The Promise of 802.1x

Kip Schroeder

kips@cisco.com

New Collaboration Tool for ISSA

- Web & audio conferencing for ISSA Presentations
- Web:

  https://at.meetingplace.net

  Meeting ID: 2659555
- Audio:

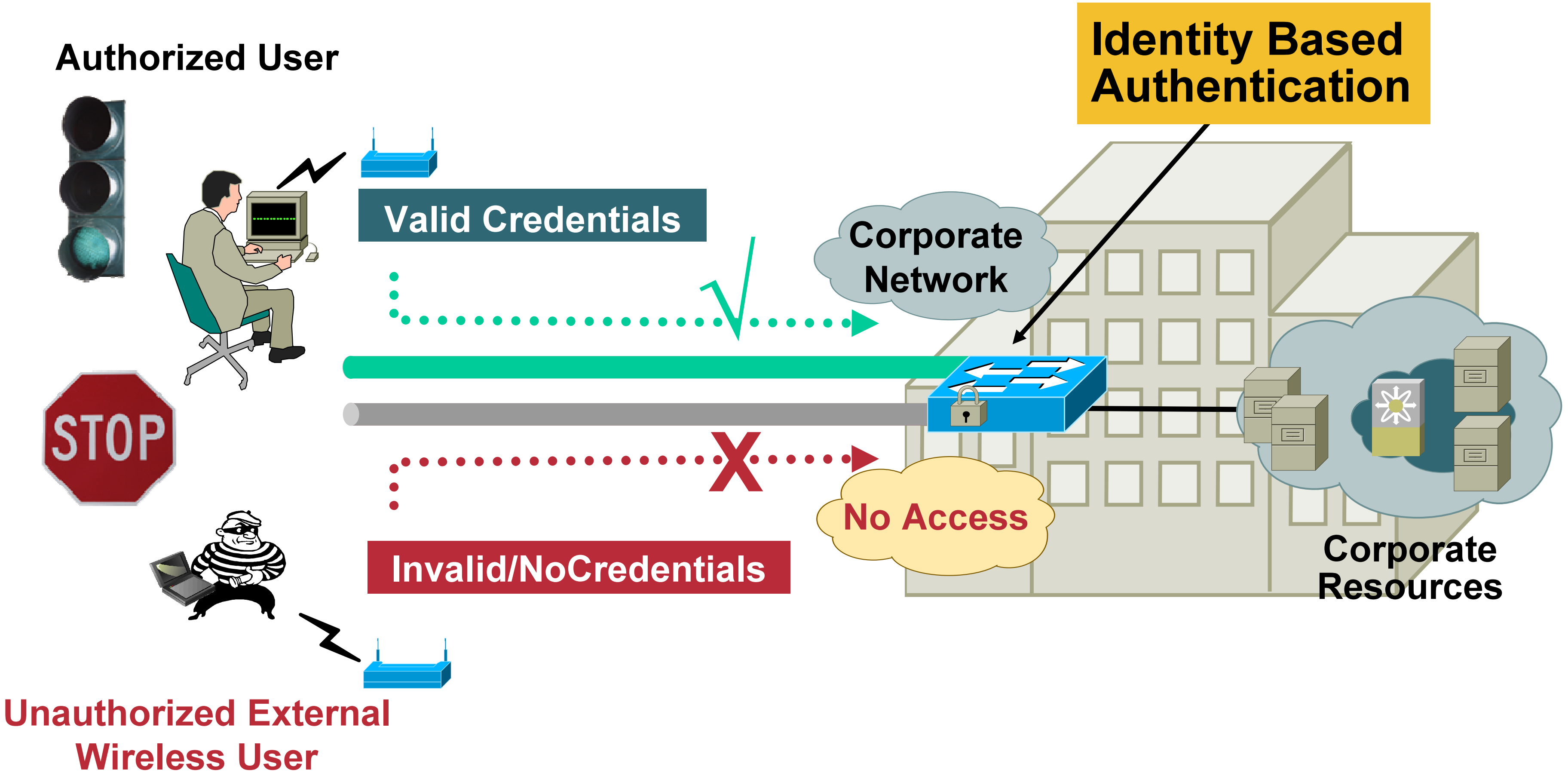
  866-MEETME-9

  Bridge ID: 265-9555
- Recordings Available Immediately After Presos

Agenda

- The Who, What, Where, When & Why of 802.1x
- 802.1x on the LAN
- 802.1x on the Wireless LAN
- Deployment Issues of 802.1x

Concepts of 802.1x in Action



Three Simple Theories of 802.1x

- **Keep the outsiders out**

  Too easy for an unsecured individual to gain physical and logical access to a network

- **Keep the insiders honest**

  A network port is either enabled or disabled; what can users do when they get network access?

- **Increase network visibility (real-time and logged)**

  Dynamic configuration (DHCP) is plug and play; what accountability does an Enterprise have for who you are doing business with?

Basic Identity Concepts

- **What is an identity?**

  An indicator of a client in a trusted domain; typically used as a pointer to a set of rights or permissions; allows us to differentiate between clients

- **What does it look like?**

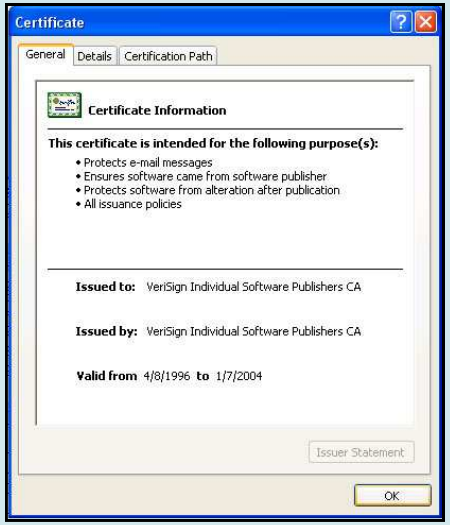
  Can look like anything

  mwilson@acme.com
  Mark Wilson

  00-0c-14-a4-9d-33

- **How do we use identities?**

  Used to provide authorizations—rights to services within a domain; services are arbitrary and can happen at any layer of the OSI model



Certificate Information

This certificate is intended for the following purpose(s):

- Protects e-mail messages
- Ensures software came from software publisher
- Protects software from alteration after publication
- All issuance policies

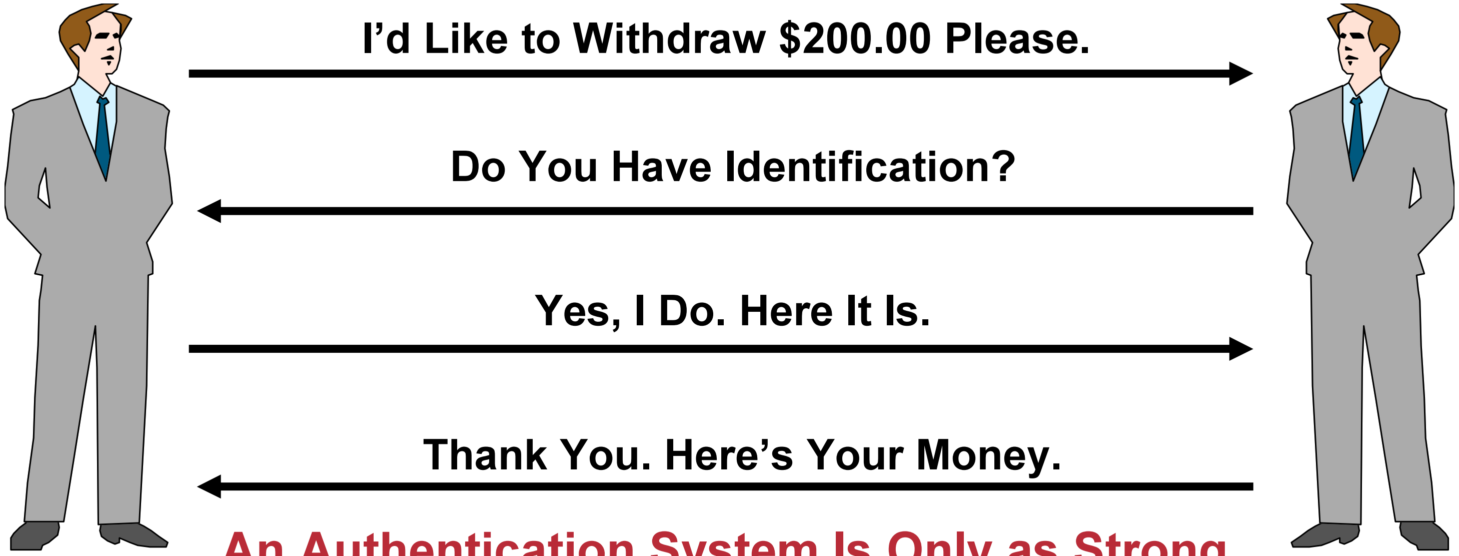
Issued to: VeriSign Individual Software Publishers CA

Issued by: VeriSign Individual Software Publishers CA

Valid from 4/8/1996 to 1/7/2004

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



I'd Like to Withdraw $200.00 Please.

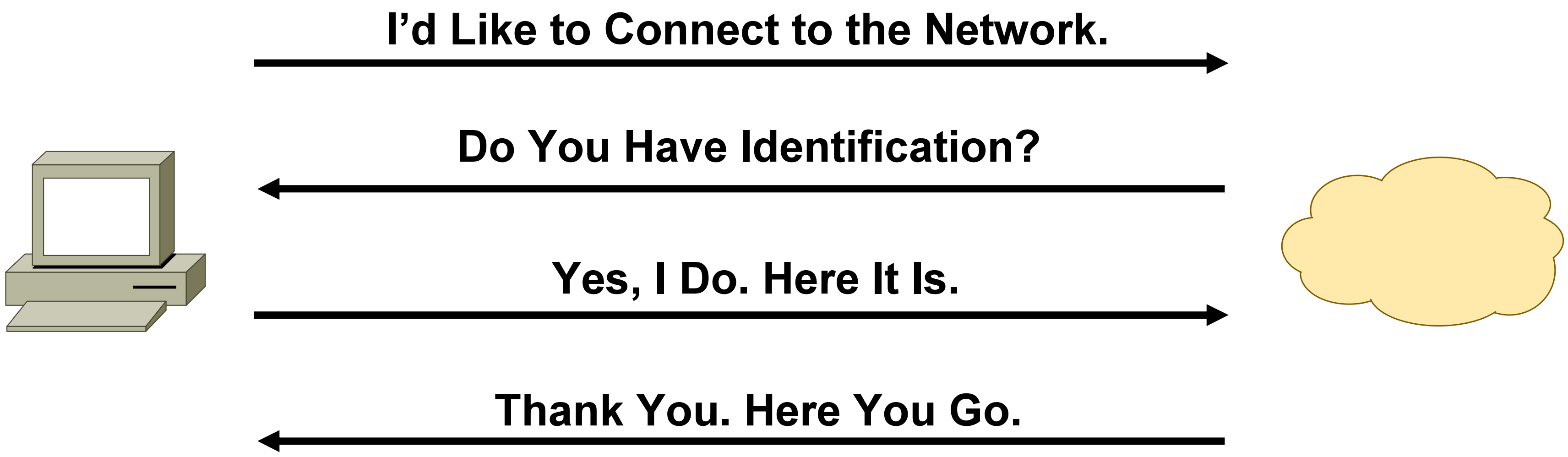
Do You Have Identification?

Yes, I Do. Here It Is.

Thank You. Here's Your Money.

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

Applying the Authentication Model to the Network



I’d Like to Connect to the Network.

Do You Have Identification?

Yes, I Do. Here It Is.

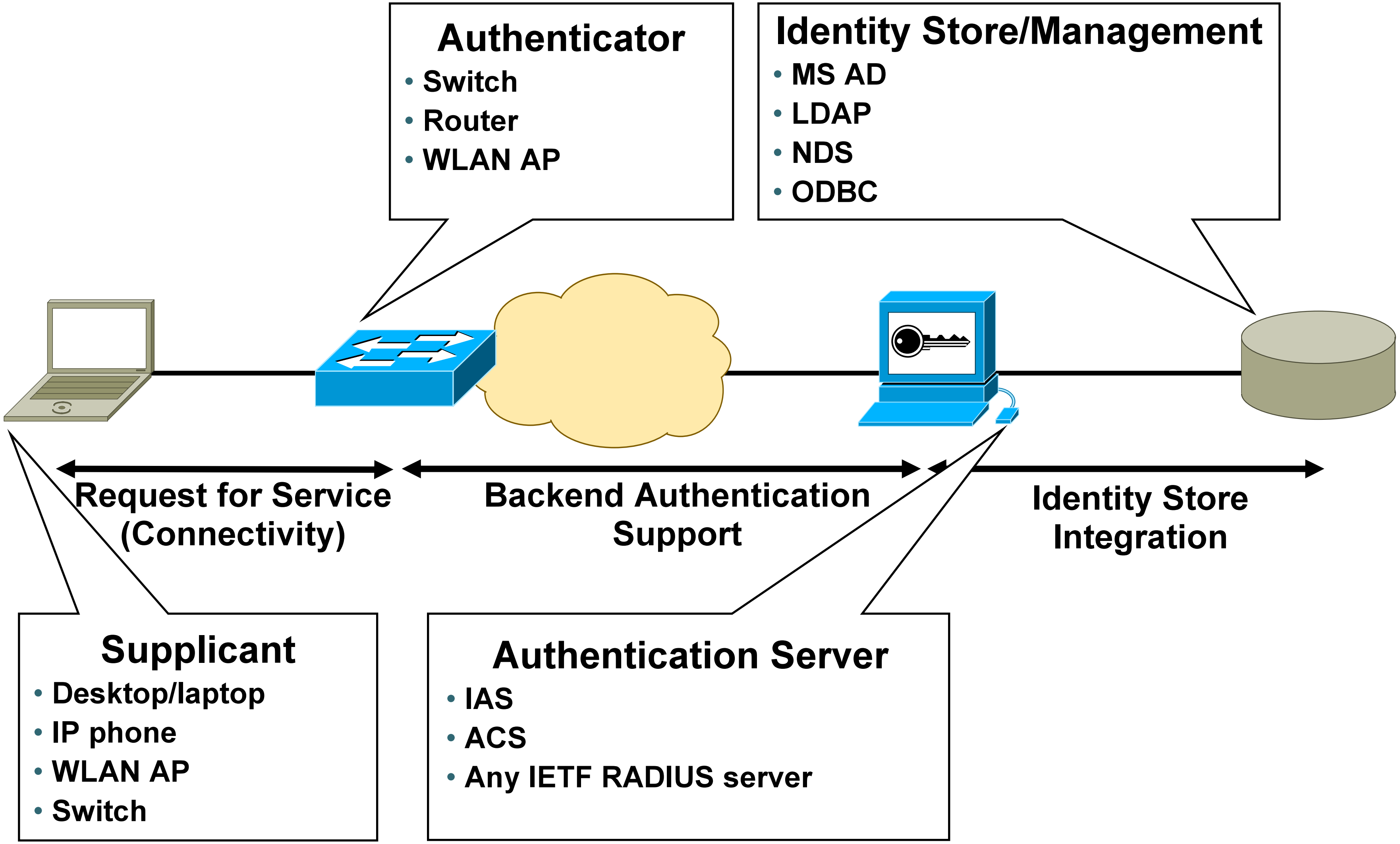
Thank You. Here You Go.

