LAN Switches mit eingebauter Sicherheit: Neue Möglichkeiten im Bereich IEEE 802.1X

Stefan Dürnberger <sduernbe@cisco.com>

Ralph Schmieder <rschmied@cisco.com>

Session Objectives

In the upcoming 60 Minutes you will…

- **Understand basic operation of Identity and IEEE 802.1X in a switched campus network,**
- **Know about previous deployment barriers -and-**
- **Learn Cisco's new tools and solutions to overcome those barriers and make IEEE 802.1X deployable in today's enterprise networks.**

Agenda

- **Identity Introduction**
- 802.1X in a nutshell
- New Cisco 802.1X Solutions
- Brief Introduction to ACS 5.0
- Q&A / Discussion

Identity for Today's Access Layer

End Users & End Points

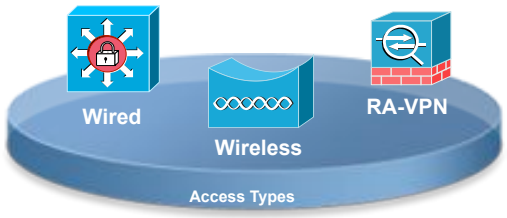
Employees

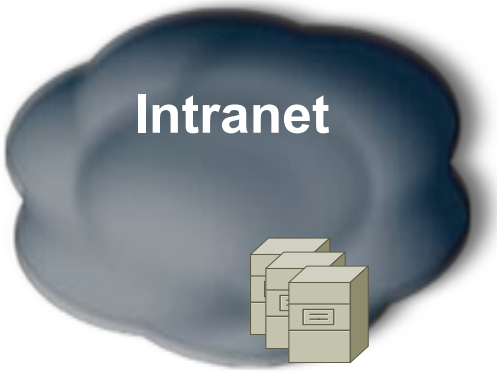
Managed Assets

Guests/Contractors

Outsiders

Network Access Devices





Identity Heuristics

- **Keep the outsiders out**

  Prevent unsecured individual gaining physical and logical access to a network

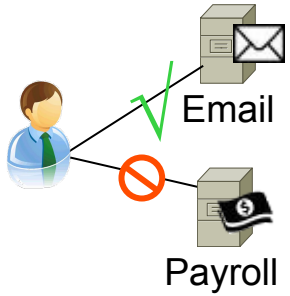
- **Keep the insiders honest**

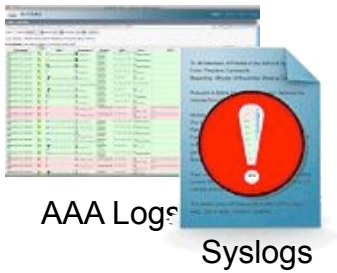
  What can validated users do when they get network access?

- **Increase network visibility**

  Real-time and logged

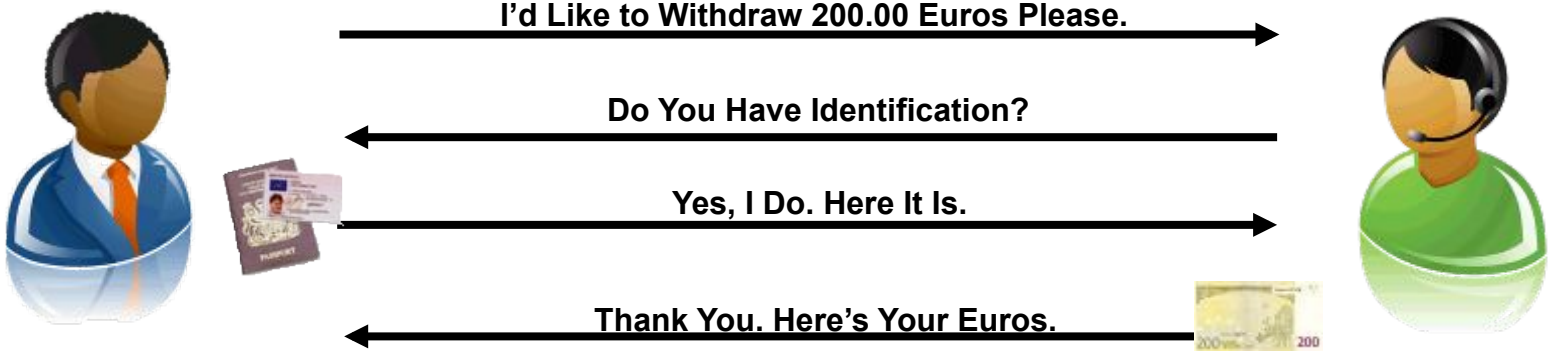
  Enterprises need accountability





What Is Authentication?

- The process of establishing and confirming the identity of a client requesting services
- Authentication is only useful if used to establish corresponding authorization
- Model is very common in everyday scenarios



An Authentication System Is Only as Strong as the Method of Verification Used

Why has Identity been so difficult in the 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 a client
- 20-Years of legacy devices, OSs and applications, all of which were built with the assumption of open connectivity
- Deployment Challenge: Required Prior Knowledge of device capabilities before configuring port
- IEEE 802.1X Breaks all of this!

Gartner Publication

Publication Date: 28 July 2008 ID Number: G00159502

Findings: Wired 802.1X Adoption on the Rise

Lawrence Orans, John Pescatore

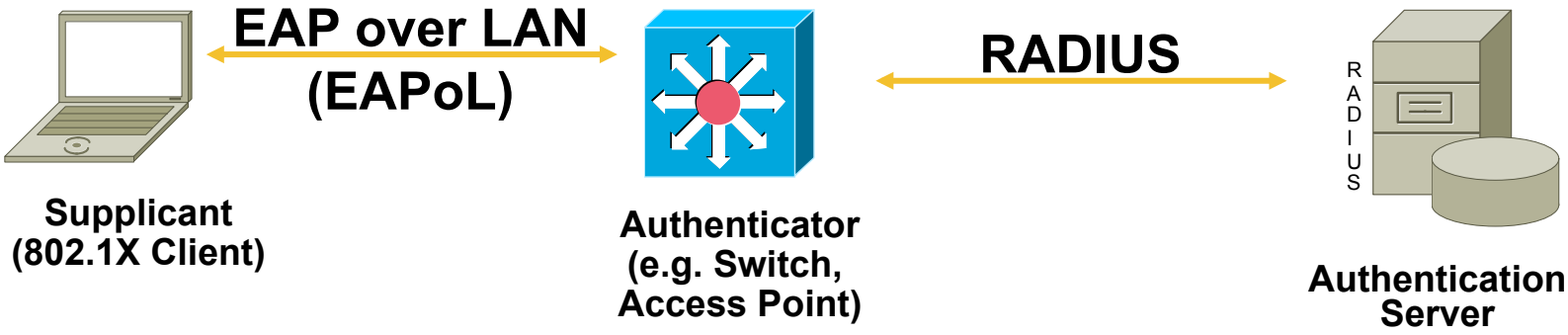
A recent Gartner survey indicates that 50% of enterprises plan to implement 802.1X in their wired networks by 2011. Gartner believes that momentum will increase strongly, and that actual enterprise adoption will reach 70% by 2011.

Adoption of wired 802.1X is growing, but only about 50% of organizations are planning to deploy it by 2011. More organizations likely will add wired 802.1X to their plans once vendors make it easier to deploy and operate, and when success stories become more visible.

