



poweredbycisco.
networkers
2005

SEC-2005

UNDERSTANDING 802.1x, IBNS, AND NETWORK IDENTITY SERVICES

Jason Halpern

Overview and Agenda

Cisco.com

- **The Concepts of Identity and Authentication**
- **Understanding the Protocols and Mechanisms Behind 802.1x**
- **Understanding the Default Security for 802.1x**
- **Identity-Based Integration Issues, Authorization and Policy Enforcement**
- **Operating System Implementations and Supplicants in Different Environments**

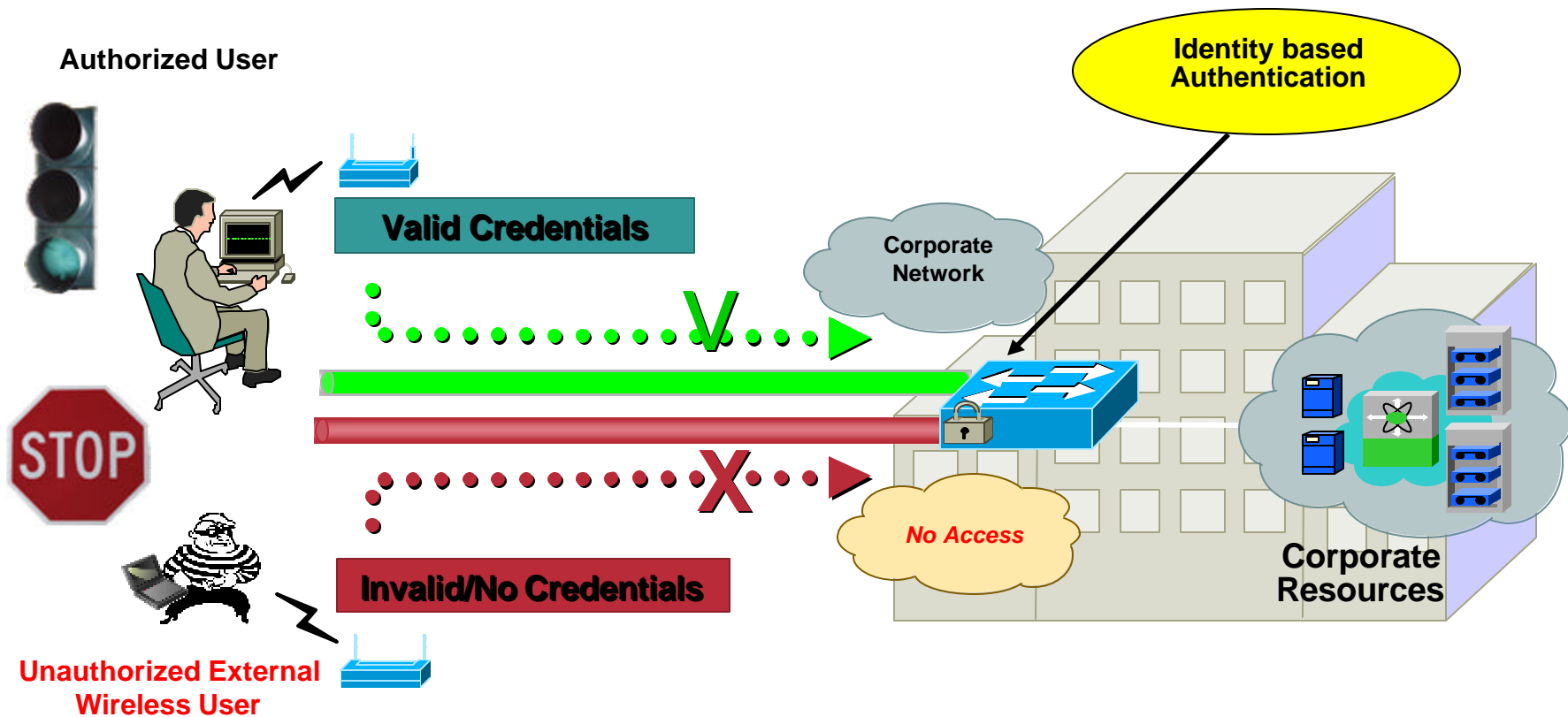
What Is Identity-Based Network Services?

Cisco.com

- **IBNS != IEEE 802.1x**
- **IBNS is a superset of IEEE 802.1x functionality**
- **IBNS is a systems framework for delivering LAN authentication, of which, a part of is using 802.1x**
- **Other enhancements and technologies complement 802.1x to form IBNS**

Concepts of IBNS in Action

Cisco.com



Three Simple Theories of IBNS

Cisco.com

- 1. Keep the outsiders out**
 - Too easy for an unsecured individual to gain physical and logical access to a network
- 2. Keep the insiders honest**
 - A network port is either enabled or disabled. What can users do when they get network access?
- 3. 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

Cisco.com

- **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

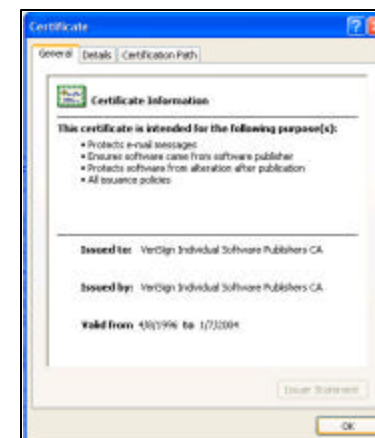
- **What does it look like?**

Can look like anything:

jhalpern@cisco.com

Jason Halpern

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

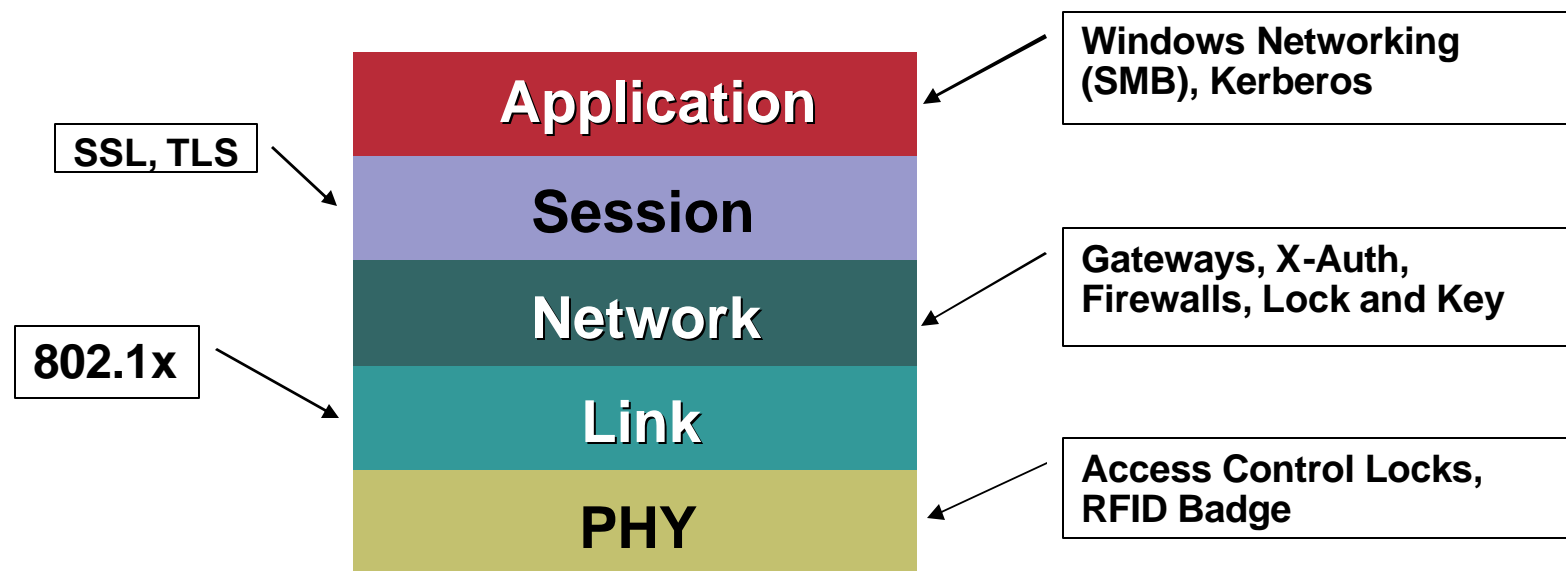


- **How do we use identities?**

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

Identity Everywhere?

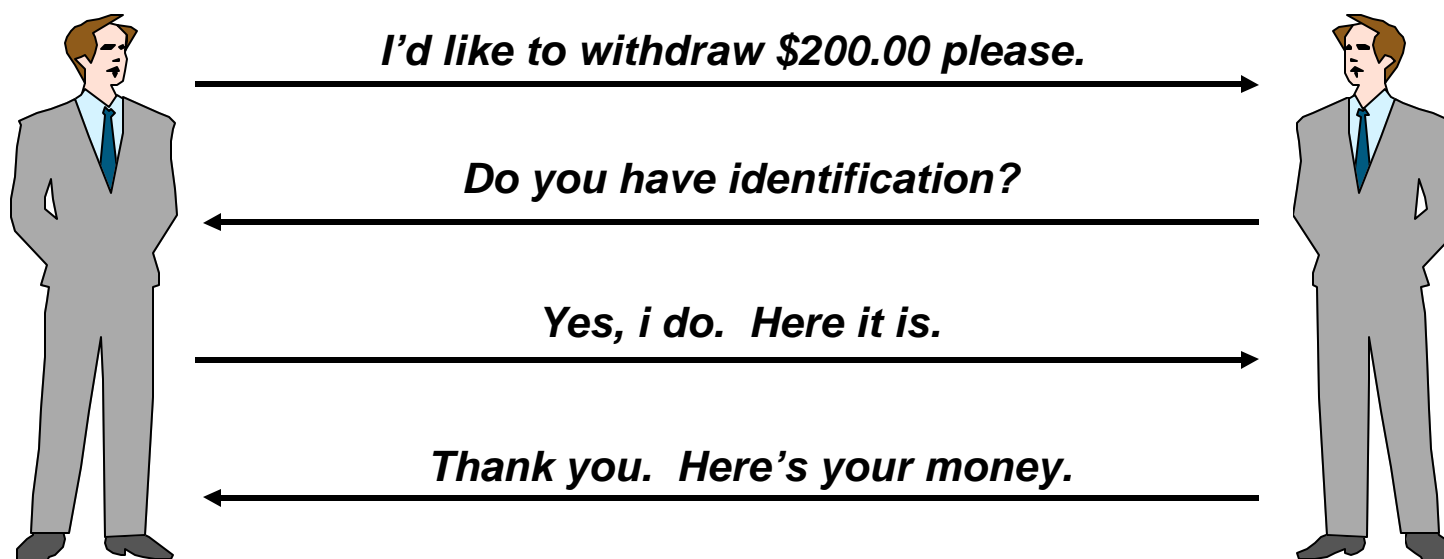
Cisco.com



- **Physical**—Access control locks, RFID proximity badge
- **Link**—802.1x
- **Network**—Gateways, X-auth, firewalls, lock and key
- **Session identity**—SSL, TLS
- **Application identity**—Windows networking, Kerberos

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

Some Important Points on Authentication

Cisco.com

- **The process of authentication is used to verify a claimed identity**
- **An identity is only useful as a pointer to an applicable policy and for accounting**
- **Without authorization or associated policies, authentication alone is pretty meaningless**
- **An authentication system is only as strong as the method of verification used**

Why Do We Care?

- **Because differentiation of services and rights control is critical in network environments**
- **Not everyone has the same privileges; not all resources or information have the same level of confidentiality**
- **The concept of being able to differentiate services amongst groups or individuals**
- **If everyone had the same rights, then we wouldn't need authorization**

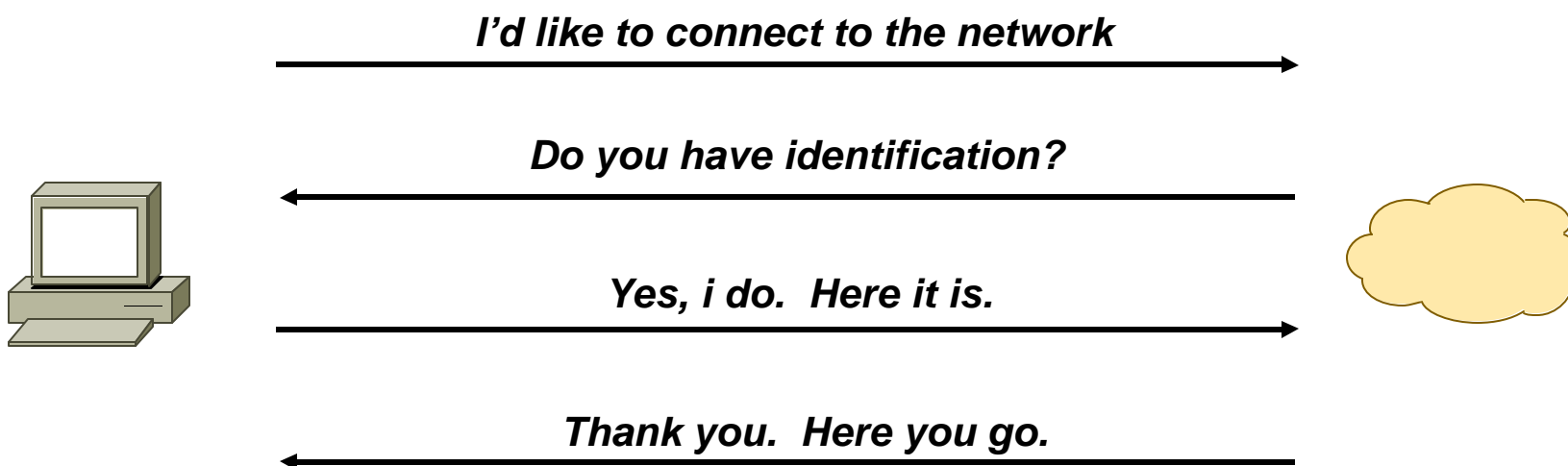
Port Based Network Authentication

Cisco.com

- **A client (a user or a device) requests a service — in this case access to the network**
- **Verify the client's claim of identity — authentication**
- **Grant or deny the services as per the policy — authorization**
- **Reference the configured policies for the requesting client**

