UNDERSTANDING IDENTITY-BASED NETWORKING SERVICES AUTHENTICATION AND POLICY ENFORCEMENT

John Stone

CTO Cisco Systems Internetworking Ireland

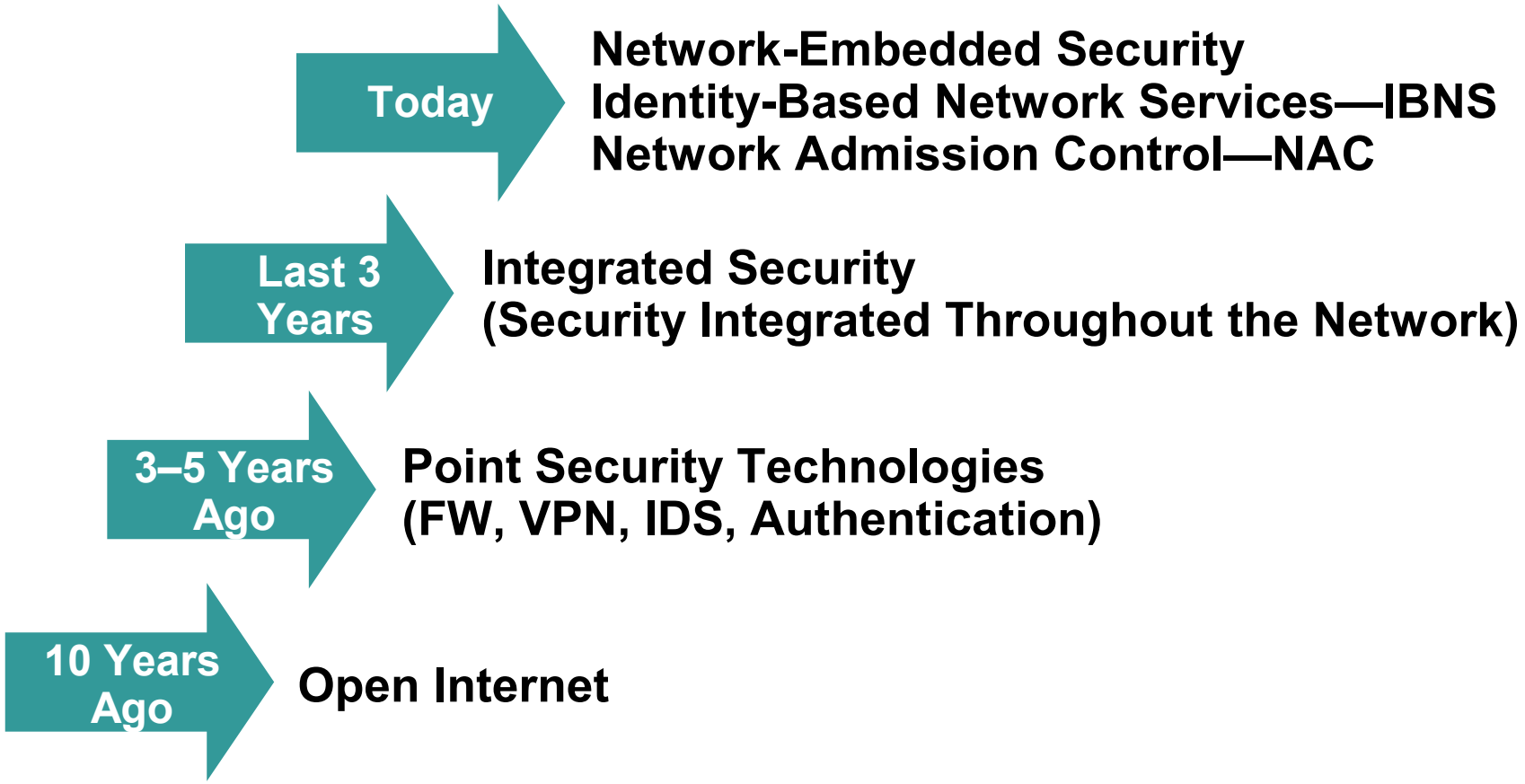
jstone@cisco.com

Overview and Agenda

- Looking at the Concepts of Identity and Authentication
- Applying the Concepts to Network Access Control
- Identity-Based Integration Issues, Authorization and Policy Enforcement
- Operating System Implementations and Supplicants in Different Environments

