
imac-3750-2#
```

```
imac-3750-2#copy ftp://anonymous@10.100.10.119/profile.tcl flash:
Destination filename [profile.tcl]?
Accessing ftp://anonymous@10.100.10.119/profile.tcl...
Loading profile.tcl !
[OK - 6838/4096 bytes]

6838 bytes copied in 5.302 secs (1290 bytes/sec)
```

```
#Determine which interfaces are trunks
lappend clicmd "show interface status | include trunk"
set showintstat [split [CLICmdProc $clicmd ] \n ]
foreach trunk $showintstat {
        if { ![regexp $routername $trunk] }
                regsub $ [lindex [split $tru
                lappend excludetrunk $trunk
}
set trunklist [join $excludetrunk |]

#Set the time at beginning of test
set time_now [clock seconds]
set time_now [clock format $time_now -format

#Get MAC addresses of Access ports
lappend showmac  "show mac-address dynamic |
set maclist [split [CLICmdProc $showmac ] \n

#Get list of Voice VLANs
lappend showvvidcmd "show run | include swit
set showvvid [split [CLICmdProc $showvvidcmd
foreach voiceline $showvvid {
        if { [regexp {switchport voice vlan ([0-9]+)} $voiceline dummy vvid] } {
                if { [lsearch $vvidlist $vvid] < 0 } {
                        lappend vvidlist $vvid
                }
```

Summary of Profile.tcl

- Scan for MACs on access ports
- Find MACs on Voice VLAN
- switch# dot1x test eapol-capable
- Email, Syslog or create file of profiled devices

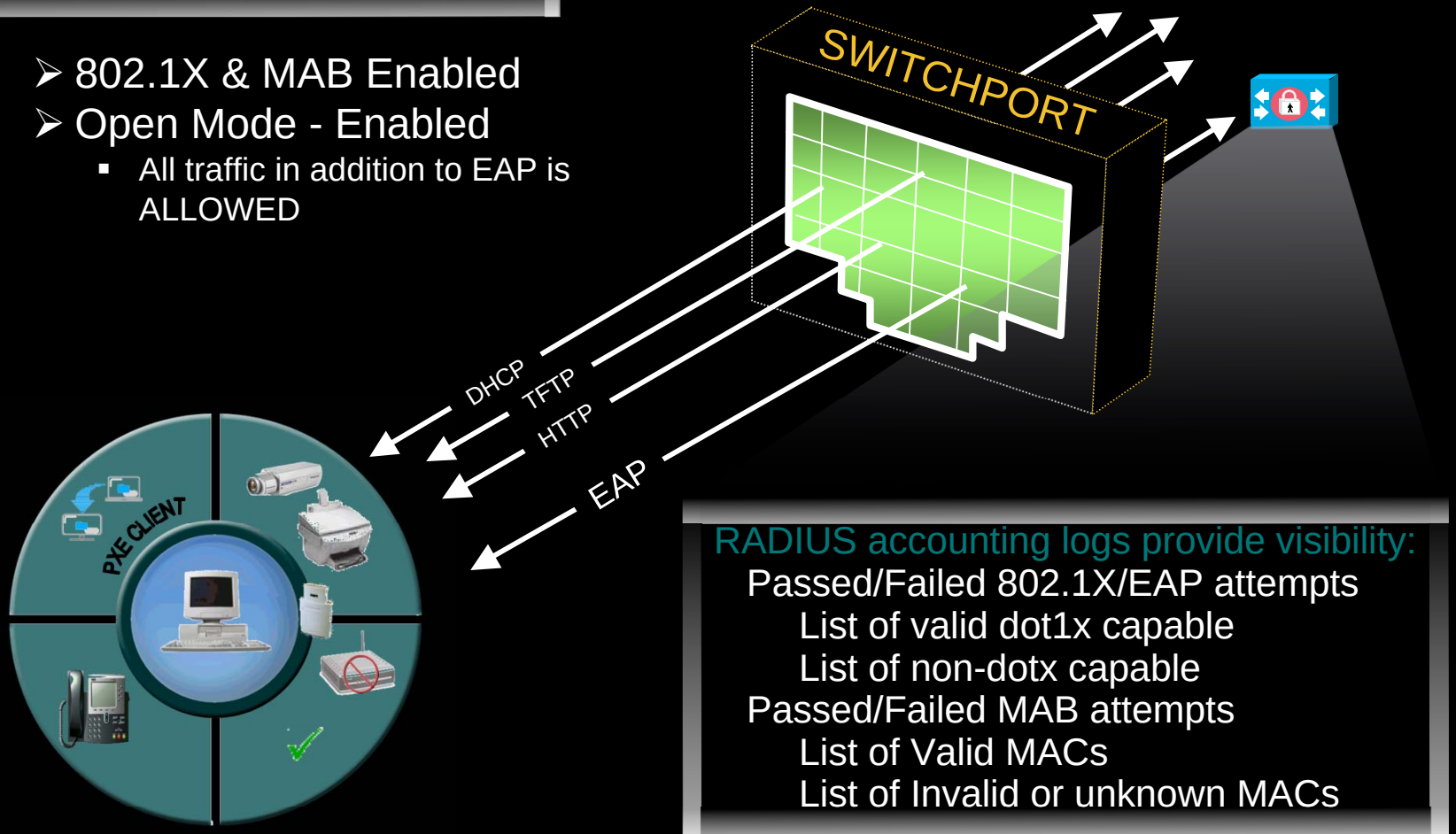
Stay Tuned for More Scripts!

Next Section
Open Mode

802.1X/MAB – Open Mode

Open Mode (No Restrictions)

- 802.1X & MAB Enabled
- Open Mode - Enabled
  - All traffic in addition to EAP is ALLOWED