Agenda

- Identity Introduction
- **802.1X in a nutshell**
- New Cisco 802.1X Solutions
- Brief Introduction to ACS 5.0
- Q&A / Discussion

IEEE 802.1X: The Foundation of Identity



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

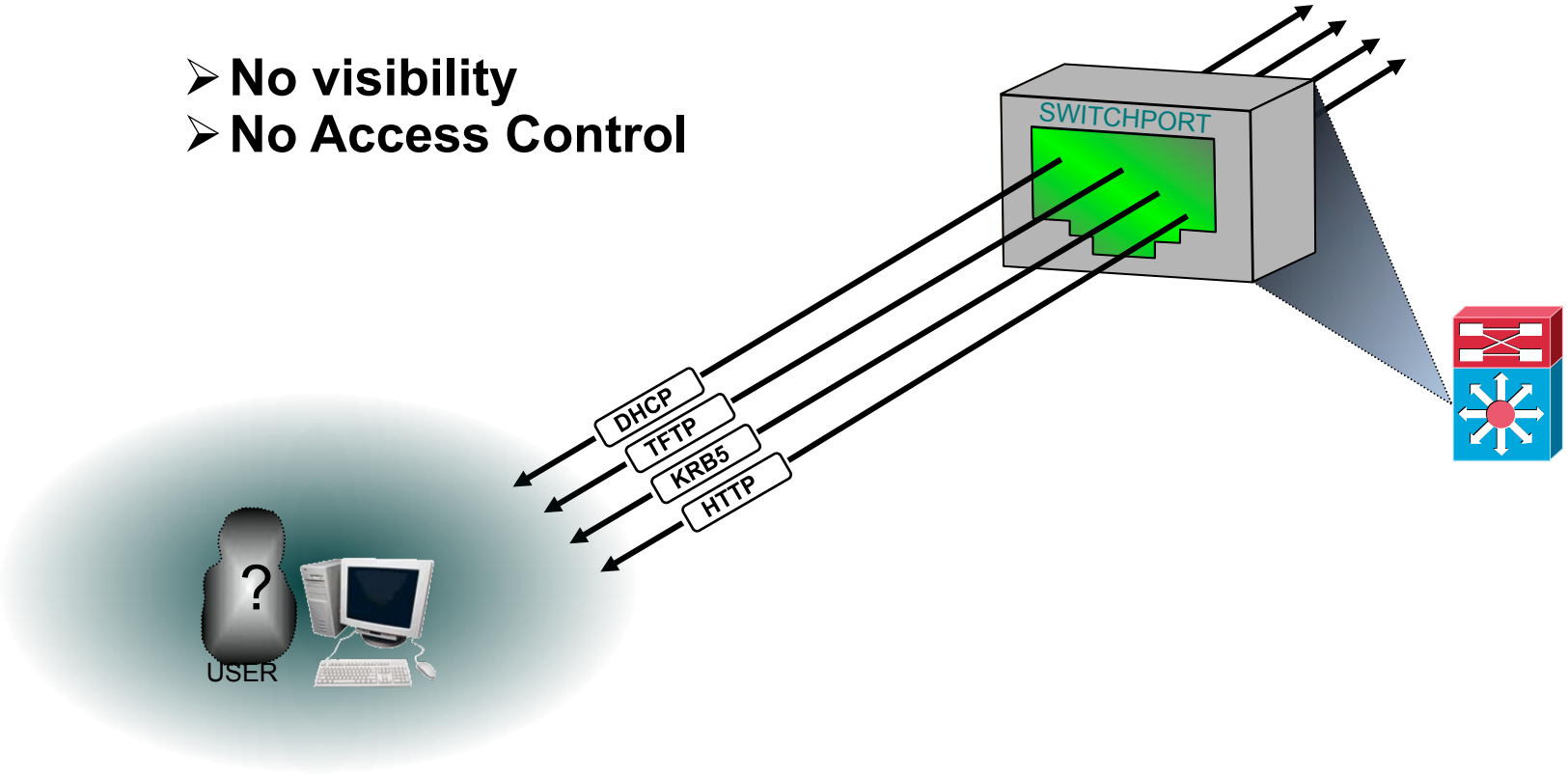
Enforcement via MAC-based filtering and port-state monitoring