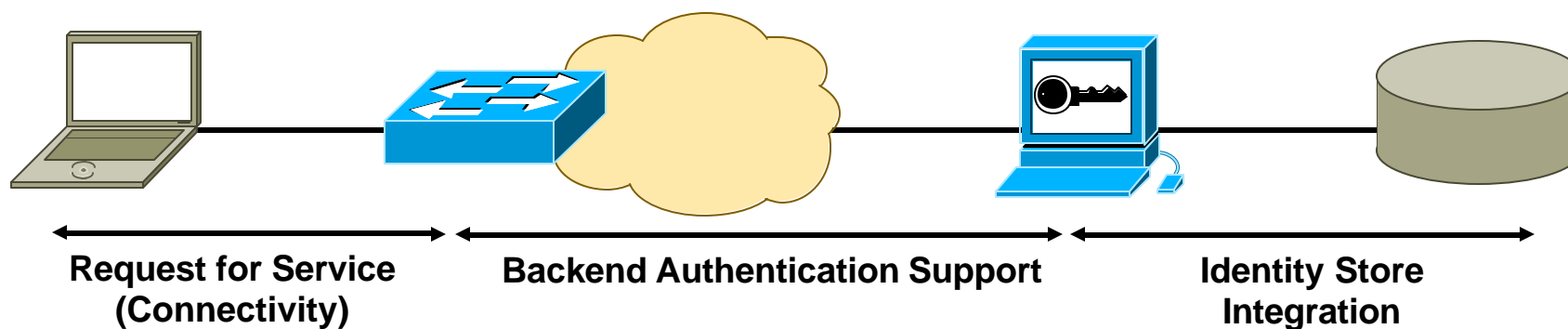
Applying the Authentication Model to the Network

Cisco.com

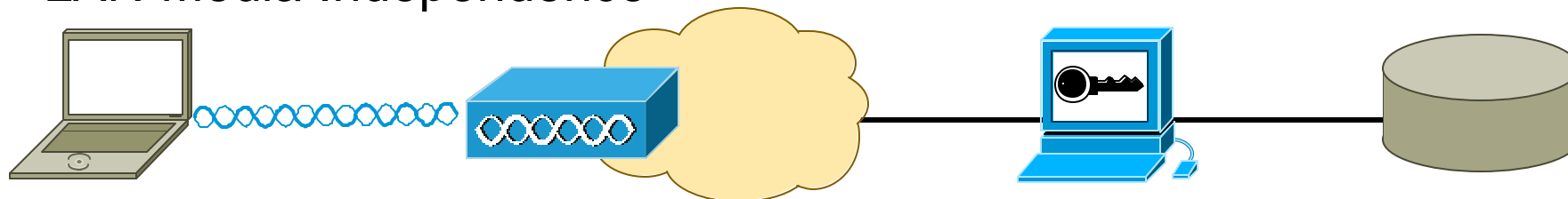


Network Access Control Model

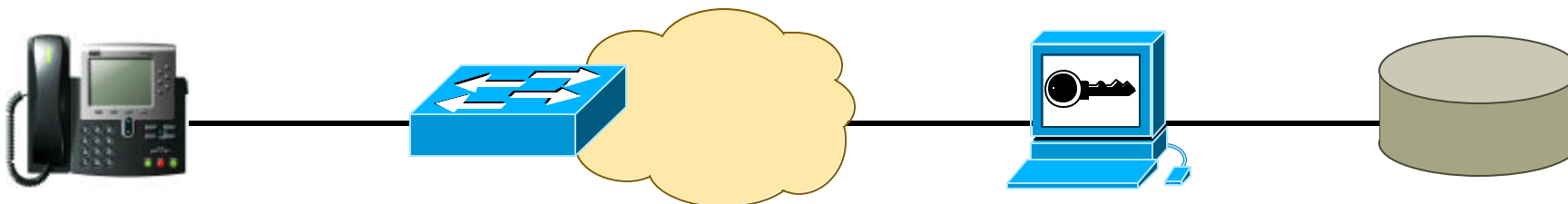
Cisco.com



LAN Media Independence



Device Authentication



Understanding the Protocols and Mechanisms Behind 802.1x



What Is EAP?

- **EAP—the Extensible Authentication Protocol**
- **A flexible transport protocol used to carry arbitrary authentication information - not the authentication method itself**
- **Rose out of need to reduce complexity of relationships between systems and increasing need for more elaborate and secure authentication methods**
- **Typically runs directly over data link layers such as PPP or IEEE 802 Media**
- **Originally specified in RFC 2284, obsoleted by RFC 3748**

What Does It Do?

- **Transports authentication information in the form of Extensible Authentication Protocol (EAP) payloads**
- **An switch or access point becomes a conduit for relaying EAP received in 802.1x packets to an authentication server by using RADIUS to carry EAP information**
- **Establishes and manages connection. Allows authentication by encapsulating various types of authentication exchanges. EAP messages can be encapsulated in the packets of other protocols, such as 802.1x or RADIUS**
- **Three forms of EAP are specified in the standard**
 - EAP-MD5—MD5 hashed username/password**
 - EAP-OTP—One-time passwords**
 - EAP-GTC—Token card implementations requiring user input**

Ethernet Header

802.1x Header

EAP Payload

Current Prevalent Authentication Methods

Cisco.com

- **Challenge-response-based**

EAP-MD5: Uses MD5 based challenge-response for authentication

LEAP: Uses username/password authentication

EAP-MSCHAPv2: Uses username/password MSCHAPv2 challenge-response authentication

- **Cryptographic-based**

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

- **Tunneling methods**

PEAP: Protected EAP tunnel mode EAP encapsulator; tunnels other EAP types in an encrypted tunnel—much like web based SSL

EAP-TTLS: Other EAP methods over an extended EAP-TLS encrypted tunnel

EAP-FAST: Recent tunneling method designed to not require certificates at all for deployment

- **Other**

EAP-GTC: Generic token and OTP authentication

- There are plenty of others
- Choosing an EAP type is a must

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**

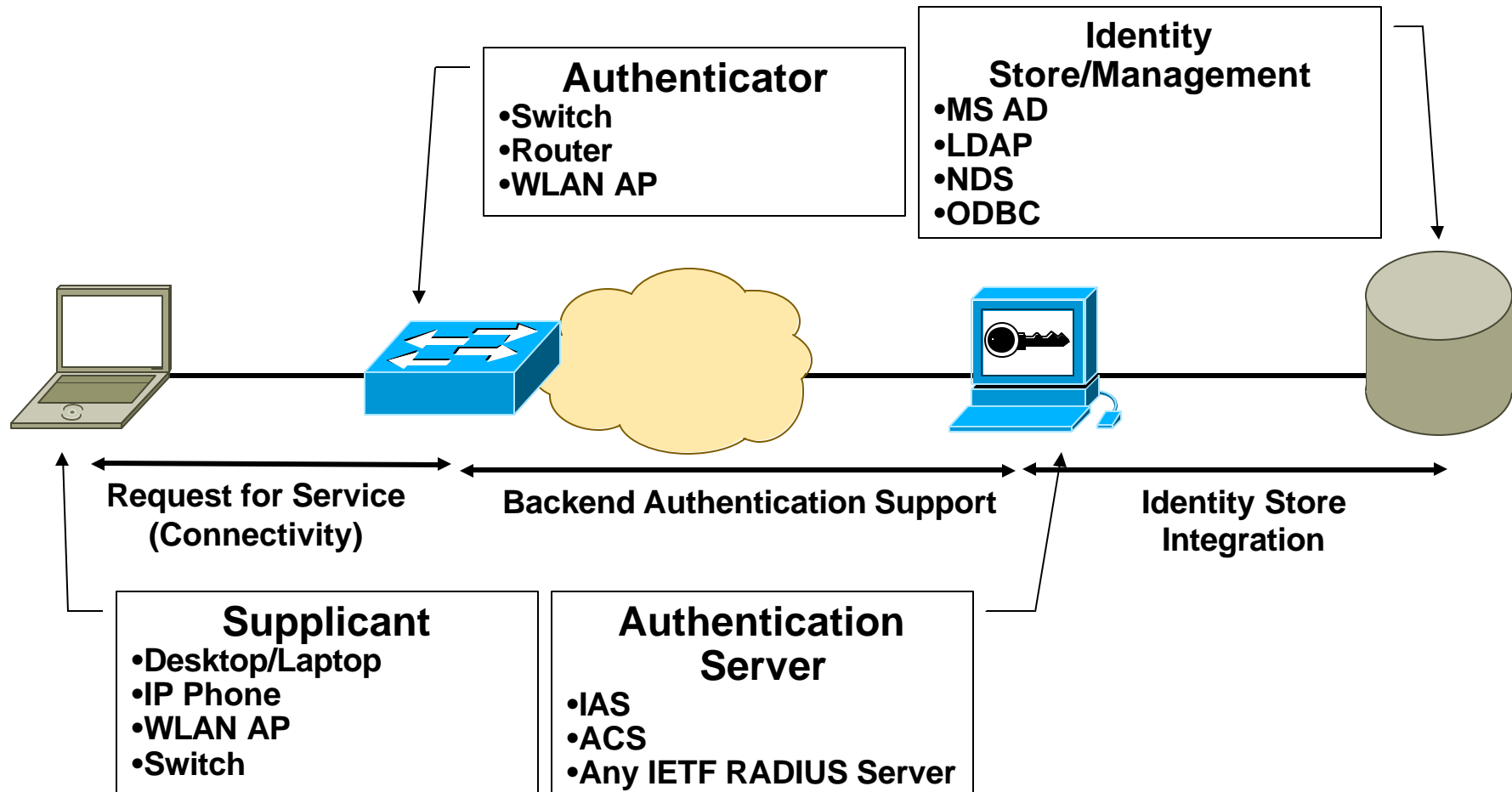
Some IEEE Terminology

Cisco.com

IEEE Terms	Normal People Terms
Supplicant	Client
Authenticator	Network Access Device
Authentication Server	AAA/RADIUS Server

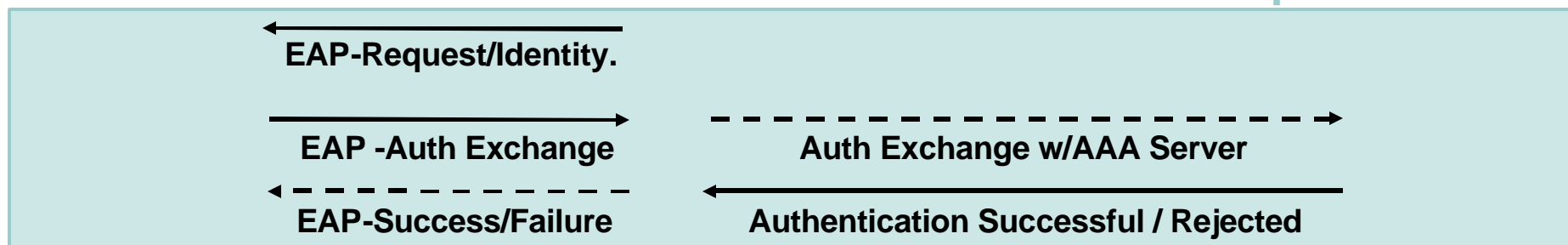
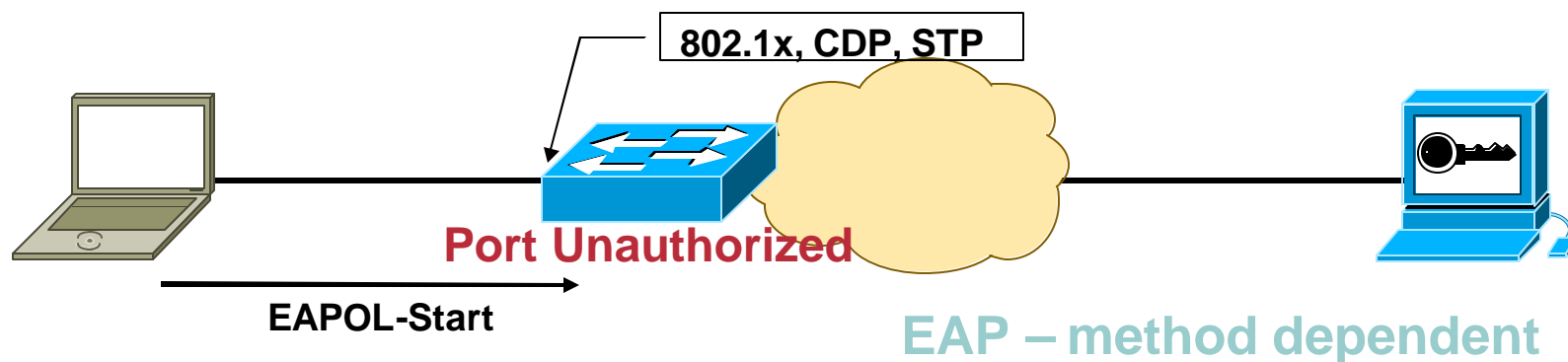
802.1x Port Access Control Model

Cisco.com



A Closer Look...