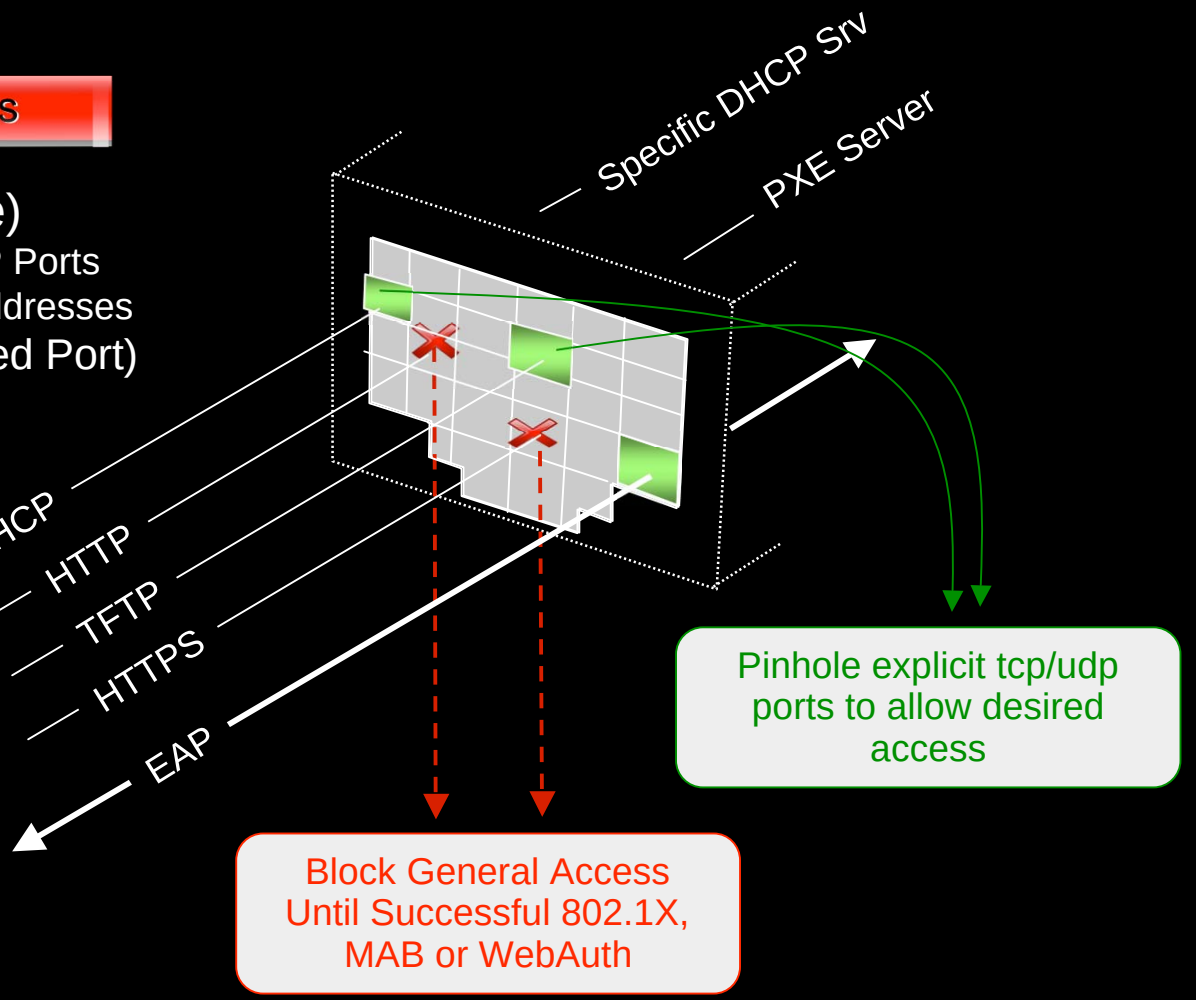
RADIUS accounting logs provide visibility:

- Passed/Failed 802.1X/EAP attempts
  - List of valid dot1x capable
  - List of non-dotx capable
- Passed/Failed MAB attempts
  - List of Valid MACs
  - List of Invalid or unknown MACs

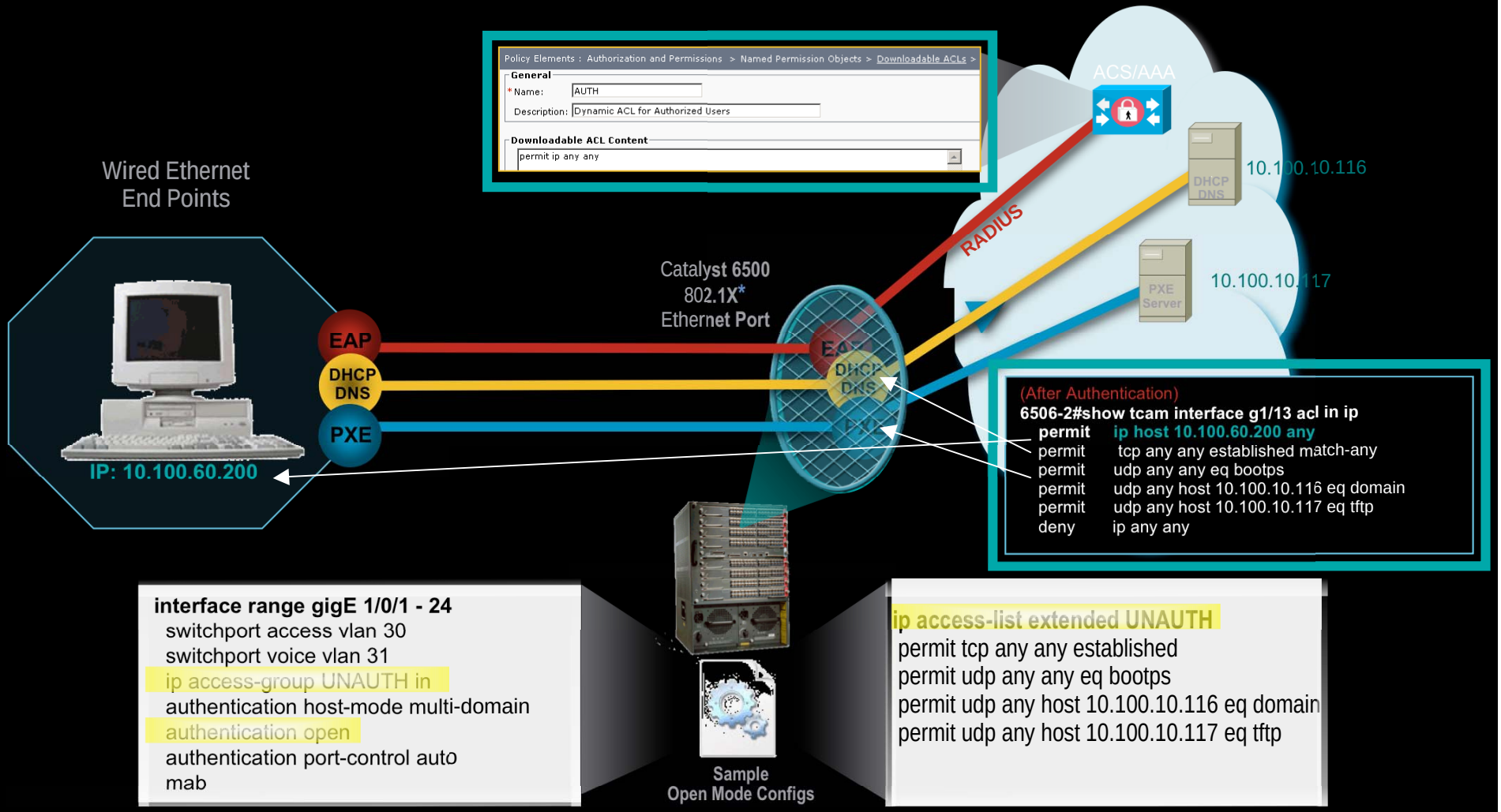
802.1X/MAB – Open Mode

Selectively Open Access

- Open Mode (Pinhole)
  - On Specific TCP/UDP Ports
  - Restrict to Specific Addresses
- EAP Allowed (Controlled Port)



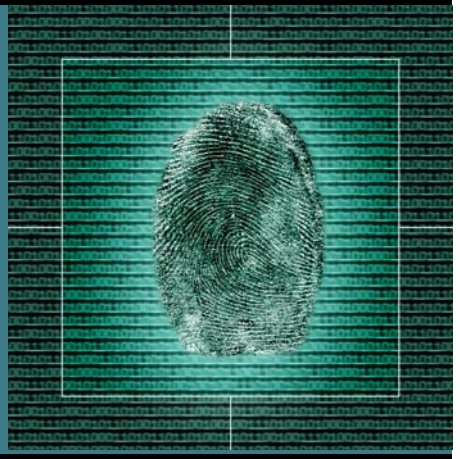
Example
Open Mode On 802.1X Port w/ Access Control



* Works on FlexAuth & MDA Enabled Ports

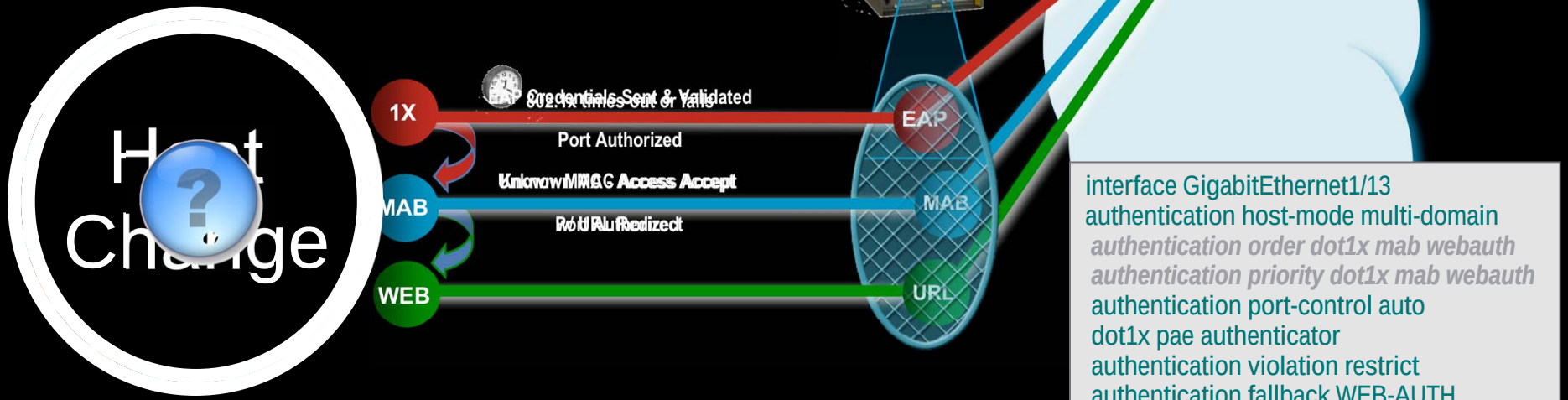
Next Section

Flexible Authentication (FlexAuth)



Flexible Authentication Host Roulette

Choice of policy enforcement mechanisms: VLAN, downloadable per-user ACL, URL