THREAT MODEL OVERVIEW

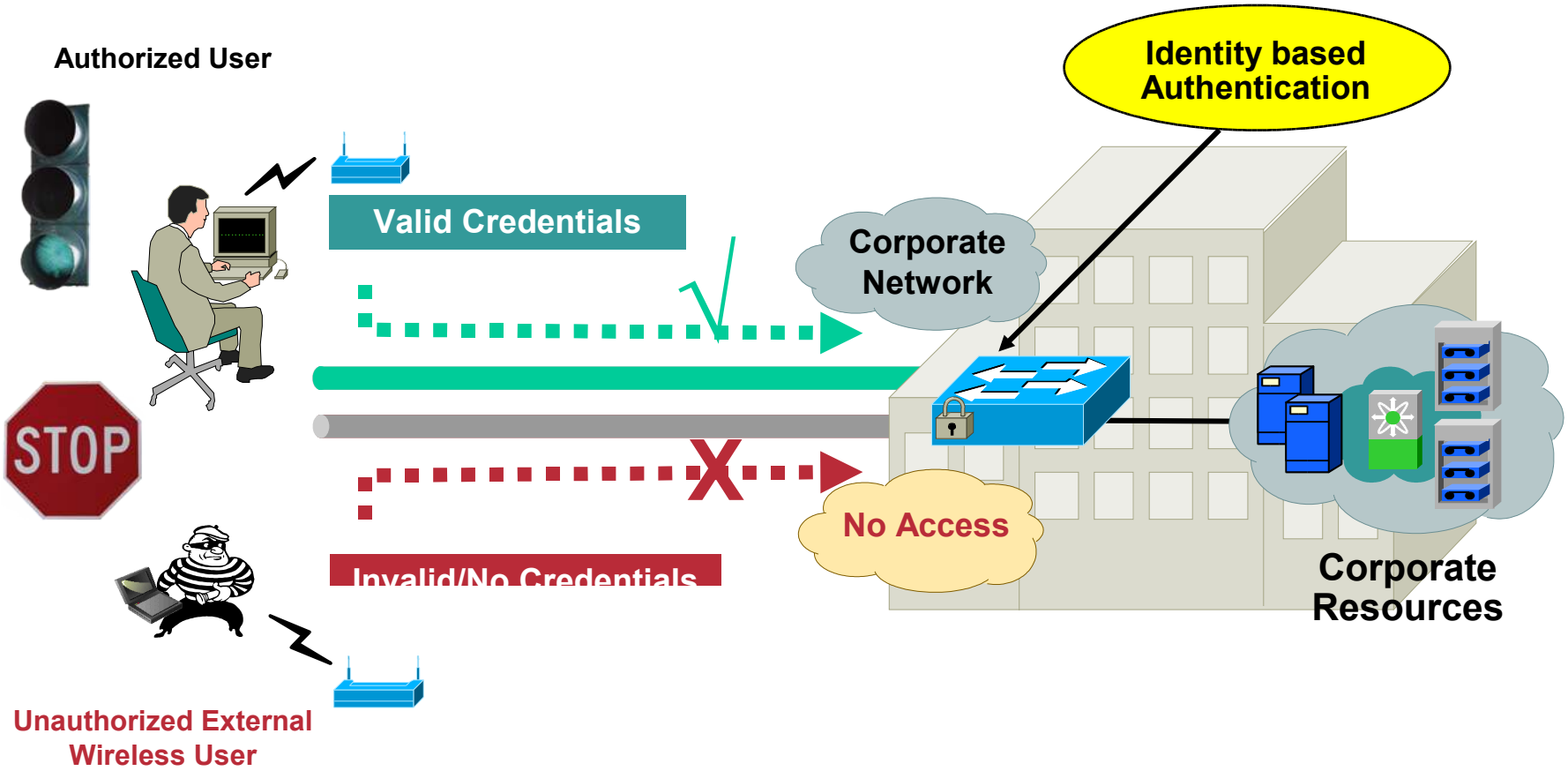
The Evolution of Security



What Is Identity-Based Network Services?

- 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



Three Simple Theories of IBNS

- **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

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?**

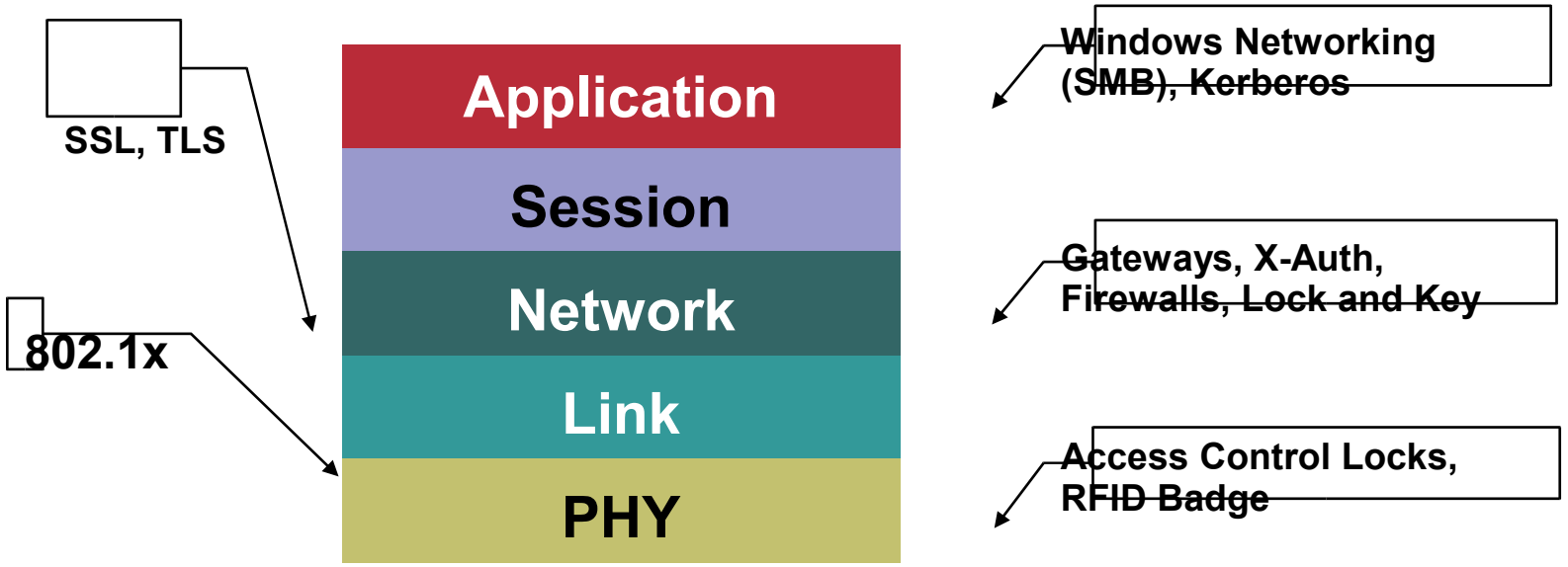
  Can look like anything:

  jafrazie@cisco.com
  Jason Frazier
  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?

