

# Implementing 802.1X

Fall 2006 Internet2 Member Meeting  
December 6, 2006

Rich Cropp

Penn State University  
rac@psu.edu

Kevin Miller

Duke University  
kevin.miller@duke.edu

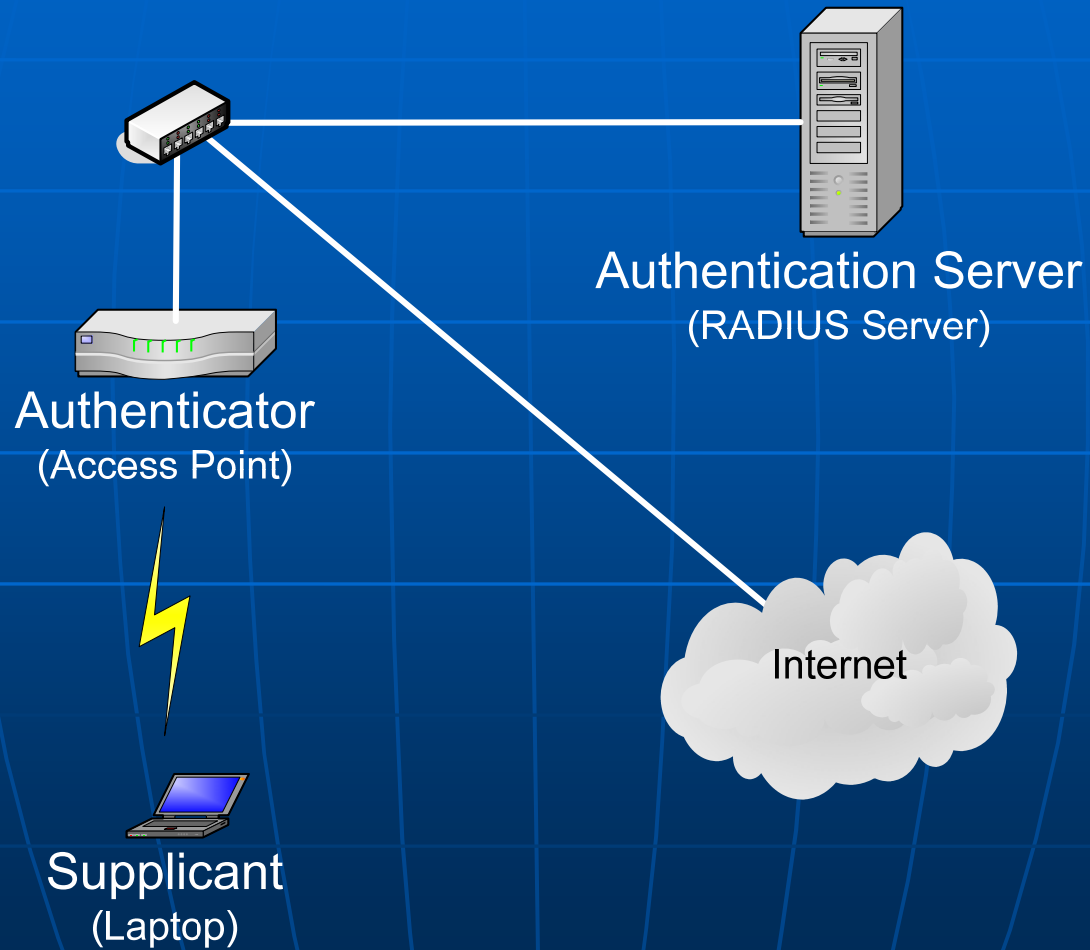
# Agenda

- What is 802.1X?
- Why use 802.1X?
- Why not use 802.1X?
- Authentication
- Infrastructure
- Deployment
- Management
- Questions?