Cisco.com



Port Authorized

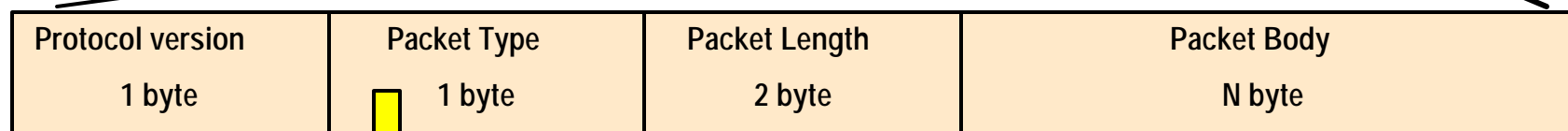
Policy Instructions



**Actual Authentication Conversation Is between Client and Auth Server Using EAP;
the Switch is an EAP conduit, but Is Aware of What's Going on**



EAPOL format



Packet Type	Packet Description
EAP Packet (0)	Both the supplicant and the authenticator send this packet Its used during authentication and contains MD5 or TLS information required to complete the authentication process
EAPOL Start (1)	Send by supplicant when it starts authentication process
EAPOL Logoff (2)	Send by supplicant when it wants to terminate the 802.1x session
EAPOL Key (3)	Send by switch to the supplicant and contains a key used during TLS authentication

How Is RADIUS Used Here?

- RADIUS acts as the transport for EAP, from the authenticator (switch) to the authentication server (RADIUS server)
- RFC for how RADIUS should support EAP between authenticator and authentication server - RFC 3579.



- RADIUS is also used to carry policy instructions back to the authenticator in the form of AV pairs



- Usage guideline for 802.1x authenticators use of RADIUS - RFC 3580.

Understanding the Default Security for 802.1x

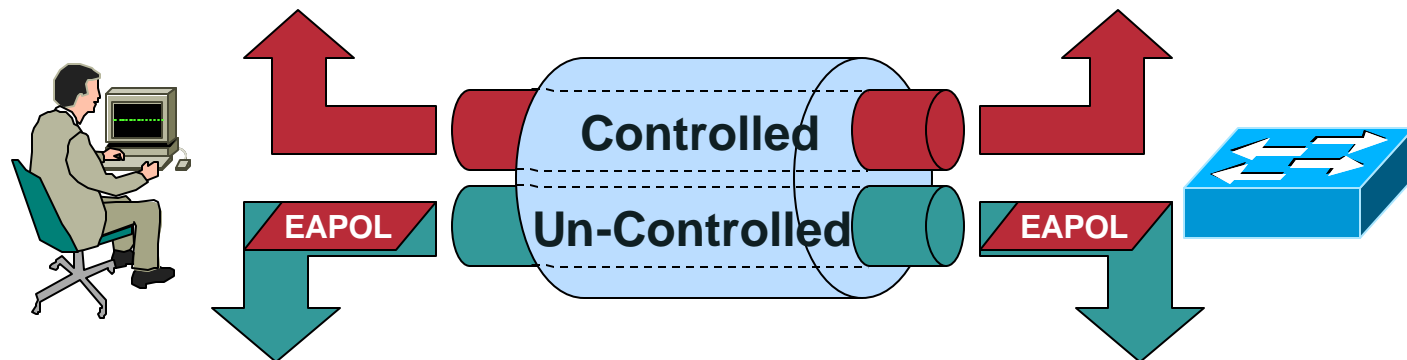


Default Security of 802.1x

Cisco.com

For each 802.1x switch port, the switch creates
TWO virtual access points at each port

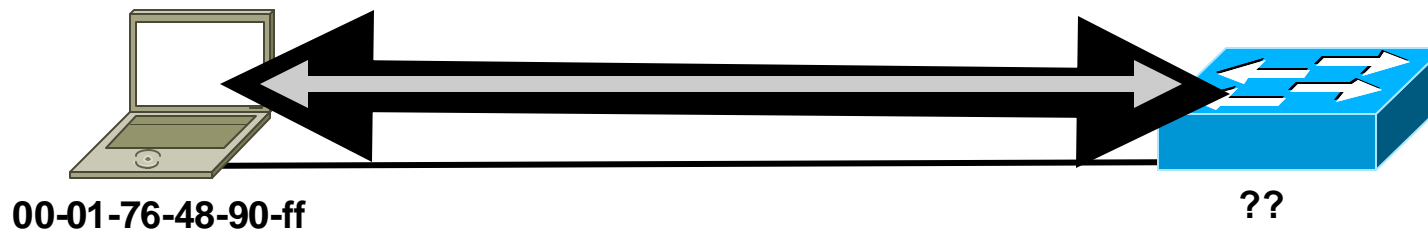
The controlled port is open only when the device connected to
the port has been authorized by 802.1x



Uncontrolled port provides a path for
Extensible Authentication Protocol over LAN (EAPOL) traffic **ONLY**

Default Security of 802.1x

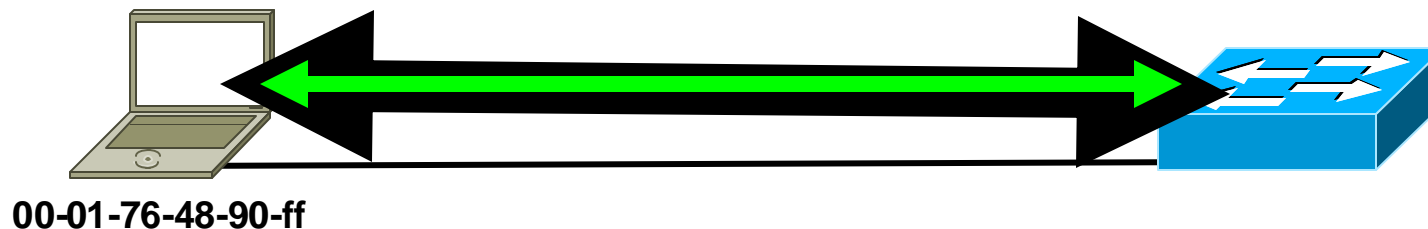
Cisco.com



- 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

Cisco.com



- **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

Cisco.com



CatOS

set port dot1x 5/1 port-control auto

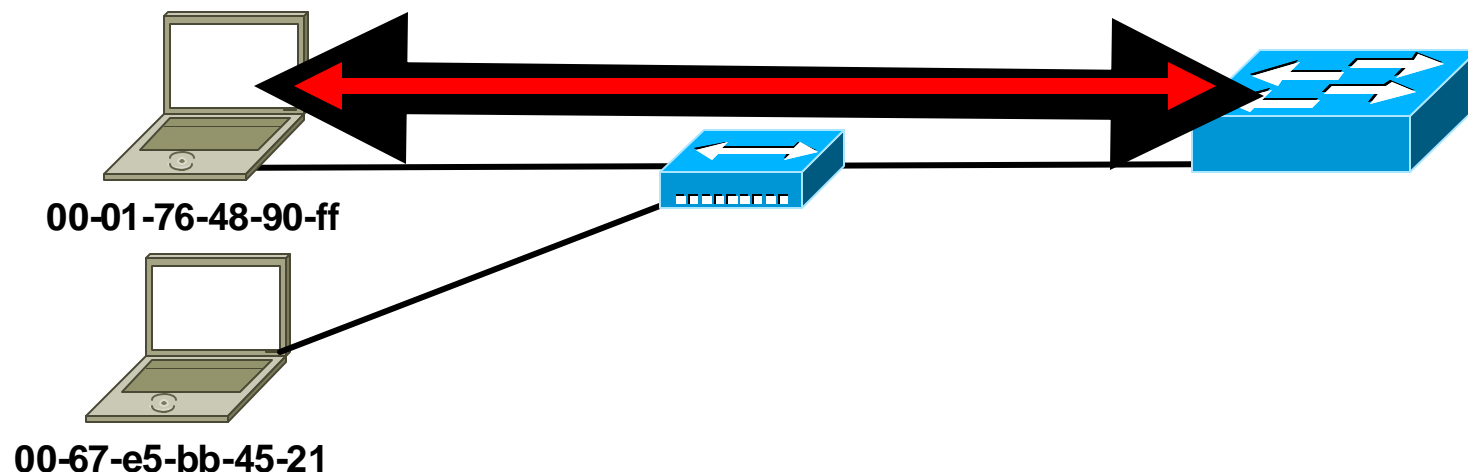
IOS

dot1x port-control auto

- **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

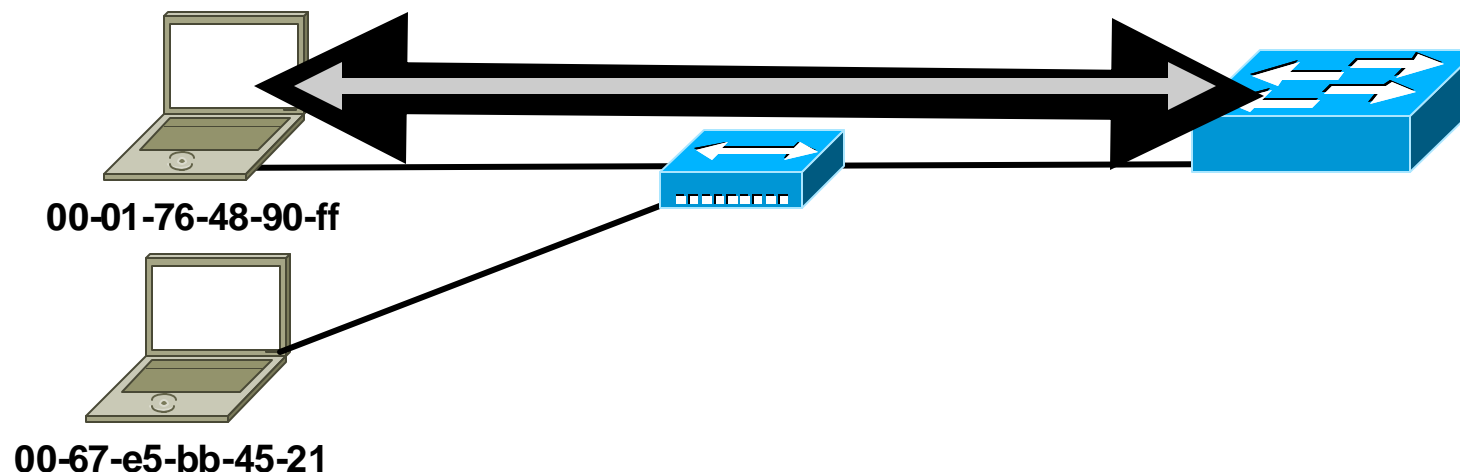
Cisco.com



- Additional MAC Addresses on wire treated as security violation
- This includes VMWARE type devices
- This includes machines that attempt to transmit gratuitous ARP frames
- **NOTE:** Any other type of data transmission or network attack is not within the scope of the 802.1x standard, nor the default deployment on a switch

Default Security of 802.1x

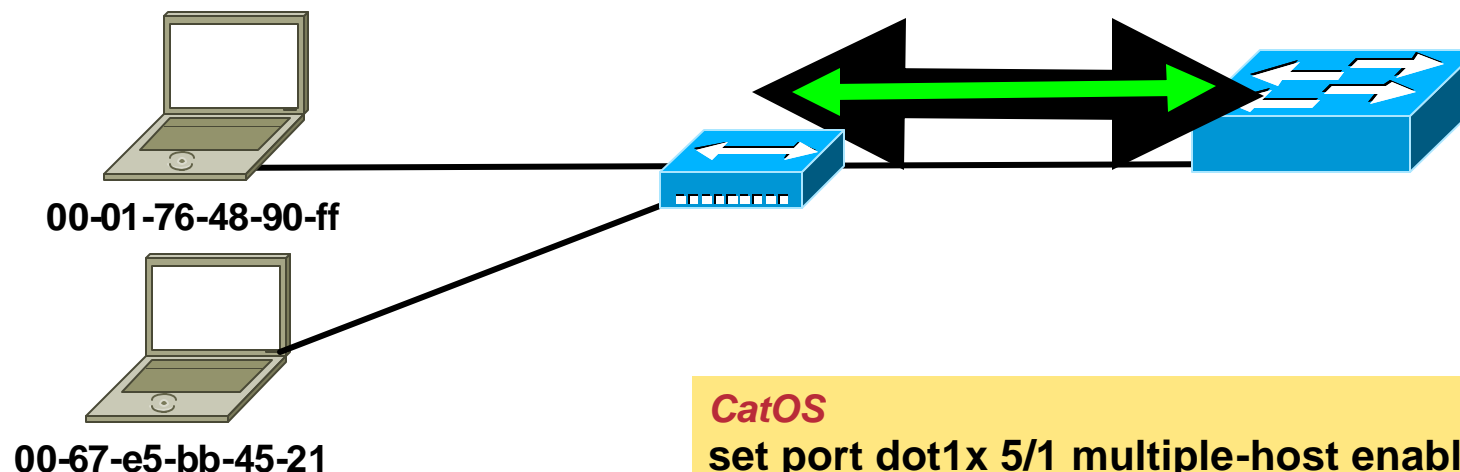
Cisco.com



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

Default Security of 802.1x

Cisco.com



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

CatOS

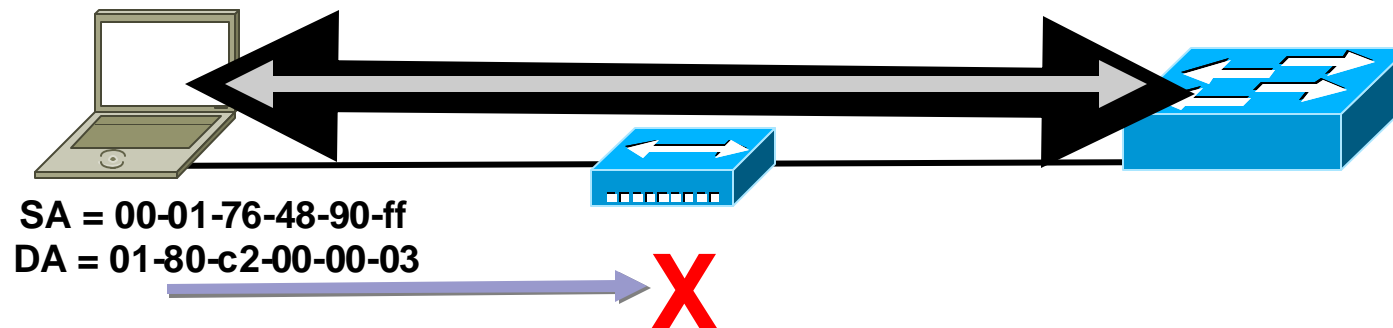
```
set port dot1x 5/1 multiple-host enable
set port security 5/1 enable
set port security 5/1 port max 3
set port security 5/1 age 2
```