Network Access Protocols and Mechanisms

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
- Primarily 802.1x is 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

802.1x Port Access Control Model



Authenticator
- Switch
- Router
- WLAN AP

Identity Store/Management
- MS AD
- LDAP
- NDS
- ODBC

Request for Service (Connectivity)

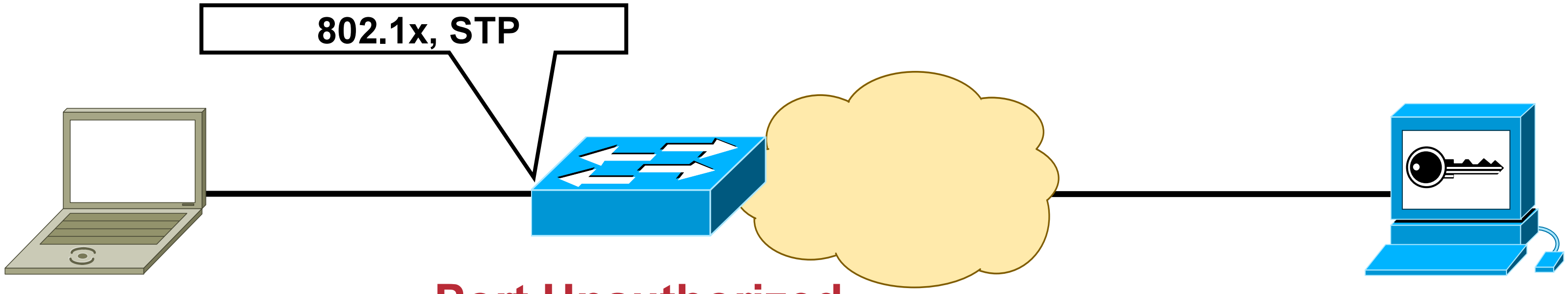
Backend Authentication Support

Identity Store Integration

Supplicant
- Desktop/laptop
- IP phone
- WLAN AP
- Switch

Authentication Server
- IAS
- ACS
- Any IETF RADIUS server

A Closer Look:



Port Unauthorized

EAPOL-Start

EAP-Identity-Request

EAP-Identity-Response

EAP—Method Dependent

EAP-Auth Exchange

Auth Exchange w/AAA Server

EAP-Success/Failure

Authentication Successful/Rejected

Port Authorized

Policy Instructions

Port Unauthorized

EAPOL-Logoff

Actual Authentication Conversation Is Between Client and Auth Server Using EAP; the Switch Is an EAP Conduit, but Aware of What's Going on

802.1x

RADIUS

Extensible Authentication Protocol (EAP)

- A flexible transport protocol used to carry arbitrary authentication information—not the authentication method itself
- EAP provides a flexible link layer security framework
  - Simple encapsulation protocol
    - No dependency on IP
  - Few link layer assumptions
    - Can run over any link layer (PPP, 802, etc.)
    - Assumes no reordering
    - Can run over loss full or lossless media

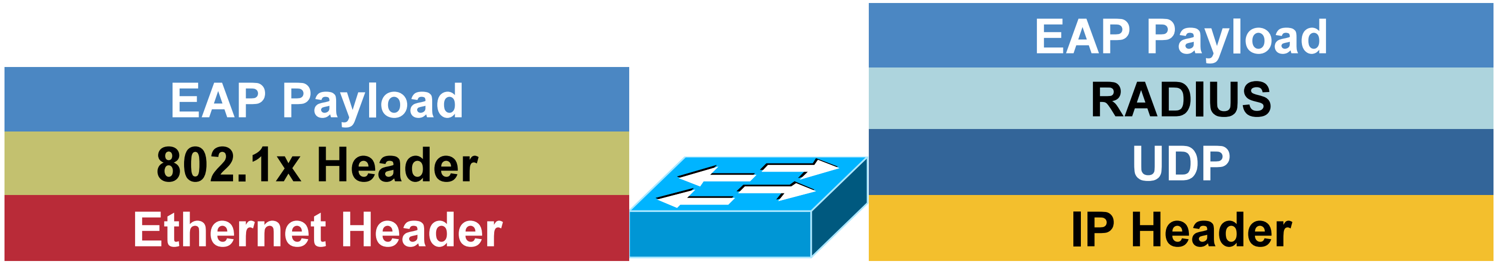
What Does EAP Do?

- Transports authentication information in the form of EAP payloads
- Establishes and manages connection; allows authentication by encapsulating various types of authentication exchanges
- Prevalent EAP types

  EAP-TLS: uses x.509 v3 PKI certificates and the TLS mechanism for authentication

  PEAP: protected EAP tunnel mode EAP encapsulator; tunnels other EAP types in an encrypted tunnel (TLS)

  EAP-FAST: designed to not require certificates; tunnels other EAP types in an encrypted tunnel (TLS)



Factors that Drive EAP Usage

- Enterprise security policy
  - Are there requirements that drive a particular type
  - Requirements, such as, two factor authentication may drive the choice of EAP-TLS
- Supplicant support
  - Windows XP supports EAP-TLS, PEAP w/EAP-MSCHAPv2
  - 3rd party supplicants support a large variety of EAP types, but not all
- RADIUS server support
  - RADIUS servers support a large variety of EAP types, but not all
- Authentication store
  - PEAP w/EAP-MSCHAPv2 can only be used with authentication stores that store passwords in MSCHAPv2 format
  - Not every identity store supports all the EAP types
- New technologies
  - Network Access Control may require EAP-FAST for identity and posture
- Customer choice of EAP type drives every other component

EAP-TLS

- Client support
  - Windows 2000, XP, Vista and Windows CE (natively supported)
  - Non-Windows platforms: third-party supplicants
  - Each client requires a user certificate
- Infrastructure requirements
  - EAP-TLS supported RADIUS servers
    - Cisco ACS, Cisco AR, MS IAS, Funk, Interlink
  - RADIUS server requires a server certificate
  - Certificate authority server (PKI Infrastructure)
- Certificate management
  - Both client and RADIUS server certificates to be managed

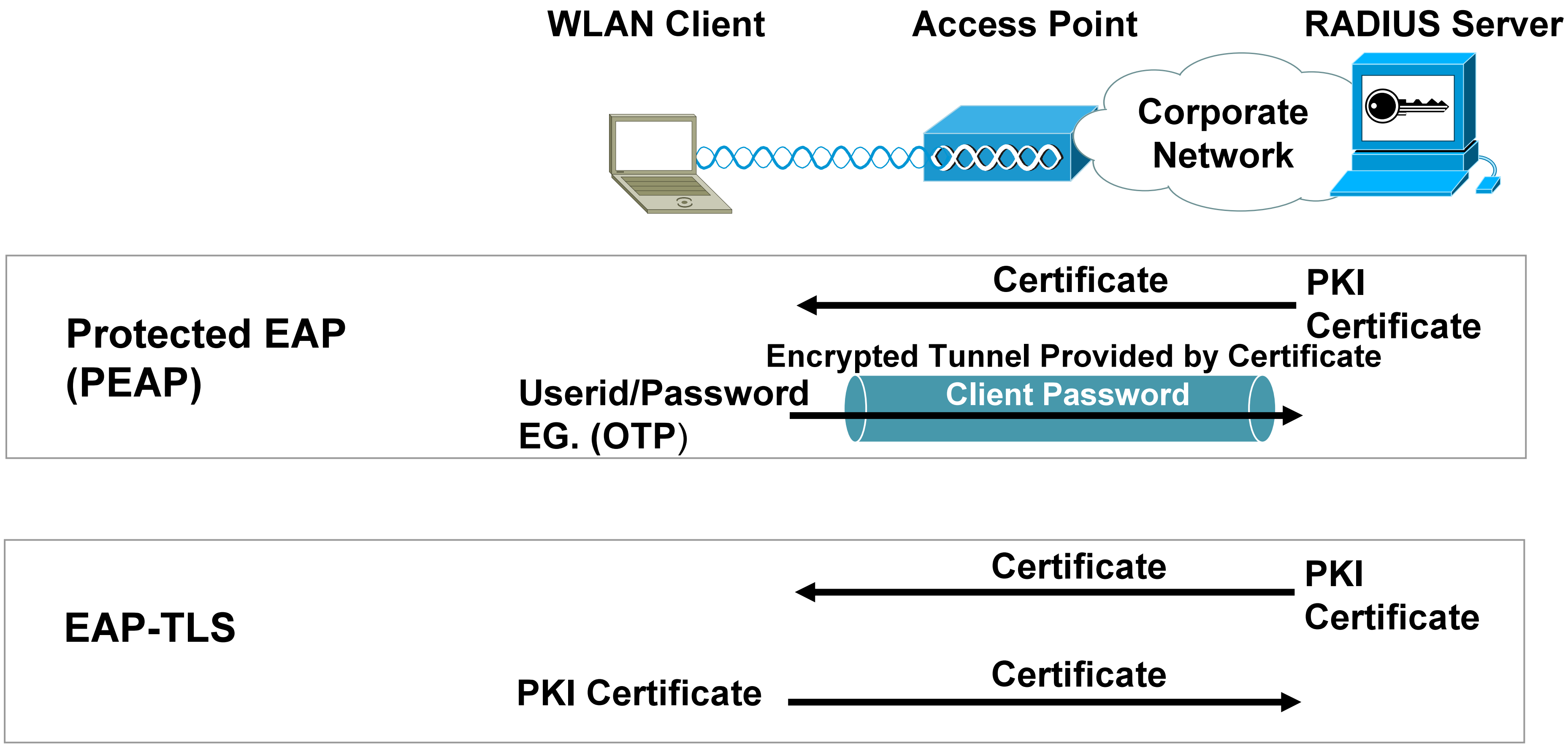
EAP-PEAP

- Hybrid authentication method
  - Server side authentication with TLS
  - Client side authentication with EAP authentication types (EAP-GTC, EAP-MSCHAPv2, etc.)
- Clients do not require certificates
  - Simplifies end user/device management
- RADIUS server requires a server certificate
  - RADIUS server self-issuing certificate capability
  - Purchase a server certificate per server from public PKI entity
  - Setup a simple PKI server to issue server certificates
- Allows for one way authentication types to be used
  - One-time-passwords
  - Proxy to LDAP, Unix, NT/AD, Kerberos, etc.

