Customized for NCET Conference 2007

802.1X:

Background, Theory & Implementation

March 16, 2007

Presented by: Jennifer Jabbusch, CISSP, HP MASE, CAD

Mike McPherson, HP ProCurve

Neal Hamilton, HP ProCurve

About Carolina Advanced Digital

For over 20 years, Carolina Advanced Digital, Inc. (CAD) has offered the highest level of engineering expertise in support of all enterprise sectors. Serving commercial accounts, hospitals, state, local and federal government, CAD focuses on IT infrastructure, security and management. The company helps customers guard their core network, ensuring network security and availability of critical data. For more information contact CAD at (800) 435-2212 or visit www.cadinc.com.

What's Covered

Part I: Background
What is 802.1X, where did it come from and why do we need it?

Part II: Theory
802.1X, what does it do and how does it work?

Part III: Implementation
How do you implement 802.1X and what are some migration considerations?

Part IV: 802.1X, NAC and IDM
How does 802.1X fit into the big picture?

Part V: Technical Overview of EAP Communications

Part I: 802.1X Background

What is 802.1X?

- Port access control via extensible authentication
- IEEE standard
- Framework for authentication and authorization on 802 LANs
- Framework for key distribution
- Link layer solution
- Solution for wired and wireless networks

Where Did 802.1X Come From?

2001- Original IEEE 802.1X standard
2004- Update of IEEE 802.1X standard

Project Purpose of 802.1X

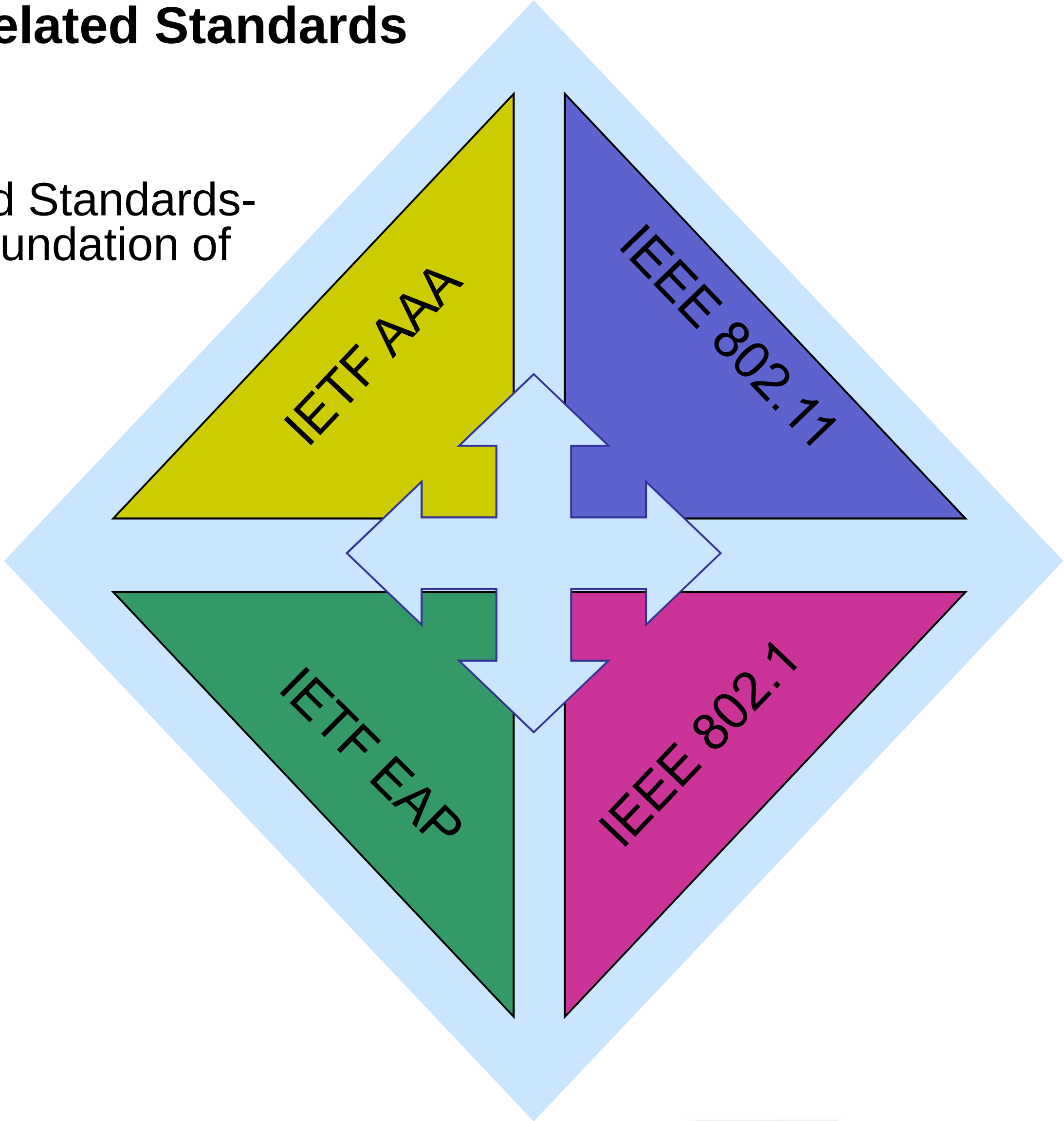
The standard provides common interoperable solutions using standards based authentication and authorization infrastructures already supporting schemes such as dial up access.

Abstract of the 802.1X Standard

Port-based network access control makes use of the physical access characteristics of IEEE 802® Local Area Networks (LAN) infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to- point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails.

802.1X Related Standards

Integrated Standards-based Foundation of 802.1X



HP: A Partner in Standards

Going With Standards

CAD has chosen ProCurve Networking by HP as its preferred partner for networking infrastructure because of its involvement in, and adoption of industry standards.

ProCurve Participation in IEEE

ProCurve and its leadership are very active in developing and adopting open networking standards to ensure interoperability of devices throughout the infrastructure

ProCurve’s CTO Paul Congdon has developed and standardized several technologies, including the 802.1X Access Security Protocol.

In 2004, Congdon was elected Vice Chair of the IEEE 802.1 Higher Layer LAN Protocols Working Group.

HP ProCurve and Standards

standards leadership

IEEE 802.1
Ethernet Switching Standards

IEEE 802.1X
Port Authentication Protocol

Trusted Computing Group
End Device Compliance Authorization

IETF Radius Extensions
Identity Driven Manager (IDM) Attributes

IETF NEA
Network Endpoint Assessment

IEEE 802.1AE
MAC Security / Ethernet Encryption

IEEE 802.1af
Encryption Key Agreement Protocol

IEEE 802.1AR
Secure Device Identity

ProCurve Networking
HP Innovation

802.1X and 'NAC'

- **802.1X, just one 'A**'. Because 802.1X leverages RADIUS servers, which are authentication, authorization, and accounting (AAA) servers, 802.1X is sometimes assumed to provide all three functions. In reality, 802.1X provides only the authentication piece.

- **NAC vs NAC.** The inconsistent use of the "NAC" acronym within the industry causes some confusion. Some vendors and research firms use it to refer to **network admission control**, a fairly narrow function, while others use it to refer to **network access control**, a much broader set of functions that includes controlling what users do once they're authenticated and on the network.

- **802.1X** is a standard method for port-based **network admission control**. User credentials (such as a password, one-time token, or digital certificate) must be validated before a physical LAN port or wireless access point can be used for network access.