IOS

```
dot1x host-mode multi-host
switchport port-security
switchport port-security maximum 3
switchport port-security aging time 2
```

Default Security of 802.1x

Cisco.com



- **Deployment consideration - The difference between a hub and a switch**
- **Switches that comply with 802.1D will discard EAPOL frames by design**
- **Most supplicants use 01-80-c2-00-00-03 in the absence of an association (like 802.11)**
- **This group MAC address is also one of the 16 addresses reserved by IEEE 802.1D in the Bridge Protocol Data Unit (BPDU) block**
- **This ensures that EAPOL is not transparently forwarded by a MAC bridge**

Identity-Based Integration Issues, Authorization and Policy Enforcement



IBNS Feature Support for Integration and Authorization

Cisco.com

- **Basic IEEE 802.1X Support**
- **IBNS: Some Extensions to 802.1x**

802.1X with Dynamic VLANs

802.1x with Private VLANs 

802.1X with VVID (IP Telephony)

802.1X Guest VLANs

802.1x with ACLs

802/1x with RADIUS Accounting

802.1x with QoS Profile

802.1x with Wake on LAN

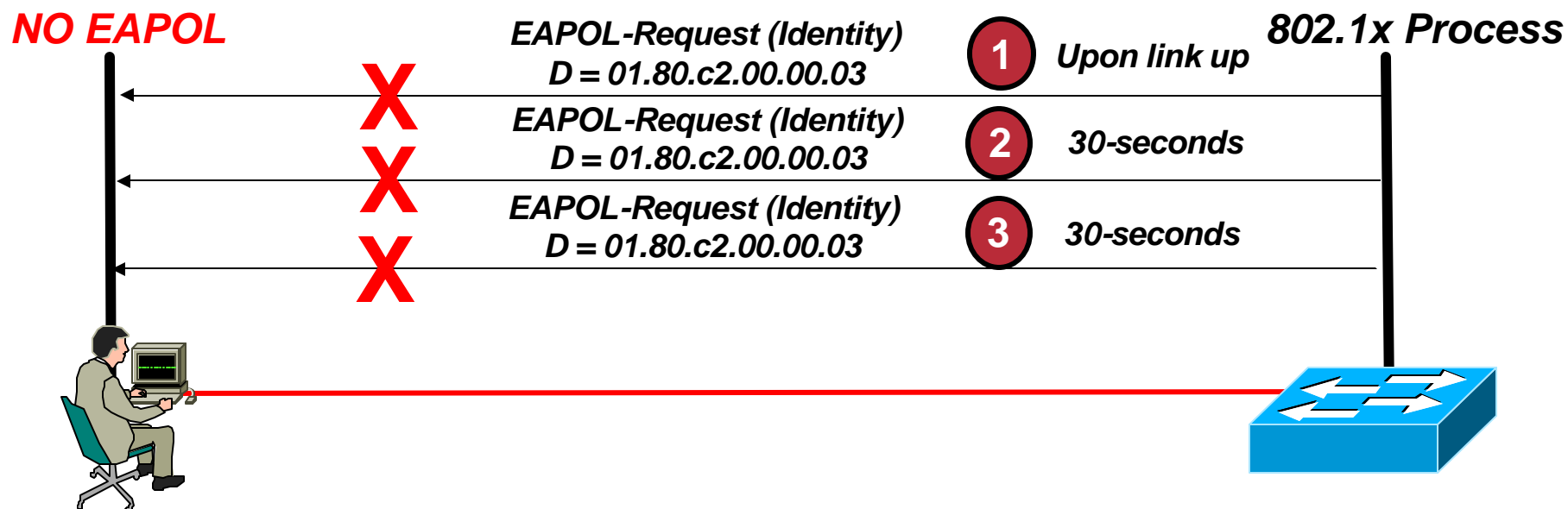
- **Enhanced Admissions Control**
- **Greater flexibility and mobility for a stratified user community**
- **Enhanced User Productivity**
- **Lowered Operational Expenses**
- **Additional Security with converged VoIP networks**

Integration

- **Integration is key to making 802.1x and IBNS deployable**
- **How do you deal with devices that cannot speak 802.1x?**
- **How does voice interoperate with port-based access control?**
- **How do you support PC applications like remote wakeup / Wake-on-LAN?**
- **How do you provide network visibility for authenticated identities?**

802.1x - Default Operation

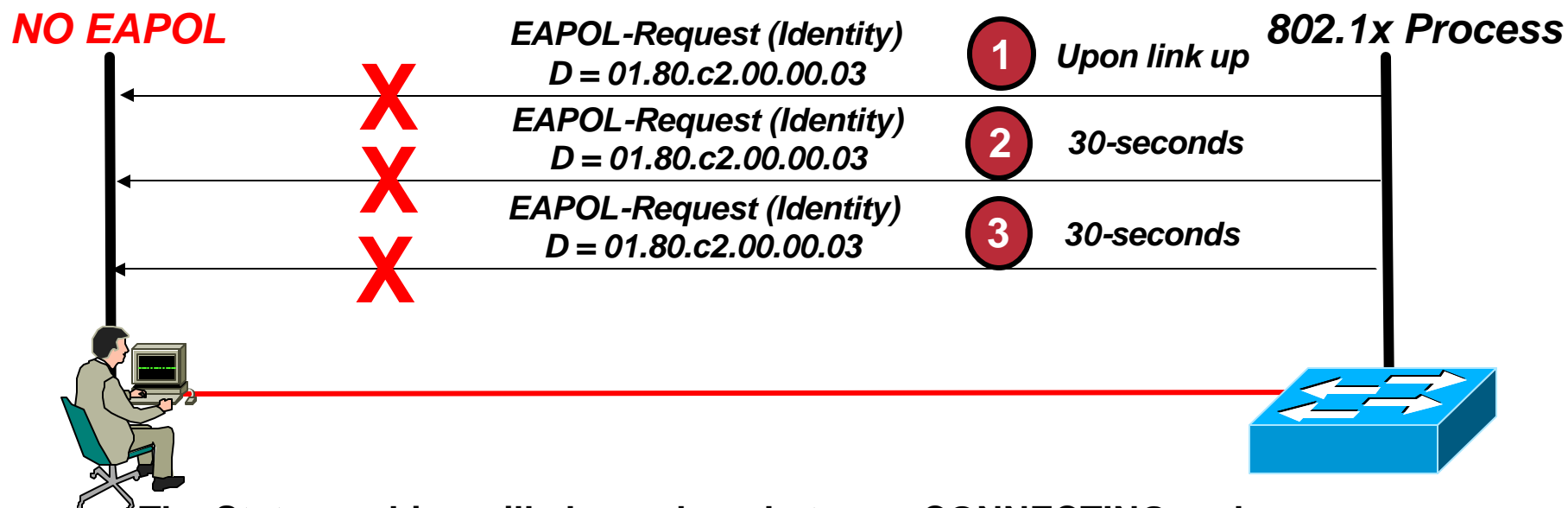
Cisco.com



- 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
- State machine transitions to a DISCONNECTED state
- No network access is given.
- DISCONNECTED state is deployed after step 3 above.

802.1x - Default Operation

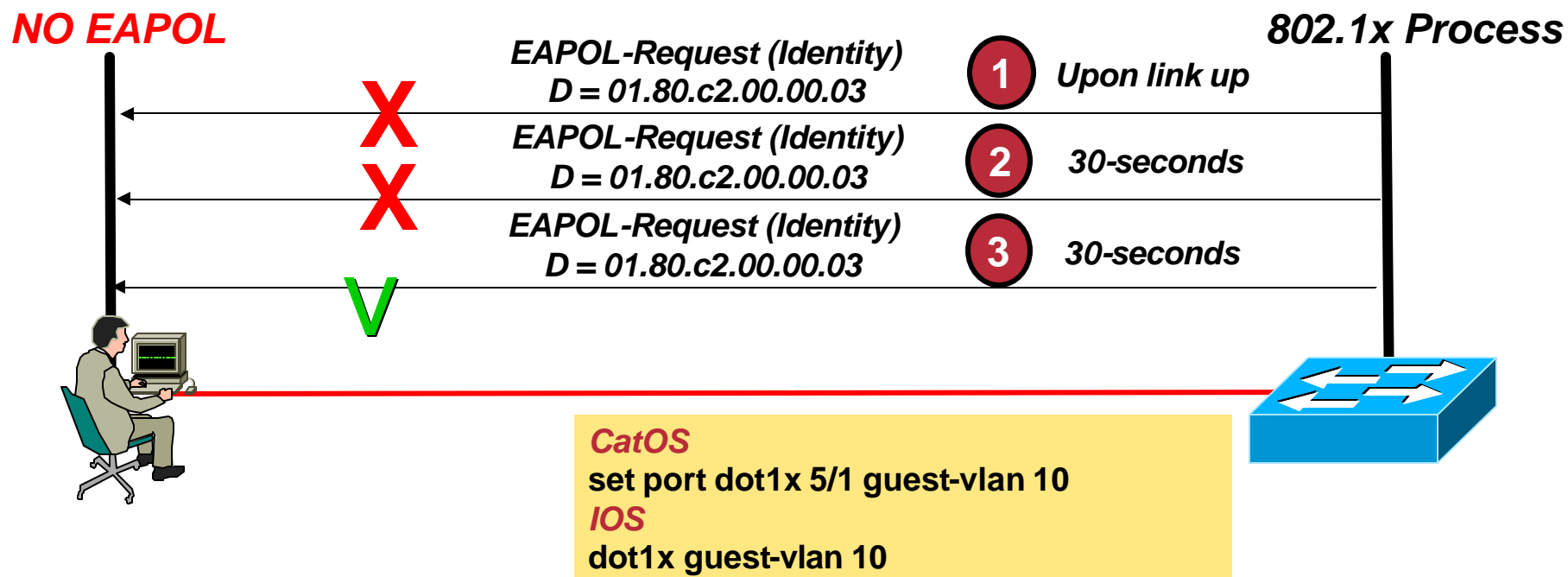
Cisco.com



- The State machine will always loop between **CONNECTING** and **DISCONNECTED** states
- **DISCONNECTED** is a transient state
- The Port-Status is **UNAUTHORIZED** and the Auth-SM state is usually **CONNECTING** since there is no supplicant on the wire
- The only thing that can transition a port from a **CONNECTING** or **DISCONNECTED** state is an EAPOL-Start from a supplicant, or if the periodic EAPOL-Identity-Frames from the switch begin to be answered by a supplicant that appears on the wire (via EAPOL-Identity-Response frames).

802.1x with Guest VLAN

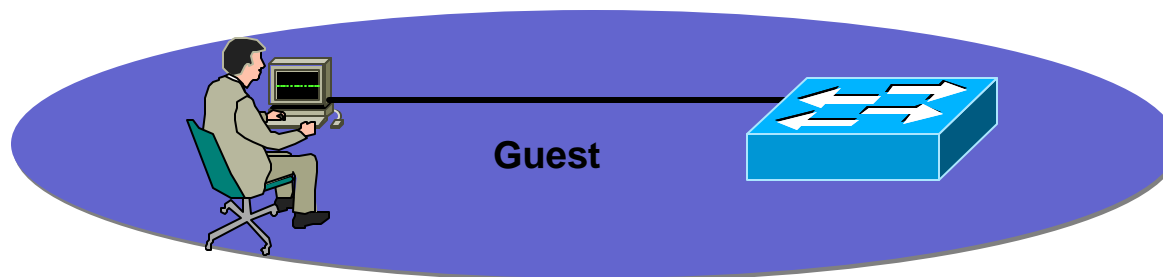
Cisco.com



- 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 3 above. Instead of transitioning to DISCONNECTED, the port immediately transitions to a state of AUTHORIZED and the Auth-SM state is AUTHENTICATED.