EAP-FAST Protocol

- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) is a TLS-based RFC3748 compliant EAP method
- The tunnel establishment relies on a Protected Access Credential (PAC) that can be provisioned and managed dynamically by EAP-FAST through AAA server
- PAC is a unique shared credential used to mutually authenticate client and server
- PAC is associated with a specific user-ID and an authority-ID
- PAC removes the need for PKI (digital certificates)

Some EAP Types Compared



WLAN Client

Access Point

RADIUS Server

Corporate Network

Protected EAP (PEAP)

Certificate ←

PKI Certificate

Encrypted Tunnel Provided by Certificate

Userid/Password EG. (OTP)

Client Password →

EAP-TLS

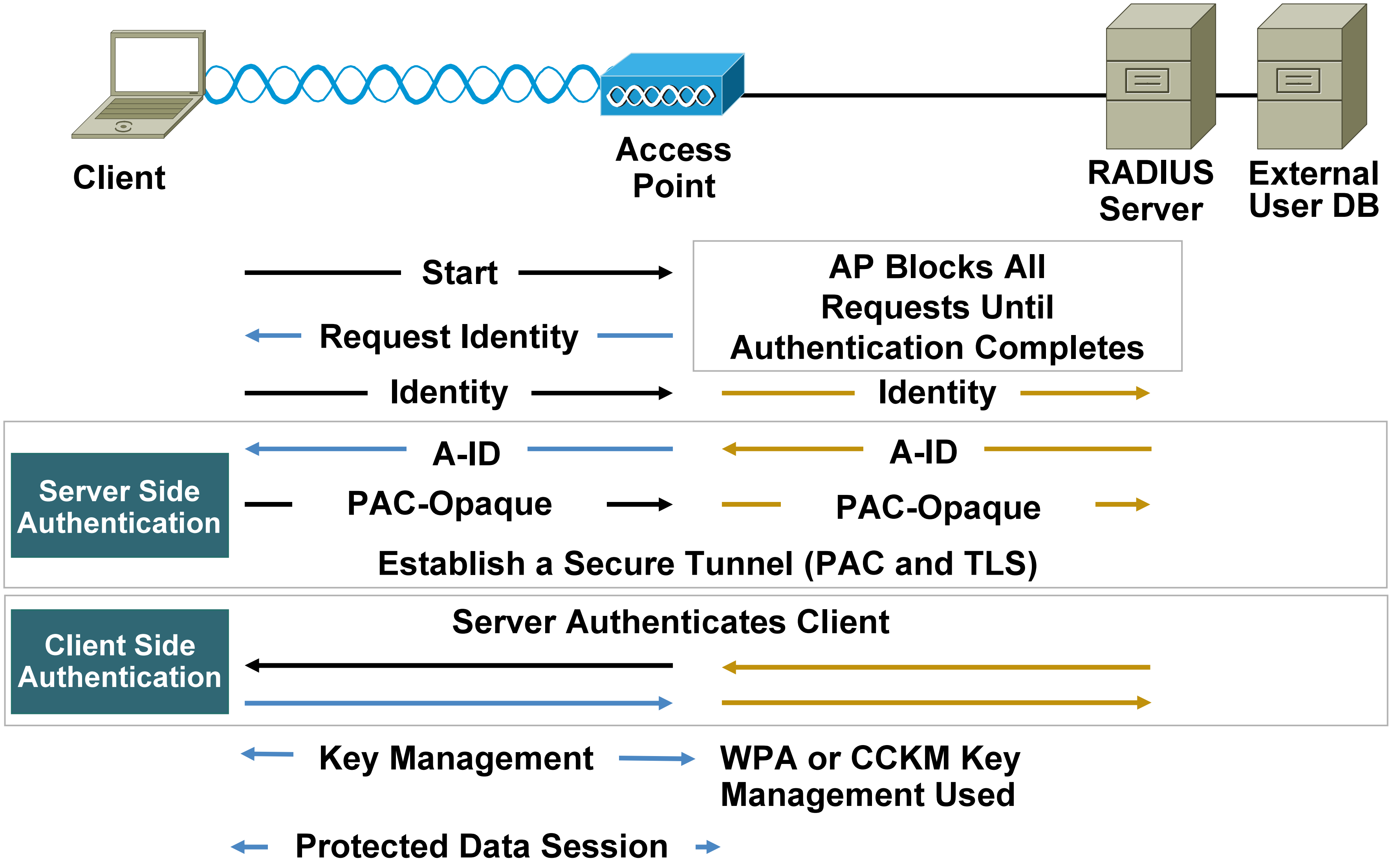
Certificate ←

PKI Certificate

PKI Certificate

Certificate →

EAP-FAST Authentication



Client

Access Point

RADIUS Server

External User DB

Start

Request Identity

AP Blocks All Requests Until Authentication Completes

Identity

Identity

Server Side Authentication

A-ID

A-ID

PAC-Opaque

PAC-Opaque

Establish a Secure Tunnel (PAC and TLS)

Client Side Authentication

Server Authenticates Client

Key Management

WPA or CCKM Key Management Used

Protected Data Session

EAP Protocols: Feature Support

	EAP-TLS	PEAP	EAP-FAST
Single Sign-on	Yes	Yes	Yes
Login Scripts (MS DB)	Yes[1]	Yes[1]	Yes
Password Expiration (MS DB)	N/A	Yes	Yes
Client and OS Availability	XP, 2000, CE, and Others[2]	XP, 2000, CE, CCXv2 Clients[3], and Others[2]	Cisco/CCXv3 Clients[4] and Others[2]
MS DB Support	Yes	Yes	Yes
LDAP DB Support	Yes	Yes[5]	Yes
OTP Support	No	Yes[5]	Yes[6]

[1] Windows OS supplicant requires machine authentication (machine accounts on Microsoft AD)

[2] Greater operating system coverage is available from Meetinghouse and Funk supplicants

[3] PEAP/GTC is supported on CCXv2 clients and above

[4] Cisco 350/CB20A clients support EAP-FAST on MSFT XP, 2000, and CE operating systems
EAP-FAST supported on CB21AG/PI21AG clients with ADU v2.0 and CCXv3 clients

[5] Supported by PEAP/GTC only

[6] Supported with 3rd party supplicant

EAP Protocols: Feature Support

	EAP-TLS	PEAP	EAP-FAST
Off-Line Dictionary Attacks?	No	No	No
Local Authentication	No	No	Yes
WPA Support	Yes	Yes	Yes
Application Specific Device (ASD) Support	No	No	Yes
Server Certificates?	Yes	Yes	No
Client Certificates?	Yes	No	No
Deployment Complexity	High	Medium	Low
RADIUS Server Scalability Impact	High	High	Low/Medium

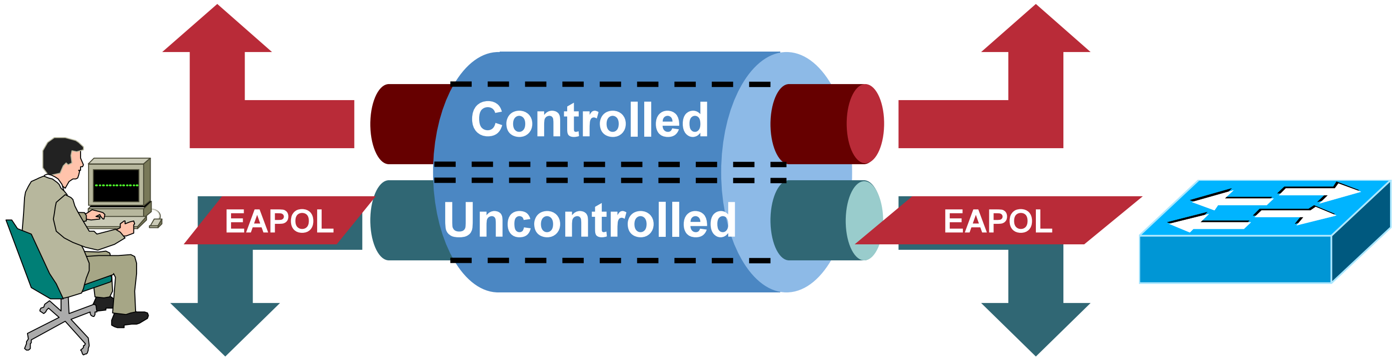
Agenda

- The Who, What, Where, Why & When of 802.1x
- 802.1x on the LAN
- 802.1x on the Wireless LAN
- Deployment Issues of 802.1x

Default Security of 802.1x

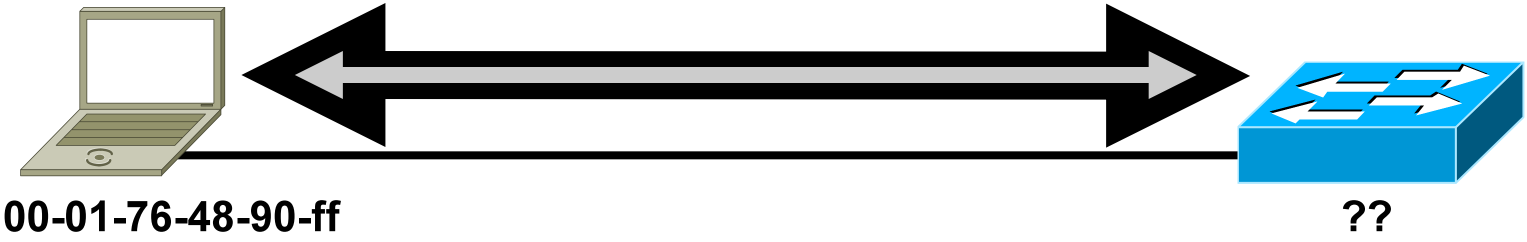
For Each 802.1x Switch Port, the Switch Creates Two Virtual Access Points at Each Port

The Controlled Port Is Open Only When the Device Connected to the Port Has Been Authorized by 802.1x



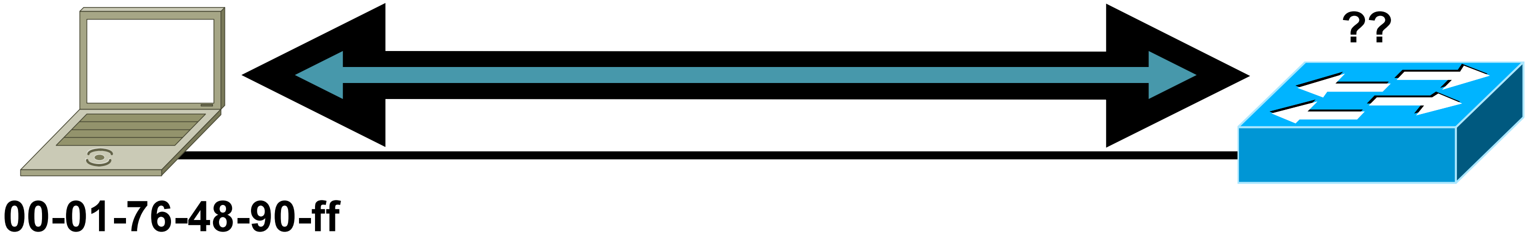
Uncontrolled Port Provides a Path for Extensible Authentication Protocol over LAN (EAPOL) Traffic Only

Default Security of 802.1x



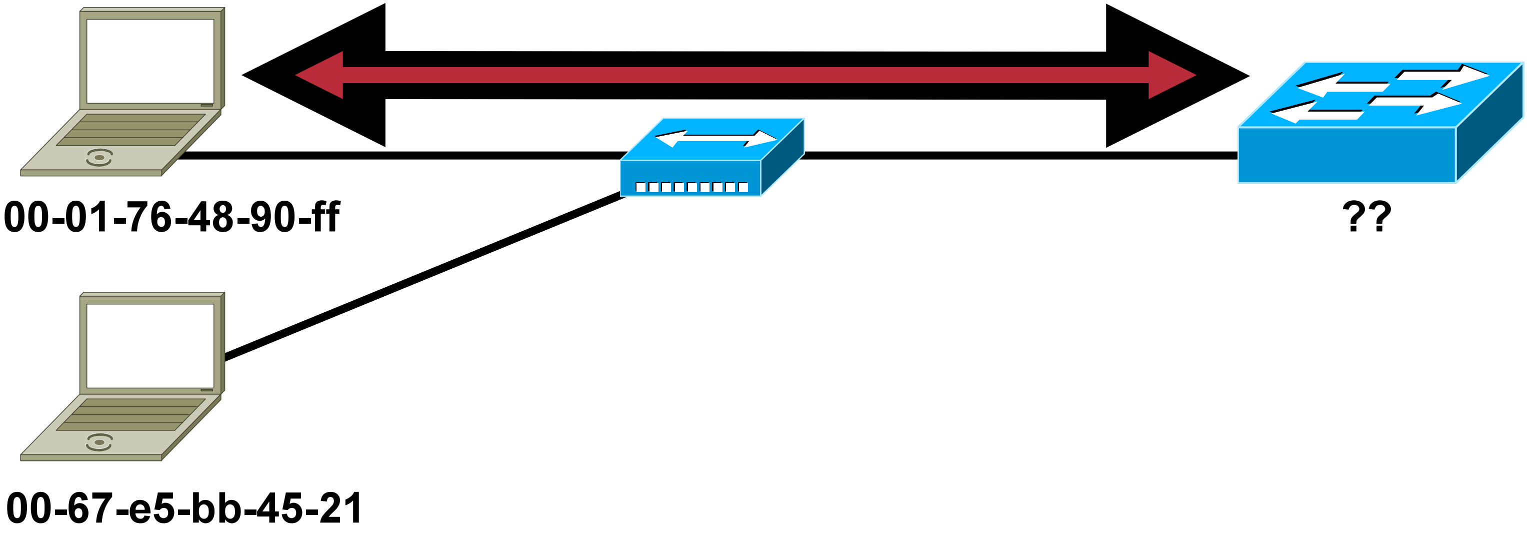
- **Before 802.1x authorization, MAC address of end-station is unknown**
- **Before 802.1x authorization, spanning-tree is not in a forwarding state for the switch port**
- **Before 802.1x authorization, no traffic can be processed by switch CPU with the exception of EAPOL**
- **802.1x state machine directly reliant on link state of port**

Default Security of 802.1x



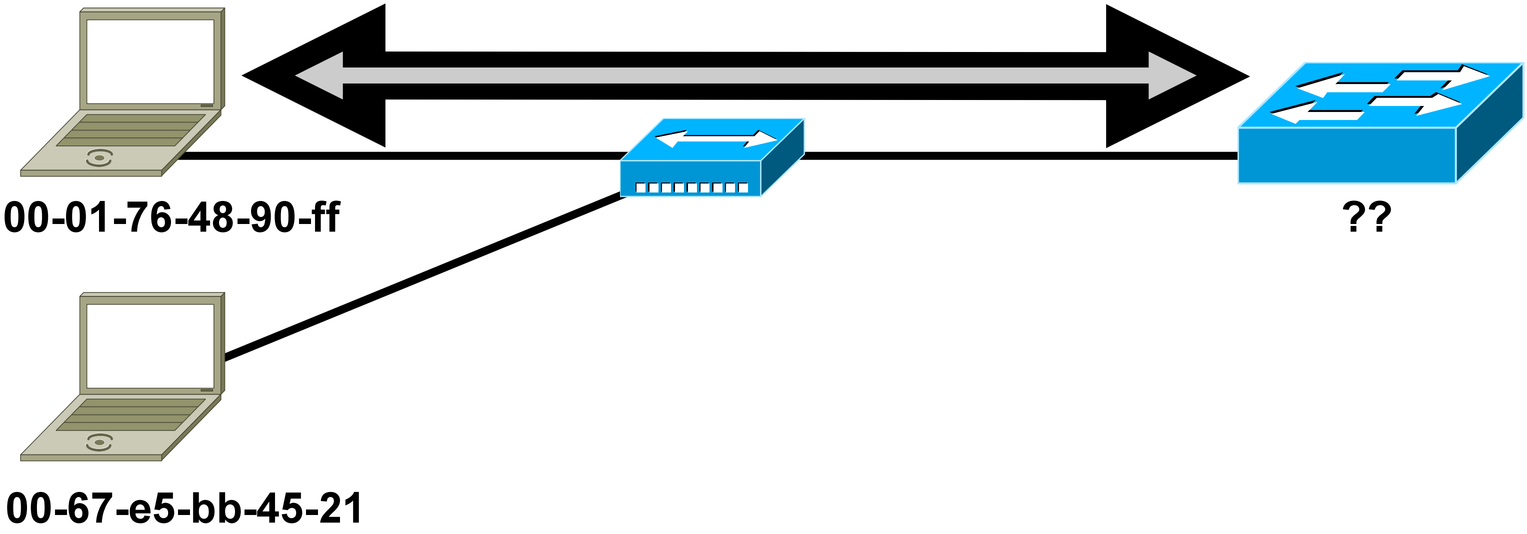
- Single-auth mode
- Authenticated session bound to MAC address used to authorize the port
- After 802.1x authorization, MAC address of end-station only one allowed on the port
- The operation ensures the validity of the authenticated session
- Network cannot be compromised by non-802.x client or an 802.1x client seen on the wire