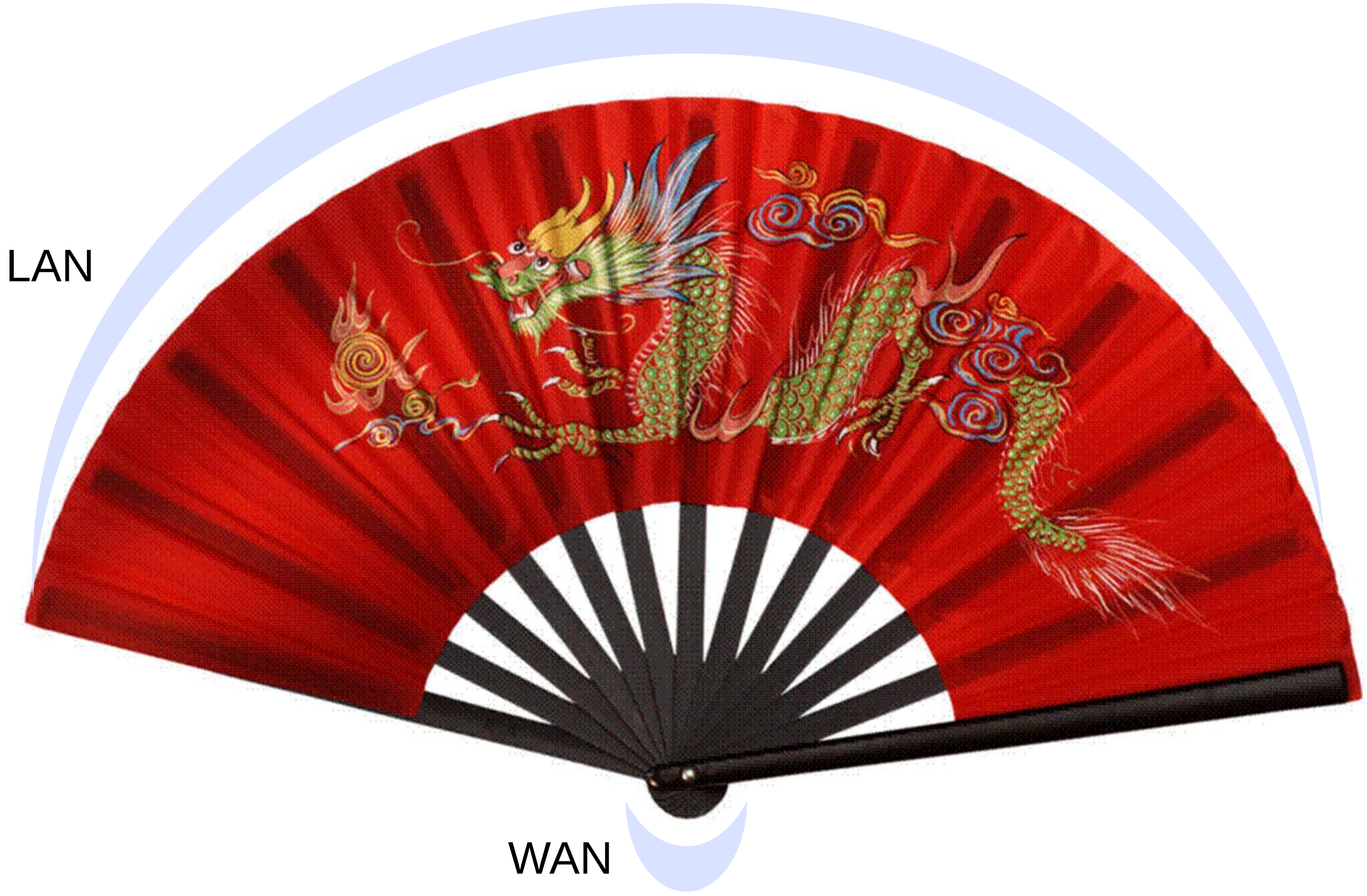
- **NAC (Network Access Control)** builds on 802.1X to provide health and compliance checks prior to connection, policy-based resource control and continuous health and behavior monitoring as well as policy enforcement while connected.

Part II: 802.1X Theory

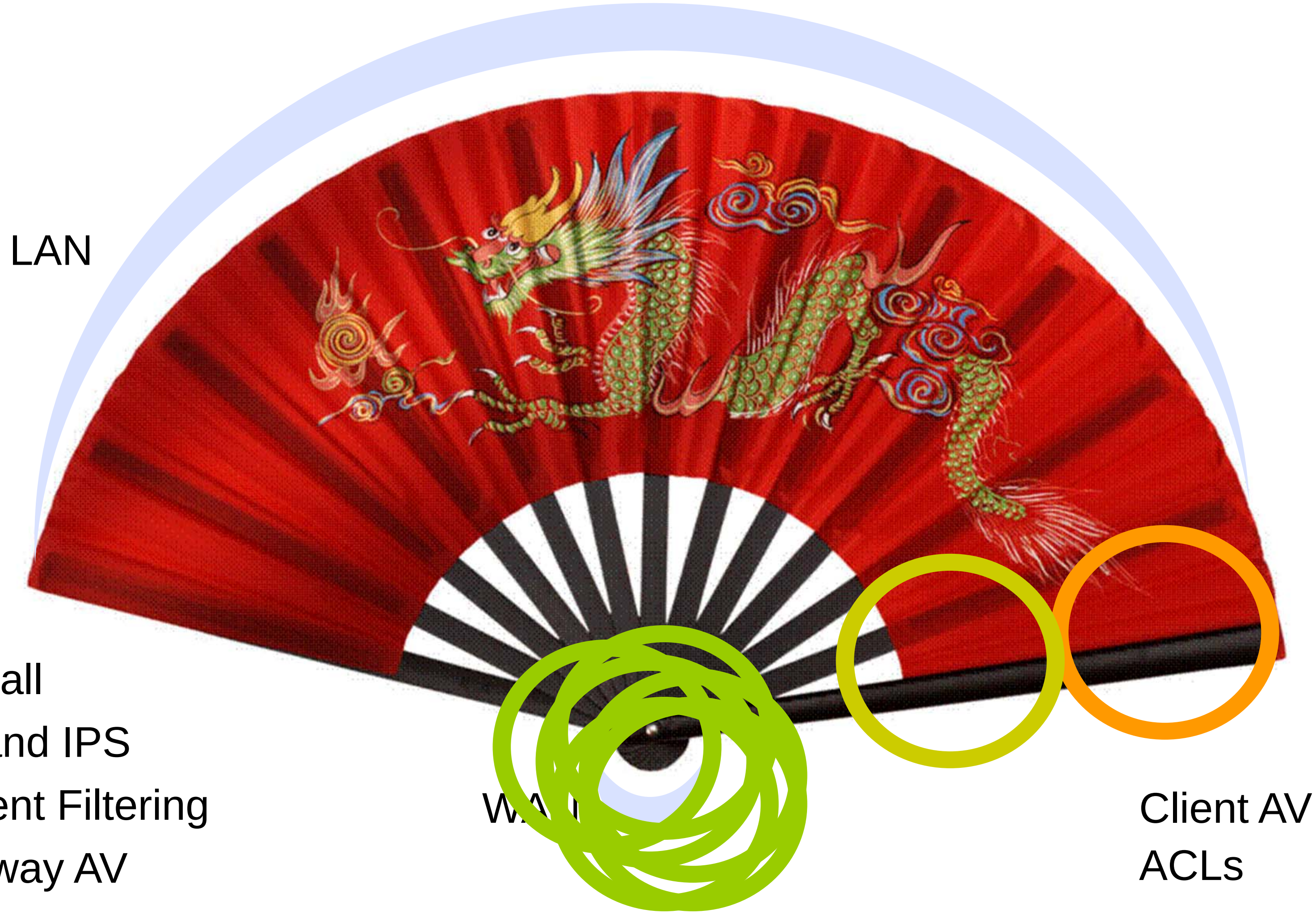
Protecting the Network

What are some network security technologies you're currently using?