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

Default Port State without 802.1X

No Authentication Required

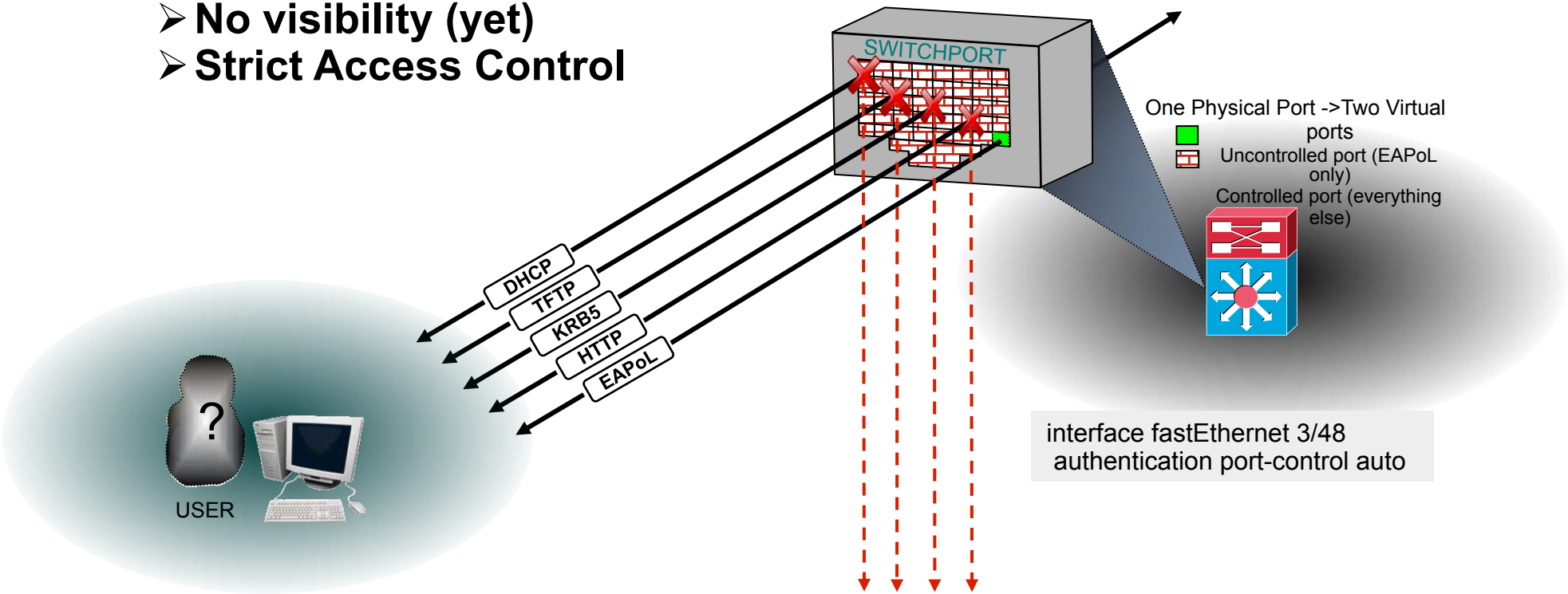
- No visibility
- No Access Control



Default Security with 802.1X

Before Authentication

- No visibility (yet)
- Strict Access Control



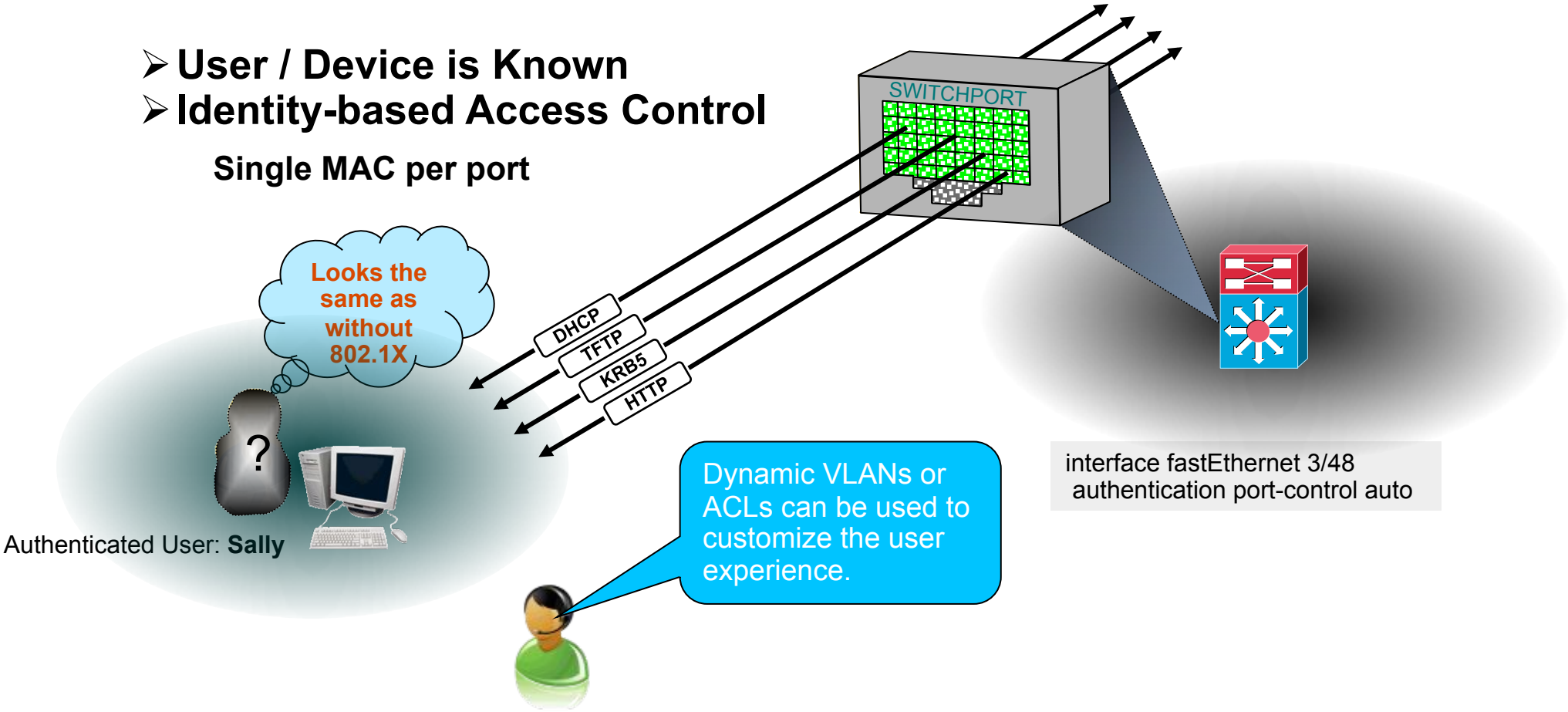
ALL traffic *except* EAPoL is dropped

Default Security with 802.1X

After Authentication

- **User / Device is Known**
- **Identity-based Access Control**

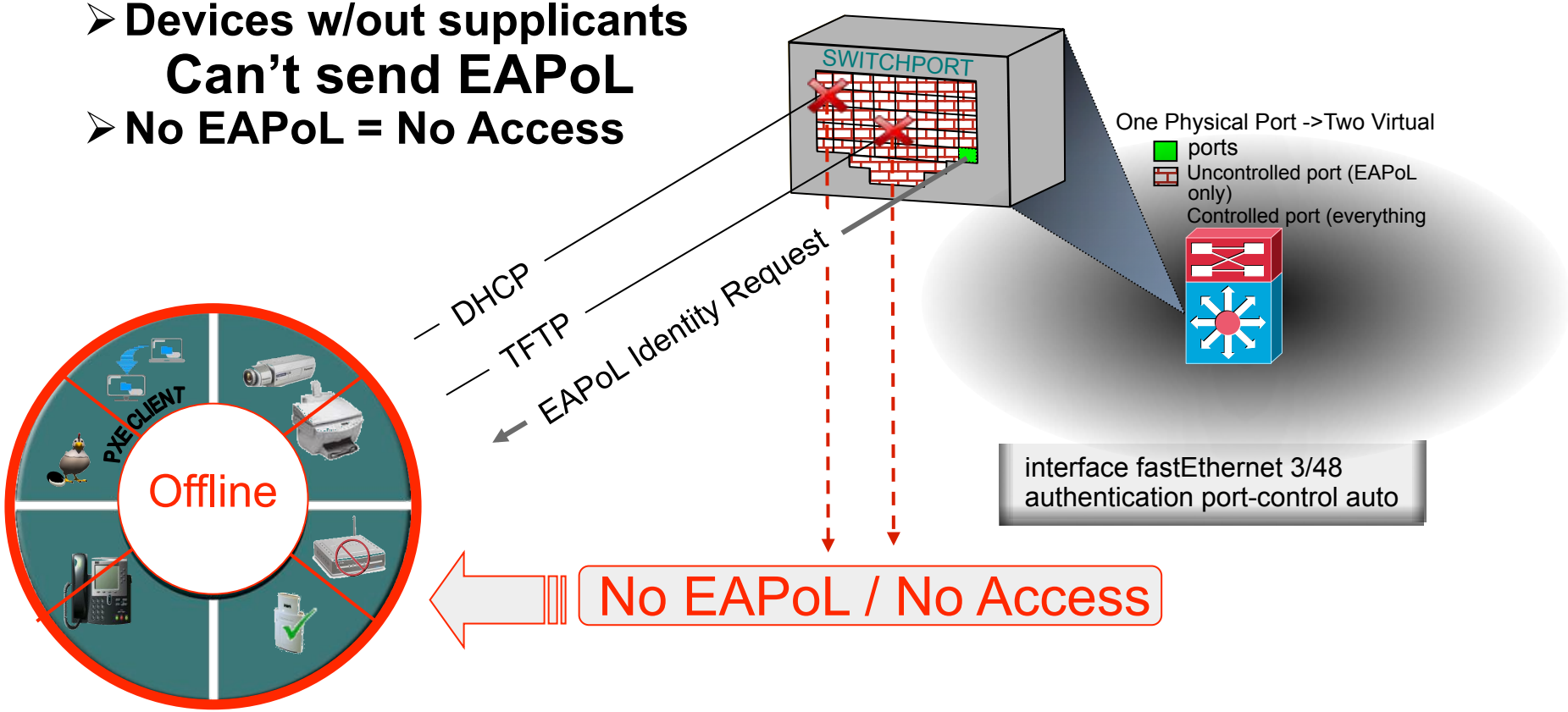
  Single MAC per port



Default Security: Consequences

Default 802.1X Challenge

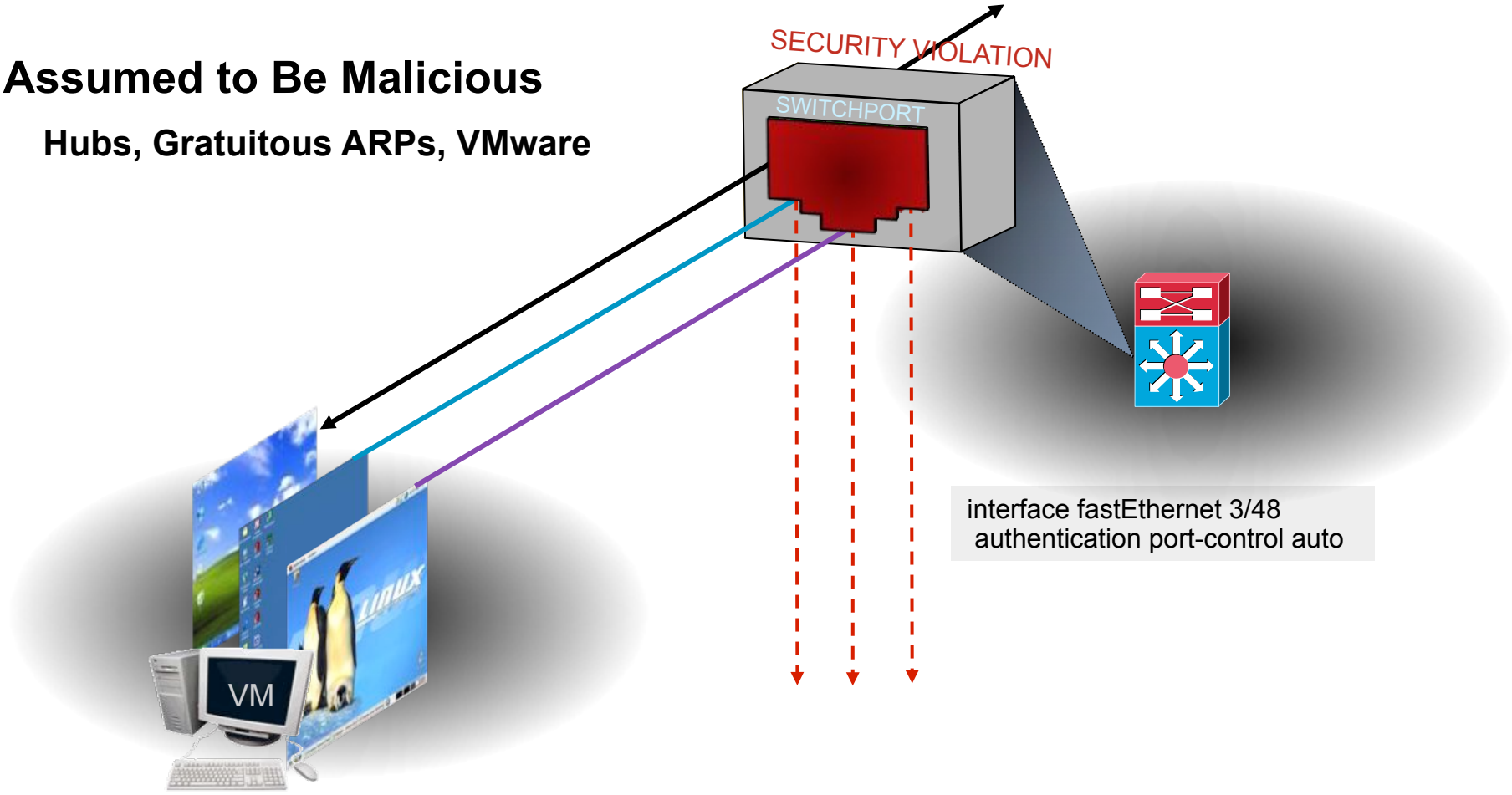
- **Devices w/out supplicants**
  Can't send EAPoL
- **No EAPoL = No Access**



Default Security: More Consequences

Multiple MACs per Port

- **Assumed to Be Malicious**
  - **Hubs, Gratuitous ARPs, VMware**



Agenda

- Identity Introduction
- 802.1X in a nutshell
- **New Cisco 802.1X Solutions**
- Brief Introduction to ACS 5.0
- Q&A / Discussion

Integration Considerations

To be deployable, 802.1X and Identity Networking must accommodate the realities of real world networks.