Default Security of 802.1x



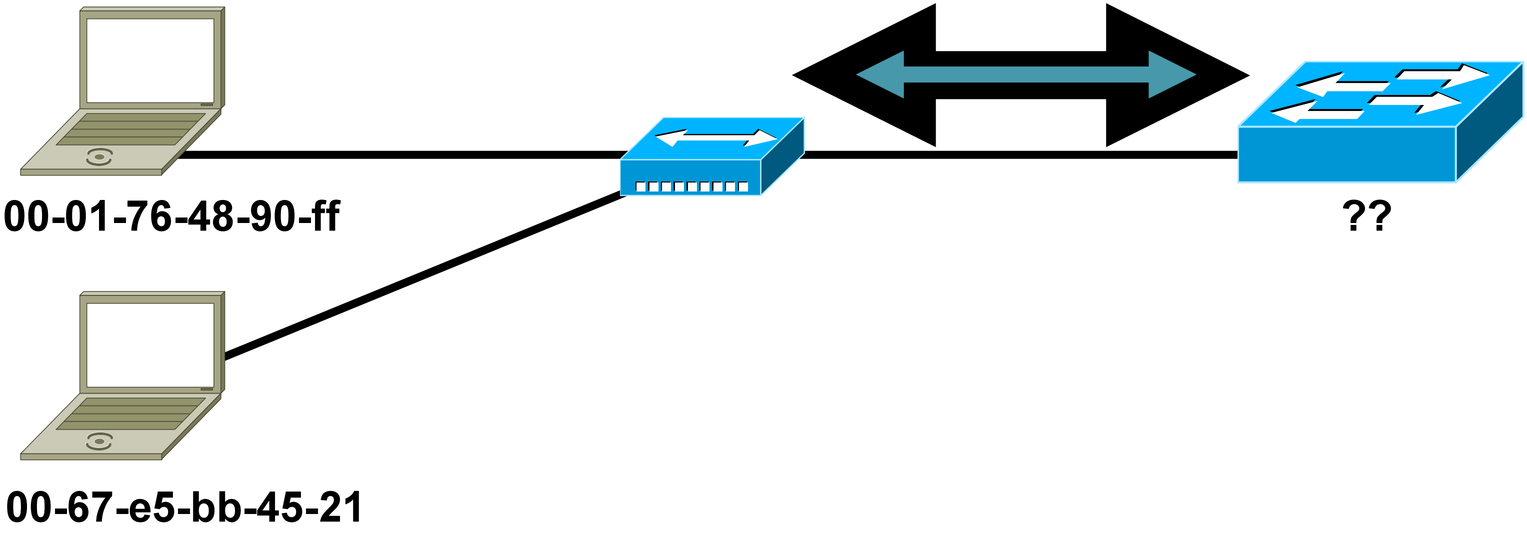
- Additional MAC addresses on wire treated as security violation
- This includes VMware type devices
- This includes machines that attempt to transmit gratuitous ARP frames

Default Security of 802.1x



- What if the physical topology does not allow a point-to-point connection? (i.e., conference room)
- Multihost mode
- Use 802.1x to authorize the port only
- Any amount of stations subsequently allowed on wire

Default Security of 802.1x



Recommendation:

- Use 802.1x to authorize the port
- Use post-security to then enforce it

Agenda

- The Who, What, Where, Why & When of 802.1x
- 802.1x on the LAN
- 802.1x on the Wireless LAN
- Deployment Issues of 802.1x

802.1X Authentication Overview

- IEEE 802.11 Task Group I recommendation for WLAN authentication
- Extensible and interoperable—supports:

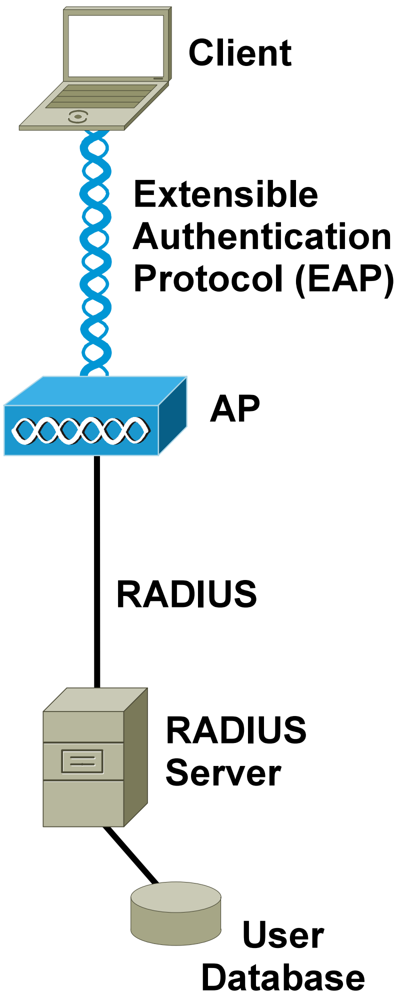
  Different EAP authentication methods or types

  New encryption algorithms, including AES as a replacement for RC4
- Key benefits

  Mutual authentication between client and authentication (RADIUS) server—mitigation for unauthorized clients/rogue AP

  Encryption keys derived after authentication—no requirement to manually manage keys

  Centralized policy control—autonomic encryption policy/user access to authorized resources



How Does Extensible Authentication Protocol (EAP) Authenticate Clients?

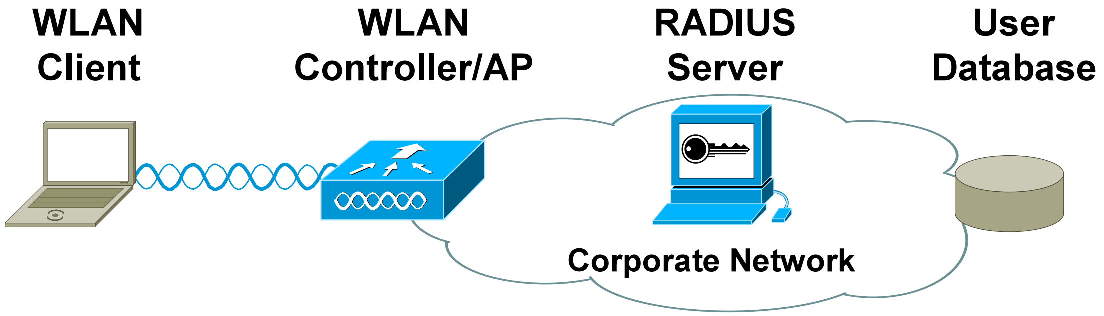
WLAN Client

WLAN Controller/AP

RADIUS Server

User Database

Client Associates



Corporate Network

Cannot Send Data Until…

Data from Client → ✗ Blocked by Controller/AP

EAP

802.1x RADIUS

…EAP Authentication Complete

Client Sends Data

Data From Client ✓ Passed by Controller/AP →

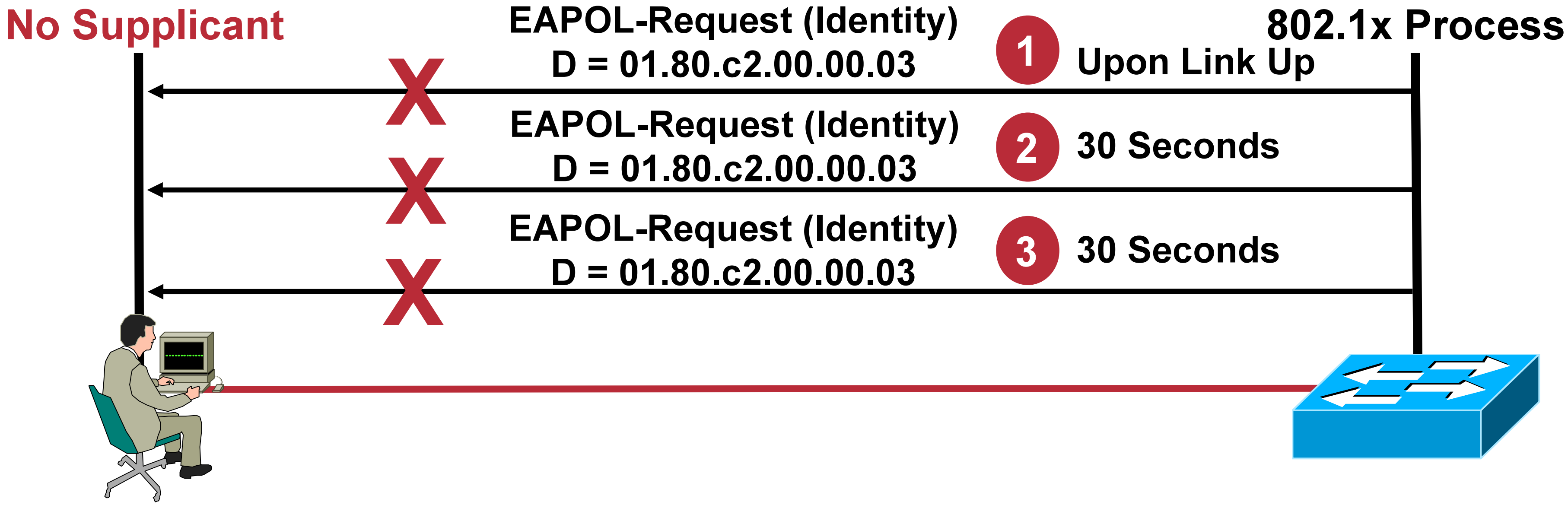
Agenda

- The Who, What, Where, Why & When of 802.1x
- 802.1x on the LAN
- 802.1x on the Wireless LAN
- Deployment Issues of 802.1x

Broken Promises of 802.1x

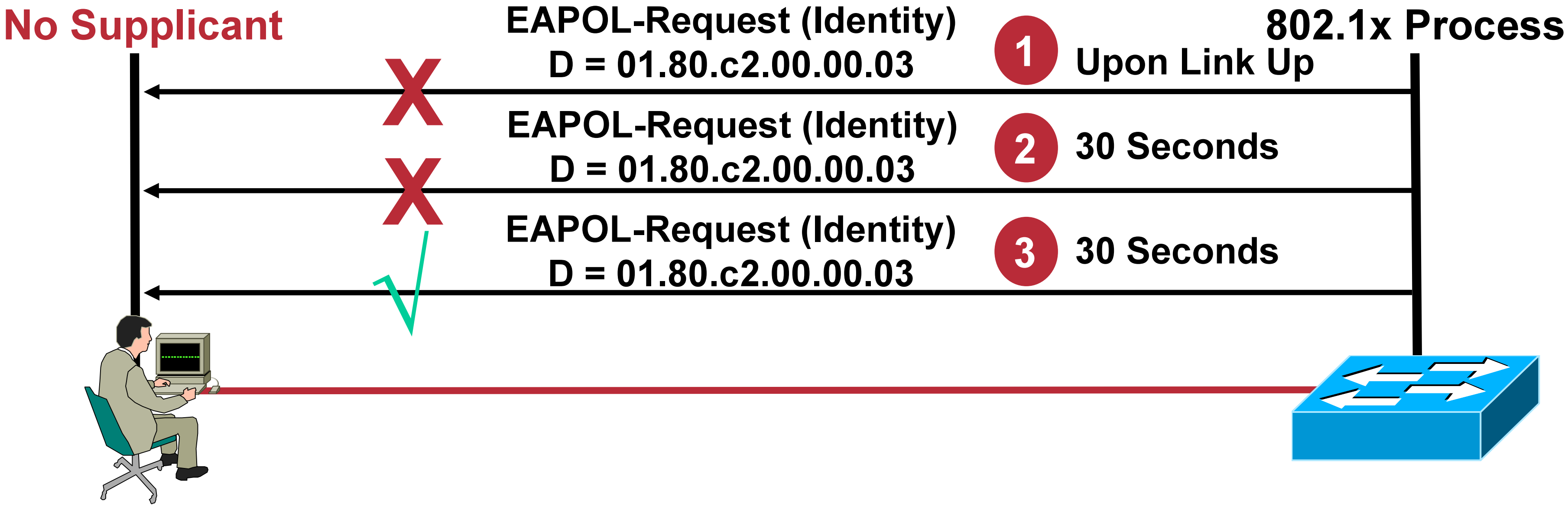
- **Integration is key to making 802.1x deployable**
- **How do you deal with devices that cannot speak 802.1x?**
- **How does voice interoperate with port-based access control?**
- **How do you provide network visibility for authenticated identities?**
- **How do handle devices that speak 802.1x but aren’t in your enterprise?**
- **How do you handle the AAA server being unavailable?**