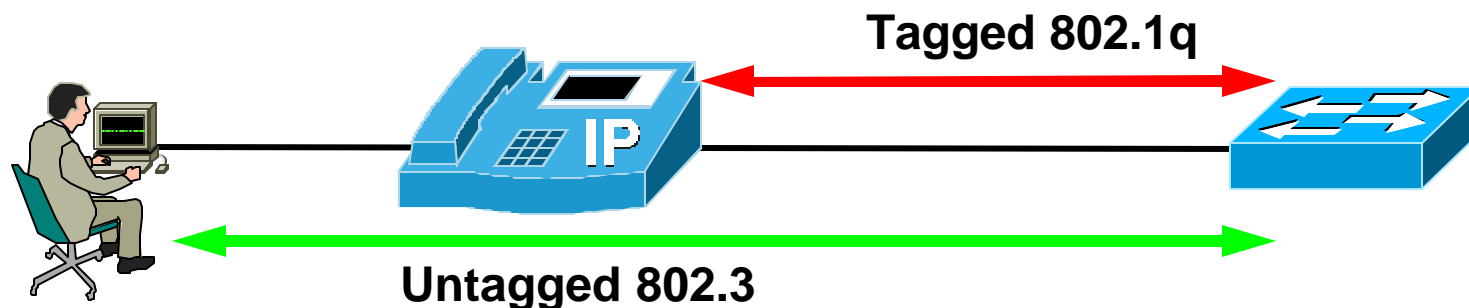
802.1x with Guest VLAN

- Default timeout is 30 seconds with 3 retries. Total timeout period is 90 seconds by default.
- A device is deployed to Guest VLAN based on lack of response to switch's EAPOL-Identity-Request frames (which can be thought of as 802.1x hellos)
- No further security or authentication to be applied.
- It is exactly like the administrator de-configured 802.1x, and hard-set the port into a determined VLAN
- No machines that speak 802.1x (or who can indeed respond to the switch via EAPOL) should ever go into the Guest VLAN.
- No passed or failed 802.1x authentication attempt should have anything to do with the Guest VLAN



802.1x with VVID

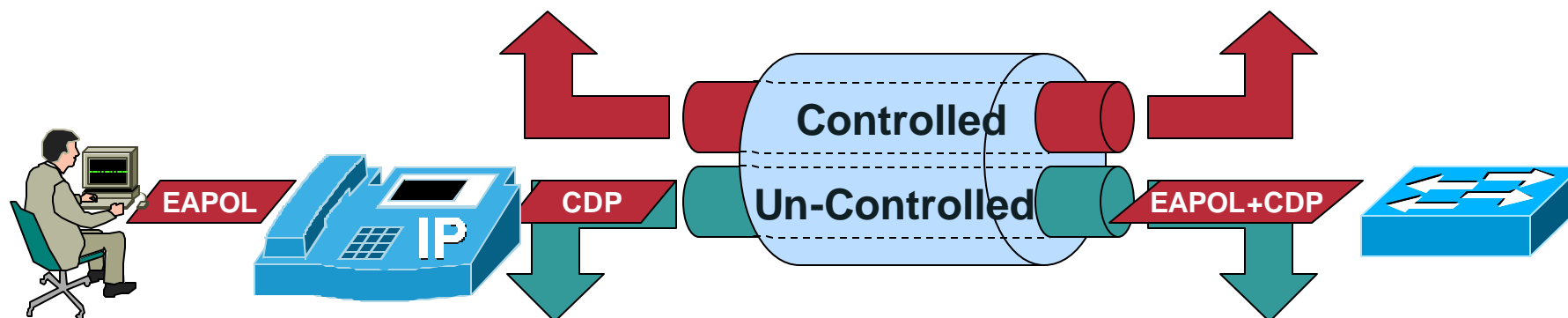
- **Multi-VLAN Access Ports (MVAP)**
With Multi-VLAN access ports, a port can belong to two VLANs, while still allowing the separation of voice/data traffic while enabling you to configure 802.1x.
- **An access port able to handle 2 VLANs**
Native or Port VLAN Identifier (PVID)
Auxiliary or Voice VLAN 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

- A dot1x-vvid port is an MVAP, that has dot1x configured.
- 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.



CatOS

```
set vlan 2 5/1
set port auxiliaryvlan 5/1 12
set port dot1x 5/1 port-control auto
```

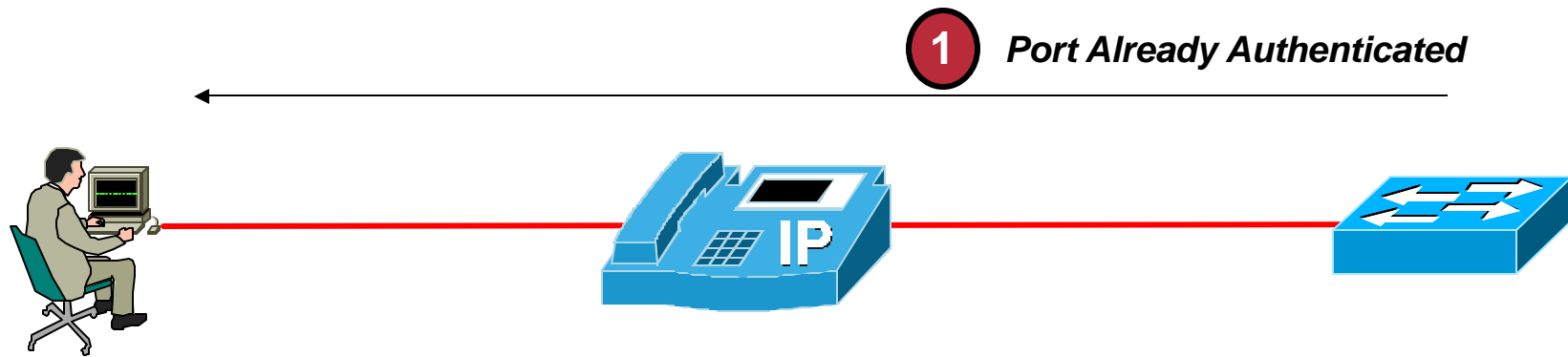
IOS

```
switchport mode access
switchport access vlan 2
switchport voice vlan 12
dot1x port-control auto
```

- Unauthenticated Voice VLAN (VVID) access
- Authenticated Data VLAN (PVID) access.
- This allows 802.1x and VoIP to co-exist at the same time.

802.1x with VVID - Previous Limitations

Cisco.com



802.1x with VVID - Previous Limitations

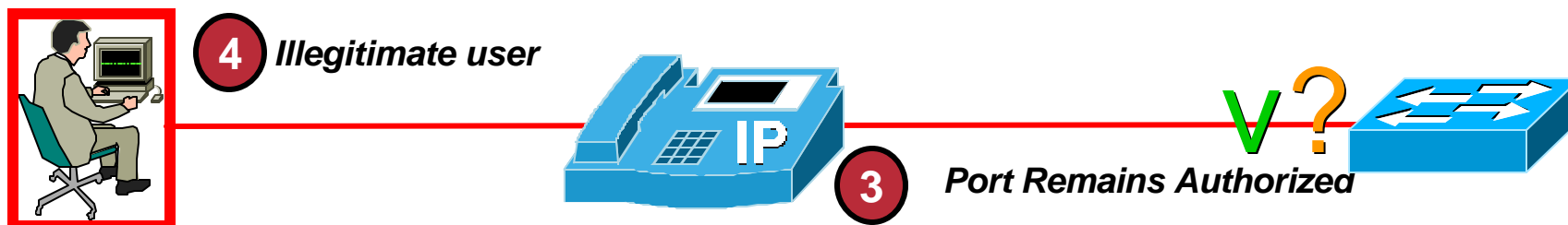
Cisco.com



- If an end-user disconnects, the port remains authorized by 802.1x.

802.1x with VVID - Previous Limitations

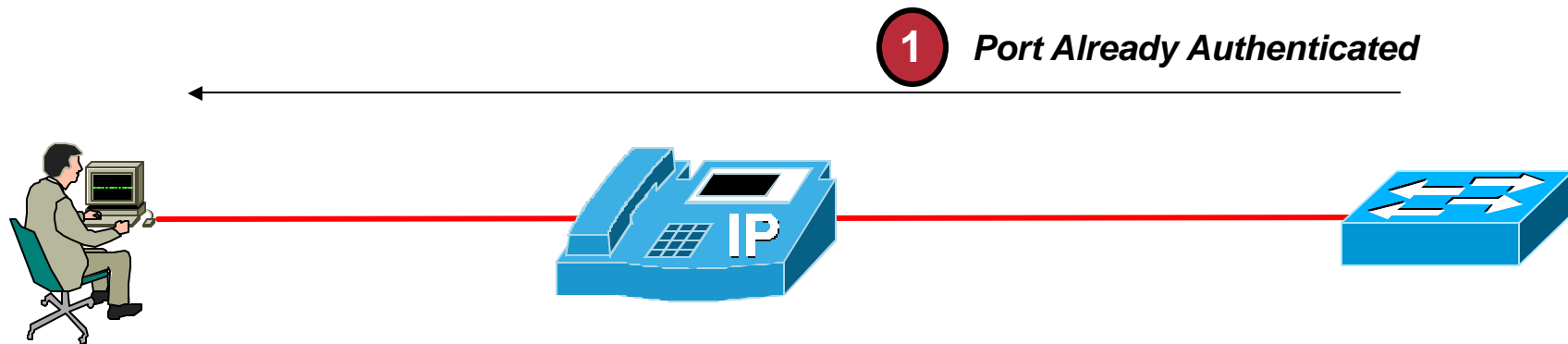
Cisco.com



- An illegitimate user can now gain access to the port by **spoofing** the authenticated MAC Address, and bypass 802.1x completely -- **SECURITY HOLE.**
- In an attempt to workaround this, some customers have enabled periodic re-authentication of end-devices.
- This is not the reason to enable re-authentication.
- We need to deal with the fact that any machine can disappear from the network and the switch (and 802.1x) does not know about it explicitly (i.e. link doesn't go down).

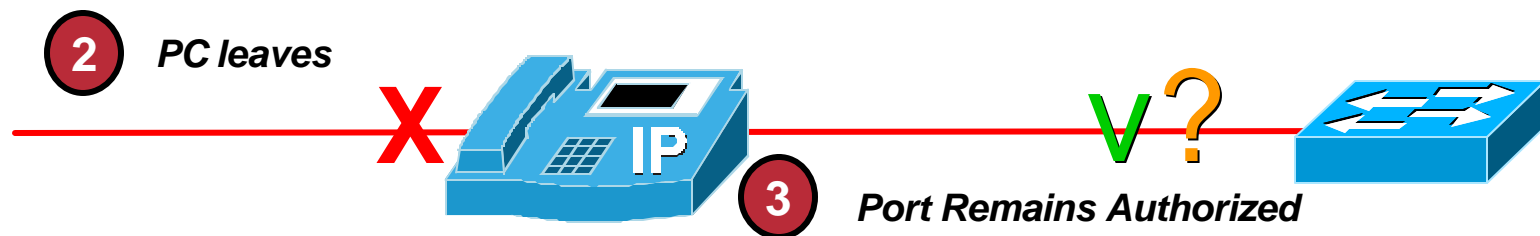
802.1x with VVID - Previous Limitations

Cisco.com



802.1x with VVID - Previous Limitations

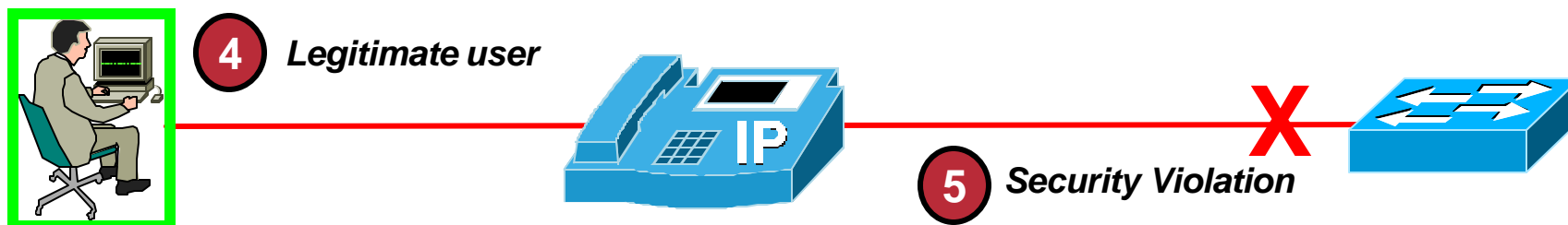
Cisco.com



- If an end-user disconnects, the port remains authorized by 802.1x.

802.1x with VVID - Previous Limitations

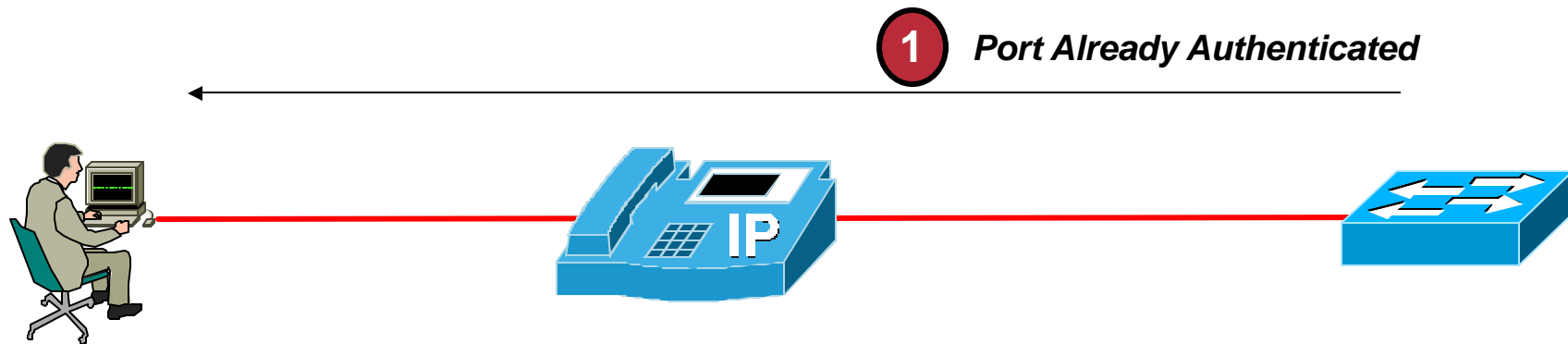
Cisco.com



- 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!
- In an attempt to workaround this, some customers have enabled periodic re-authentication of end-devices.
- This is not the reason to enable re-authentication.
- Overall, same issue as previous slides.