Real World Networks May Have:

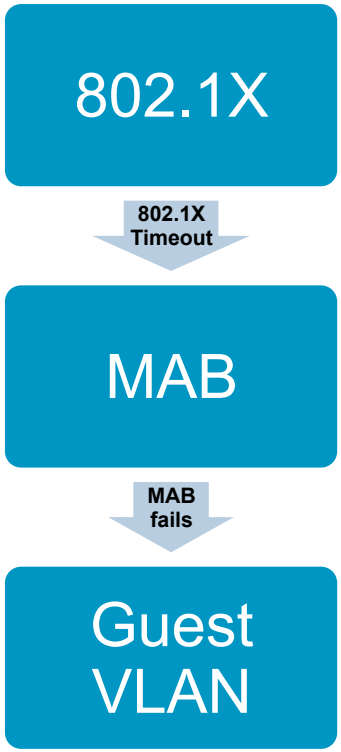
- **Devices that do not speak 802.1X**
- **Supplicants without valid credentials**
- **AAA server outages**
- **Multiple devices per port**

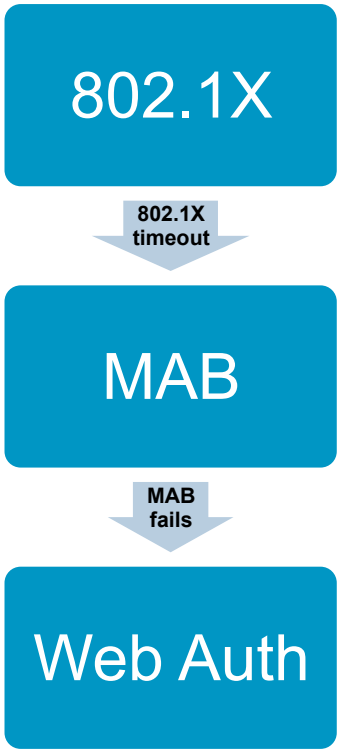
Authentication

Flexible Authentication ("Flex-Auth") refers to a set of features that enable configurable sequencing, priority and fallback behavior of authentication methods:

- **Configurable behavior after 802.1X timeout**
- **Configurable behavior after 802.1X failure**
- **Configurable behavior before & after AAA server dies**
- **Configurable order of authentication methods**
- **Configurable priority of authentication methods**

Default Ordering:
802.1X, MAB, Web Auth, Guest VLAN interactions



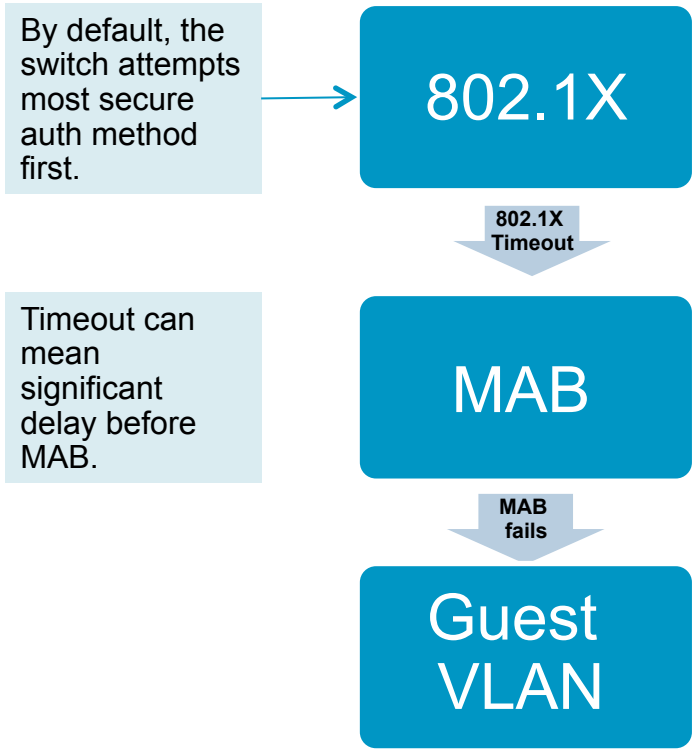



```
interface GigabitE 3/13
 authentication port-control auto
 dot1x pae authenticator
 mab
 authentication event no-response action authorize vlan 40
```

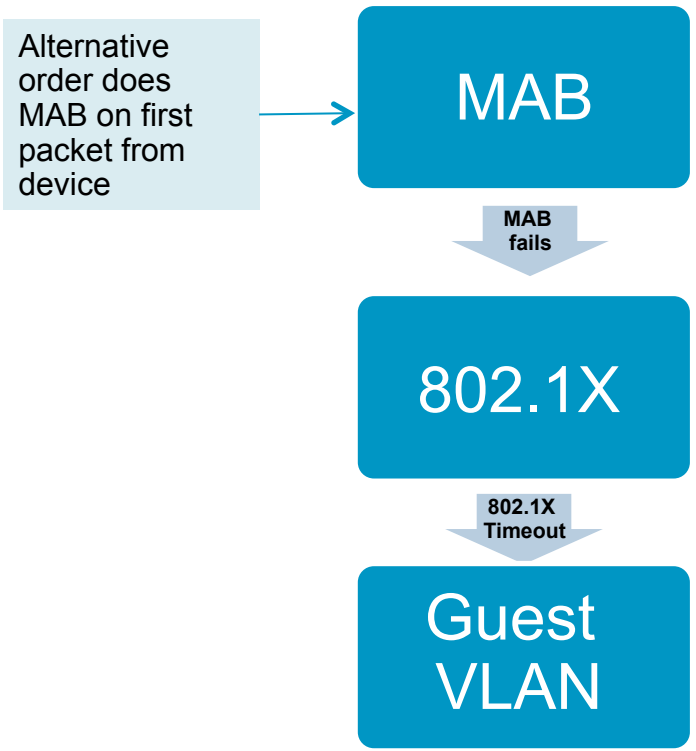
```
interface GigabitE 3/13
 authentication port-control auto
 dot1x pae authenticator
 mab
 authentication fallback WEB-AUTH
```