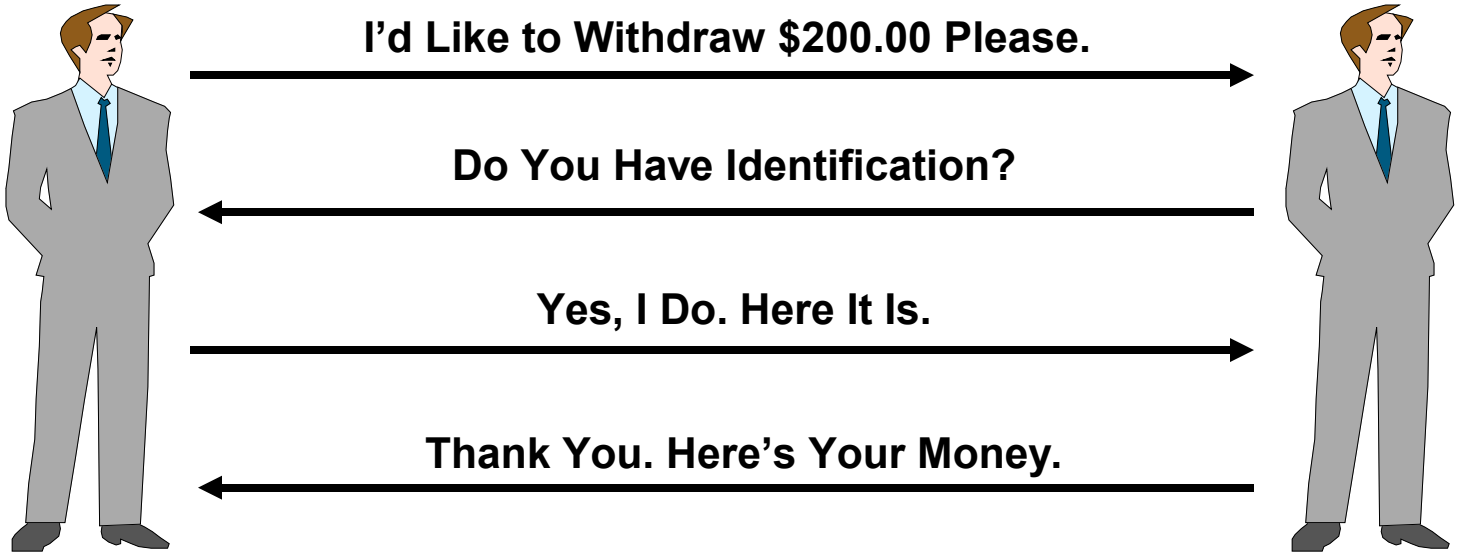


- Physical—access control locks, RFID proximity badge
- Link—802.1x
- Network—gateways, x-auth, firewalls, lock and key
- Session identity—SSL, TLS
- Application identity—Windows networking, Kerberos

AUTHENTICATION OF IDENTITIES

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

- 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?

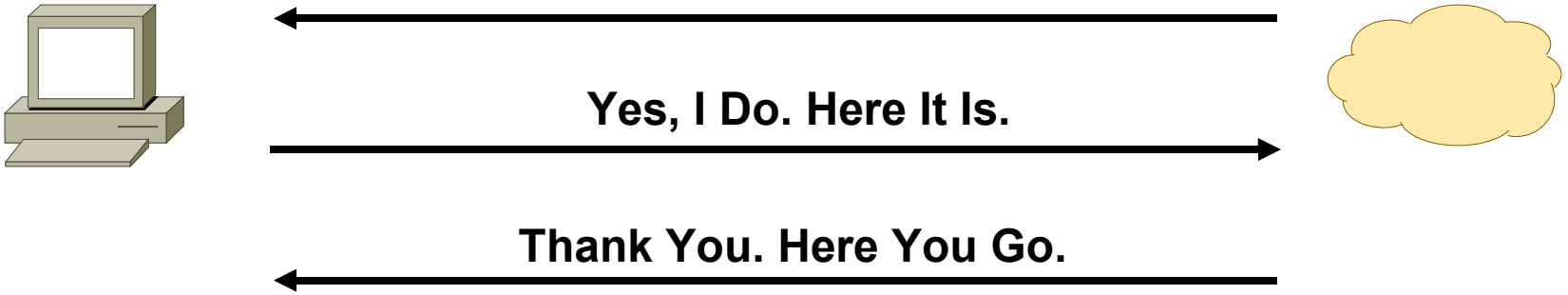
- Because differentiation of services and rights control is critical in network environments
- Not everyone has the same privileges; not all resources or information have the same level of confidentiality
- The concept of being able to differentiate services amongst groups or individuals
- If everyone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