```
interface GigabitEthernet1/13
authentication host-mode multi-domain
 authentication order dot1x mab webauth
 authentication priority dot1x mab webauth
 authentication port-control auto
 dot1x pae authenticator
 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

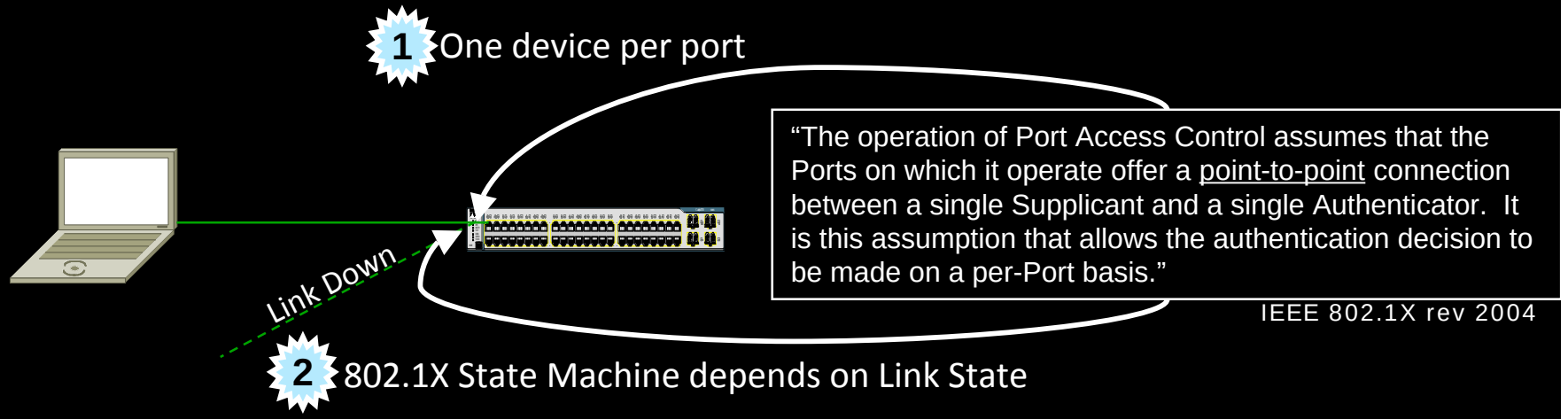
Benefit

- **Greater flexibility & deterministic behavior**

Next Section

IP Telephony Integration

IPT & 802.1X: Fundamental Challenges



"The operation of Port Access Control assumes that the Ports on which it operate offer a point-to-point connection between a single Supplicant and a single Authenticator. It is this assumption that allows the authentication decision to be made on a per-Port basis."

IEEE 802.1X rev 2004

IPT Breaks the Point-to-Point Model

Multi-Domain Authentication (MDA)