Alternate Approach

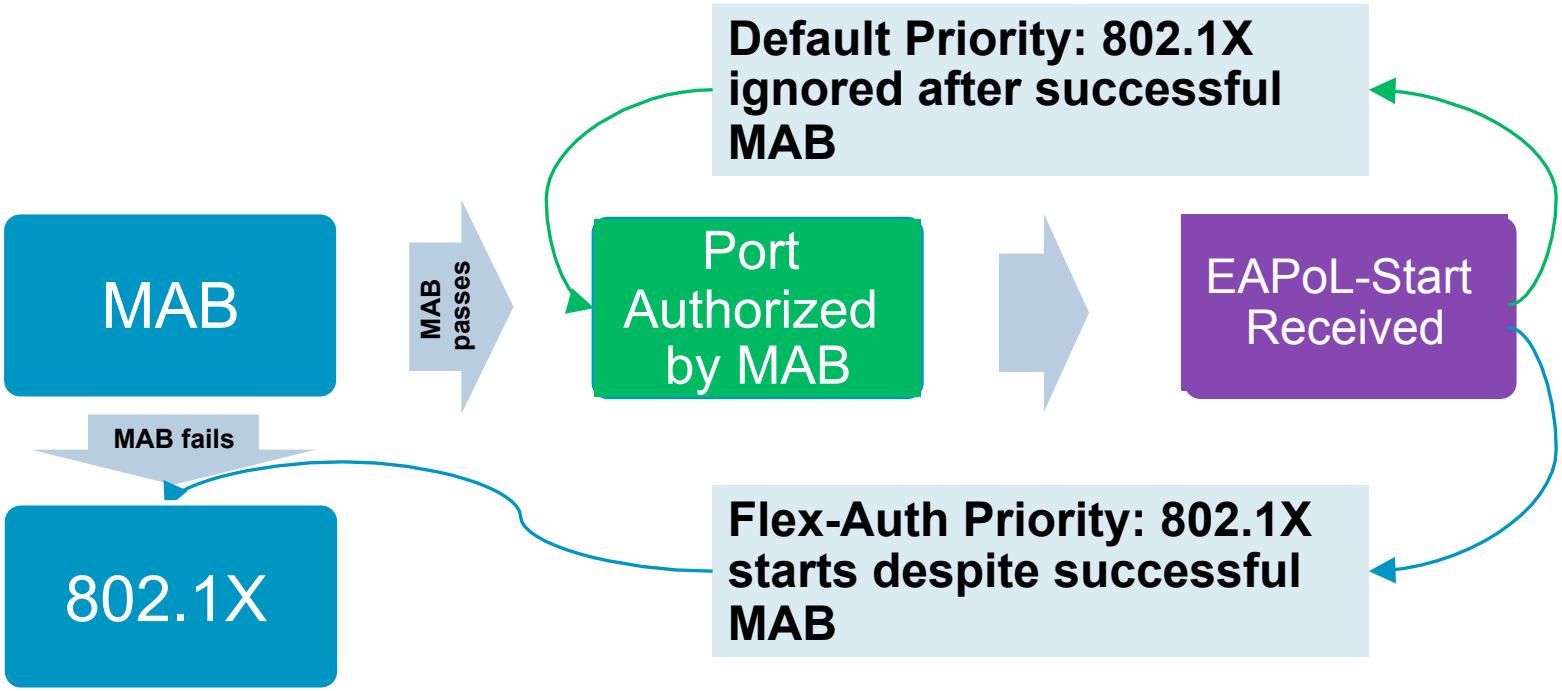
Default Order: 802.1X First



Flex-Auth Order: MAB First



Flex-Auth Order with Flex-Auth Priority

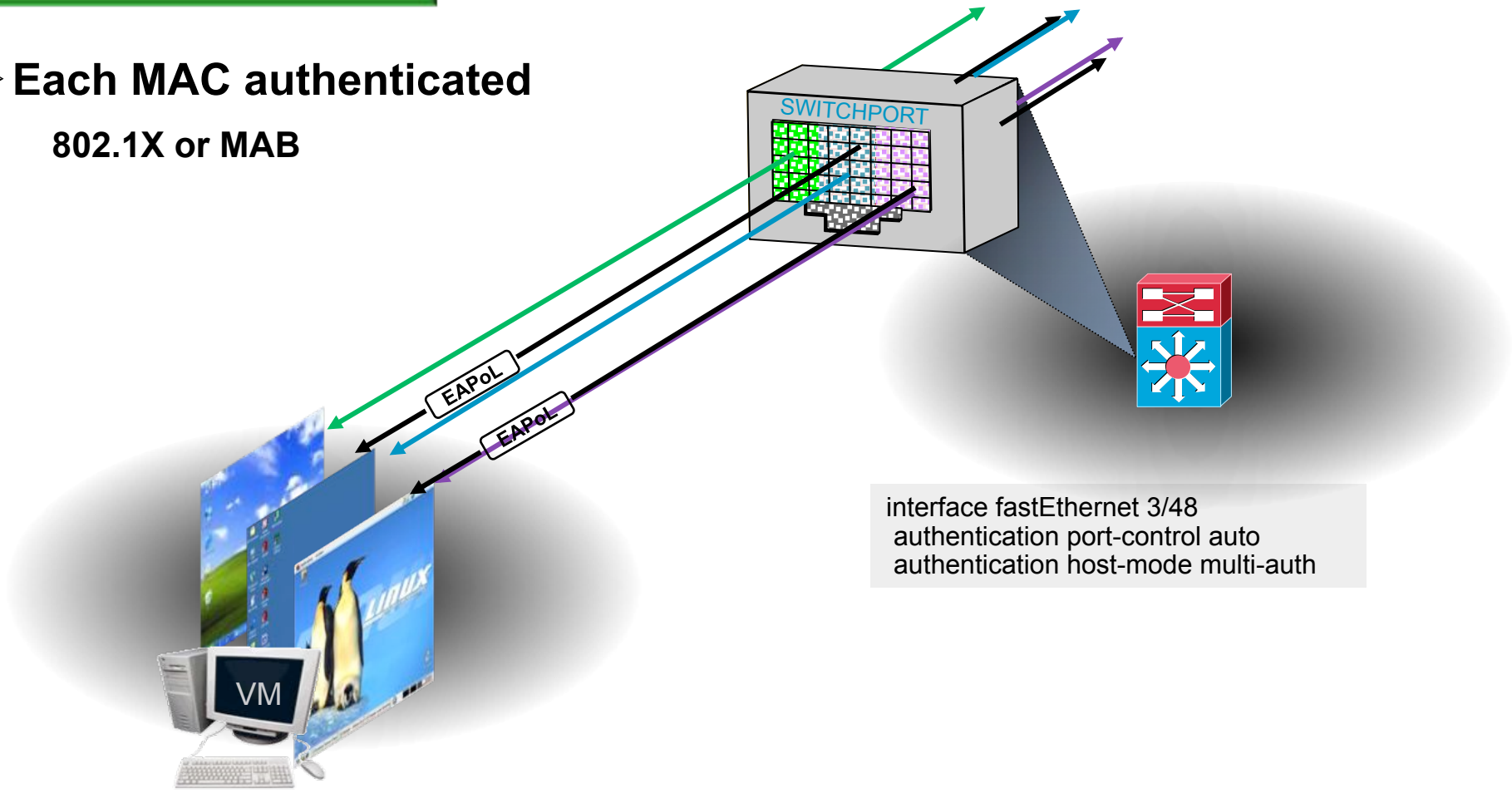


- Priority determines which method can preempt other methods.
- By default, method sequence determines priority (first method has highest priority).
- If MAB has priority, EAPoL-Starts will be ignored if MAB passes.

Modifying Default Security with 802.1X

Multiple MACs on Port

- **Each MAC authenticated**
  - **802.1X or MAB**




```
interface fastEthernet 3/48
 authentication port-control auto
 authentication host-mode multi-auth
```

Multiple Hosts per Port

Host Mode	Enforcement
Single	Single MAC address per port
Multi-Domain Auth (MDA)	One Voice Device + One Data Device per port
Multi-Auth	Superset of MDA with multiple Data Devices per port
Multi-Host	One authenticated device allows any number of subsequent MAC addresses.

Authorization

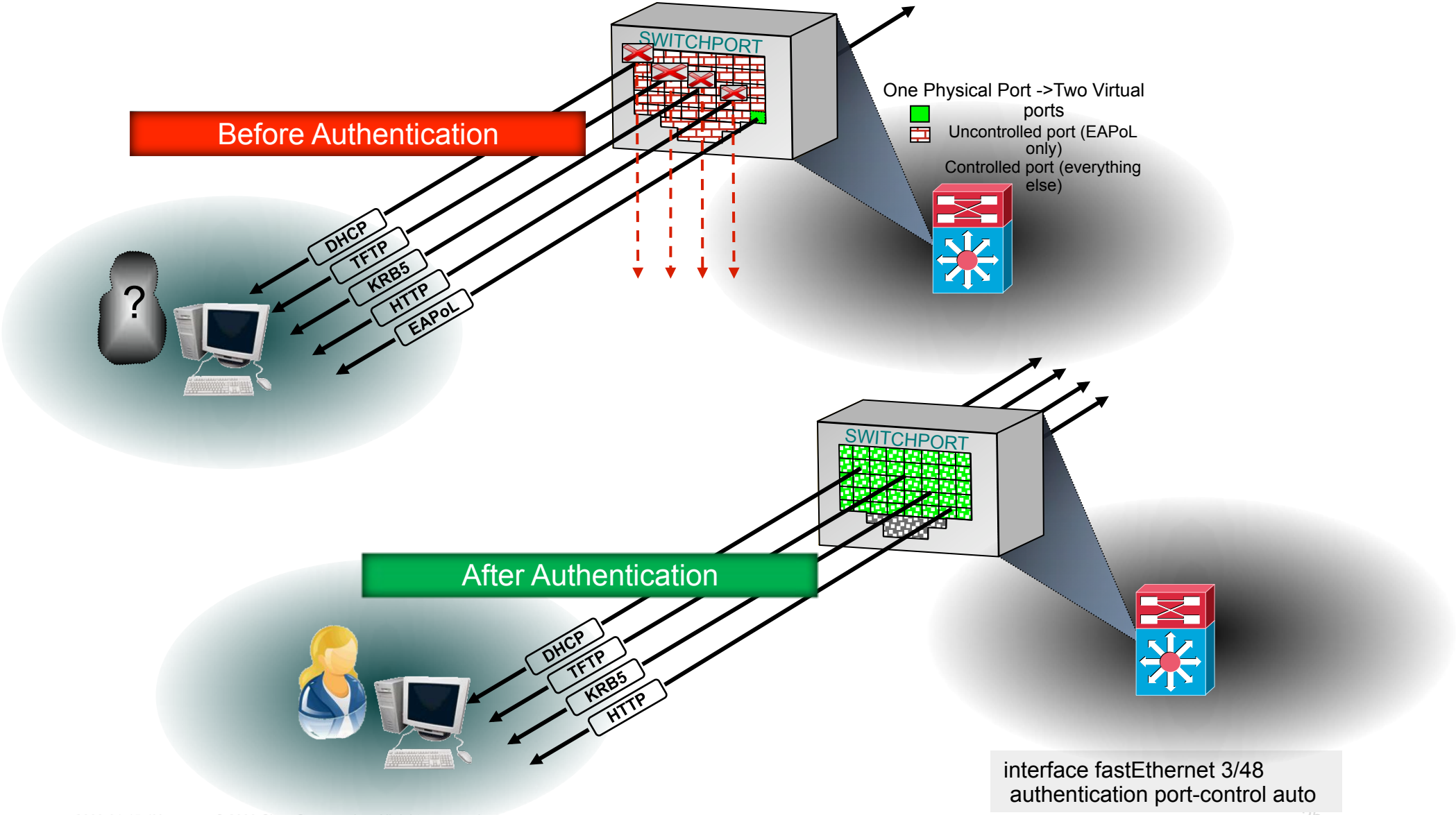
- Authorization is the embodiment of the ability to enforce policies on identities
- Typically policies are applied using a group methodology – allows for easier manageability
- The goal is to take the notion of group management and policies into the network
- Types of Authorization:

  Default: Closed until authenticated.

  Dynamic: VLAN assignment, ACL assignment

  Local: Guest VLAN, Auth-fail VLAN, Critical Auth VLAN

Default Authorization – “Closed Mode”

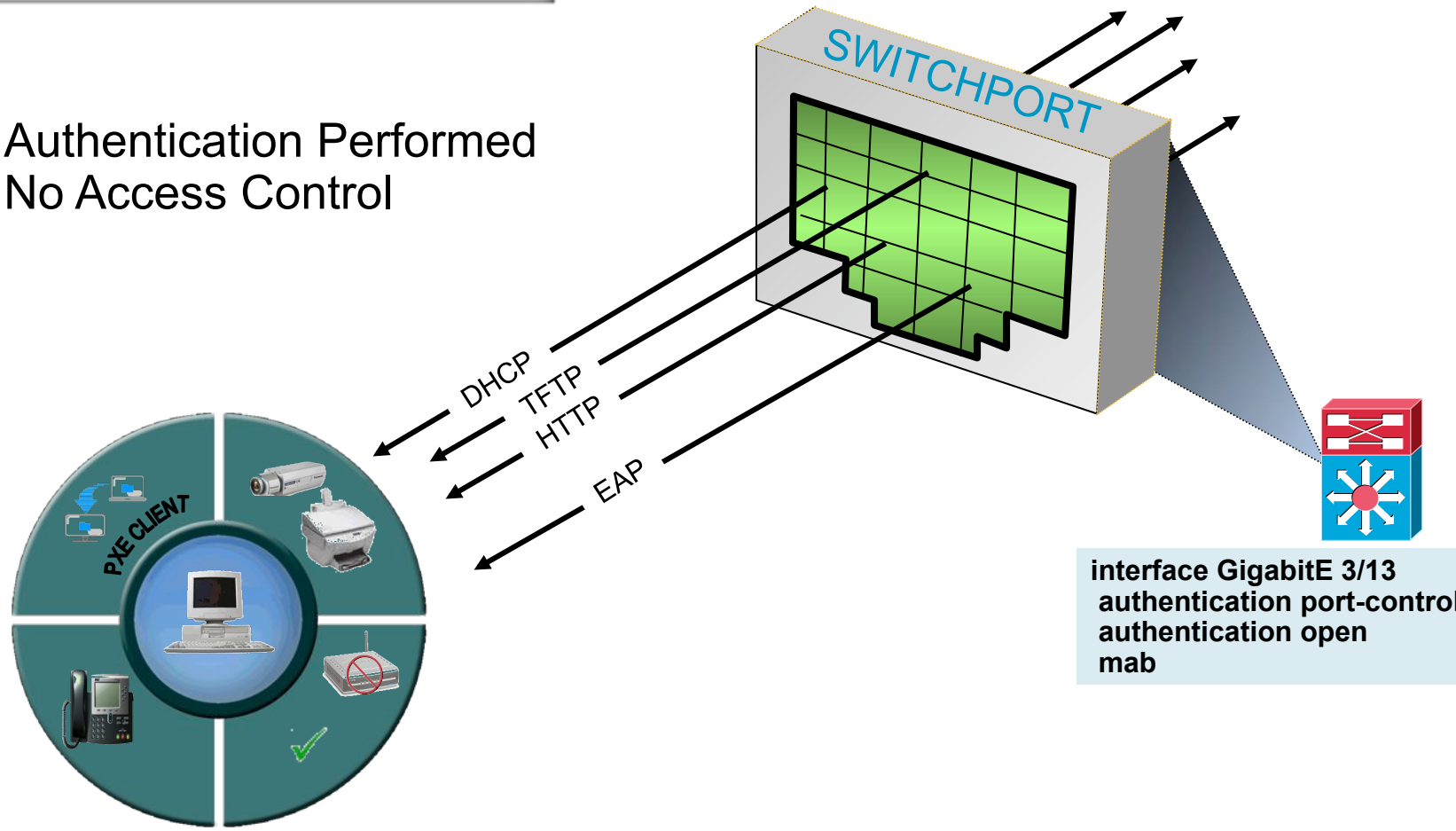



```
interface fastEthernet 3/48
 authentication port-control auto
```

Changing the Default Authorization: "Open Access"

Open Access (No Restrictions)

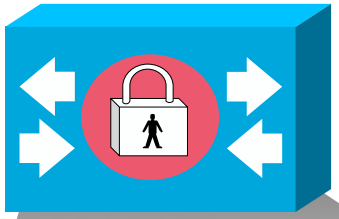
- Authentication Performed
- No Access Control




```
interface GigabitE 3/13
 authentication port-control auto
 authentication open
 mab
```

Open Access Application 1:
Monitor Mode

Monitor the network, see who's on, address future connectivity problems by installing supplicants and credentials, creating MAB database



TO DO Before implementing access control:
- Confirm that all these should be on network
- Install supplicants on X, Y, Z clients
- Upgrade credentials on failed 802.1X clients
- Update MAC database with failed MABs
- …