802.1x: Default Operation



- **Any 802.1x-enabled switch port will send EAPOL identity-request frames on the wire (whether a supplicant is there or not)**
- **Switch defaults to no supplicant being on the wire based on no EAPOL response to its requests**
- **No network access is given**
- **Transient state; whole process restarts after a hold timer**
- **Process can start again if a supplicant appears on the port**

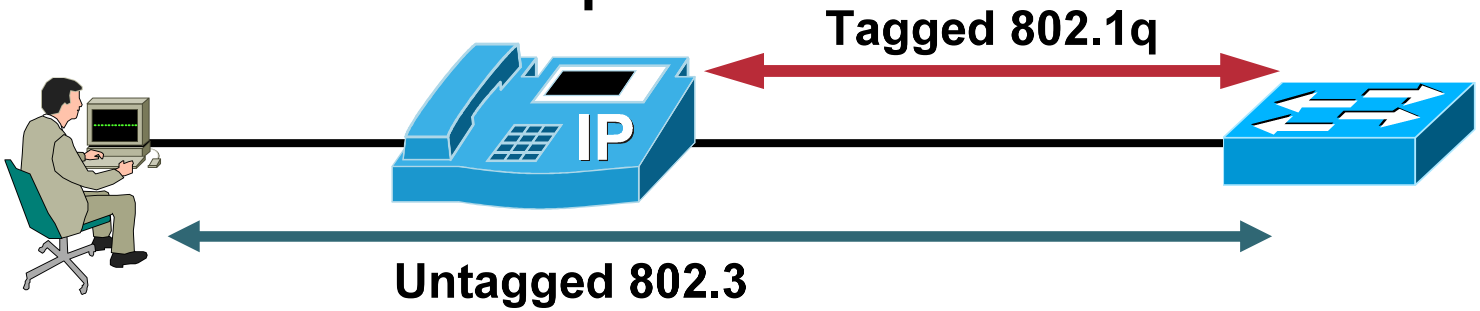
802.1x with Guest VLAN



- Any 802.1x-enabled switch port will send EAPOL-Identity-Request frames on the wire (whether a supplicant is there or not)
- Port is moved to guest VLAN after step three above; instead of transitioning to disconnected, the port immediately transitions to a state of authorized and the device is authenticated

802.1x with VVID

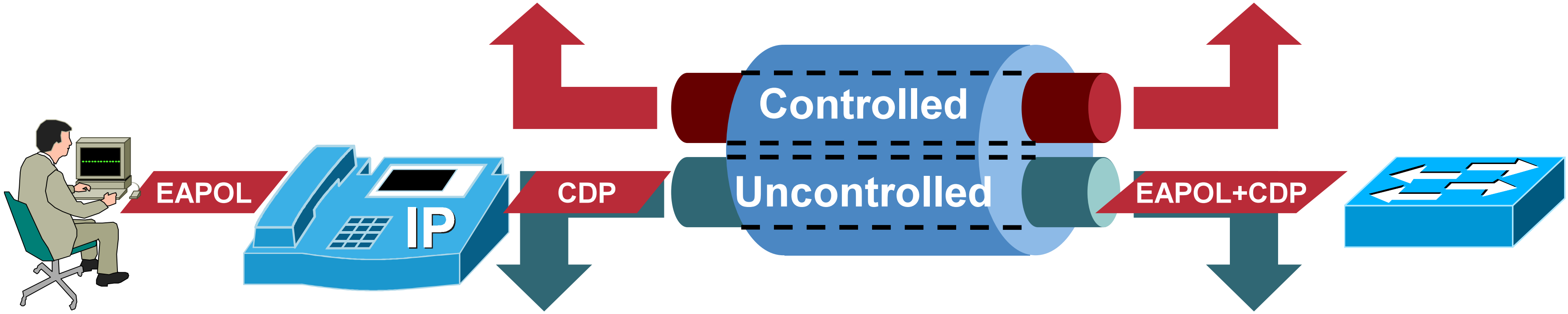
- Multi-VLAN Access Ports (MVAP)
- With Multi-VLAN Access Ports, a port can belong to two VLANs, while still allowing the separation of voice/data traffic while enabling you to configure 802.1x
- An access port able to handle two VLANs
  - Native or Port VLAN Identifier (PVID)
  - Auxiliary or Voice VLAN Identifier (VVID)
- Hardware set to dot1q trunk



802.1x with VVID

For Each 802.1x Switch Port, the Switch Creates
Two Virtual Access Points at Each Port

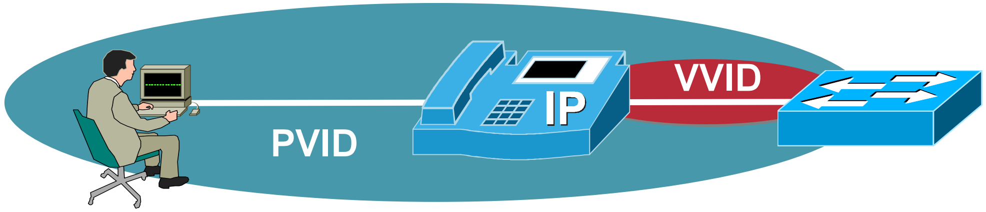
The Controlled Port Is Open Only When the Device
Connected to the Port Has Been Authorized by 802.1x



Uncontrolled Port Provides a Path for
Extensible Authentication Protocol over LAN (EAPOL) and CDP Traffic only

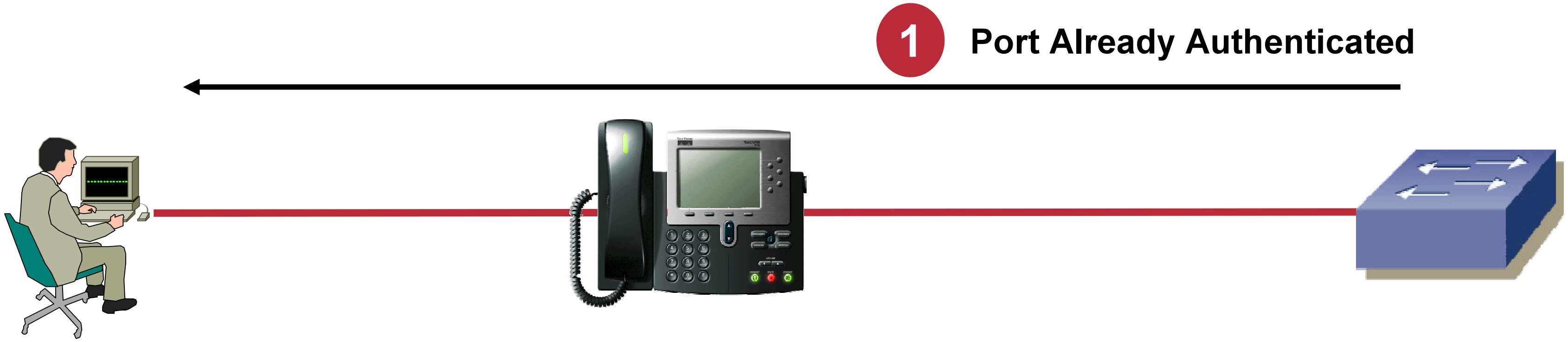
802.1x with VVID

- The PC has to authenticate before getting access to the data VLAN
- The IP phone (without dot1x supplicant implementation) can get access to the voice VLAN after sending proper CDP packets, regardless of the dot1x state of the port

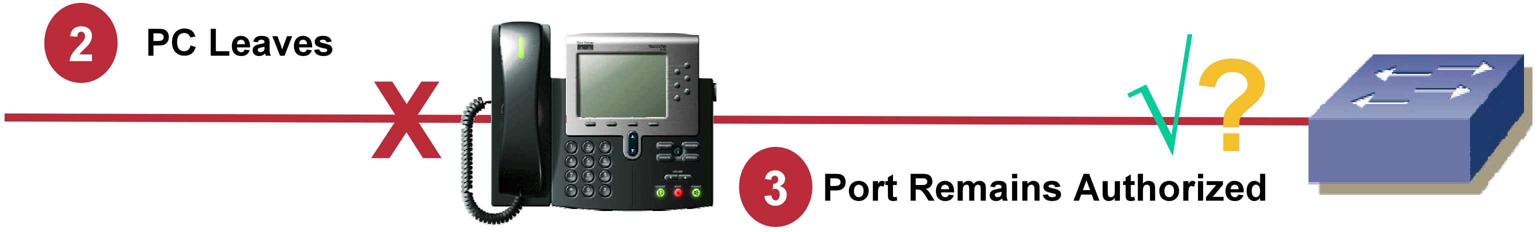


- Unauthenticated voice VLAN (VVID) access
- Authenticated data VLAN (PVID) access
- This allows 802.1x and VoIP to coexist at the same time

Issues with 802.1X and IP Phones

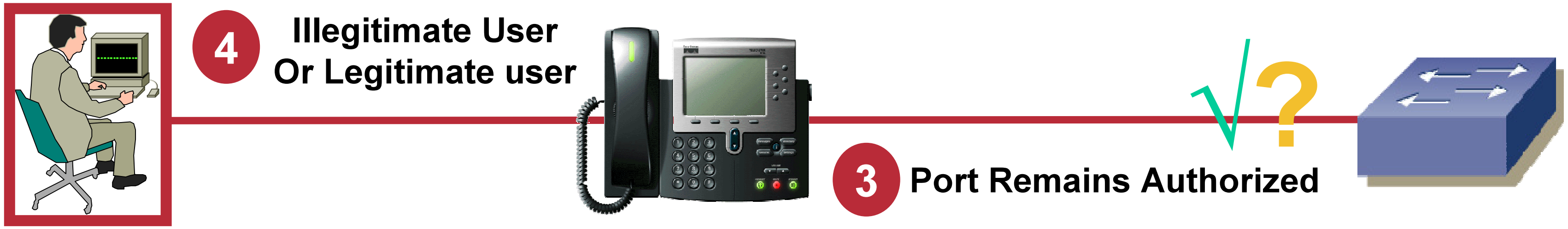


Issues with 802.1X and IP Phones



If an End-User Disconnects, the Port Remains Authorized by 802.1X !!!

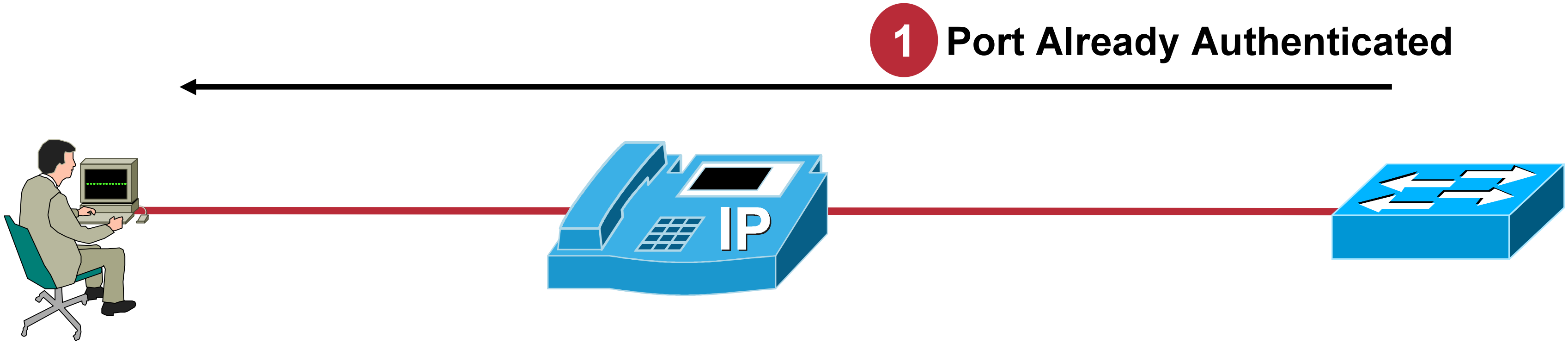
Issues with 802.1X and IP Phones



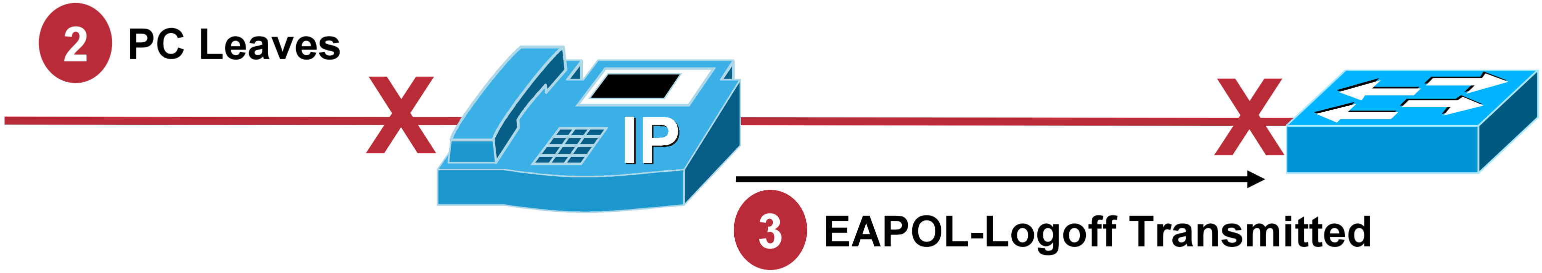
- An illegitimate user can now gain access to the port by spoofing the authenticated MAC address, and bypass 802.1X completely—SECURITY HOLE
- A legitimate user may now attempt to gain access to the port by way of 802.1X

  However, assuming MAC addresses are different, now the switch may treat this as a security violation!
- EAPOL Logoff feature in phone firmware closed this issue