Your Network Simplified



A Shift Towards Protecting the LAN



Firewall

IDS and IPS

Content Filtering

Gateway AV

Bandwidth Mgmt

DMZs

Client AV

ACLs

How 802.1X Protects Your Network

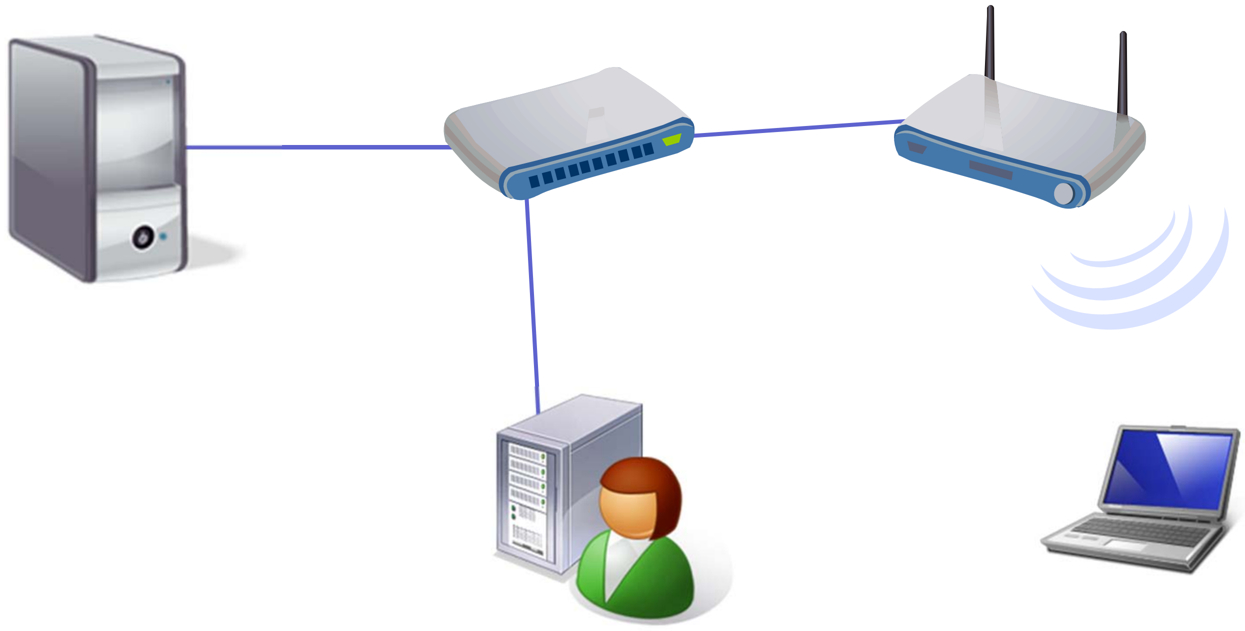
802.1X will help you…

- Prevent unauthorized access to the network
- Extend physical security to each port
- Protect the network from malicious users and propagation of traffic
- Create a ‘trusted infrastructure’
- Eliminate rogue APs, unauthorized switches
- Increase security and flexibility with dynamic VLAN assignment
- Enhanced wireless security
- Stop broadcast storms from loops
- Provide a means for compliance reporting
- Ease interoperability with a variety of other security software and hardware solutions

What’s Inside: Parts of 802.1X

Tech Terms	English
Authenticator An Authenticator is an entity that require authentication from the Supplicant. The Authenticator may be connected to the Supplicant at the other end of a point-to-point LAN segment or 802.11 wireless link.	Switch or network device that enforces authentication policies
Authentication Server An Authentication Server is an entity that provides an Authentication Service to an Authenticator. This service verifies from the credentials provided by the Supplicant, the claim of identity made by the Supplicant.	RADIUS server (or internal database)
Supplicant A Supplicant is an entity that is being authenticated by an Authenticator. The Supplicant may be connected to the Authenticator at one end of a point-to-point LAN segment or 802.11 wireless link.	Software on device (computer or switch) that communicates via EAP to gain authorization

What’s Inside: How 802.1X Works



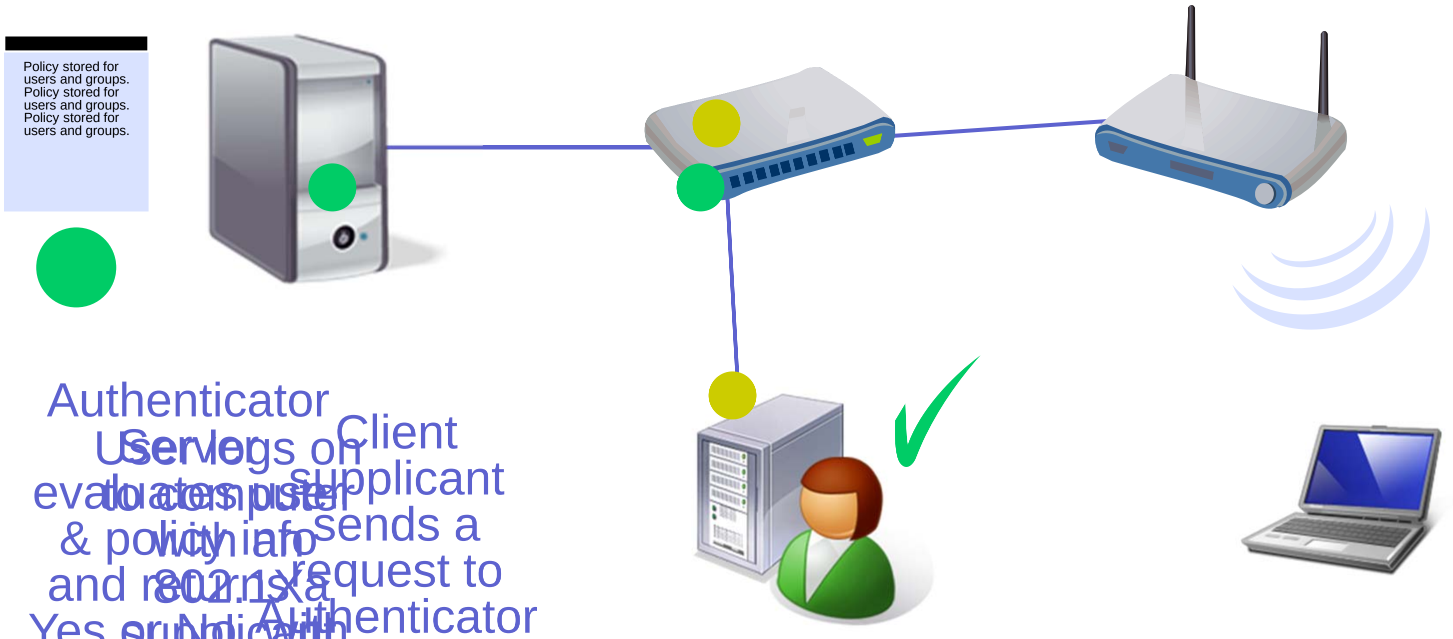
RADIUS Server
(Authentication Server)

Switch or AP
(Authenticator)

Computer with Supplicant

Laptop with Supplicant

What’s Inside: 802.1X in Action



RADIUS Server
(Authentication Server)

Switch or AP
(Authenticator)

Authenticator
forwards
request and
credentials to
Authentication
Server

Authenticator
gets OK reply,
forwards to
user and
opens the port

If special instructions are
in RADIUS (such as
VLAN assignment), they
are returned with the Yes
or No to the
Authenticator

Policy stored for
users and groups.
Policy stored for
users and groups.
Policy stored for
users and groups.