AN OPERATIONAL OVERVIEW OF NETWORK AUTHENTICATION

Port-Based Network Authentication

- 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



PROTOCOLS AND MECHANISMS

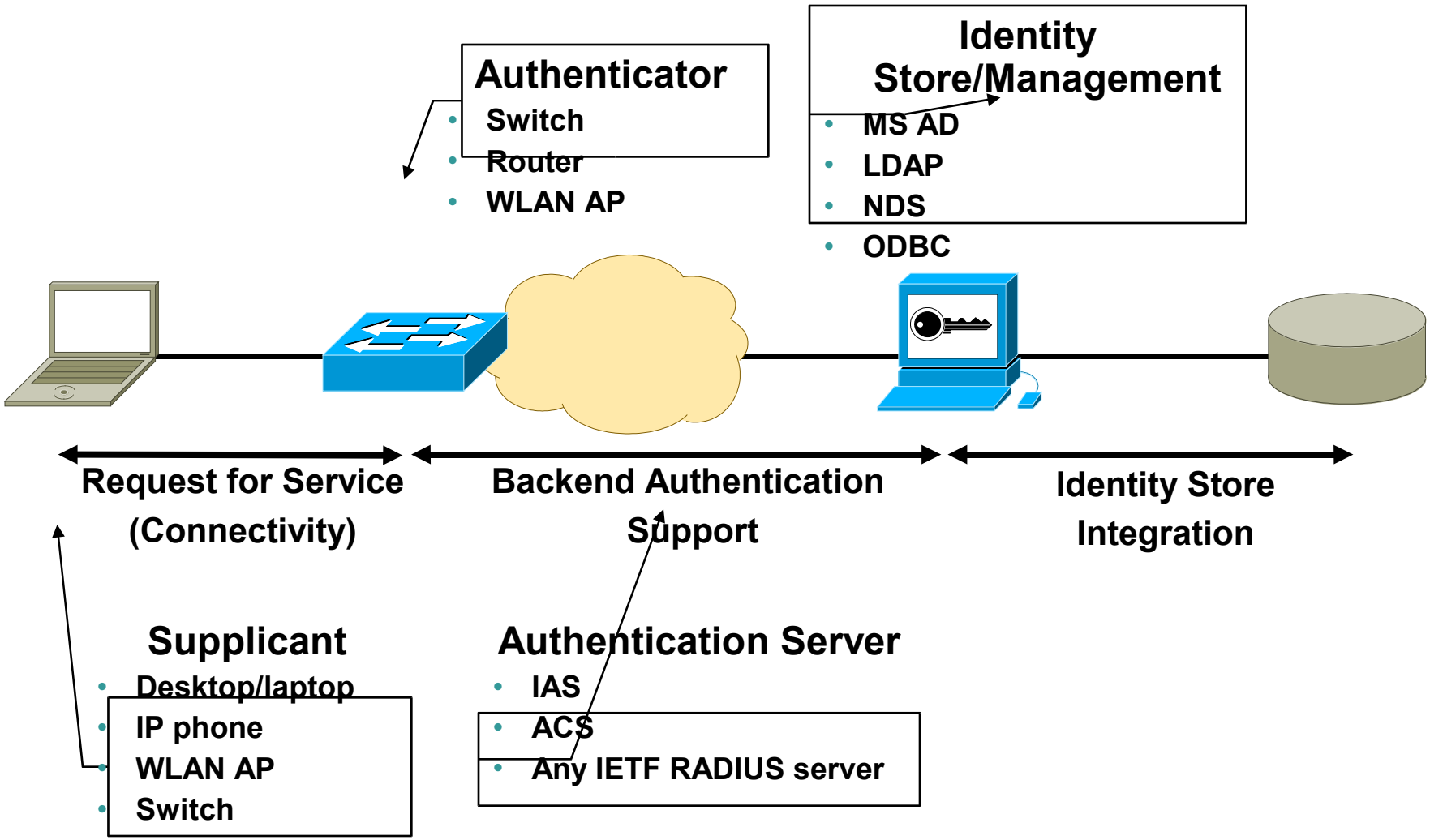
Protocol Options

- Extensible Authentication Protocol (EAP-RFC 3748)
- IEEE 802.1x framework
- Use of RADIUS

Some IEEE Terminology

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

802.1x Port Access Control Model



INTEGRATION, AUTHORIZATION, AND POLICY ENFORCEMENT

IBNS Feature Support for Integration and Authorization

- Basic IEEE 802.1X support
- IBNS: some extensions to 802.1x
  - 802.1X with Dynamic VLANs
  - 802.1x with Private VLANs — Soon
  - 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

Secure Mobility and Workforce Optimization = Enhanced Productivity
Reduced OpEx for IT with Less Work for Adds/Moves/Changes
Remove Barriers to Deployment

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 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>**

CatOS

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

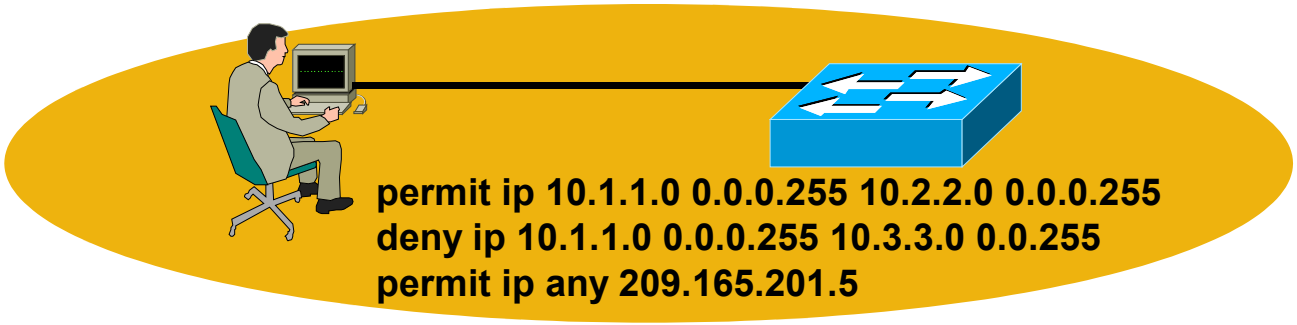
IOS

```
aaa authorization network default group radius
```