Addressing IP Phone Issue

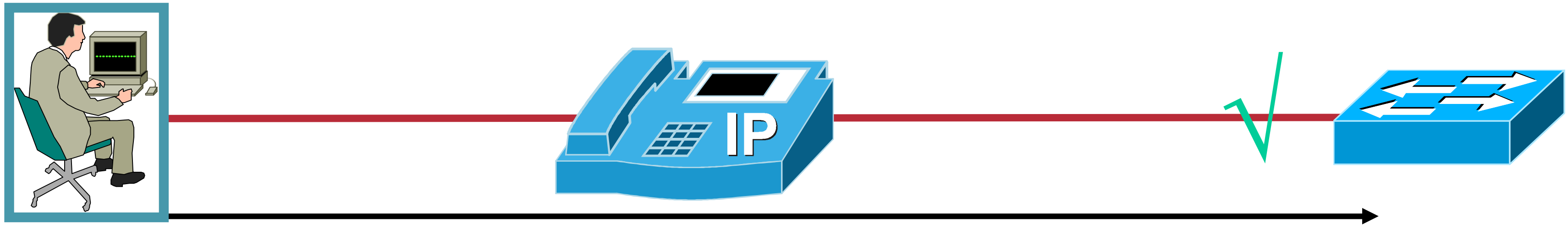


Addressing IP Phone Issue



- **If an end-user disconnects, an IP phone transmits an EAPOL-logoff frame to the switch**
  - **SA = PC MAC address**
  - **DA = 01-80-C2-00-00-03**
  - **Two basic functions needed from phone**
    - **Monitor the PAE group address to determine who and where supplicant**
    - **Actually transmit the EAPOL-logoff frame**

Addressing IP Phone Issue



4 New Authenticated Session

- The switch thinks it is a standard EAPOL-logoff frame transmitted by a supplicant indicating end of service
- This closes the current security hole, and promotes subsequent mobility

Multi-Domain-Auth

- Switch ports to authenticate the PC and the IP phone separately
- Switch port is an MVAP (aka Aux-VLAN port)
- Supports 1X functionality

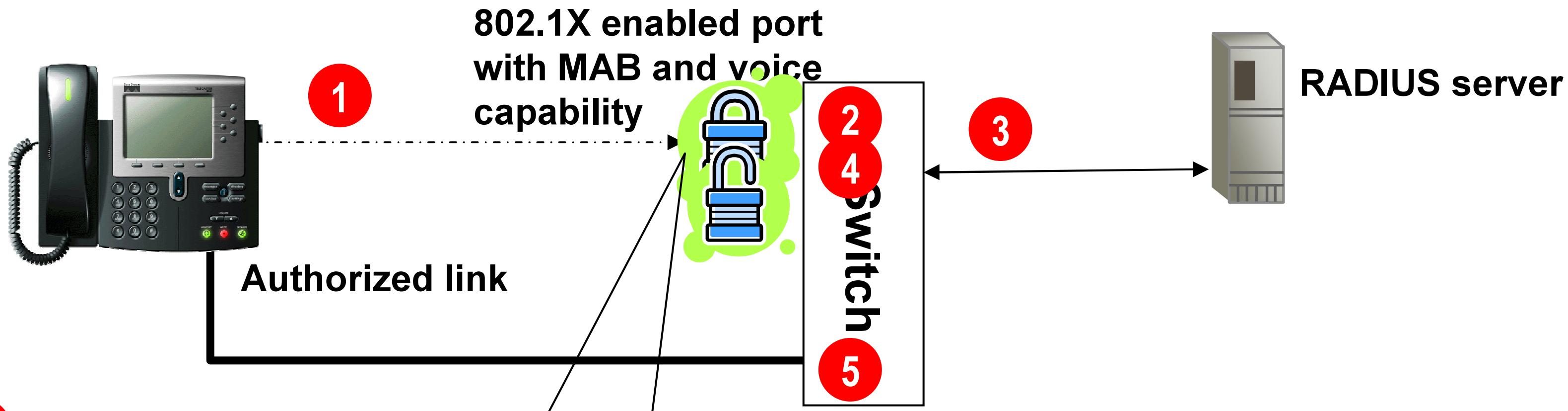
  On Voice-VLAN as well as Data-VLAN
- Supports MAB functionality

  On Voice-VLAN as well as Data-VLAN

  IP Phones without 802.1X capability require MAC Authentication Bypass (MAB) support
- The solution is extensible in order to support the planned launch of 802.1X supplicant capability on IP phones
- The solution supports both static as well as dynamic configuration on IP phones (for VVID)

Solution for Cisco IP Phones

No supplicant on phone



1 - Phone sends/received CDP requests, processed by switch

2 - Phone gets VVID info and 802.1X times out (phone not allowed to communicate to the network yet)

3 - Switch initiates MAB Access-Request on behalf of the phone

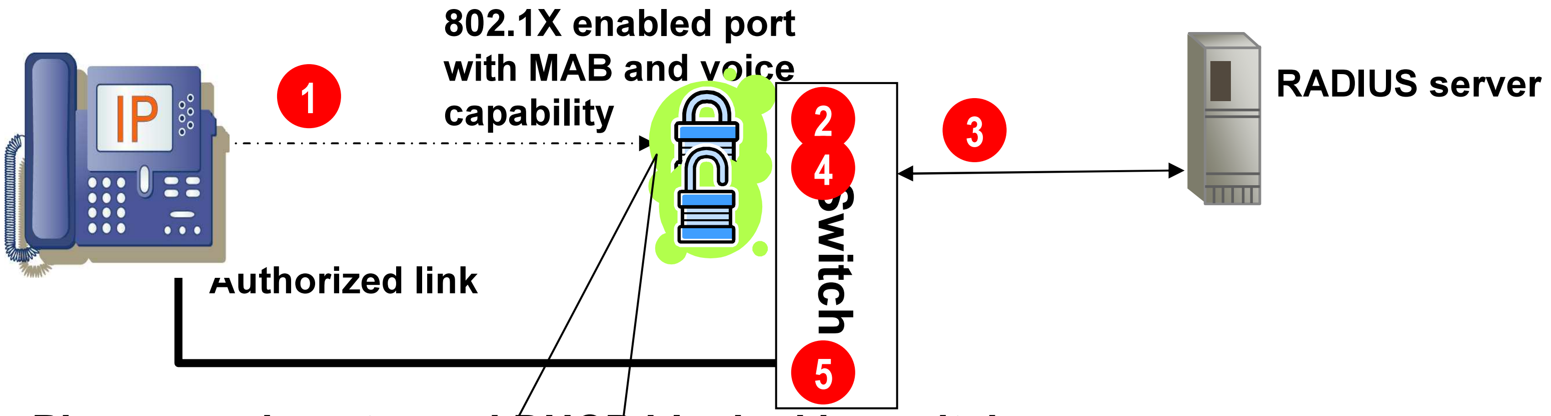
4 - Switch receives Access-Accept & information that the device is an IP phone. Port-forwarding state on either VLAN.

5 - The IP phone (now tagging its packets with the same voice VLAN that was received in the CDP response) continues to send traffic which is now allowed on the VVID as a result of authenticating the MAC-Address.

- Data VLAN VP state-machine is in blocking state and
- Voice VLAN VP state-machine is in ask state

Solution for non-Cisco IP Phones

No supplicant on phone



1 - Phone sends untagged DHCP blocked by switch

2 - 802.1X times out (phone not allowed to communicate to the network yet)

3 - Switch initiates MAB Access-Request on behalf of the phone

4 - Switch receives Access-Accept & information that the device is an IP phone. Port-forwarding is allowed on either VLAN.

5 - Non-Cisco phone continues to send traffic which is now allowed on the PVID as a result of authenticating the MAC-Address. Phone then reboots onto VVID normally.

- Data VLAN VP state-machine is in blocking state and
- Voice VLAN VP state-machine is in ask state

MAB and Guest VLAN

- These features work together

  MAB First

  Guest VLAN if MAB fails

- Be VERY careful tweaking timers.

  You don’t want a 802.1X capable machine to do MAB or Guest VLAN before 802.1X can respond to the EAPOL Identity requests

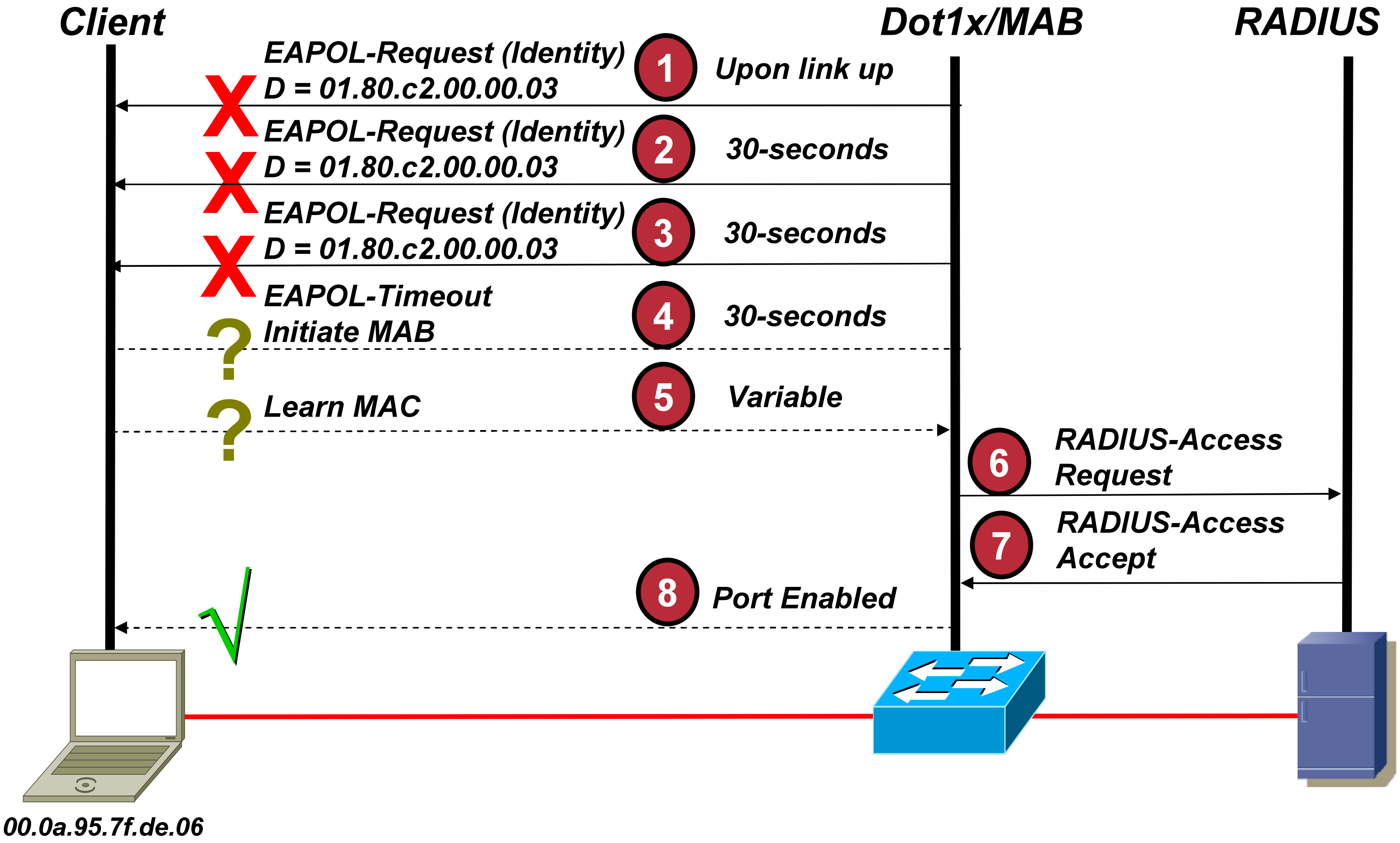
802.1X/MAB with IPT

- **802.1X resolved this issue by having the phone snoop for EAPOL and proxy and EAPOL-Logoff when 802.1X device leaves the port.**
- **MAB has same issue as 802.1X except there is no control plane between the switch and phone to snoop on.**
- **If a MAB device moves from behind a phone and reconnects to the same switch on a different port it triggers a security violation since link on the original port doesn't go down and clear the mac address from the port.**
- **This has been a show stopper for a few customers with large amounts of MAB devices behind phones**