Process works
the same for
wired and
wireless
access

Authenticator
Server
evaluates user
& policy info
and returns
Yes or No, with
details

User logs on
to computer
with an
802.1x
supplicant

Client
supplicant
sends a
request to
Authenticator
using EAP

Computer with Supplicant

Laptop with Supplicant

What’s Inside: It’s All About the EAP

Just some EAPs…

- **LEAP**
- **EAP-TLS**
- EAP-MD5
- EAP-PSK
- EAP-TTLS
- EAP-IKEv2
- **PEAP**
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- **EAP-FAST**
- EAP-SIM
- EAP-AKA
- Many more…

All of these communications happen via EAP (Extensible Authentication Protocol), as outlined in the 802.1X standard.

EAP is a universal authentication framework frequently used in wireless networks and Point-to-Point connections. Although the EAP protocol is designed for both wired and wireless authentication, it presents some unique advantages for wireless security.

Choosing the right EAP method for your environment is key. Some are popular, a few are standard, many are proprietary and they all have their quirks.

EAP
Method

What’s Inside: Supplicants

Some Supplicants

•**Windows** 2000 SP3+

•**Mac OS**

•**Cisco Secure Sevices Client** (formerly MeetingHouse)

•**Juniper Odyssey Access Client** (formerly by Funk)

•**Alfa & Arris SecureW2**

•**Open1x** (Linux)

•**WIRE1x** (Modified Open1x for Windows & legacy)

Supplicants are the software on the device that’s authenticating via 802.1X and may be on:

-Computers, laptops, servers

-Portable and handheld devices

-Infrastructure, switches, APs

-Devices without supplicants will use MAC Auth

Supplicants are available several ways:

-Embedded/included in operating system

-Purchased (typically licensed per device)

-Open Source

Supplicant

What’s Inside: Authentication Server

Popular RADIUS Servers

- **Microsoft IAS** (Included with Windows Server 200X)
- **Juniper Steel-belted Radius** (formerly by Funk)
- **FreeRADIUS**
- **Cisco ACS** (Access Control Server)

Authentication Server in 802.1X is your RADIUS Server.

Most organizations have an authentication server in place, connected to a user database, such as Microsoft Active Directory.

When we get into implementation sections later, you’ll see the importance of your Authentication Server and how it will affect your other 802.1X choices for supplicants and EAP methods.

RADIUS Server (Auth Server)

What's Inside: RADIUS Attributes

- User-Name
- NAS-IP-Address
- NAS-Port
- Service-Type
- Framed-Routing
- Filter-Id
- Framed-MTU
- **Reply-Message**
- Framed-Route
- State
- Class
- Vendor-Specific
- Session-Timeout
- Idle-Timeout
- Termination-Action
- Called-Station-ID
- Calling-Station-ID
- NAS-Identifier
- Proxy-State
- **NAS-Port-Type**
- Password-Retry
- **Connect-Info**
- EAP-Message
- Message-Authenticator
- NAS-Port-Id
- **Tunnel-attributes**

Your RADIUS server becomes your 802.1X Authentication Server and will require some tweaking of current settings.

In addition to the necessary configurations, there are also RADIUS attributes which may be set to customize the user experience, by returning messages, defining allowed connections or dynamically assigning VLANs.

Attributes used to customize a response from RADIUS:

Reply-Message: This attribute is used to indicate text which may be displayed to the user. Display properties vary based on supplicant used.

NAS-Port-Type: To limit the connection type allowed for a user. NAS-Port-Type values of Ethernet (15) Wireless - IEEE 802.11 (19), Token Ring (20) and FDDI (21) may be used in 802.1X.

Connect-Info: Can be used for information and QoS purposes, especially for wireless connections.

Tunnel Attributes: Used for dynamic VLAN assignments

What’s Inside: MAC Auth and Web Auth

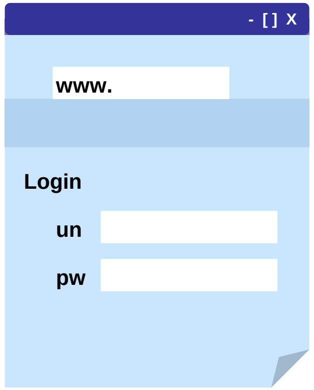
- **MAC Auth** Authentication based on device MAC addresses.
- **Web Auth** Authentication via web browser interface. Mostly for guest users web auth is similar to hotel wireless logins.
- **802.1X** Authentication using a supplicant

Although MAC Auth and Web Auth are not part of the 802.1X standard, they do use the same standard communication protocols and are closely related to and integrated with 802.1X functions.

The process of closing and opening ports and dynamically assigning VLANs is similar for MAC Auth and Web Auth as it is for 802.1X.

MAC: 00-08-74-4C-7F-1D

Authenticated on MAC Address



Browser-based login

Part III: Implementing 802.1X

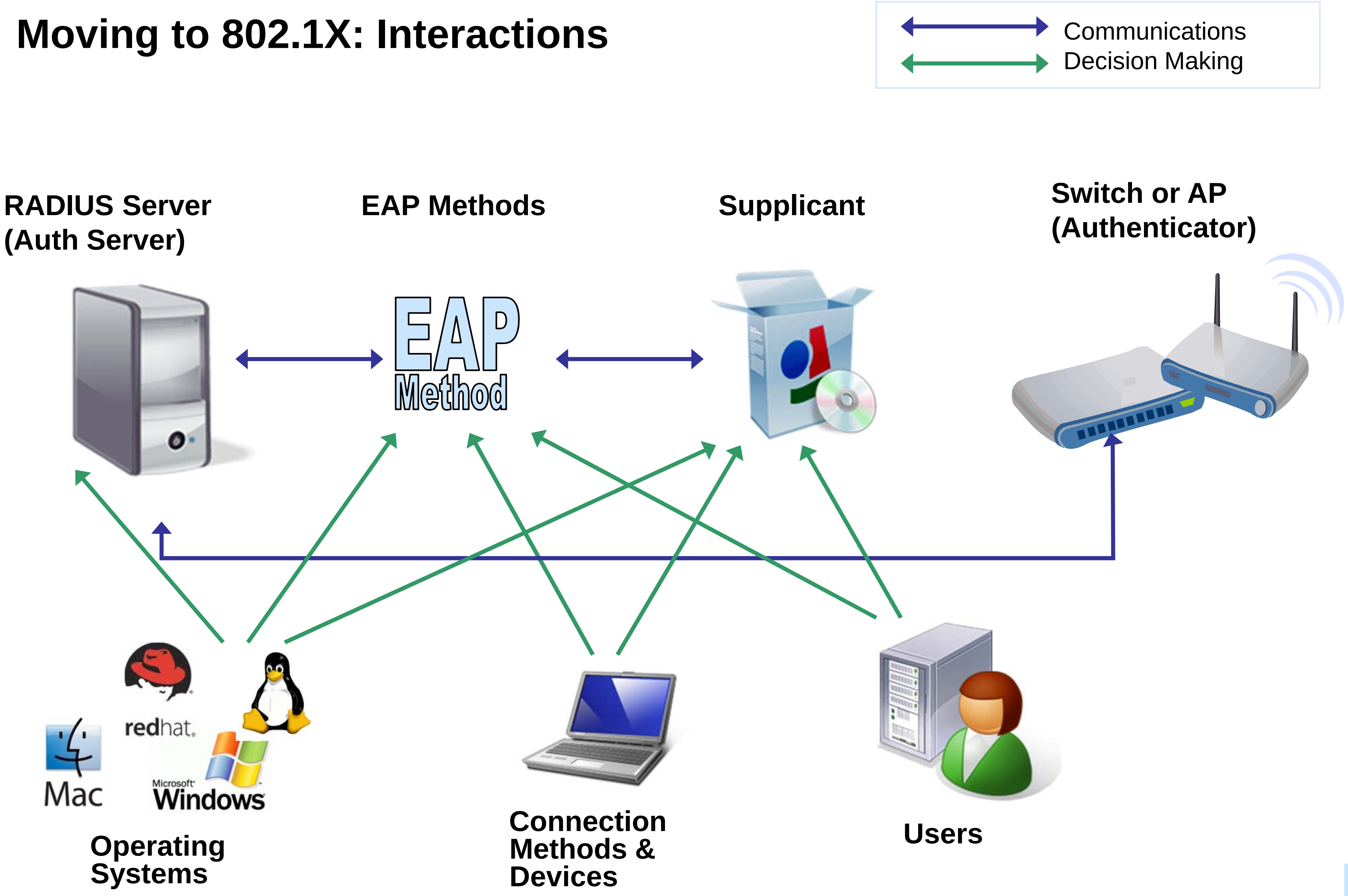
Moving to 802.1X: Steps to a Successful Implementation