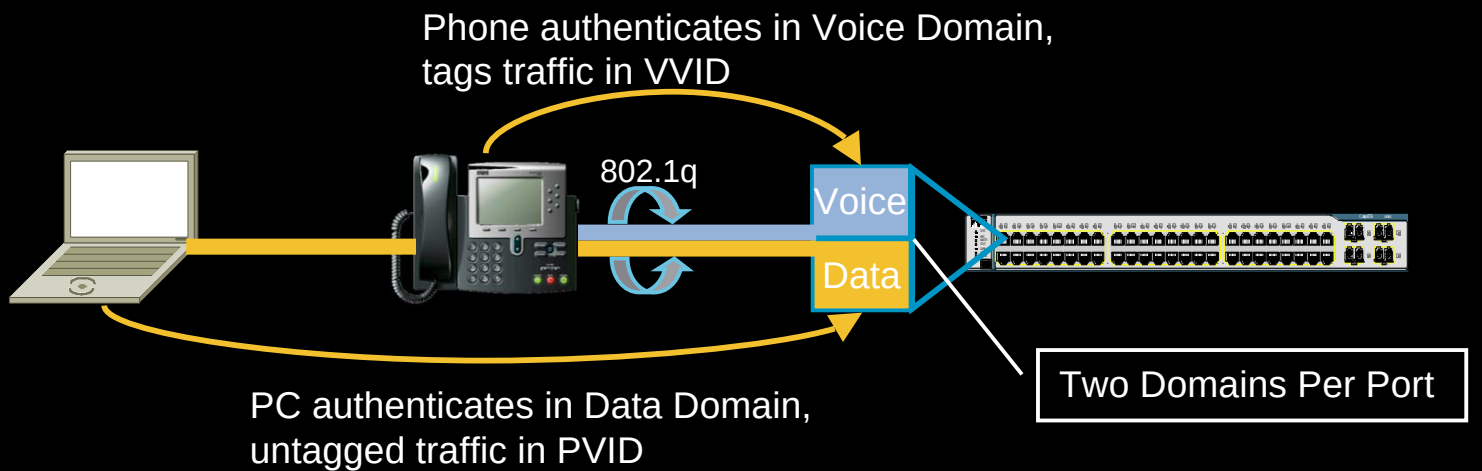
Solving the two-devices-per-port problem

IEEE 802.1X

Single device per port

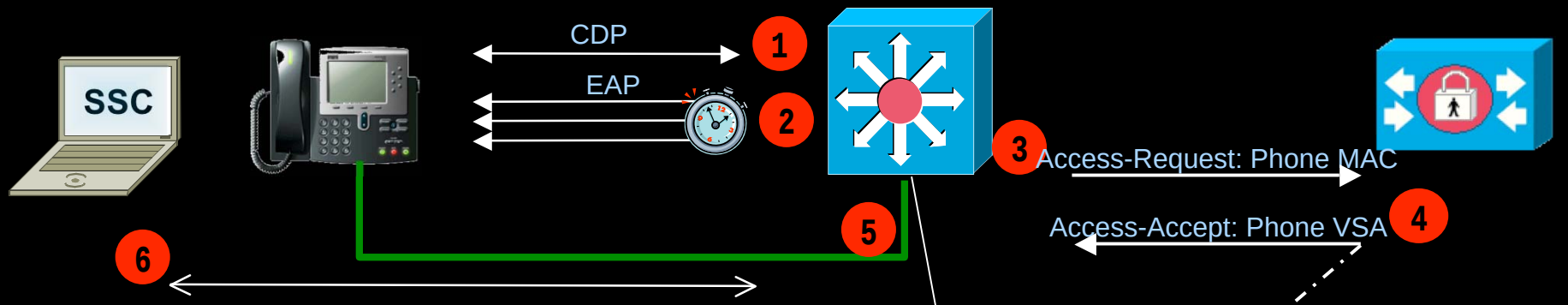
MDA

Single device ***per domain*** per port



3K: 12.2(35)SEE
4K: 12.2(37)SG
New 6K: 12.2(33)SXI

MDA for Cisco IP Phones



1) Phone learns VVID from CDP
2) 802.1X times out
3) Switch learns phone's MAC, in
4) ACS returns Access-Accept wi
5) Phone traffic allowed on either VLAN until it sends tagged packet, then only voice VLAN
6) (Asynchronous) PC authenticates using 802.1X or MAB
   - Authenticated PC traffic allowed on data VLAN only