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

802.1x with 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



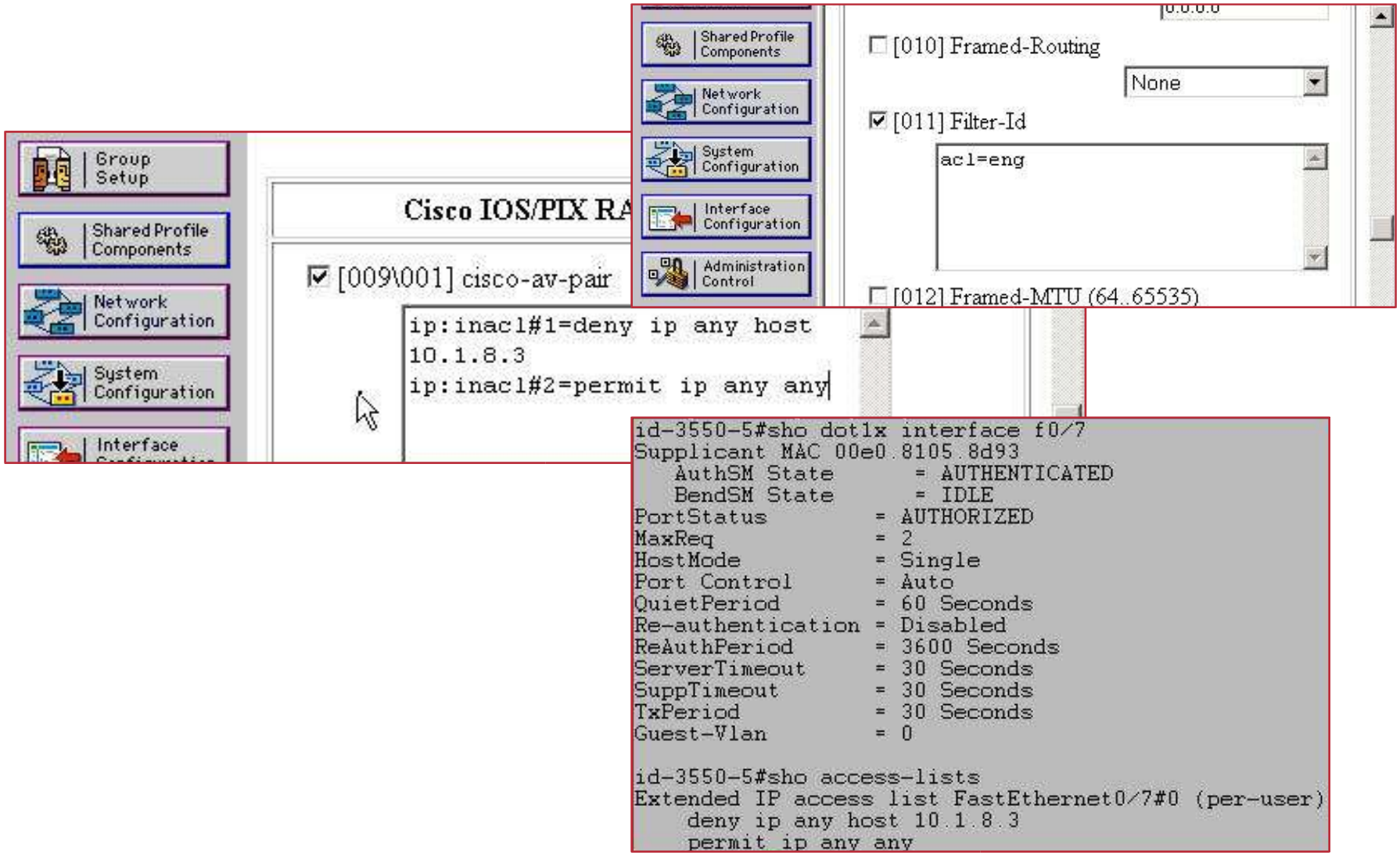
CatOS

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

IOS

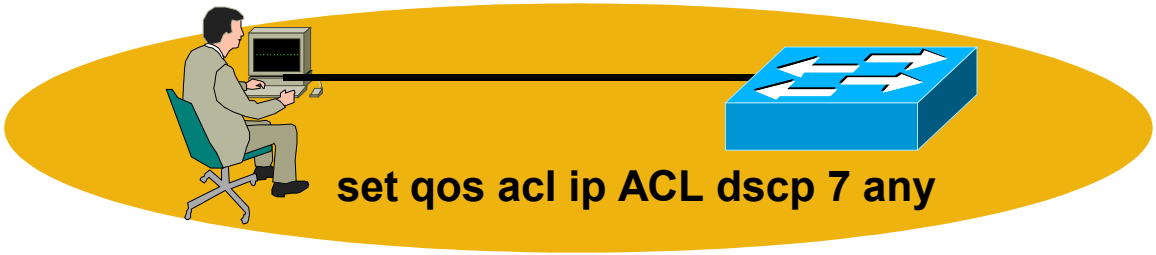
```
aaa authorization network default group radius
```