802.1x with VVID - EAPOL-Logoff

Cisco.com



802.1x with VVID - EAPOL-Logoff

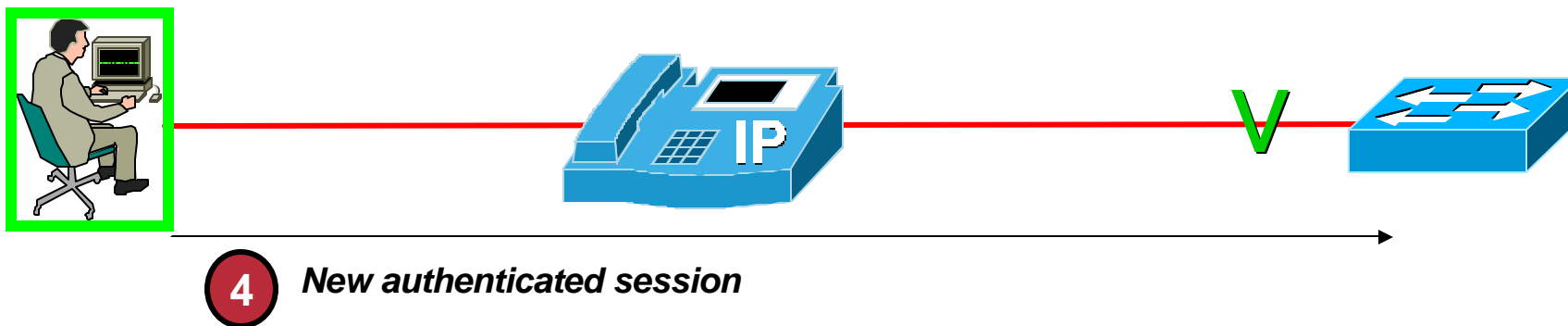
Cisco.com



- 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 (PAE group address)
- Two basic functions needed from phone
 - 1) Monitor the PAE group address to determine who and where supplicant is.
 - 2) Actually transmit the EAPOL-Logoff frame.

802.1x with VVID - EAPOL-Logoff

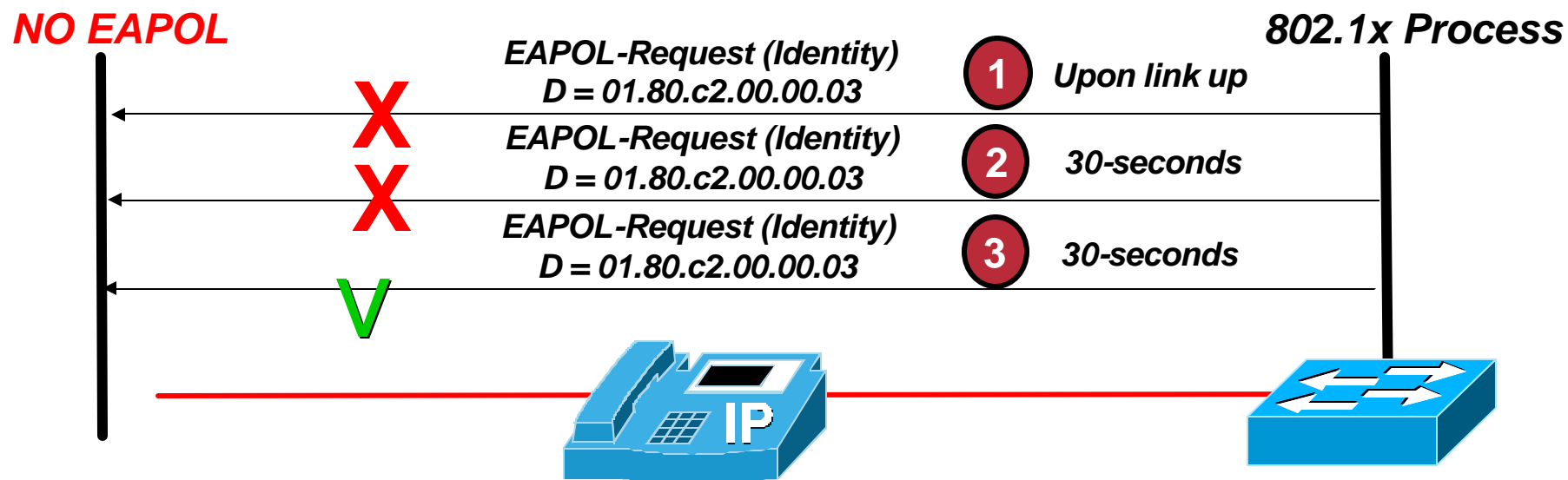
Cisco.com



- 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

802.1x with VVID - Deployment issues

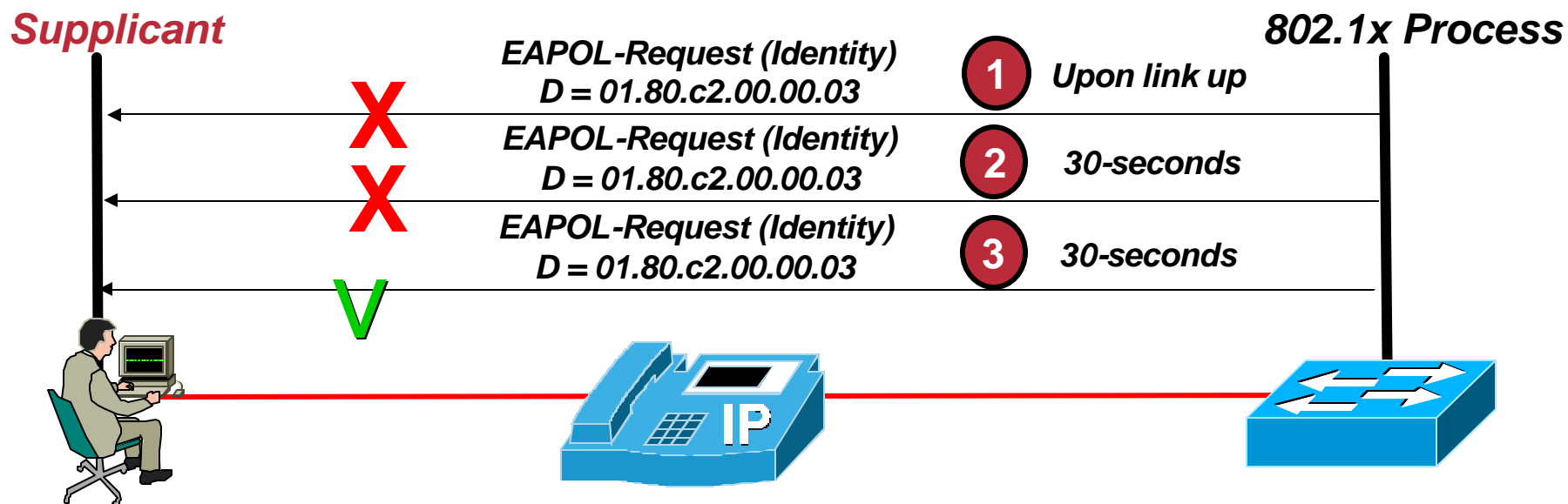
Cisco.com



- Assuming no supplicant on the wire, a port will be deployed into the Guest-VLAN after Step3 above, if Guest-VLAN is configured

802.1x with VVID - Deployment issues

Cisco.com



- If any user plugs into a phone, 802.1x is now totally dependent on how their supplicant is configured to operate.
- By default, **Microsoft Windows supplicants do NOT send EAPOL-Starts**. You will want to know why 802.1x works when you plug into a switch, and why it doesn't work when you plug into a phone!

802.1x with WoL

Cisco.com

Supplicant

802.1x Process



```
id-6506-1> (enable) sho port dot1x 3/11
Port  Auth-State      BEnd-State  Port-Control  Port-Status
-----
3/11  connecting         idle       auto          unauthorized

Port  Port-Mode      Re-authentication  Shutdown-timeout  Control-Mode
-----
3/11  MultiHost     disabled          disabled          admin   oper
                                     Both   Both
```

Notice the default control mode

802.1x with WoL

Cisco.com

Supplicant

802.1x Process

CatOS
set port dot1x 5/1 port-control-direction in
IOS
dot1x control-direction in



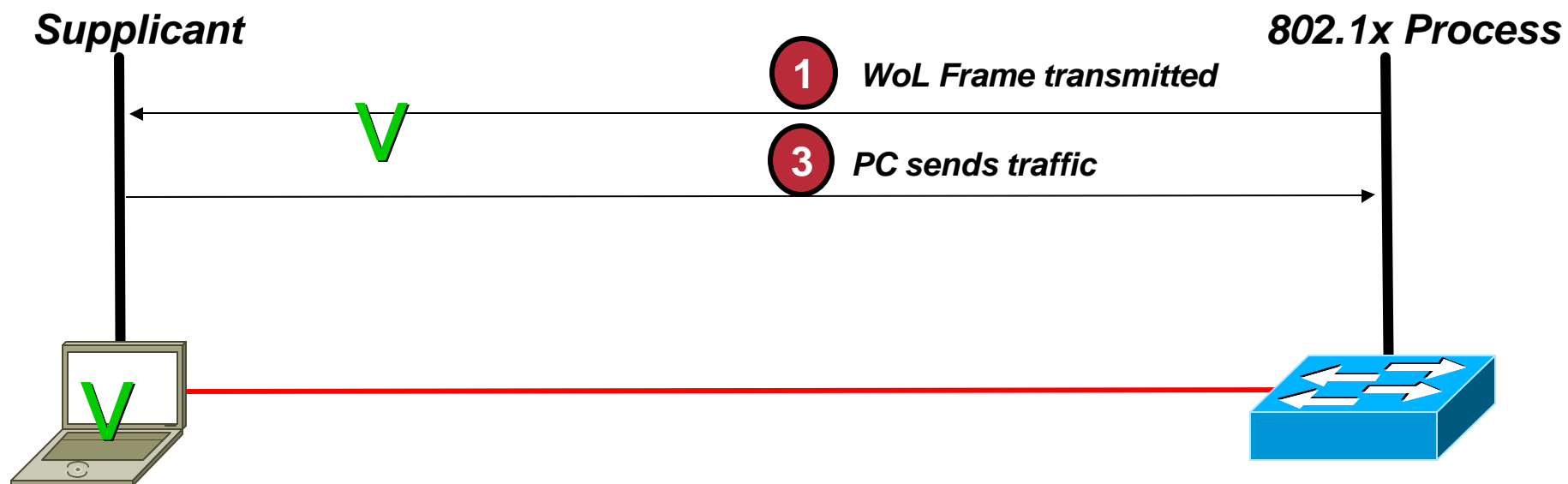
Port	Auth-State	BEnd-State	Port-Control	Port-Status
3/11	connecting	idle	auto	unauthorized

Port	Port-Mode	Re-authentication	Shutdown-timeout	Control-Mode
3/11	SingleAuth	disabled	disabled	In In

Notice the control mode

802.1x with WoL

Cisco.com



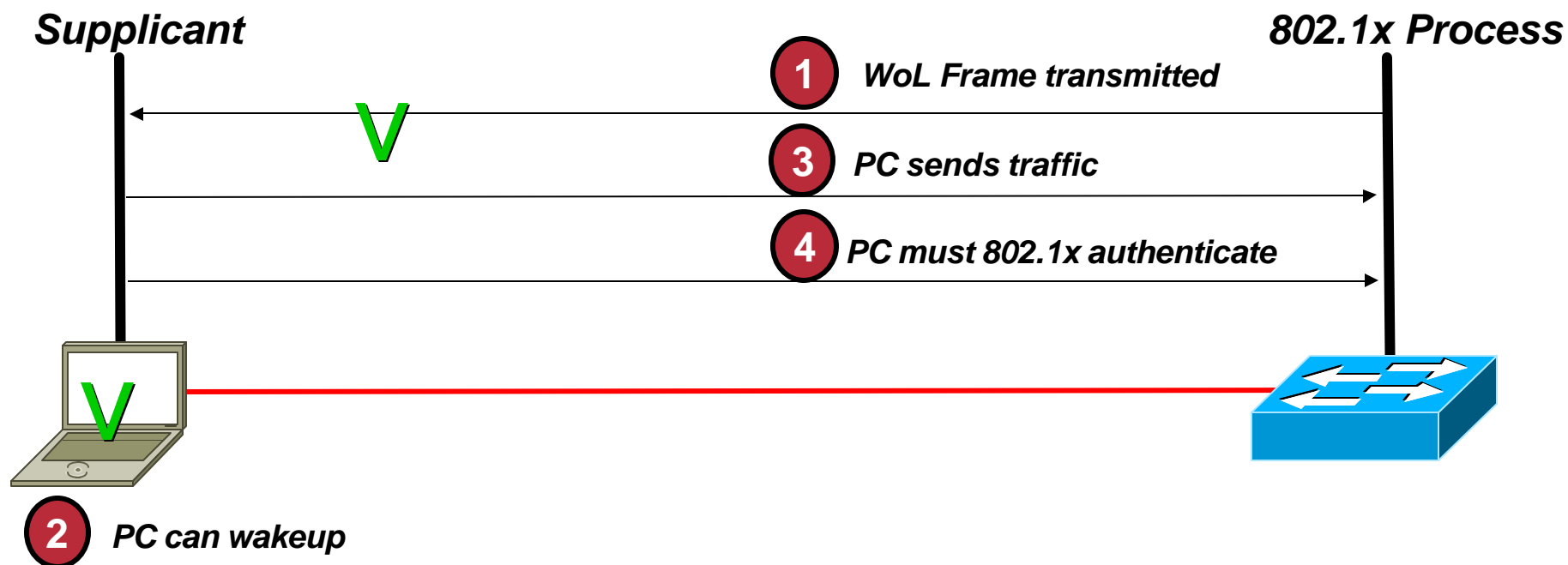
Notice the mode now

```
id-6506-1> (enable) sho port dot1x 3/6
Port  Auth-State      BEnd-State Port-Control  Port-Status
-----
3/6   authenticated      idle         auto           authorized

Port  Port-Mode      Re-authentication  Shutdown-timeout  Control-Mode
-----
3/6   SingleAuth     disabled           disabled           admin    oper
                                     In      Both
```