1. Evaluate Current Network Environment
2. Choose a Supplicant
3. Choose an EAP method
4. Choose/Configure your RADIUS Server
5. Configure your Switches and APs

Moving to 802.1X: Considerations

- **Identify Organizational Policies**
  Get management blessing and align network policies with written policies
- **Operating systems on computers**
  Affects supplicants and EAP methods
- **Users, Environment and Culture**
  Does your environment have shared PCs, how long is average use time, are connections wired, wireless, or both
- **Machine Logon**
  Does your environment require machine logon capabilities for group policies?
- **User Management**
- **Switches and Access Points**
  Brands, interoperability, capability and management
- **Authentication Server**
  RADIUS type affects available EAP methods and compatible supplicants
- **Access Policies**
  802.1X enforcement should be in line with written policies
- **VLANs currently in place**
- **DHCP servers & scopes**

Moving to 802.1X: Interactions



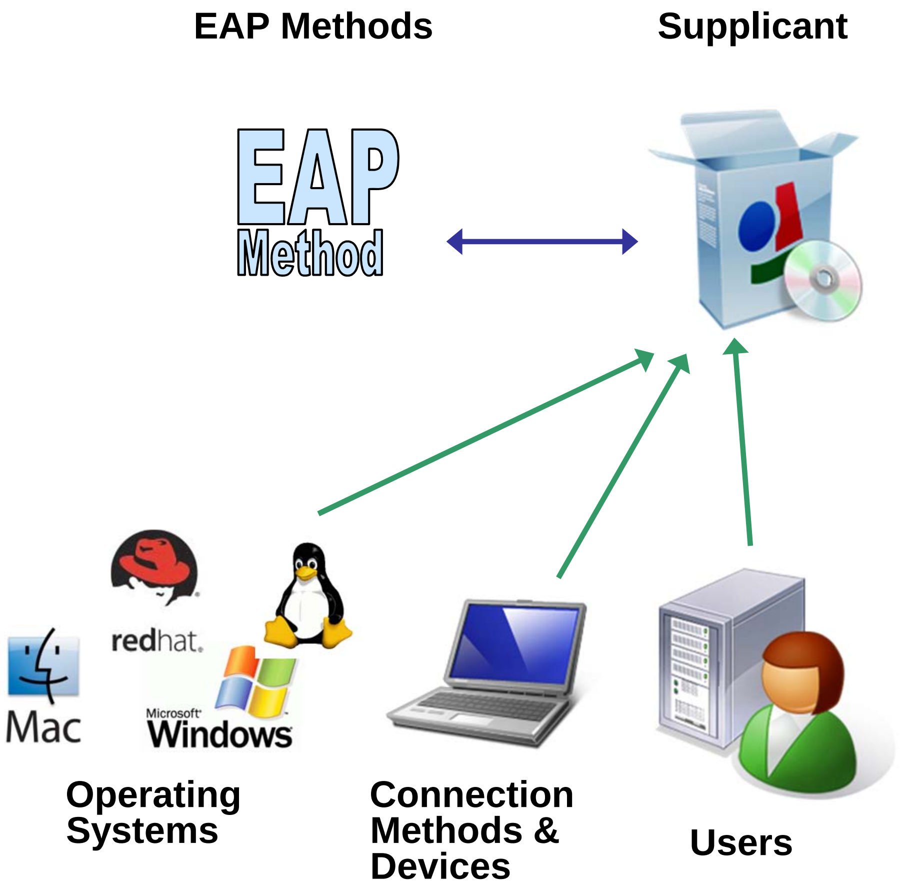
How To: Pick Supplicant(s)

Your chosen supplicant(s) should be compatible with the operating systems you’re supporting.

Open-source supplicants are available for free and are often the most cost-effective choice for a mixed environment.

You may choose to use more than one supplicant, as long as the EAP methods are supported on both. Keep in mind this may cause some difficulties with user support.

Make sure your choice will support all your enterprise needs. Some supplicants, such as the Cisco Client, do not support machine logon, which is required for most AD enterprises with group policies.



EAP Methods

Supplicant

Operating Systems

Connection Methods & Devices

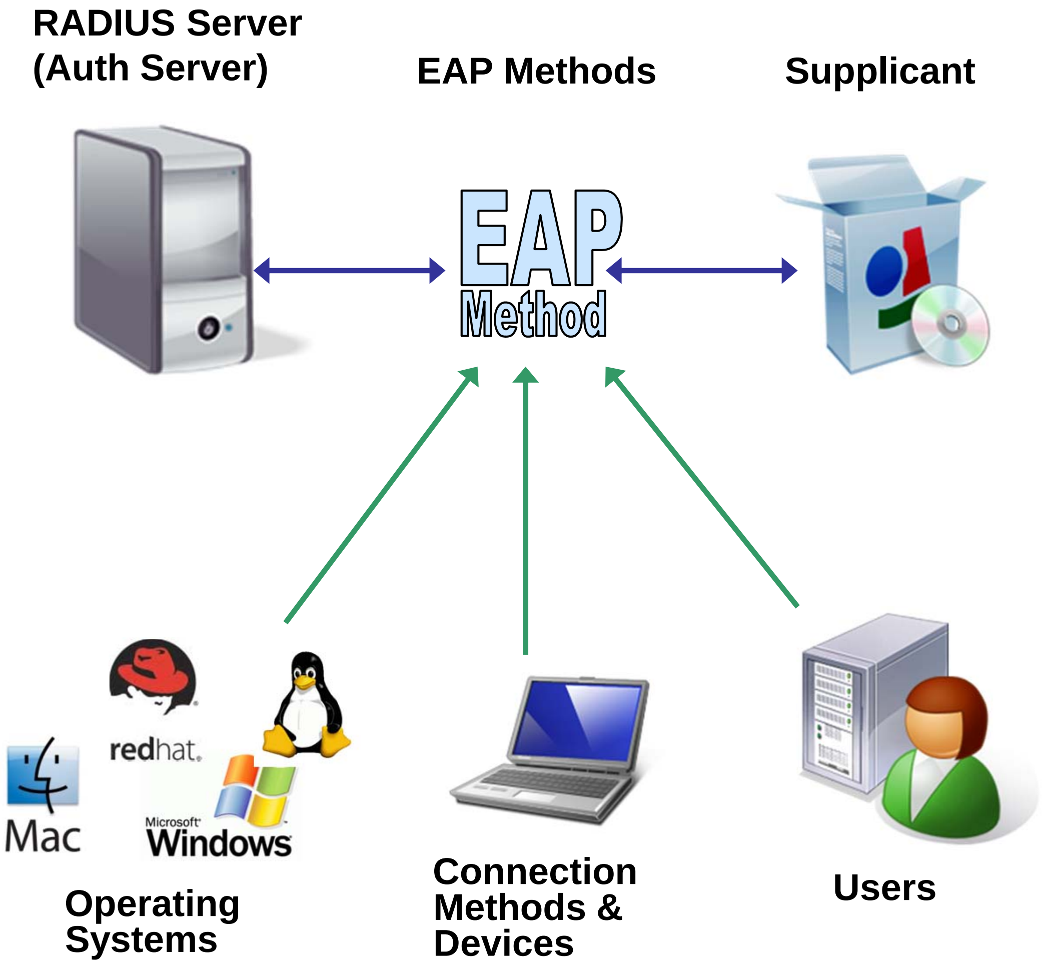
Users

How To: Pick an EAP Method

Your chosen EAP method needs to be supported by your supplicant (which may be dependent on your OS) and your RADIUS server.