802.1x with ACLs



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

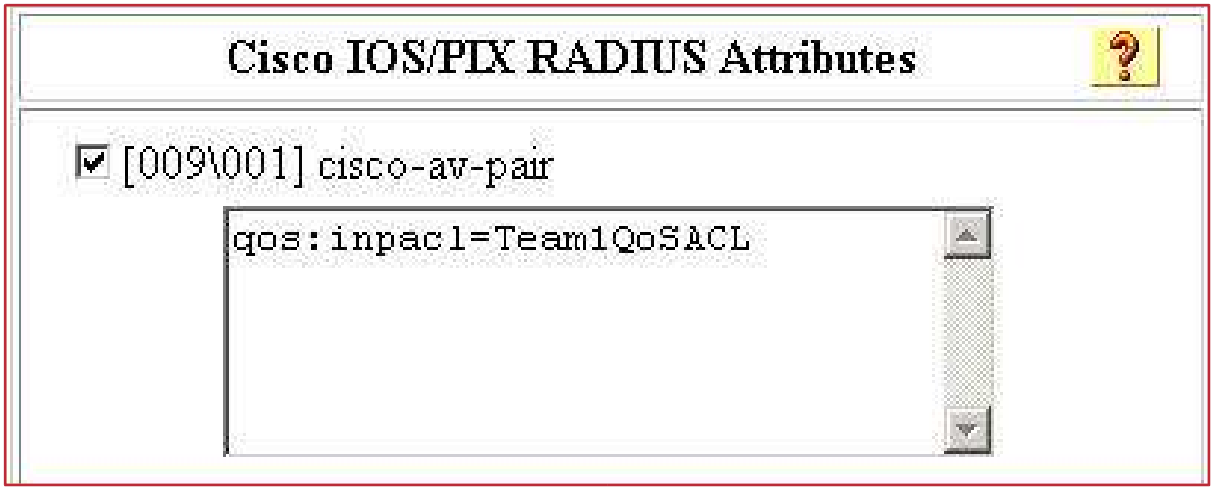
```
RADIUS attributes received in CatOS are automatically
implemented if 802.1x is enabled.
```