802.1x with WoL

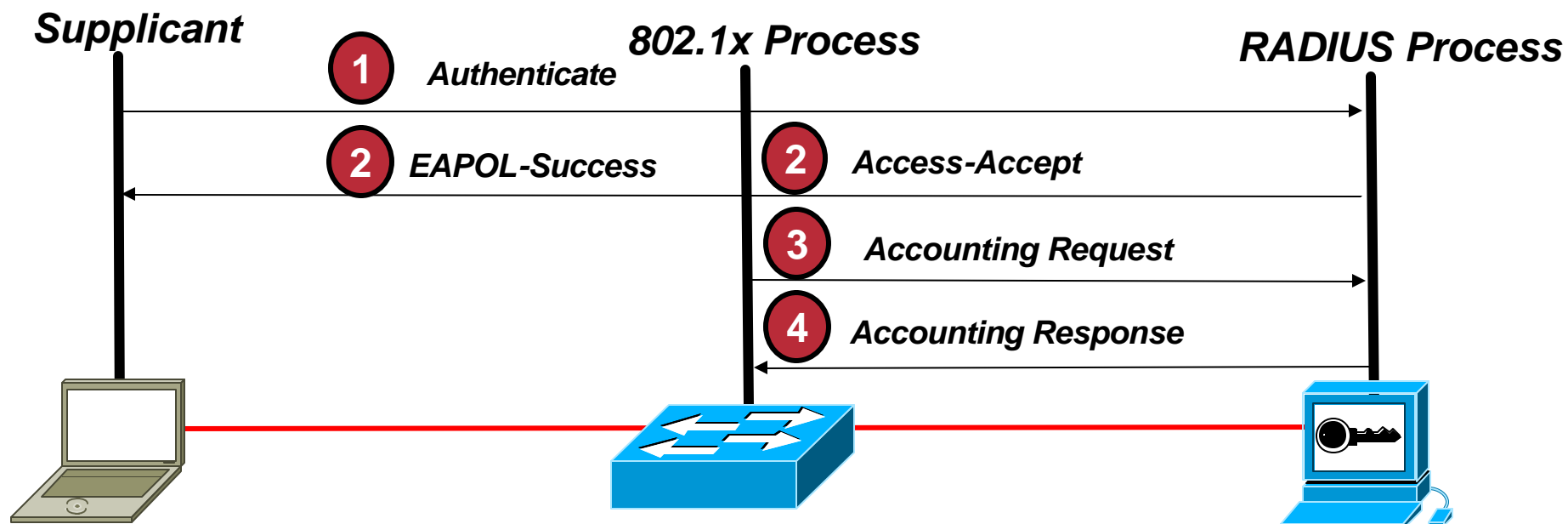
Cisco.com



- Outgoing traffic from a port allowed
- Still dropping all incoming traffic on a port that has not yet authorized.
- Once traffic sensed on wire, port reverts back to default mode and PC must authenticate

802.1x with RADIUS Accounting

Cisco.com



- **Accounting-Request packets**
- **Contains one or more AV pairs to report various events and related information to the Radius server**
- **Tracking user-level events are used in the same mechanism**

802.1x with RADIUS Accounting

Cisco.com

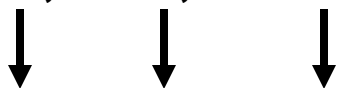
- Similar to other accounting and tracking mechanisms that already exist using RADIUS

Can now be done through 802.1x.

- Increases network session awareness
- Provide information into a management infrastructure about who logs in, session duration, support basic billing usage reporting, etc.

- Provides a means to map the information of authenticated:

Identity, Port, MAC, Switch



IP, Port, MAC, Switch

=

Identity → IP

Switch + Port = Location

CatOS

set dot1x radius-accounting enable

IOS

aaa accounting dot1x default start-stop group radius

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 and IBNS 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

Cisco.com

- 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>



CatOS

RADIUS attributes received in CatOS are automatically implemented if 802.1x is enabled.

IOS

aaa authorization network default group radius

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

802.1x with VLAN Assignment

Cisco.com

- **Dynamic VLAN assignment based on identity of group, or individual, at the time of authentication**
- **VLANs assigned by name—allows for more flexible VLAN management**
- **Allows Dynamic VLAN policies to be applied to groups of users (i.e., VLAN QoS, VLAN ACLs, etc.)**
- **Tunnel Attributes used to send back VLAN configuration information to authenticator.**
- **Tunnel Attributes are defined by RFC 2868**
- **Usage for VLANs is specified in the 802.1x standard**

802.1x with ACL Assignment

Cisco.com

- Vendor Specific Attributes used for RADIUS

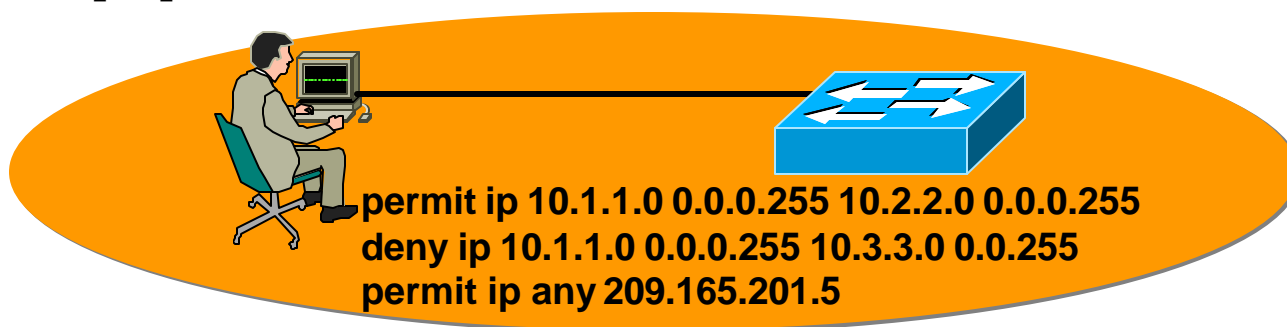
- [026] - vendor specific

- [009] - vendor ID for Cisco

- [001] - refers to the VSA number

- Attribute used for pre-defined ACLs

- [11] - Filter-ID



CatOS

RADIUS attributes received in CatOS are automatically implemented if 802.1x is enabled.

IOS

aaa authorization network default group radius

802.1x with ACLs

The screenshot displays the Cisco IOS configuration interface for a RADIUS server. The left sidebar contains navigation options: Group Setup, Shared Profile Components, Network Configuration, System Configuration, and Interface Configuration. The main window is titled "Cisco IOS/PIX RADIUS" and shows the configuration for a RADIUS group named "cisco-av-pair". The configuration includes a checkmark for "[009\001] cisco-av-pair" and a text area containing the following commands:

```
ip:inacl#1=deny ip any host
10.1.8.3
ip:inacl#2=permit ip any any
```

On the right, there is a "Cisco.com" header and a configuration panel with the following options:

- ☐ [010] Framed-Routing (set to None)
- ☒ [011] Filter-Id (set to acl=eng)
- ☐ [012] Framed-MTU (64..65535)

At the bottom right, a terminal window shows the output of the following commands:

```
id-3550-5#sho dot1x interface f0/7
Supplicant MAC 00e0.8105.8d93
AuthSM State = AUTHENTICATED
BendSM State = IDLE
PortStatus = AUTHORIZED
MaxReq = 2
HostMode = Single
Port Control = Auto
QuietPeriod = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod = 3600 Seconds
ServerTimeout = 30 Seconds
SuppTimeout = 30 Seconds
TxPeriod = 30 Seconds
Guest-Vlan = 0

id-3550-5#sho access-lists
Extended IP access list FastEthernet0/7#0 (per-user)
deny ip any host 10.1.8.3
permit ip any any
```

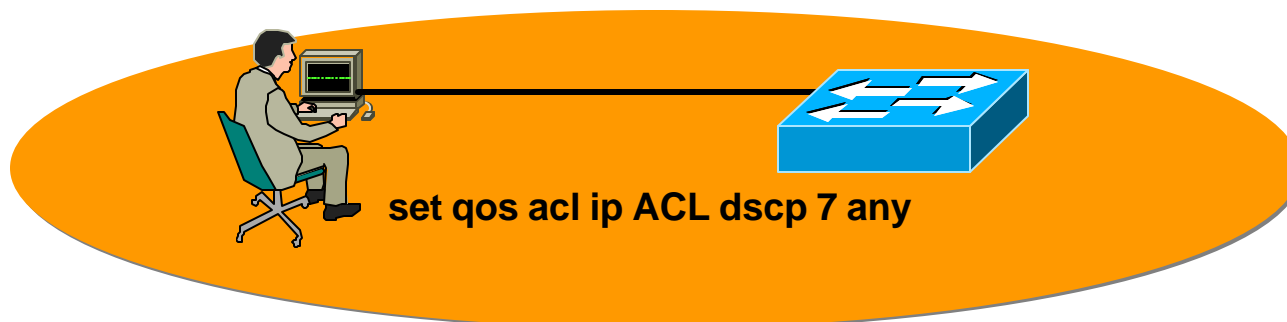

802.1x with QoS Policy

- Vendor Specific Attributes used for RADIUS

[026] - vendor specific

[009] - vendor ID for Cisco

[001] - refers to the VSA number



CatOS


RADIUS attributes received in CatOS are automatically implemented if 802.1x is enabled.

IOS

`aaa authorization network default group radius`

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

802.1x with QoS Policy

Cisco IOS/PIX RADIUS Attributes

☒ [009\001] cisco-av-pair

qos:inpacl=Team1QoSACL

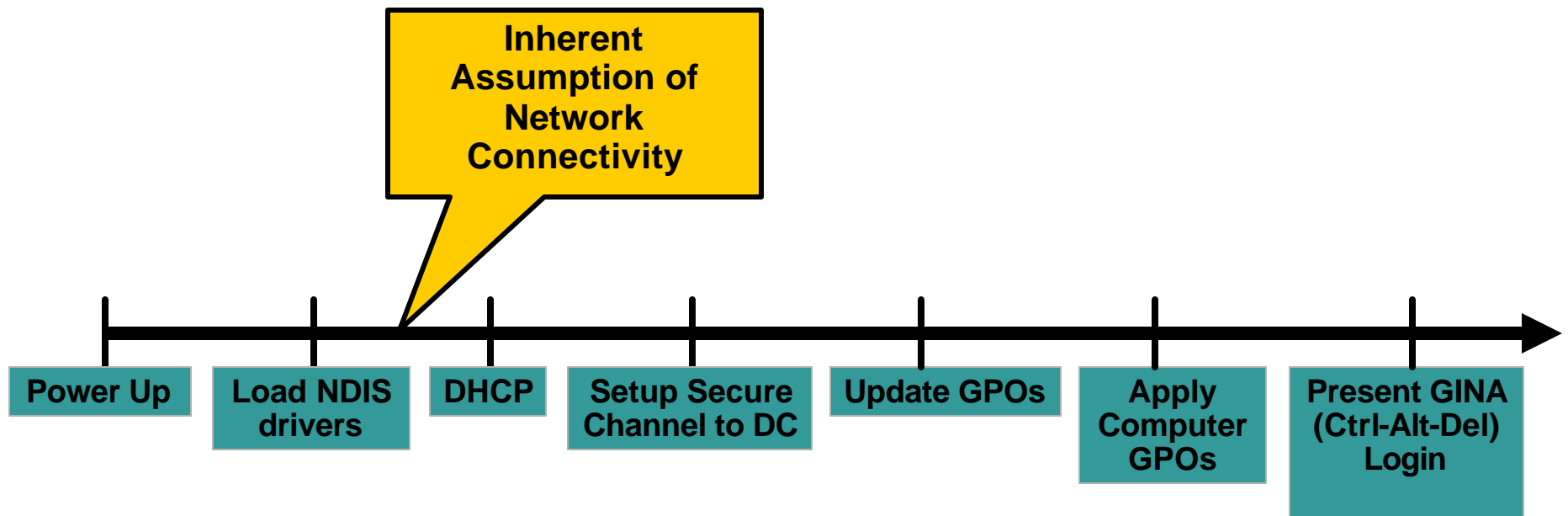
```
id-switch> (enable)
id-switch> (enable) sho qos acl map runtime Team1QoSACL
QoS ACL mappings on input side:
ACL name                               Type Vlan
-----
Team1QoSACL                             IP
ACL name                               Type Ports
-----
Team1QoSACL                             IP 3/11
QoS ACL mappings on output side:
ACL name                               Type Vlan
-----
Team1QoSACL                             IP
id-switch> (enable)
```

Operating System Implementations and Supplicants in Different Environments



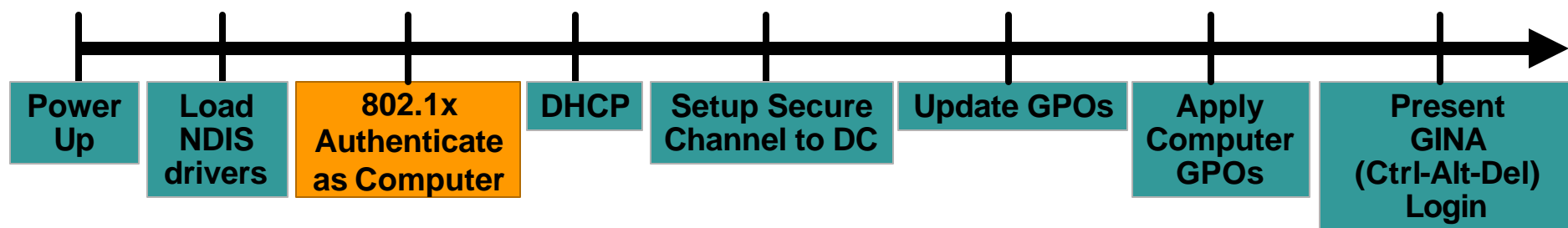
Windows Boot Cycle Overview

Cisco.com



Windows Machine Authentication

Cisco.com



Microsoft and Machine Authentication

- **What is Machine Authentication?**

The ability of a Windows workstation to authenticate under its own identity, independent of the requirement for an interactive user session

- **What is it used for?**


Machine authentication is used at boot time by Windows OSes to authenticate and communicate with Windows Domain Controllers in order to pull down machine group policies

- **Why do we care?**

Pre-802.1x this worked under the assumption that network connectivity was a given; post-802.1x the blocking of network access prior to 802.1x authentication breaks the machine-based group policy model—UNLESS the machine can authenticate using its own identity in 802.1x

Windows Login Procedure

 Network Connectivity

 Point of 802.1x Authorization

Cisco.com

User Authentication



* No connectivity to Domain Controller until user logs in.