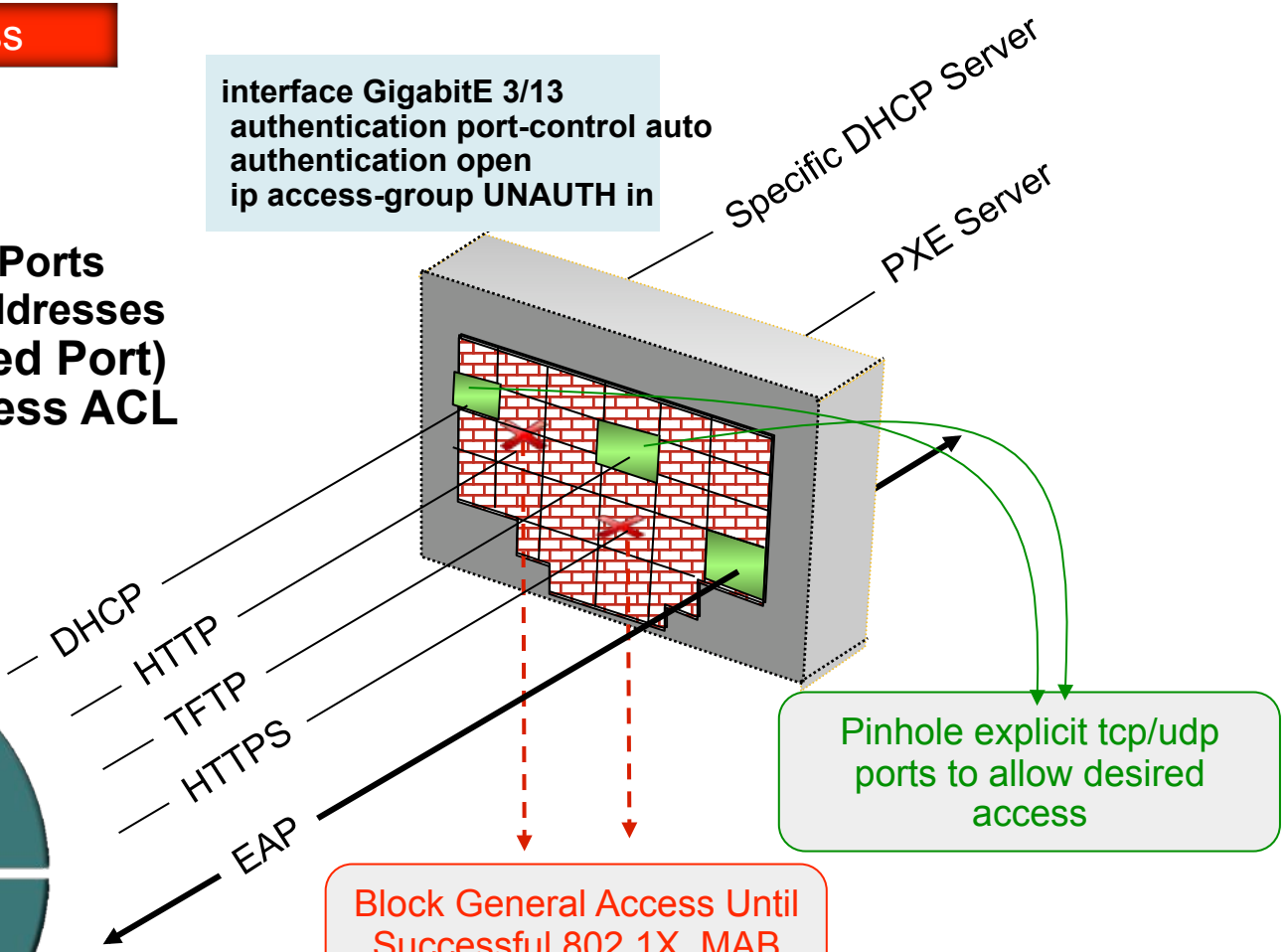
RADIUS accounting logs provide visibility:
- Passed/Failed 802.1X/EAP attempts
  - List of valid dot1x capable
  - List of non-dotx capable
- Passed/Failed MAB attempts
  - List of Valid MACs
  - List of Invalid or unknown MACs

Open Access Application 2:
Selectively Open Mode

Selectively Open Access

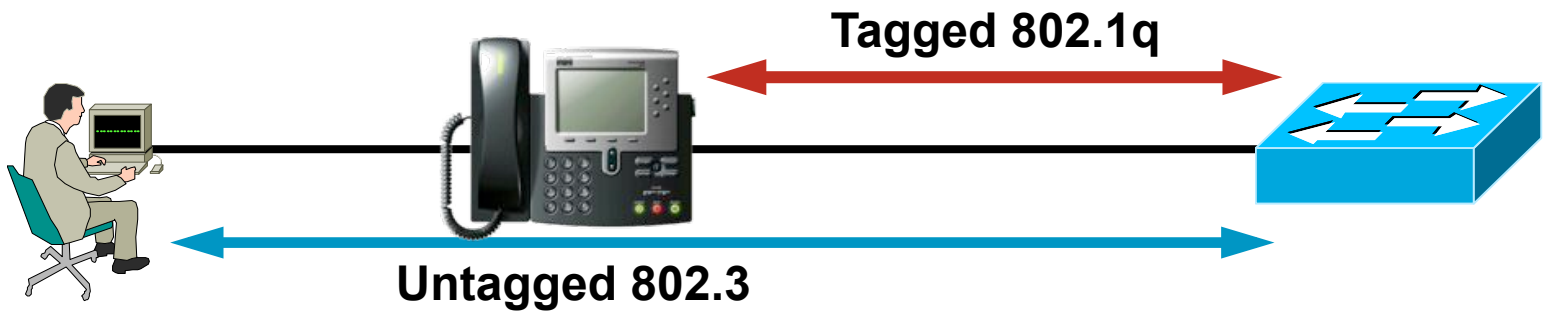
- Open Mode (Pinhole)
  - On Specific TCP/UDP Ports
  - Restrict to Specific Addresses
- EAP Allowed (Controlled Port)
- Download general-access ACL upon authentication

```
interface GigabitE 3/13
 authentication port-control auto
 authentication open
 ip access-group UNAUTH in
```

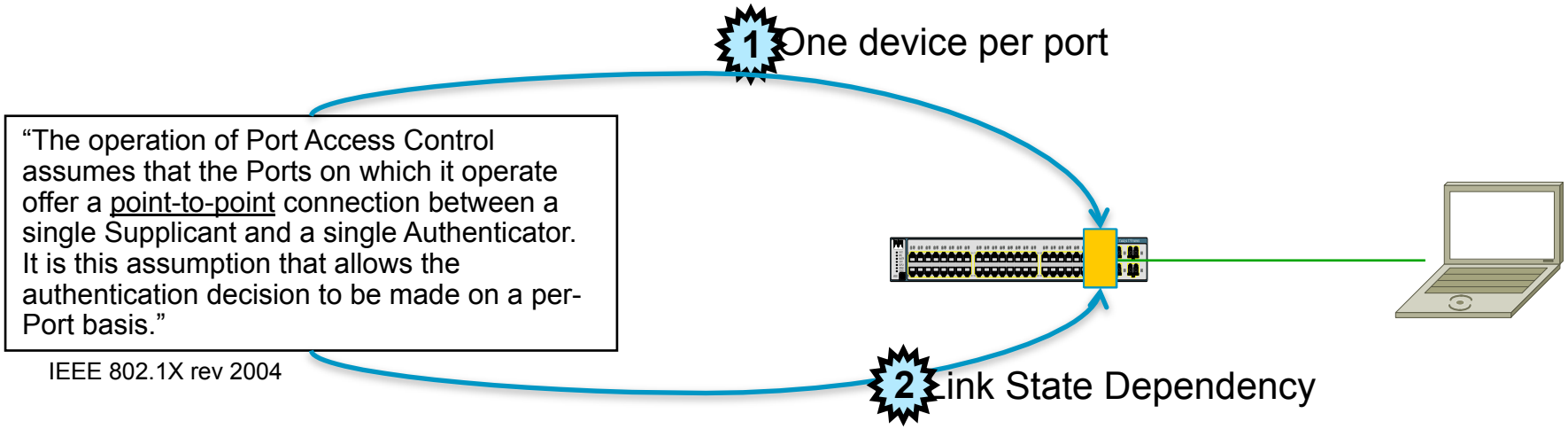


802.1X & IPT: A Special Case

- Voice Ports
- With Voice Ports, a port can belong to two VLANs, while still allowing the separation of voice / data traffic while enabling you to configure 802.1X
- An access port must be able to handle two VLANs:
  - 1) Native or Port VLAN Identifier (PVID) / Authenticated by 802.1X
  - 2) Auxiliary or Voice VLAN Identifier (VVID) / "Authenticated" by CDP
- Hardware set to dot1q trunk