Choosing an open standard EAP type will ensure your system is interoperable and upgradeable.

EAP types require different authentication schemes, some require encryption key management and PKI infrastructure. Some are better suited for wired and some better suited for wireless.



Popular EAP Methods

method	common implementation	server	clients	authentication attributes	standard	deployment difficulty	wireless security
EAP-MD5	challenge-based password	none	***	←	RFC 1994 RFC 2284	◆◇◇◇	◇◇◇◇
EAP-TLS	certificate-based two-way authentication	📜	📜	↔	RFC 2716	◆◆◆◆	◆◆◆◆
EAP-TTLS	server auth via certificates; client auth via another method	📜	TLS	↔	draft-ieft-pppext-eap-ttls-01.txt	◆◆◆◇	◆◆◆◇
PEAP	server auth via certificates; client auth via another eap method	📜	MS-CHAPv2 EAP-TLS EAP-GTC*	↔	IETF	◆◆◆◇	◆◆◆◇
LEAP	two-way challenge-based password	***	***	↔	Proprietary	◆◆◇◇	◆◇◇◇
EAP-FAST*	certificate-based two-way Authentication*	📜	📜 PAC	↔	draft-cam-winget-eap-fast-03	◆◆◆◆ ◆◆◇◇	◆◆◆◇ ◆◇◇◇

How To: Configure Your RADIUS Server

-Based on Microsoft IAS RADIUS

-Add RADIUS clients (Authenticators, such as switches and APs) by IP or DNS

-Add remote access policy (select connection apply to selected group(s), choose EAP method)

-Import server certificate (either x.509 from CA, or self-signed)

-Enable remote access logging

-In AD, enable Dial-in access

-Tweak policies for custom configurations (dynamic VLANs, group associations)

-With some authentication methods, it may be necessary to set *store password using reversible encryption*

RADIUS Server (Auth Server)

How To: Configure Your Switches and APs

-Switches and APs acting as 802.1X Authenticators must support 802.1X

-Add RADIUS servers to authentication list

-Setup RADIUS server shared secret(s)

-Turn on 802.1X per port, or on the entire switch

Switch or AP
(Authenticator)

Part IV: 802.1X, NAC & IDM

Back to… 802.1X and ‘NAC’

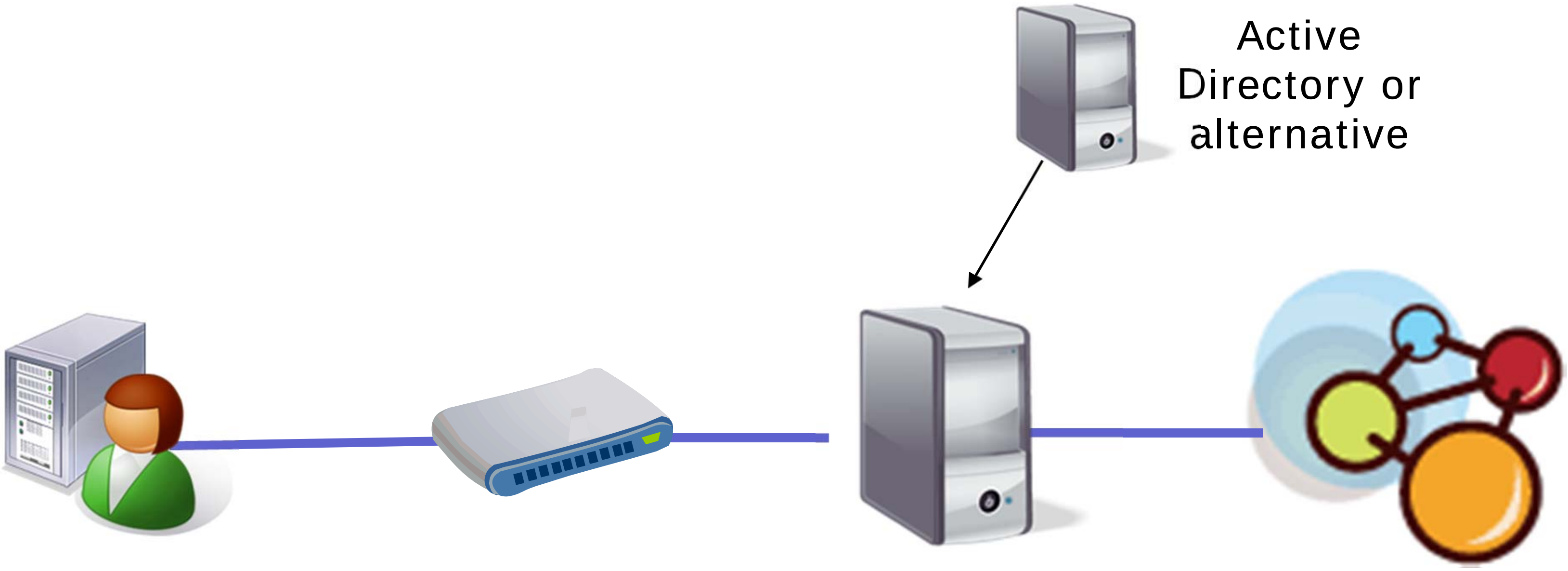
- **802.1X, just one ‘A**’. Because 802.1X leverages RADIUS servers, which are authentication, authorization, and accounting (AAA) servers, 802.1X is sometimes assumed to provide all three functions. In reality, 802.1X provides only the authentication piece.

- **NAC vs NAC.** Adding to the confusion is the inconsistent use of the “NAC” acronym within the industry. Some vendors and research firms use it to refer to **network admission control**, a fairly narrow function, while others use it to refer to **network access control**, a much broader set of functions that includes controlling what users do once they’re authenticated and on the network.

- **802.1X** is a standard method for port-based **network admission control**. User credentials (such as a password, one-time token, or digital certificate) must be validated before a physical LAN port or wireless access point can be used for network access.

- **NAC (Network Access Control)** builds on 802.1X to provide health and compliance checks prior to connection, policy-based resource control and continuous health and behavior monitoring as well as policy enforcement while connected.