Machine Authentication



* 802.1x early in boot process

User + Machine Authentication



* Users can be individually authenticated

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

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 PEAP or 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 too**
- **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

Cisco.com

- **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

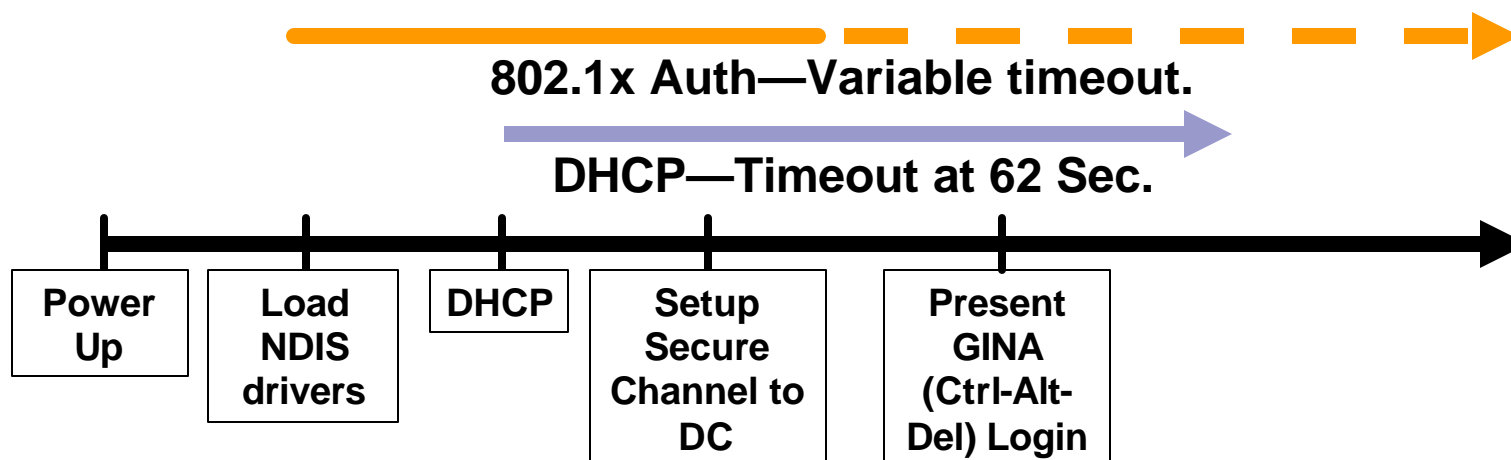
If doing mutual authentication, the computer MUST trust the signing CA of the RADIUS server's cert

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...



How to Address DHCP Timeout with 802.1x?

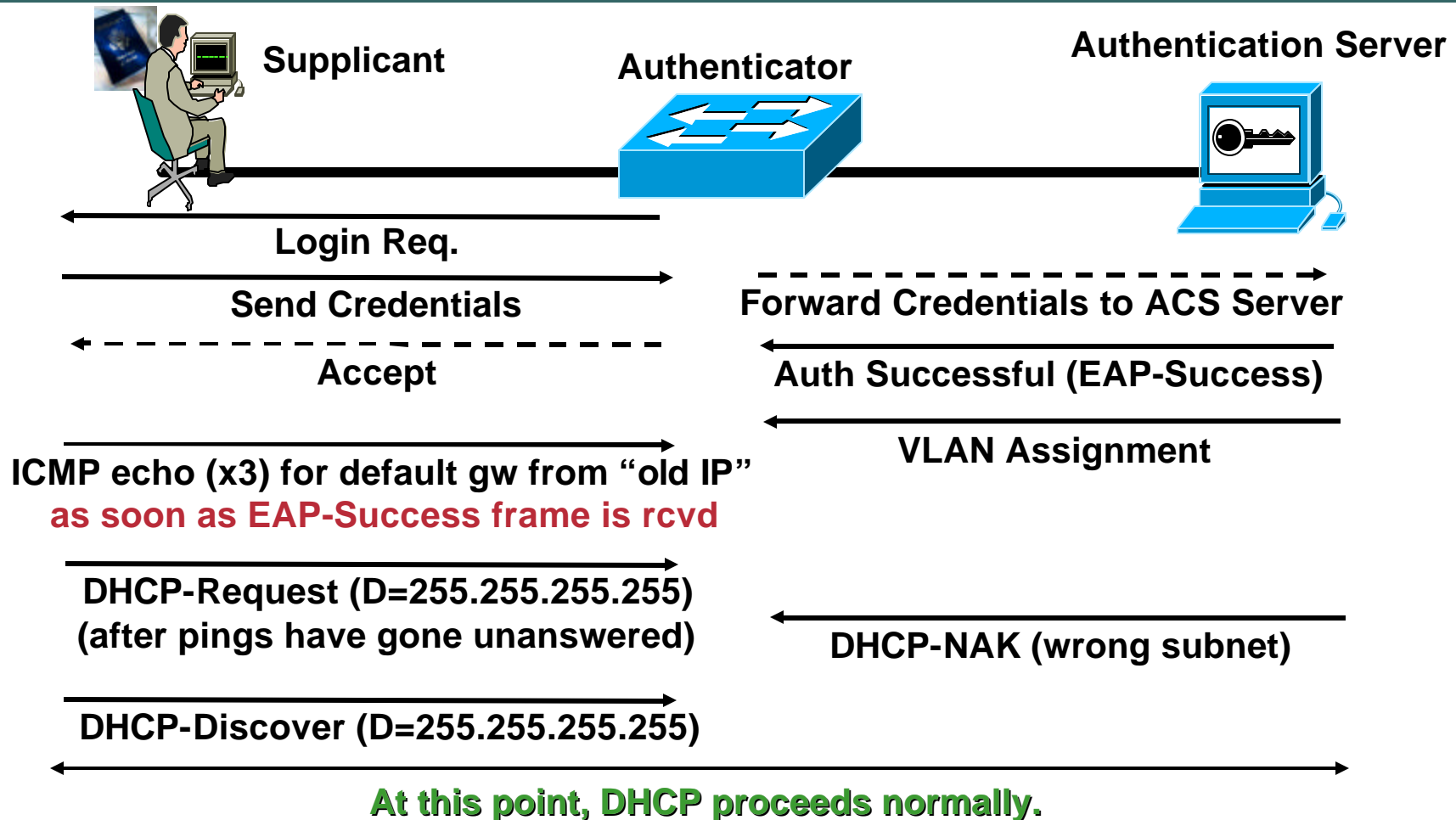
- **Use Machine authentication**—this allows the initial machine authentication to obtain an IP address
- **Supplicant behavior has been addressed by Microsoft:**
 - Windows XP: Install Service Pack 1a + KB 826942
 - Windows 2000: Install Service Pack 4
- **Updated supplicants trigger DHCP IP address renewal**
 - Successful authentication causes client to ping default gateway (3 times) with a sub-second 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

Microsoft Fixes

Windows XP: Install Service Pack 1a + KB 826942

Windows 2000: Install Service Pack 4

Cisco.com



802.1x and Machine Access Restriction

Cisco.com



Machine Authentication

User Authentication

Note: These are two independent Authentications

Machine boots up

Interface becomes active (not authenticated)

802.1x authentication starts

Machine sends its credential (Using EAP-TLS „Machine Certificate“ or using PEAP-MS-Chapv2 „Windows AD shared secret“) machine authentication name prefix „host/“

If user logs on to machine, machine sends EAPOL-Start message to notify the Access Point or Switch that a new authentication is being performed.

Following EAP-TLS or PEAP-MS-Chapv2 authentication will be done with users credential

802.1x and Machine Access Restriction

Cisco.com

If Machine Authentication fails or is not enabled, a user can still successfully access the network.

So Machine Authentication does not prevent users from accessing the network with a unregistered machine.



User Authentication

If user logs on to machine, machine sends EAPOL-log-off message to notify the Access Point or Switch that previous authentication is no longer valid anymore.

Following EAP-TLS or PEAP-MS-Chapv2 authentication will be done with users credential

802.1x and Machine Access Restriction

Cisco.com

- **User authentication is only successful after a previous successful machine authentication**
- **PEAP with EAP-MS-CHAPv2 and EAP-TLS only**
- **Allows to use machine authentication as a condition for user authorization**
- **This provides a way to deny authentication for a user because machine authentication to the network was not completed prior to a login attempt**
- **Machine authentication by itself does not prevent users from accessing the network with an unregistered machine. To enforce this restriction, ACS now only completes a user authentication if the MAC address associated with the attempt was previously included in a successful machine authentication.**

802.1x Supplicant Support

Cisco.com

- **802.1x requires client side code (supplicant code)**
- **Growing support for supplicants in the industry**

Microsoft - Native in Win2K, XP, and 2003

Funk Software - support for WinNT, Win2k, WinXP, PocketPC (Windows Mobile)

Meetinghouse - support for WinNT, Win2K, WinXP, Win98, WinME, Solaris, Red Hat Linux

Opensource – Open1x xsupplicant for Unix/Linux platforms.

Apple - native OS X support.

Cisco – WLAN Only support in ACU.

802.1x Supplicant Support

Cisco.com

- What endpoints are covered?

Windows XP—Yes

Windows 2000—Yes

Linux—Yes

HP-UX—Yes

Solaris—Yes

HP Printers—Yes

Windows ME—Limited

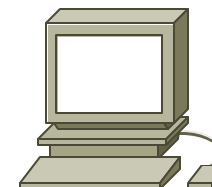
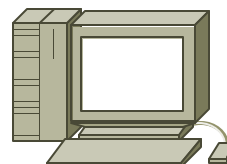
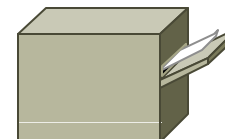
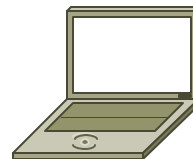
Windows 98—Limited

Windows NT4—Limited

Apple OS X 10.3—Yes

3rd Party: Meeting House—Now

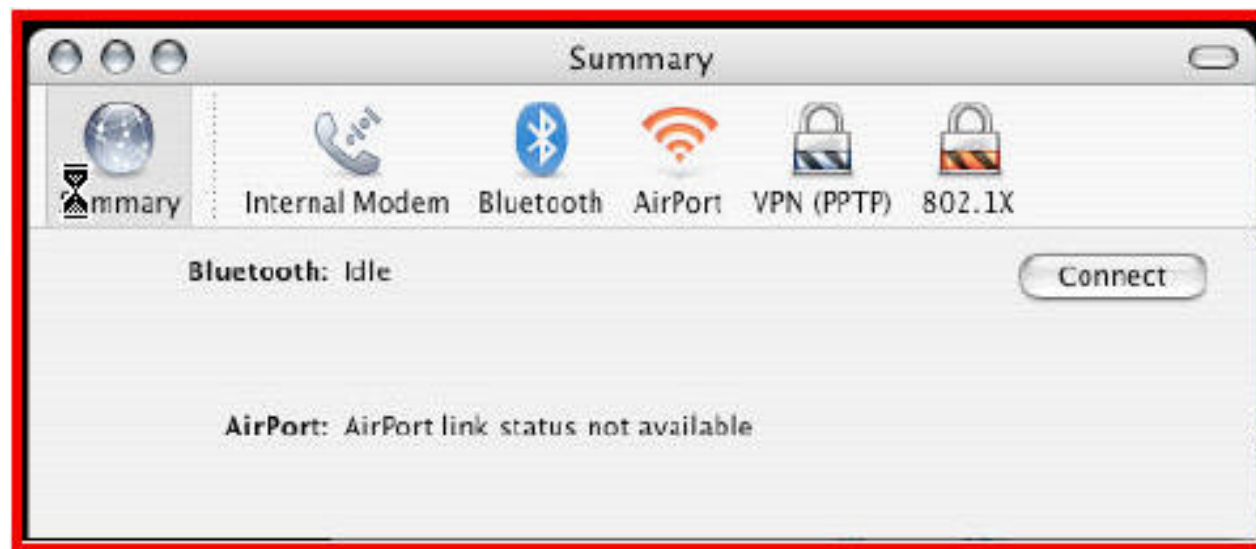
3rd Party: Funk Software—Now



802.1x Supplicants - MAC OS X

Cisco.com

- **Native Apple Supplicant Support in OS X 10.3**
- **802.1x is turned off by default!**
- **Default Parameters - TTLS, LEAP, PEAP, MD5 supported**
Client needs to be configured
- **Support for Airport and Wired interfaces**



Suplicants – Summary

Cisco.com

Supplicant	WinXP	Win2k	Funk	Meetinghouse	Apple
Support					
DHCP Support w/ VLANs					
Guest VLAN					
EAP-MD5					
PEAP w/ MSCHAPv2					
PEAP w/ OTP					
EAP-TLS					
LEAP					
EAP-TTLS					

Complete Your Session Evaluation Form

Cisco.com

Thank you for attending this session.

Complete your session evaluation, por favor.

Give to the room attendants as you leave the room.

Muchas Gracias