IOS

```
aaa authorization network default group radius
```

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

802.1x with QoS Policy




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

OPERATING SYSTEM IMPLEMENTATIONS SUPPLICANTS IN DIFFERENT ENVIRONMENTS

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

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

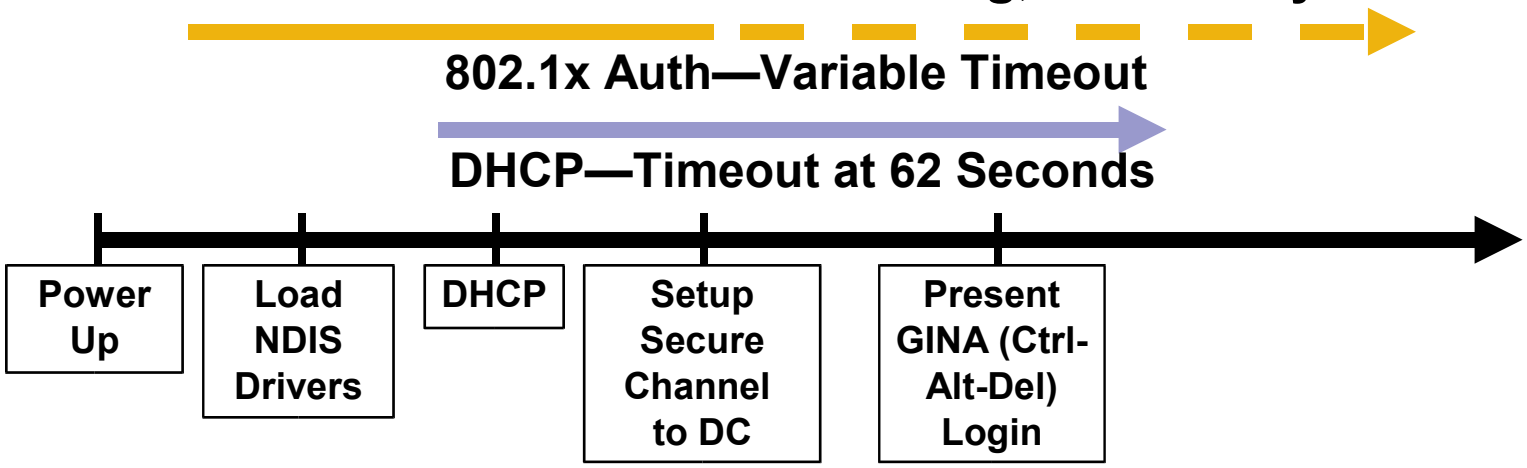
Network Connectivity

Point of 802.1x Authorization

Microsoft Issues with DHCP

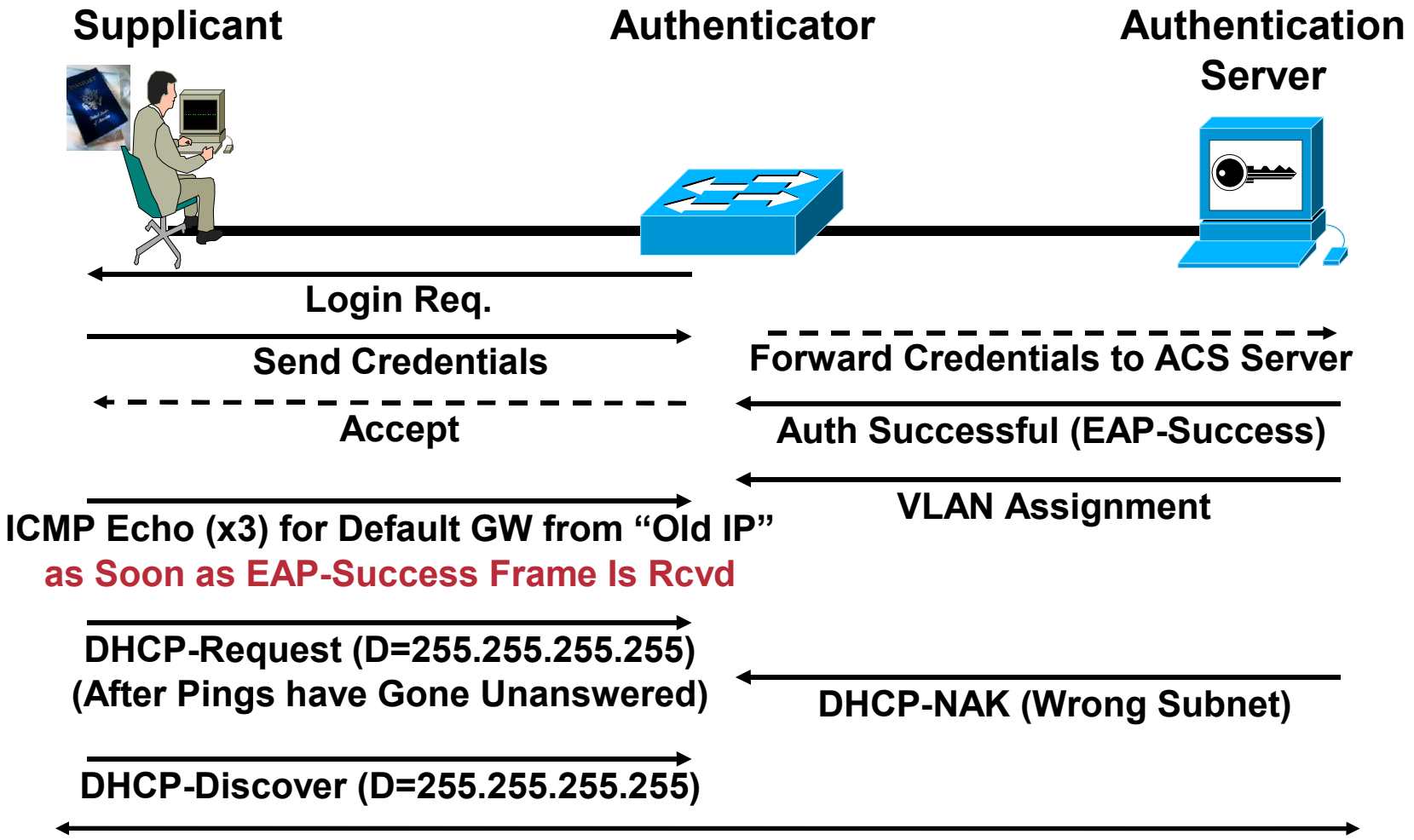
DHCP Is a Parallel Event, Independent of 802.1x Authentication

- 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…



Microsoft Fixes

Windows XP: Install Service Pack 1a + KB 826942
Windows 2000: Install Service Pack 4



802.1x Supplicant Support

- 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

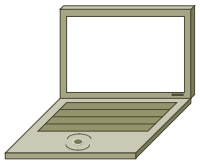
  Apple—native OS X support

  Cisco—WLAN support in ACU

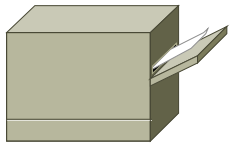
802.1x Supplicant Support

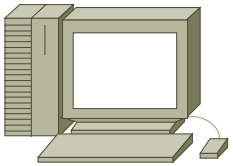
What Endpoints Are Covered?

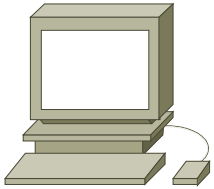
- Windows XP—Yes
- Windows 2000—Yes
- Linux—Yes
- HP-UX—Yes
- Solaris—Yes
- HP printers—Yes
- Windows ME—Limited
- Windows 98—Limited
- Windows NT4—Limited
- Apple OS X 10.3—Yes
- Third party: Meeting House—Now
- Third party: Funk Software—Now