IPT & 802.1X: Fundamental Challenges

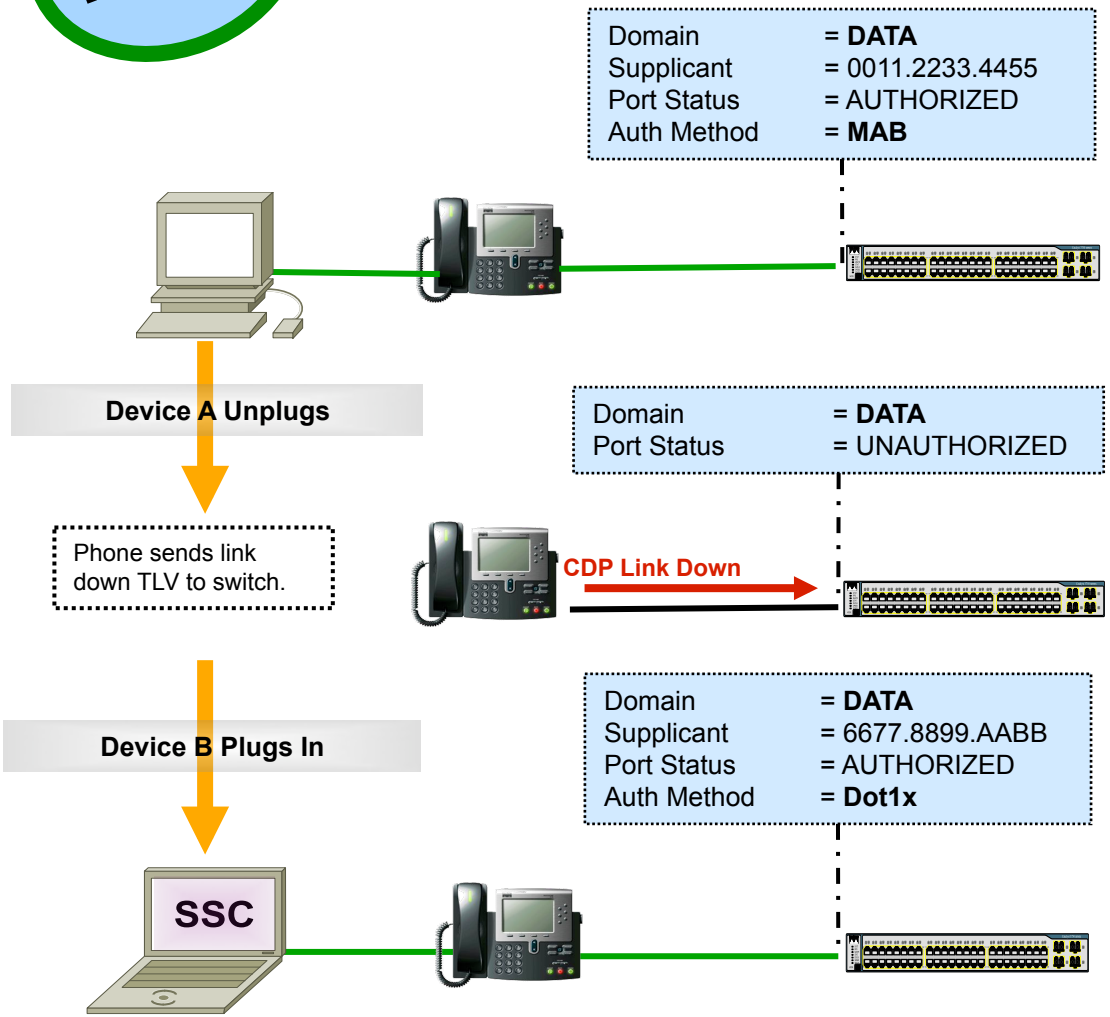


IPT Breaks the Point-to-Point Model

30

Solution: CDP 2nd Port Notification

NEW!



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

IP Phone: 8.4(2)
3K: 12.2(50)SE (Q1CY09)
4K: 12.2(50)SG (FCS)
6K: 12.2(33)SXI (FCS)

31

Multi-Domain Authentication (MDA)

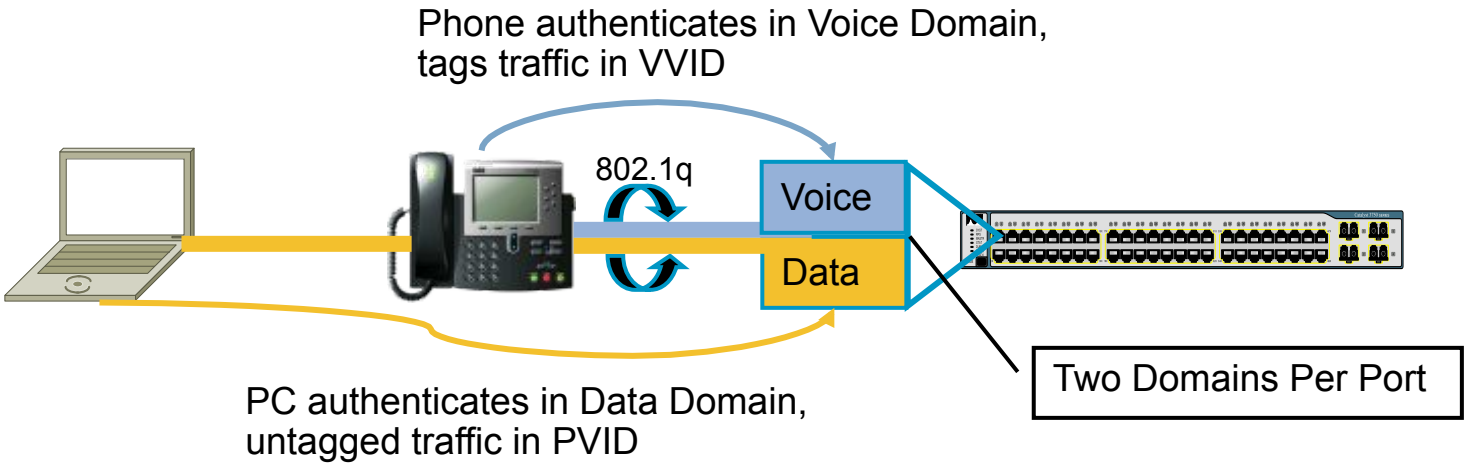
Solving the two-devices-per-port problem

IEEE 802.1X

Single device per port

MDA

Single device *per domain* per port



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

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

Non-802.1X Devices: Summary

Solution	For Devices or Users?	Differentiated Access?	Authorization Type	Authorization Method	Credentials Required
Guest VLAN	Both	No	Local	Static Guest VLAN only	None
MAB	Both	Yes	Centralized	Dynamic VLAN or Dynamic ACL	None (switch detects MAC)
Web-Auth	Users only	Yes	Centralized	Dynamic ACL only	Username / Password

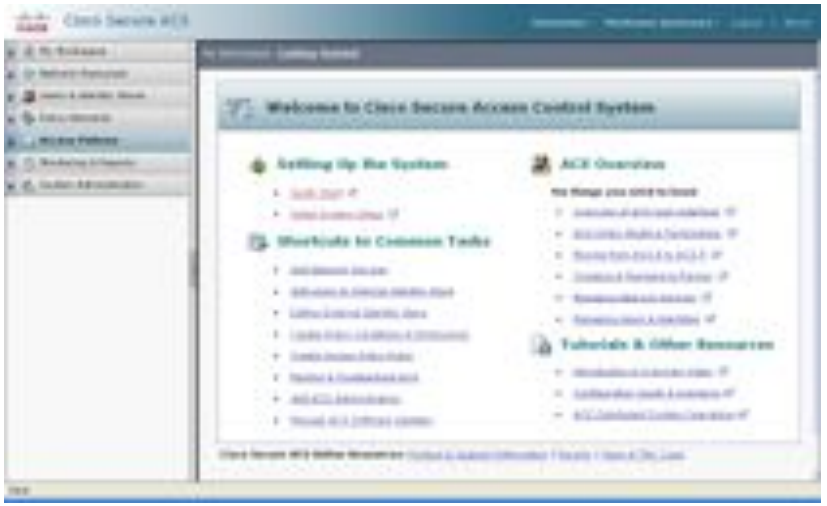
New Feature Availability on Catalyst Switches

	Catalyst 6500 series	Catalyst 4500 series	Catalyst 356x, 37xx, 2960
Open Access	12.2(33)SXI	12.2(50)SG	Q1CY09
Flex-Auth	12.2(33)SXI	12.2(50)SG	Q1CY09
Multi-Auth	12.2(33)SXI	12.2(50)SG	Q1CY09
dACL	12.2(33)SXI	12.2(50)SG	Q1CY09
CDP 2nd port	12.2(33)SXI	12.2(50)SG	Q1CY09

Agenda

- Identity Introduction
- 802.1X in a nutshell
- New Cisco 802.1X Solutions
- **Brief Introduction to ACS 5.0**
- Q&A / Discussion

ACS 5: Next Generation ACS



- ACS 5 is a platform
- Improved admin paradigm
  - Revised policy model & new GUI
  - New interfaces (web services)
  - Centralized management
- More powerful access control policy management
- Integrated monitoring, reporting, & troubleshooting
- Architectural improvements and improved scalability

ACS 5: Rule-Based Policy Model

- Old concept of “group” is split up into multiple pieces

  Identity Group : Classification based on identity and related attributes

  No authorization permissions in Identity Group

  Conditions : Other environment or session (non-identity) attributes defined independently

  Location, access type, time and date, etc.

  Permissions : “Authorization Profiles” contain access authorization information

- A set of authorization rules assign permissions for the session

  IF <condition(s)> THEN <resulting permissions>

Key Takeaways

- IEEE 802.1X is deployable.
- Gartner predicts wide adoption of this technology.
- Cisco has the tools and solutions to make your deployment successful.


Q&A


CISCO