Access Control Example: 802.1X and ProCurve IDM



Active Directory or alternative

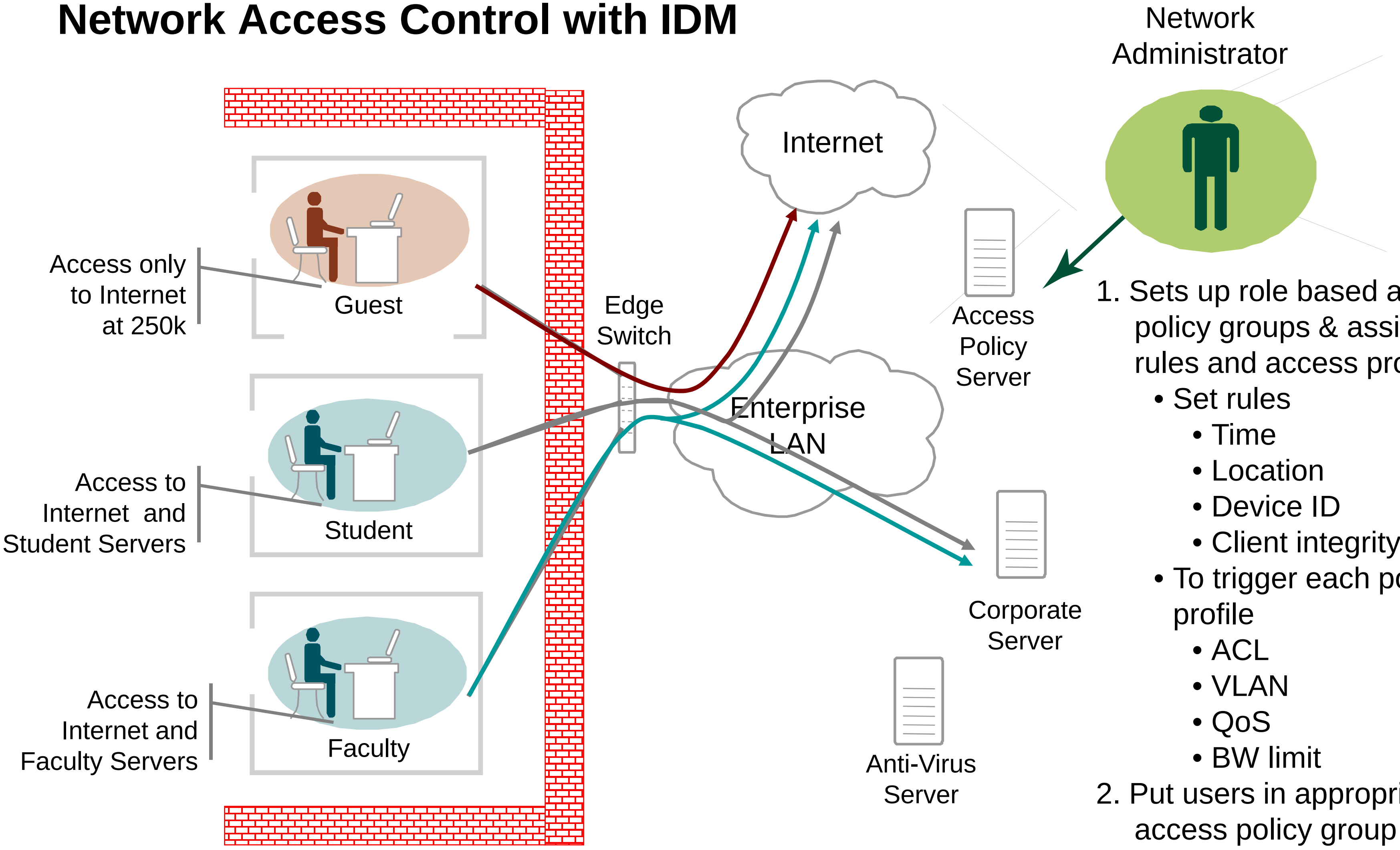
802.1x Client Supplicant or Web/MAC Auth

ProCurve Switch 802.1x Enforcement with VLAN quarantine, ID based NW configuration and Virus Throttling