MDA in Action

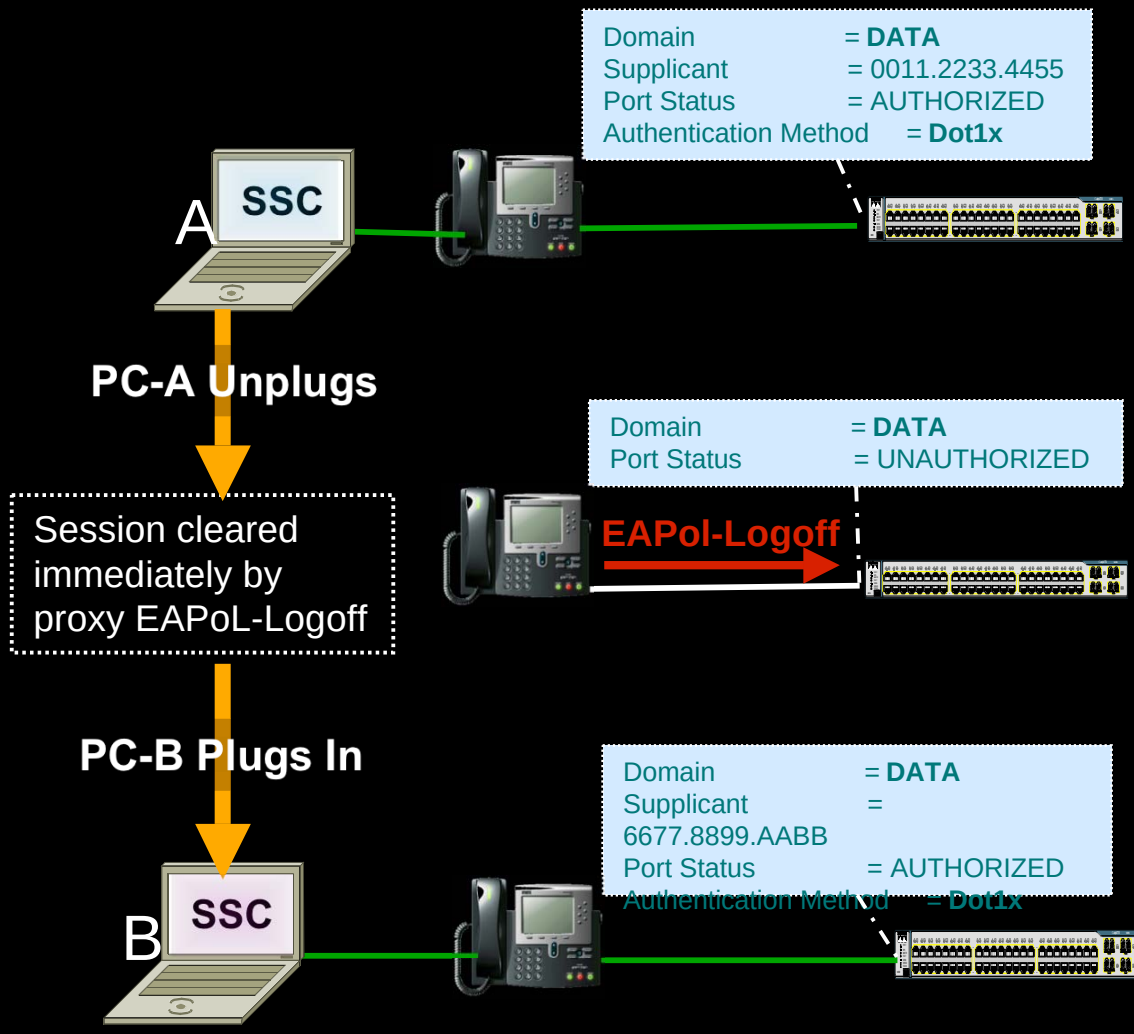
```
3750-1(config-if)#do sh dot1x int G1/0/5 details
<...>

Dot1x Authenticator Client List
-------------------------------
Domain                          = DATA
Supplicant                      = 0014.5e42.66df
    Auth SM State               = AUTHENTICATED
    Auth BEND SM State          = IDLE
Port Status                     = AUTHORIZED
Authentication Method           = Dot1x
Authorized By                   = Authentication Server

Domain                          = VOICE
Supplicant                      = 0016.9dc3.08b8
    Auth SM State               = AUTHENTICATED
    Auth BEND SM State          = IDLE
Port Status                     = AUTHORIZED
Authentication Method           = MAB
Authorized By                   = Authentication Server
```

IPT & 802.1X: The Link-State Problem

1) Legitimate users cause security violation

2) Hackers can spoof MAC to gain access without authenticating

Previous Solution: Proxy EAPoL-Logoff



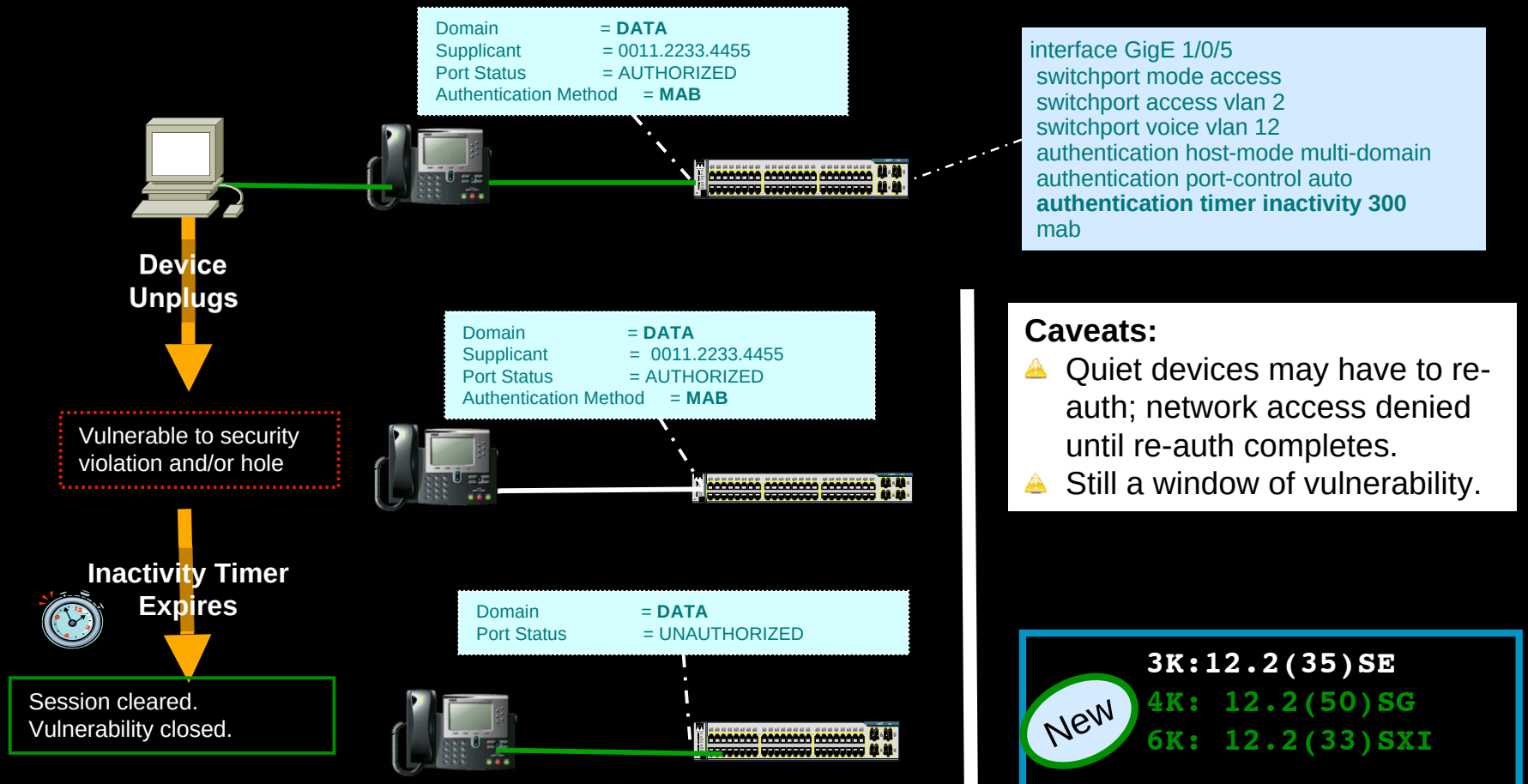
Caveats:

- Only for 802.1X devices behind phone

Requires:

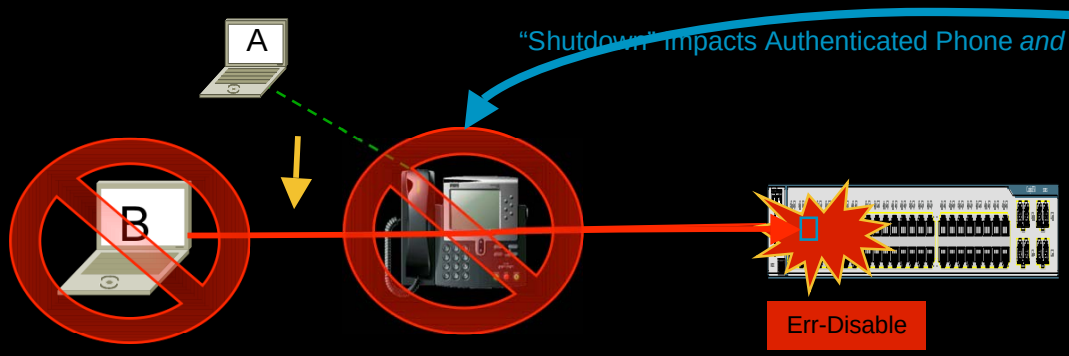
Logoff-capable Phones

Previous Solution: MAB Inactivity Timeout



NEW!

New Mitigation Technique: Security Violation Handling



"Shutdown" Impacts Authenticated Phone *and* PC-B

```
interface GigE 1/4
 dot1x mac-auth-bypass
 dot1x mac-auth timeout inactivity 300
 dot1x port-control auto
 dot1x host-mode multi-domain
 dot1x violation-mode shutdown
```