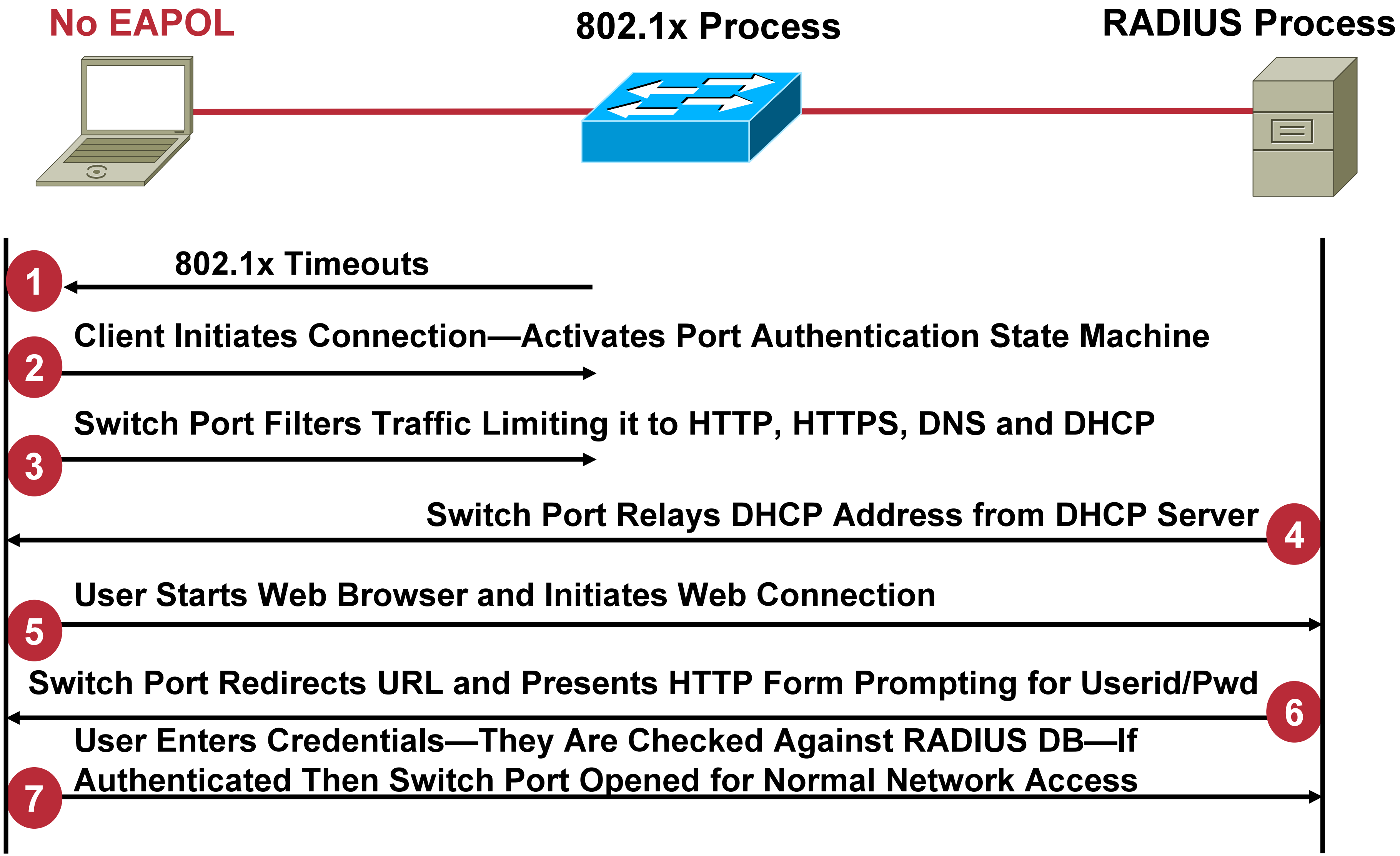
  Guests

  OSX supplicant with SSO isn't very good ☺
- **Workaround is mac address aging**
- **There is an initiative to deliver a deterministic notification from phone to switch for all authentication methods (802.1X, MAB, Web Auth)**

MAC Authentication Bypass (MAB)



Web Based Proxy Authentication



1. 802.1x Timeouts
2. Client Initiates Connection—Activates Port Authentication State Machine
3. Switch Port Filters Traffic Limiting it to HTTP, HTTPS, DNS and DHCP
4. Switch Port Relays DHCP Address from DHCP Server
5. User Starts Web Browser and Initiates Web Connection
6. Switch Port Redirects URL and Presents HTTP Form Prompting for Userid/Pwd
7. User Enters Credentials—They Are Checked Against RADIUS DB—If Authenticated Then Switch Port Opened for Normal Network Access

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
- The most basic authorization in 802.1x is the ability to allow or disallow access to the network at the link layer
- Other forms of authorization include VLAN assignment, ACL assignment, QoS policy assignment, 802.1x with ARP inspection, etc.

802.1x with VLAN Assignment

AV Pairs Used—All Are IETF Standard

- [64] Tunnel-type—“VLAN” (13)
- [65] Tunnel-medium-type—“802” (6)
- [81] Tunnel-private-group-ID—<VLAN name>

- VLAN name must match switch configuration
- Mismatch results in authorization failure

802.1x with ACL Assignment

- **Vendor-specific attributes used for RADIUS**

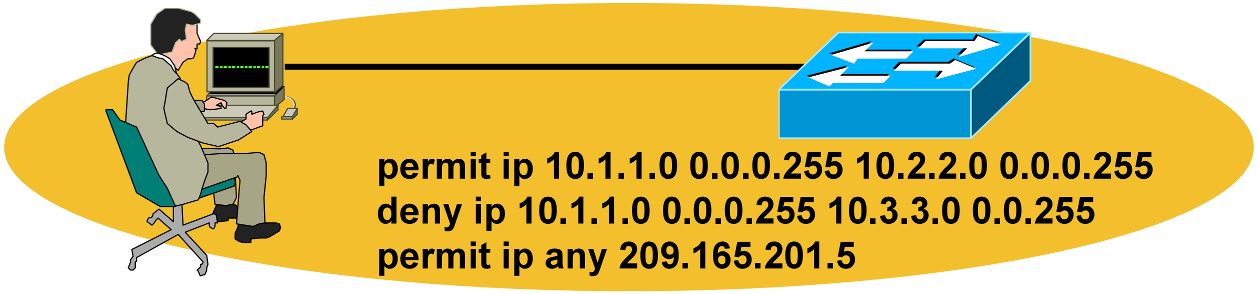
  [026]—vendor specific

  [009]—vendor ID for Cisco

  [001]—refers to the VSA number

- **Attribute used for predefined ACLs**

  [11]—filter ID

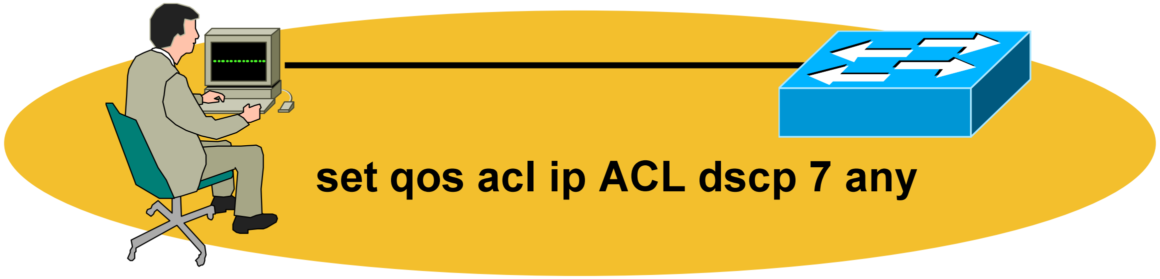


```
permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
deny ip 10.1.1.0 0.0.0.255 10.3.3.0 0.0.255
permit ip any 209.165.201.5
```

802.1x with QoS Policy

- **Vendor-specific attributes used for RADIUS**

  [026]—vendor specific
  [009]—vendor ID for Cisco
  [001]—refers to the VSA number

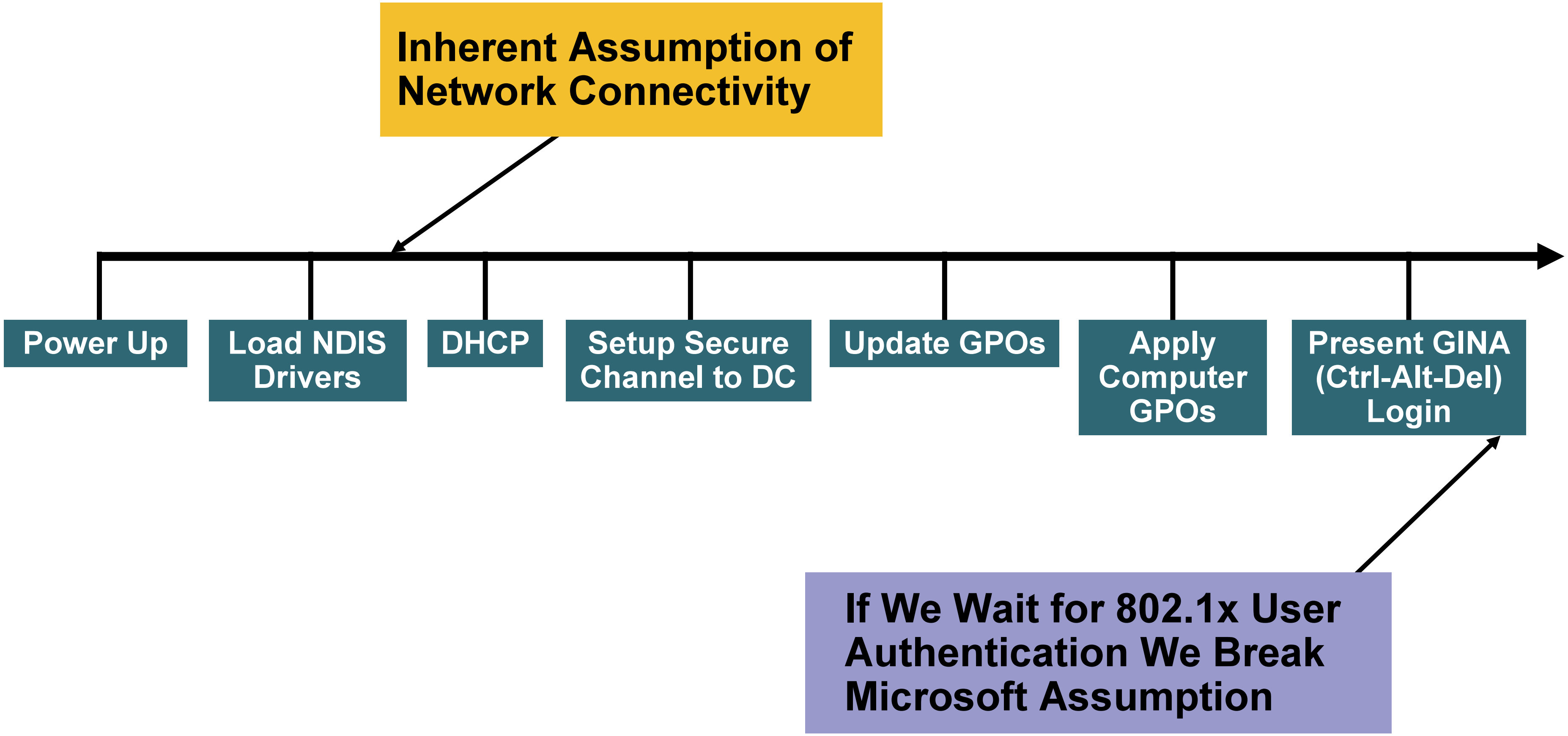


set qos acl ip ACL dscp 7 any

- **Use to enable the automatic QoS provisioning of users**
- **In this example, RADIUS will send down a QoSPACL name along with an accept packet**
- **Policy converted into ACEs and installed on the switch**