ProCurve IDM policy engine working with Radius Server

Network is customized for each User via IDM

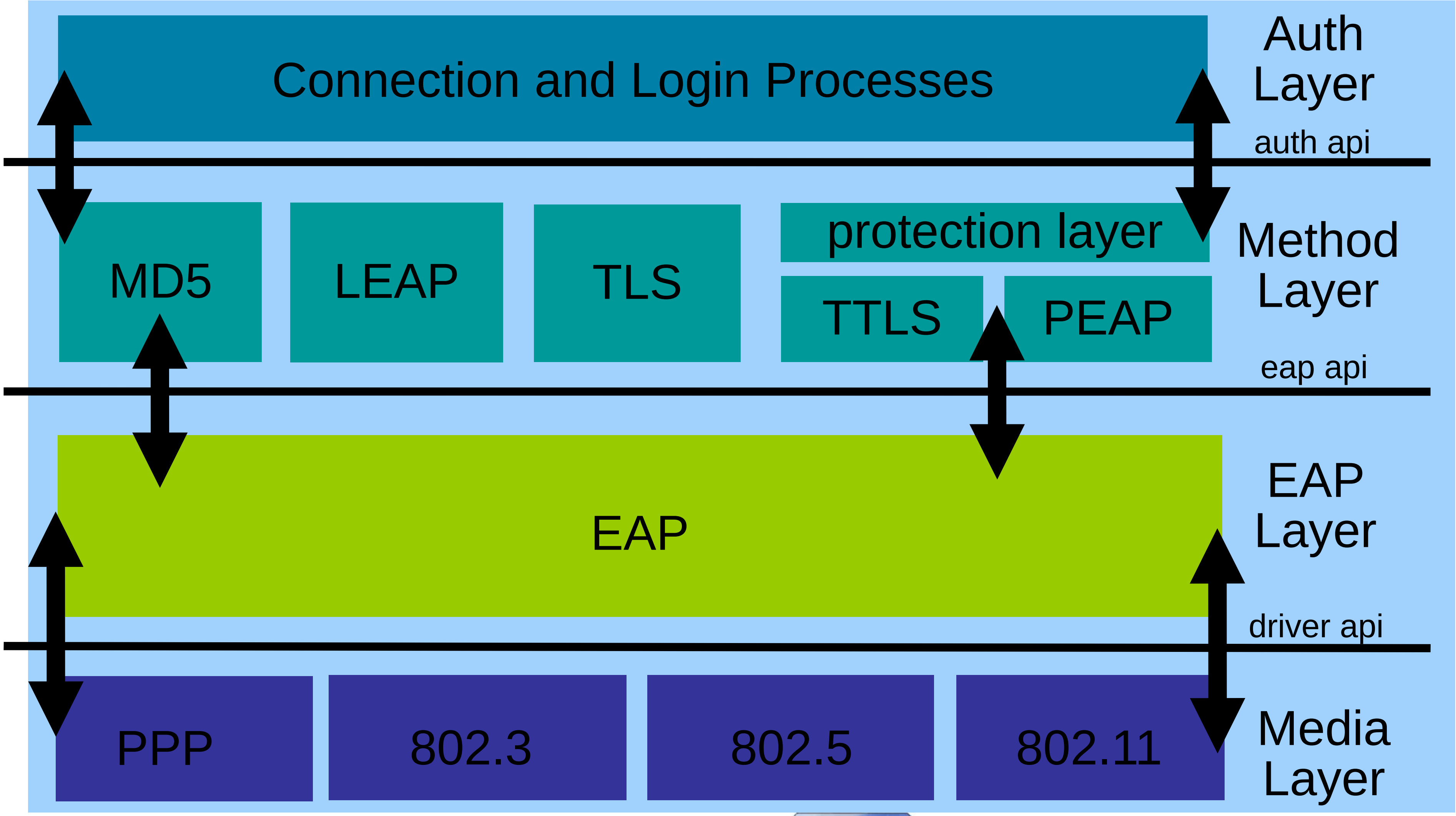
Network Access Control with IDM



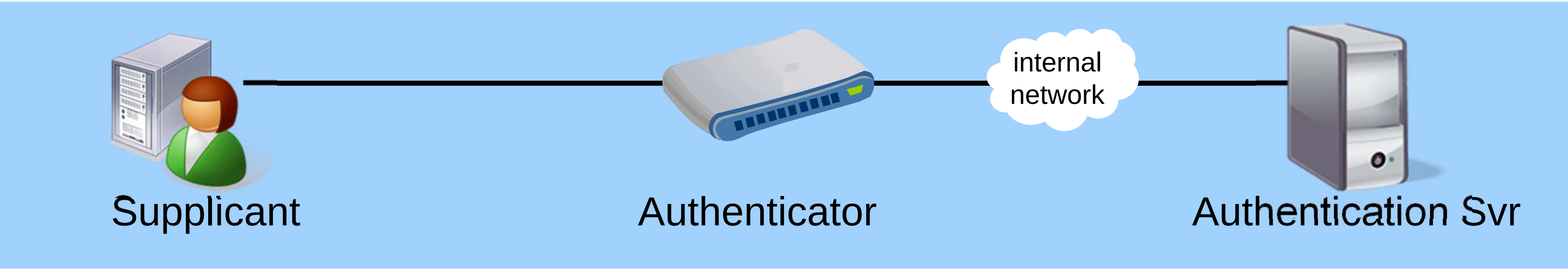
1. Sets up role based access policy groups & assigns rules and access profiles:
   - Set rules
     - Time
     - Location
     - Device ID
     - Client integrity status
   - To trigger each policy profile
     - ACL
     - VLAN
     - QoS
     - BW limit
2. Put users in appropriate access policy group

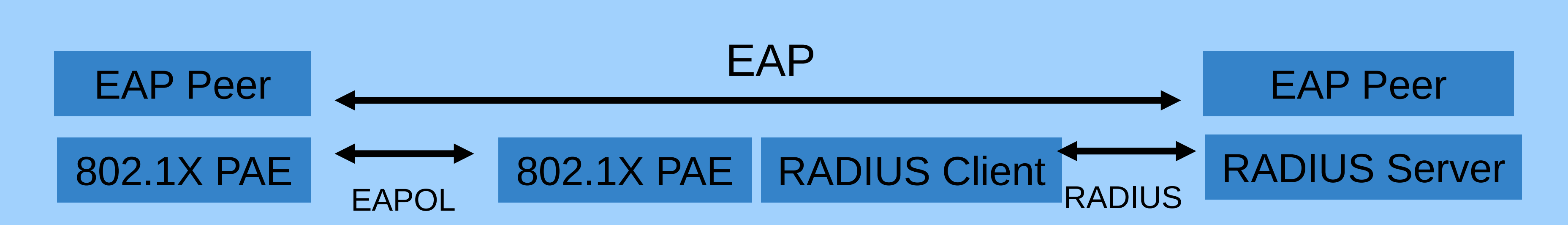
Part V: Technical Review

EAP Block Diagram



802.1X Physical & Logical Topologies




EAP

EAP Peer

EAP Peer

802.1X PAE

EAPOL

802.1X PAE

RADIUS Client

RADIUS

RADIUS Server

802.1X Port Access Entitity (PAE):

Protocol entity associated with each port that implements EAP over lans (EAPOL)

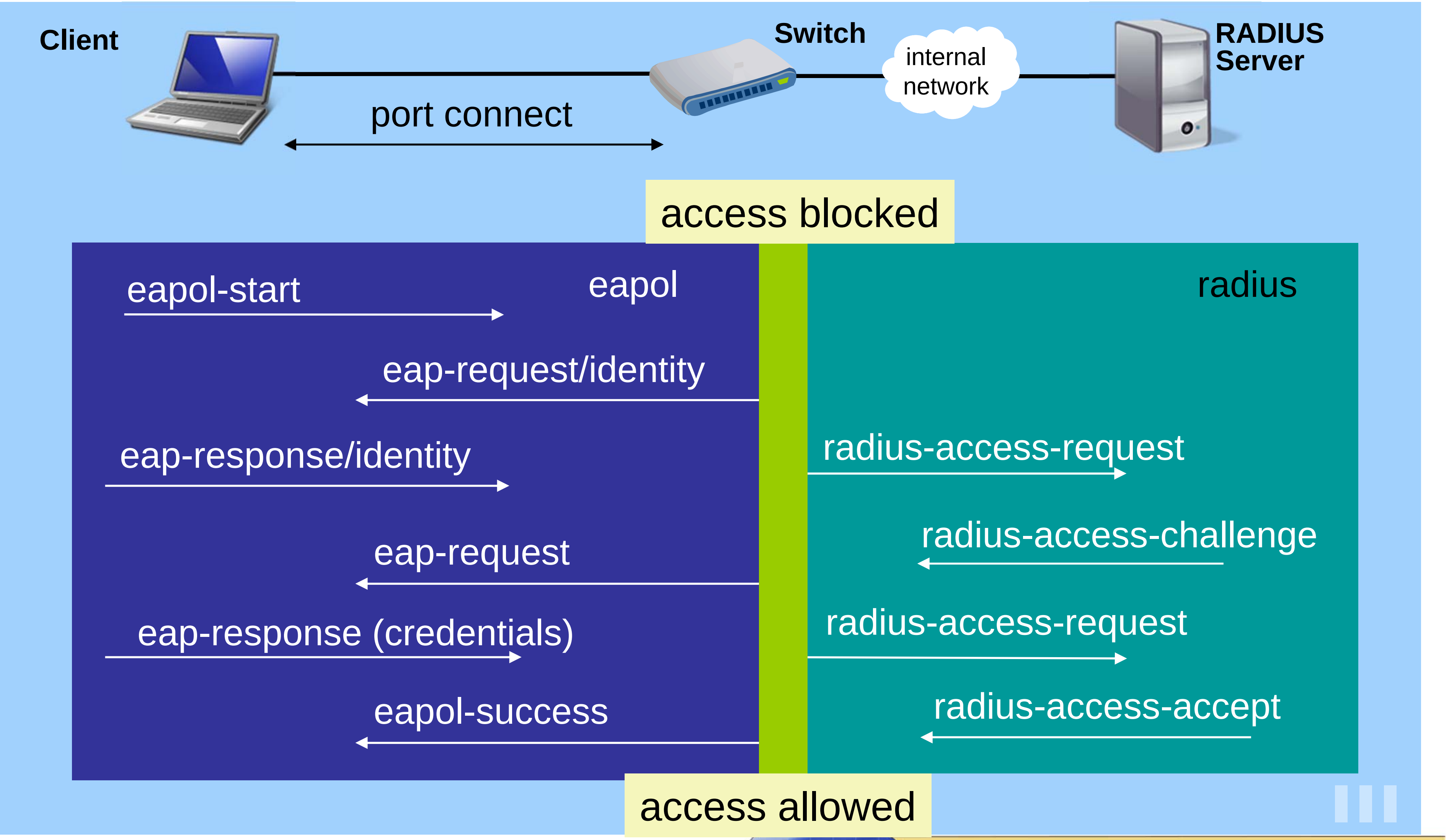
Extensible Authentication Protocol (EAP):

Simple encapsulation protocol support numerous authentication methods (RFC 2284)

RADIUS Client & Server:

Backend protocol entity supporting authentication, authorization & accounting for network access (RFC 2865)

EAP 802.1X Wired Communications



Recap of 802.1X Benefits

802.1X will help you…

- Prevent unauthorized access to the network
- Extend physical security to each port
- Protect the network from malicious users and propagation of traffic
- Create a ‘trusted infrastructure’
- Eliminate rogue APs, unauthorized switches
- Increase security and flexibility with dynamic VLAN assignment
- Enhanced wireless security
- Stop broadcast storms from loops
- Provide a means for compliance reporting
- Ease interoperability with a variety of other security software and hardware solutions

Thank You

Questions or Comments?
Contact:

Jennifer Jabbusch, CAD
jj@cadinc.com

Neal Hamilton, ProCurve by HP
neal.hamilton@hp.com

Mike McPherson, ProCurve by HP
mcpherson@hp.com