Err-Disable

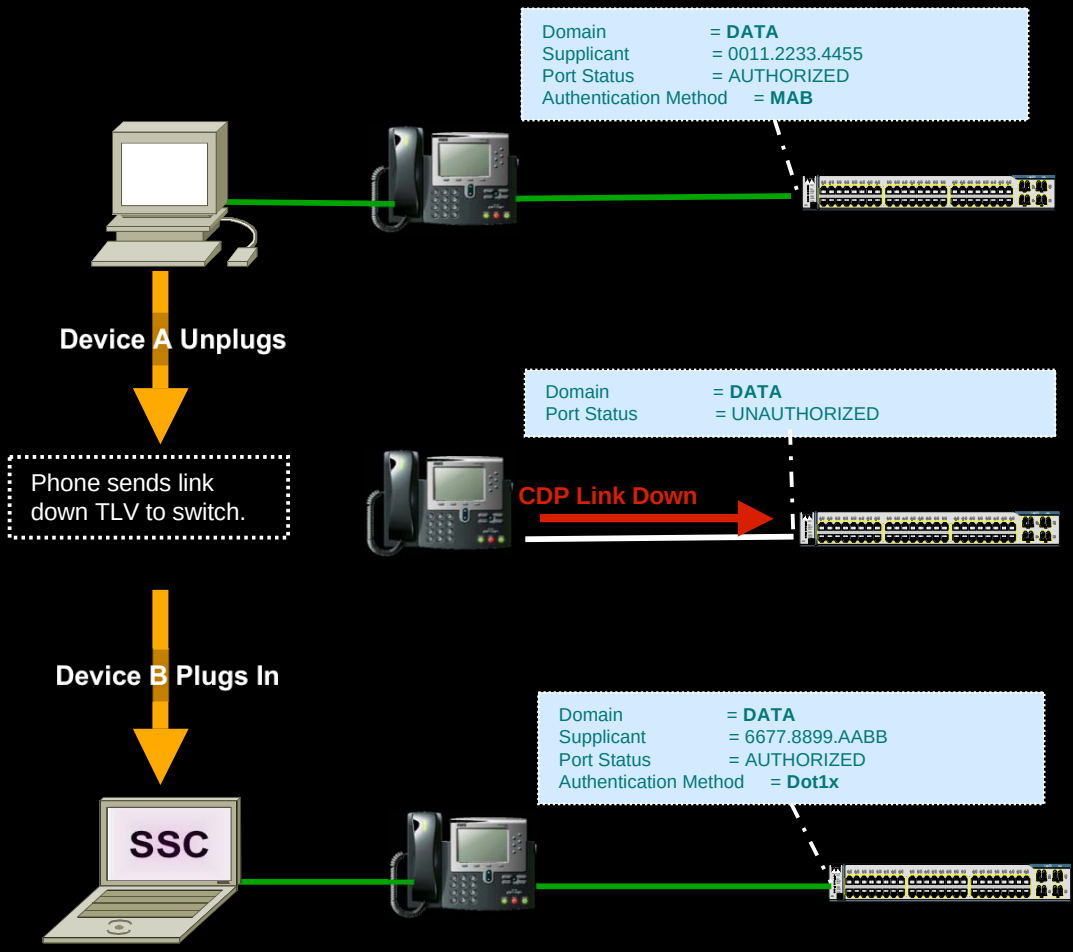
"Restrict" Blocks B, Preserves Authenticated Phone

```
dot1x violation-mode restrict
```

Drop MAC B
No Err-Disable

```
3K:12.2(44)SE
4K: 12.2(50)SG
6K: 12.2(33)SXI
```

NEW! Solution: CDP 2nd Port Notification

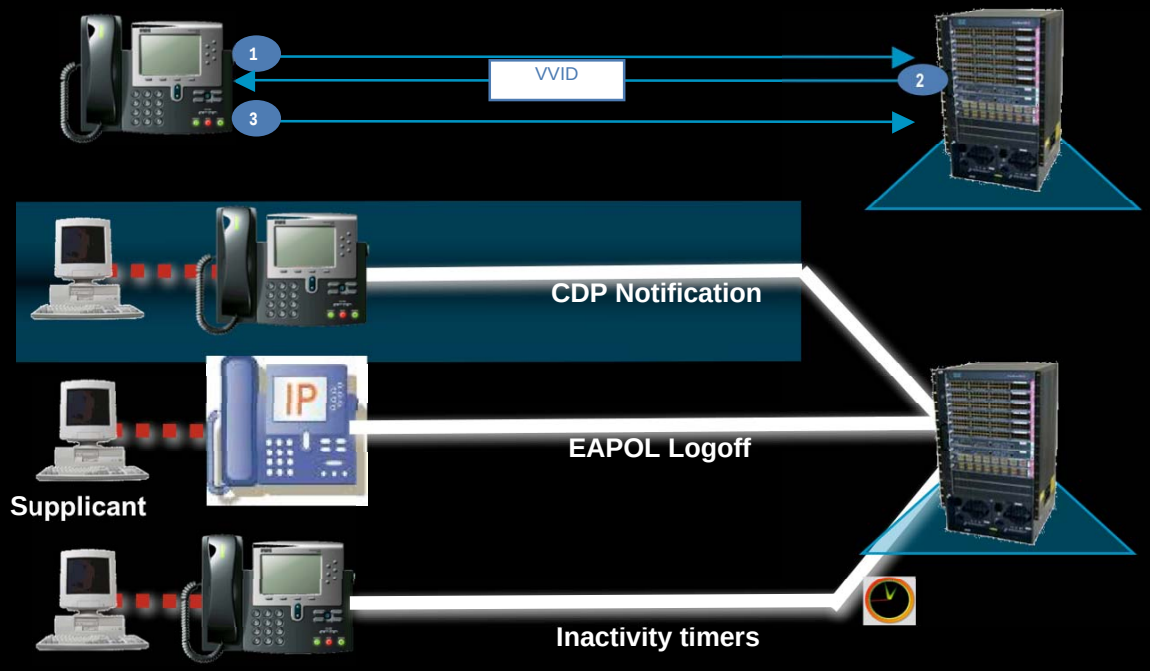


- ✓ Link status msg addresses root cause
- ✓ Session cleared immediately.
- ✓ Works for MAB *and* 802.1X
- ✓ Nothing to configure
- ✓ Cisco on Cisco Value

New

```
IP Phone: 8.4(2)
3K: 12.2(50)SE
4K: 12.2(50)SG
6K: 12.2(33)SXI
```

IP Telephony Integration -- Summary



- Use Case: PC disconnect behind an IP Phone

- Allows Cisco/non-Cisco IP phones without supplicants to be identified and authenticated
- First-hop switch snoops protocols
- First-hop switch proxies requests to authentication service

Customer benefits

- Allows more devices to participate in the identity network
- Eliminates CAPEX/OPEX of having to upgrade/replace all IP phones