Operating System Issues

Windows Boot Cycle Overview



Inherent Assumption of Network Connectivity

Power Up

Load NDIS Drivers

DHCP

Setup Secure Channel to DC

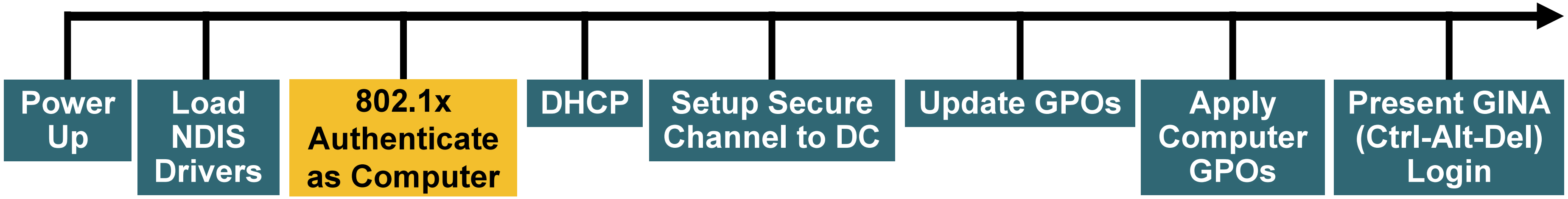
Update GPOs

Apply Computer GPOs

Present GINA (Ctrl-Alt-Del) Login

If We Wait for 802.1x User Authentication We Break Microsoft Assumption

Windows Boot Cycle Overview



Power Up

Load NDIS Drivers

802.1x Authenticate as Computer

DHCP

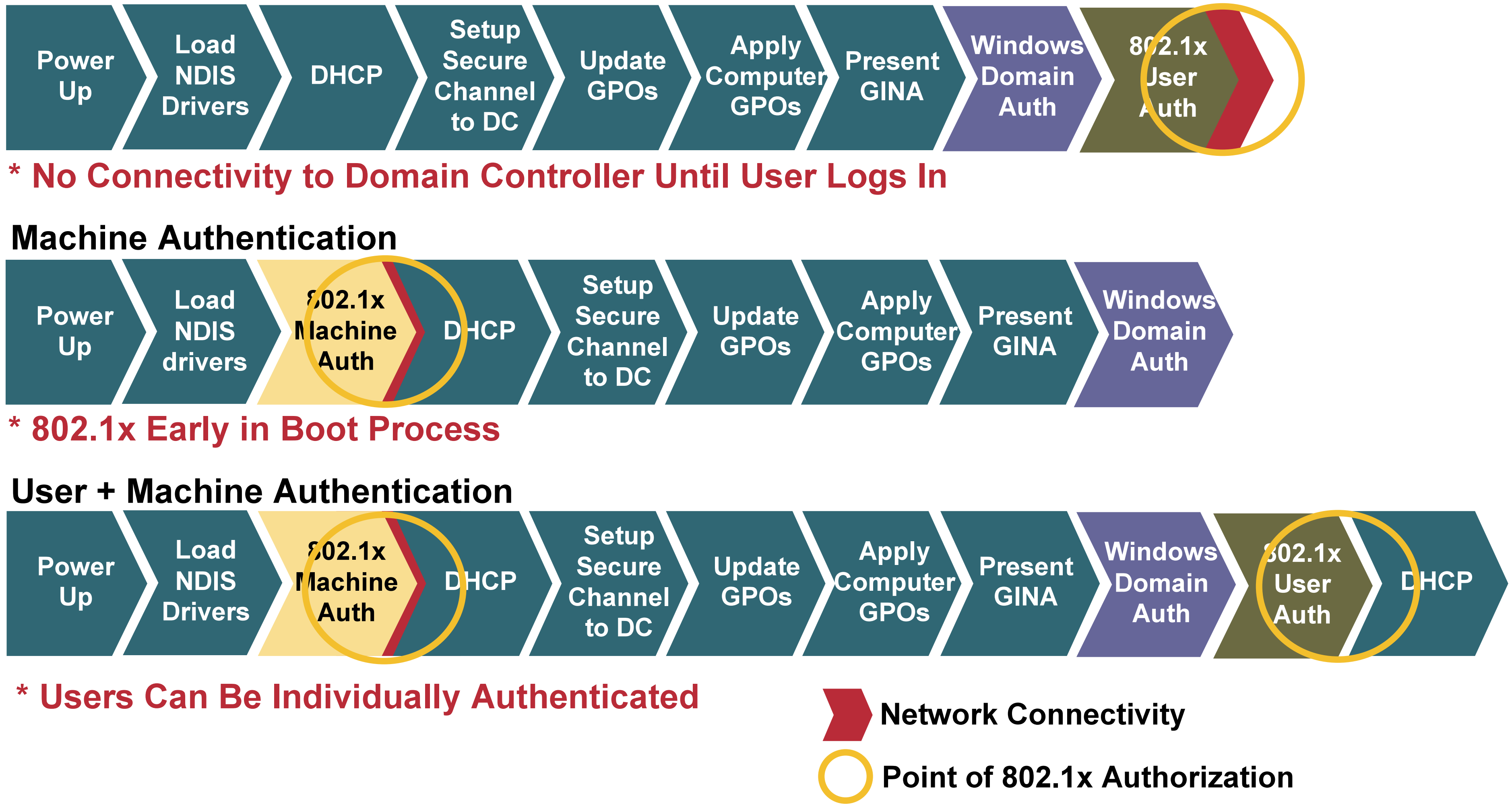
Setup Secure Channel to DC

Update GPOs

Apply Computer GPOs

Present GINA (Ctrl-Alt-Del) Login

Windows Login Procedure



User Authentication

Power Up → Load NDIS Drivers → DHCP → Setup Secure Channel to DC → Update GPOs → Apply Computer GPOs → Present GINA → Windows Domain Auth → 802.1x User Auth

* No Connectivity to Domain Controller Until User Logs In

Machine Authentication

Power Up → Load NDIS drivers → 802.1x Machine Auth → DHCP → Setup Secure Channel to DC → Update GPOs → Apply Computer GPOs → Present GINA → Windows Domain Auth

* 802.1x Early in Boot Process

User + Machine Authentication

Power Up → Load NDIS Drivers → 802.1x Machine Auth → DHCP → Setup Secure Channel to DC → Update GPOs → Apply Computer GPOs → Present GINA → Windows Domain Auth → 802.1x User Auth → DHCP

* Users Can Be Individually Authenticated

🟥 Network Connectivity

○ Point of 802.1x Authorization

Different Modes of Authentication in Microsoft Environments

- Controlled by registry keys
- Authentication by machine only

  No need for user authentication if machine authentication is successful
- Authentication by user only

  No machine authentication taking place at all—be careful, this breaks group and system policies
- Authentication by user and machine

  Uses authentication of both user and machine; switches contexts when going from one to the other

802.1X authentication

- Recommend you start simple with your authentication
- Recommend machine authentication only

  You need to manage auth behavior on XP/2000 via registry keys

  http://support.microsoft.com/kb/309448/en-us

  http://www.microsoft.com/technet/network/wifi/wififaq.mspx

- Recommend that you use the automatic provisioning built into AD if possible

  Machines are provisioned automatically with a machine password.

  Can have certificates automatically provisioned via AD GPOs

How Do You Enable Machine Auth?

- Make sure the computer is a member of the domain
- If using TLS, make sure the computer gets a cert—either through auto-enrollment or manually
- If using EAP-FAST, PEAP or EAP-TLS make sure that the CA cert is in the local machine store; typically added if CA is up when machine is added to the domain; if not, you can force via auto-enrollment
- Click the check box for the “authenticate as computer when computer information is available” in the authentication tab of the local-area connection properties window

Machine Auth Using PEAP or TLS

- Machine authentication using PEAP

  Uses account information for the computer created at the time the machine is added to the domain

  Computer must be a member of the domain

  If doing mutual authentication, the computer must trust the signing CA of the RADIUS server's cert

- Machine authentication using EAP-TLS

  Authenticates the computer using certs

  The computer must have a valid cert

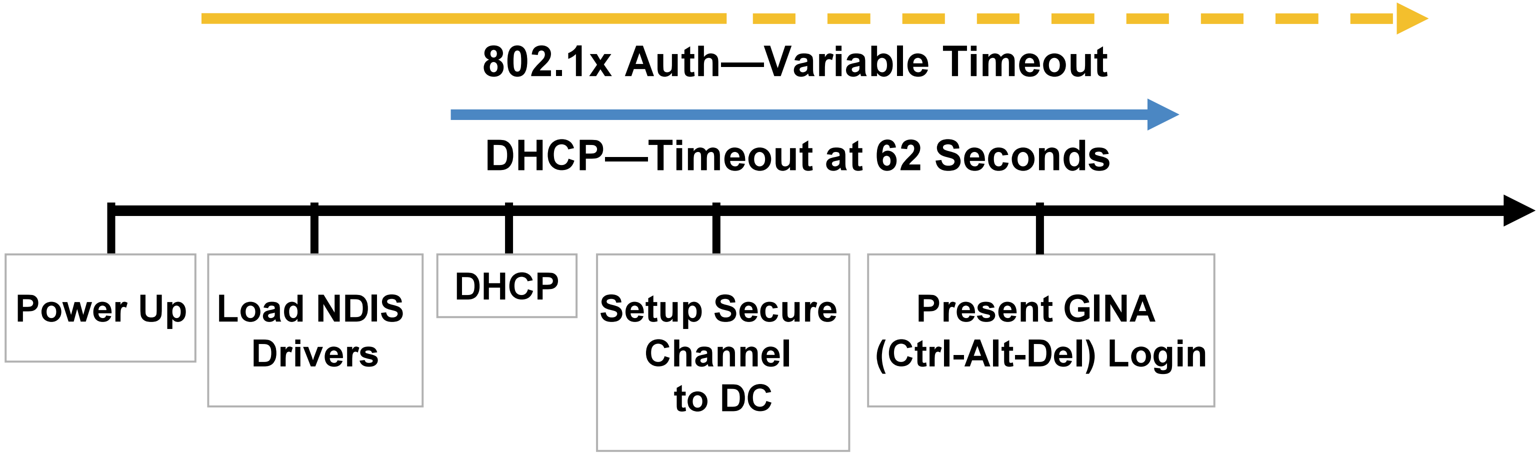
  If doing mutual authentication, the computer must trust the signing CA of the RADIUS server's cert

  Easiest way to deploy is using MS-CA and Windows GPOs

Microsoft Issues with DHCP

DHCP Is a Parallel Event, Independent of 802.1x Authentication

- With wired interfaces a successful 802.1x authentication does not force an DHCP address discovery (no media-connect signal)
- This produces a problem if not properly planned
- DHCP starts once interface comes up
- If 802.1x authentication takes too long, DHCP may time out



802.1x Auth—Variable Timeout

DHCP—Timeout at 62 Seconds

Power Up

Load NDIS Drivers

DHCP

Setup Secure Channel to DC

Present GINA (Ctrl-Alt-Del) Login

How to Address DHCP Timeout with 802.1x?

- Use machine authentication—this allows the initial machine authentication to obtain an IP address
- Supplicant behavior has been addressed by Microsoft
  - Windows XP: install service pack 1a + KB 826942
  - Windows 2000: install service pack 4
- Updated supplicants trigger DHCP IP address renewal
  - Successful authentication causes client to ping default gateway (three times) with a subsecond timeout
  - Lack of echo reply will trigger a DHCP IP renew
  - Successful echo reply will leave IP as is
  - Pre-renewal ping prevents lost connections when subnet stays the same but client may be WLAN roaming

Supplicant Considerations

- ## Microsoft Windows

  User and machine authentication

  DHCP request time out

  Machine authentication restriction

  Default methods : MD5, PEAP, EAP-TLS, EAP-FAST

- ## Unix/Linux considerations

  Open source : xsupplicant Project (University of Utah)

  Available from http://www.open1x.org

  Supports EAP-MD5, EAP-TLS,

  PEAP/MSCHAPv2, PEAP/EAP-GTC

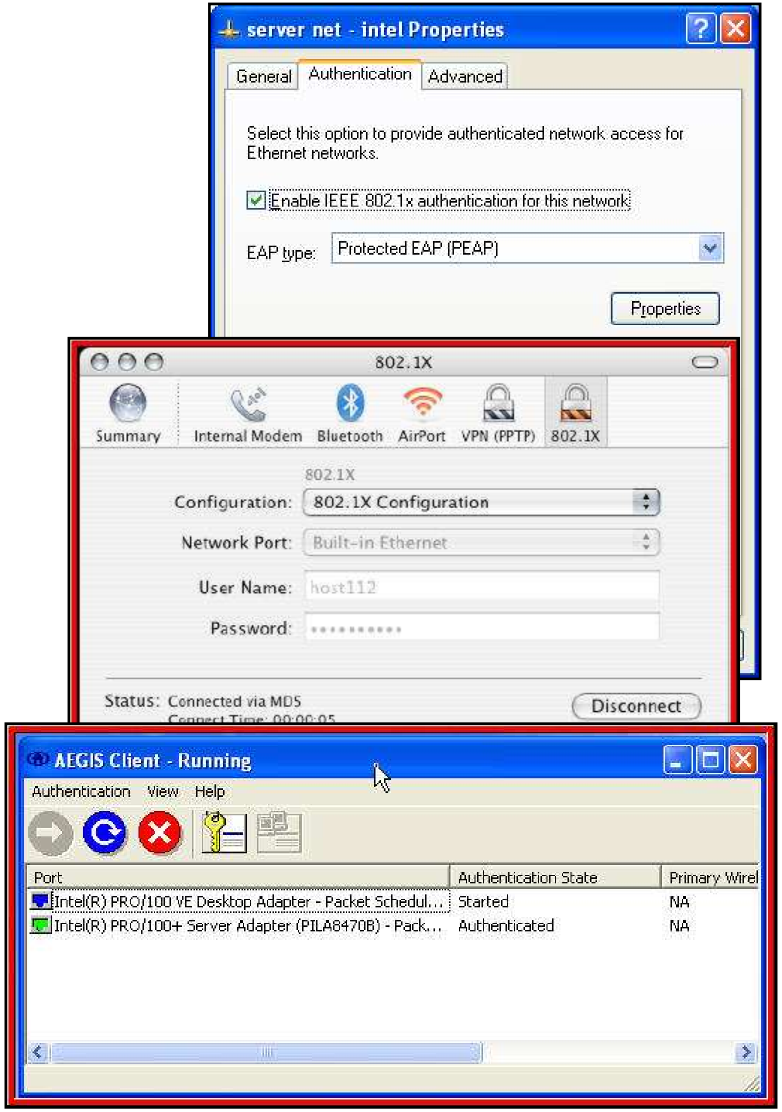
- ## Native Apple supplicant support in OS X 10.3

  802.1x is turned off by default!

  Default parameters—TTLS, LEAP, PEAP, MD5 supported

  Support for airport and wired interfaces

  Single sign on can be accomplished w/Applescripts



Select this option to provide authenticated network access for Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Protected EAP (PEAP)

802.1X

Configuration: 802.1X Configuration

Network Port: Built-in Ethernet

User Name: host112

Password: ••••••••••

Status: Connected via MD5

Connect Time: 00:00:05

Port	Authentication State	Primary Wirel
Intel(R) PRO/100 VE Desktop Adapter - Packet Schedul...	Started	NA
Intel(R) PRO/100+ Server Adapter (PILA8470B) - Pack...	Authenticated	NA

Pre eXecution boot Environment - PXE

- Very common way to image new machines and reimage existing machines. i.e. “F12 - Network Boot”
- Assumes IP connectivity and happens before OS loads

  Uses DHCP extensions and TFTP to download boot image typically

  No 802.1X supplicant therefore no connectivity

- Only LAN workarounds at this time are MAB or Guest VLAN

  Challenge is to initiate MAB or Guest VLAN access before the PXE firmware times out

  PXE firmware per spec should timeout in 60 seconds.

  Some PXE firmware has been observed to expire in as little as 5 seconds – Lots of testing required to verify the solution

PXE (cont.)

- Customer reaction is subjective on this issue.
  - Customers have deployed with MAB and Guest VLAN
  - Customers have deployed and just designate a secure build room where PXE happens without 802.1X
  - Customers have deployed by registering a help desk item and force authorizing the port via SNMP
  - Some customers don’t like the workarounds and consider this a show stopper to 802.1X deployment
- Ask the customer first thing if they use PXE for their access devices!
- There are initiatives to develop deterministic switch based mechanisms for PXE

Wake On LAN (WOL)

- There is a feature that enables support of WOL on the switches
- Issue: With MAB or Guest VLAN configured

  If the device goes to sleep and drops link or if reauth is triggered and the device is asleep; MAB/Guest VLAN handling will be triggered and the device will potentially get placed on a new VLAN.

  The WOL magic packet to wake the machine will be sent to the original 802.1X auth vlan.

- Workaround some customers have used

  Make sure all managed assets are in a mac address database and assign the device to the same VLAN with MAB

Q & A

ISSA™
Information Systems Security Association
CENTRAL PLAINS CHAPTER