Windows


7920


HP Jet Direct


Solaris

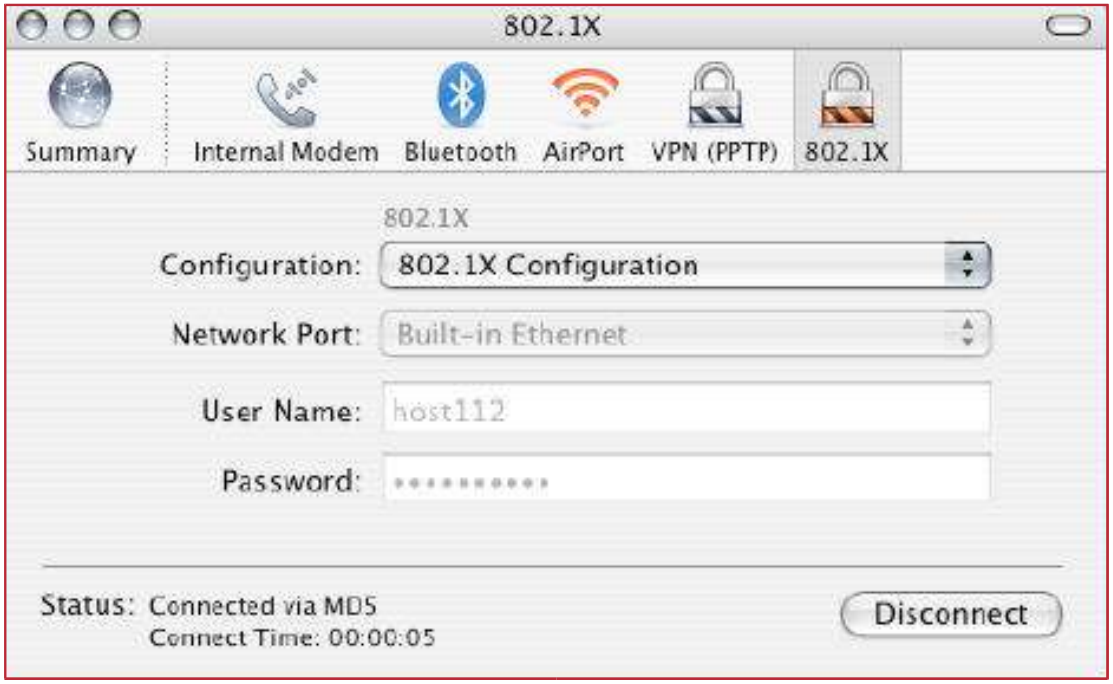

Apple


WLAN APs


IP Phones

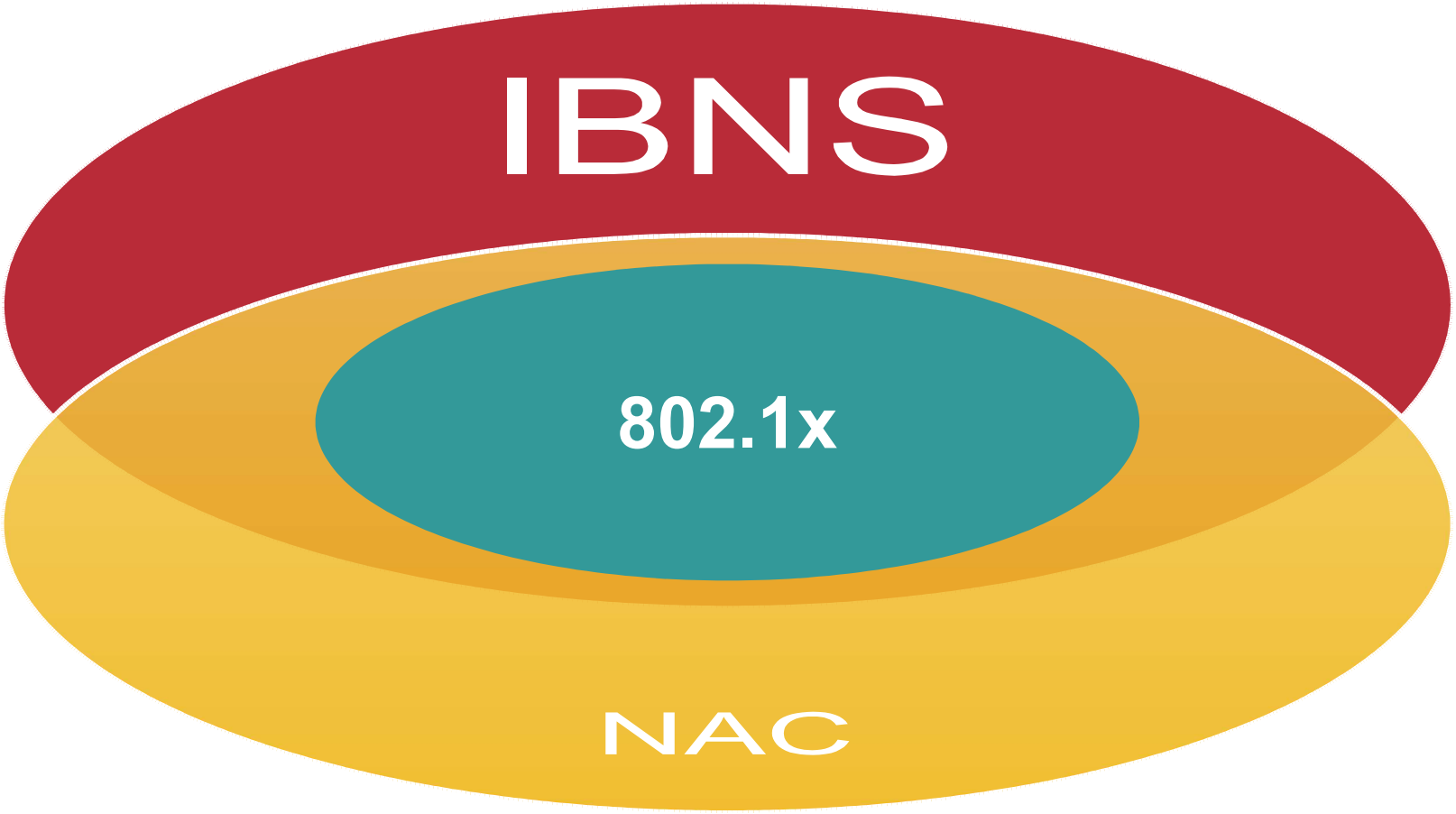

Pocket PC

802.1x Supplicants: MAC OS X



- **NOTE: Apple machines can be added to Windows domains, so PEAP can be accomplished**
- **Apple supplicant info (for further information)**
  http://www.apple.com/macosx/features/networkin
  http://docs.info.apple.com/article.html?artnum=151759

Trust and Identity Solutions



Control Who/What Has Access…
Authorization Based on Identity and Host Posture ????

Summary

- Identity for both man and machine is a reality
- Authentication for both is deployable today
- Policy Enforcement can be implemented at a network level
- Posture with SW Revision checking available via NAC

- **What does this mean ????**

- You can move to the monitoring of the Users,

  their application traffic flows

  Invalid access attempts etc …….

Q and A