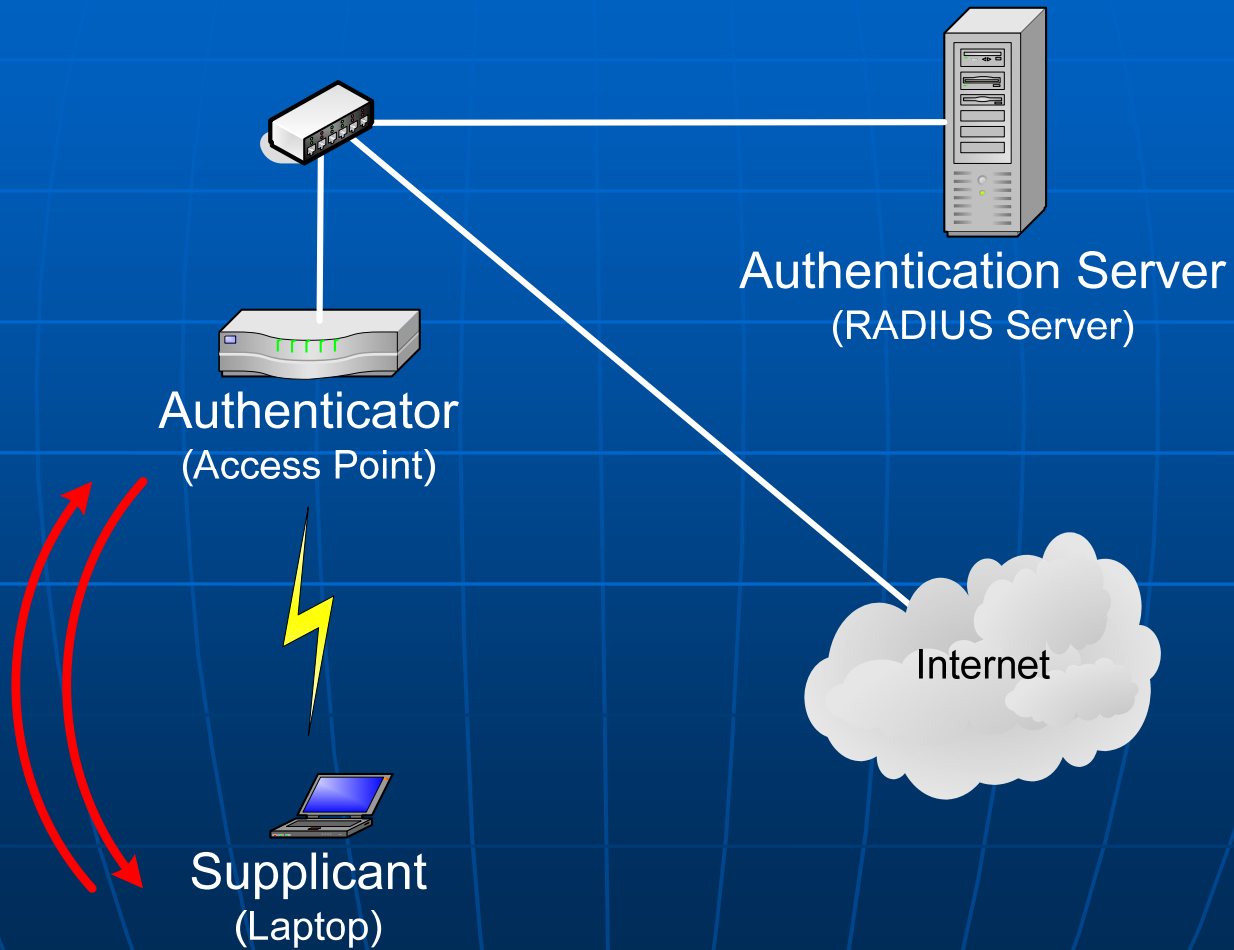
# What is 802.1X

- IEEE Standard for Port-Based Network Access Control
- Provides authentication framework for LAN access
- Uses the Extensible Authentication Protocol (EAP)
- One of the components of 802.11i

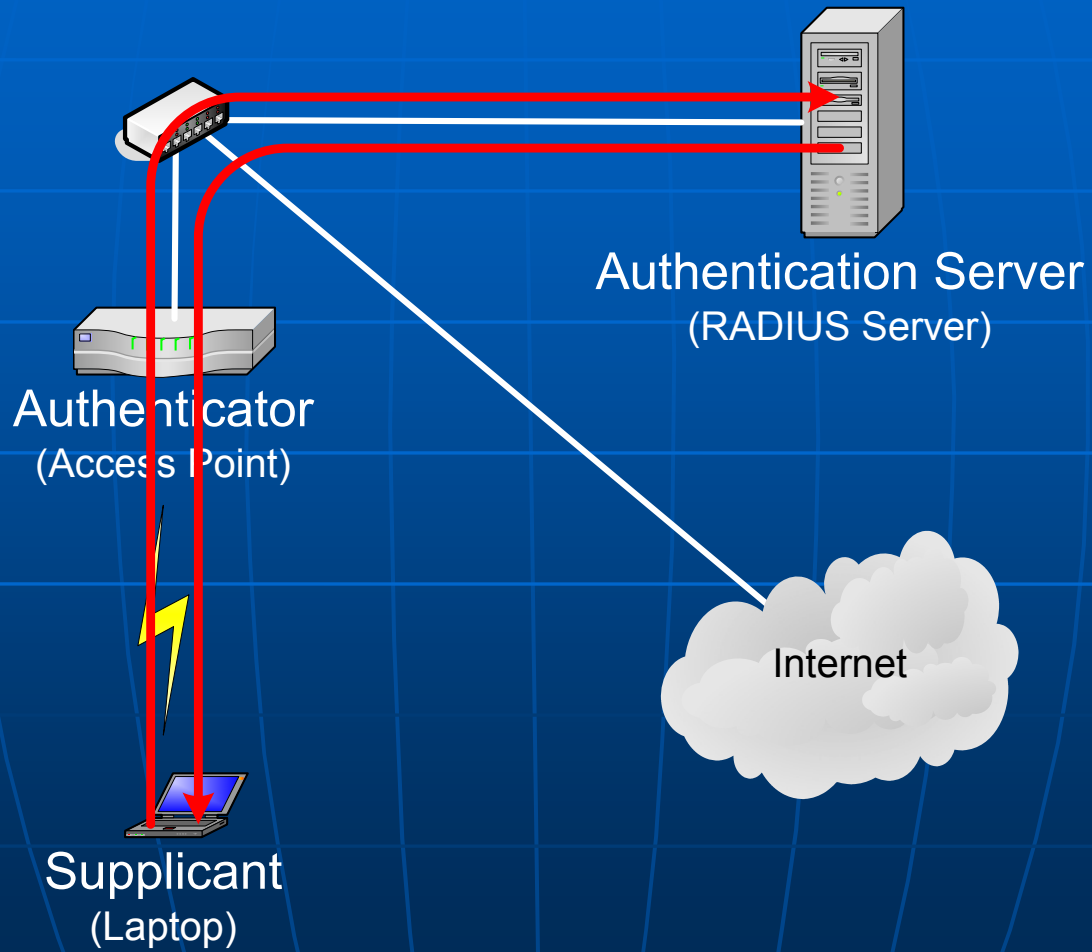
# 802.1X



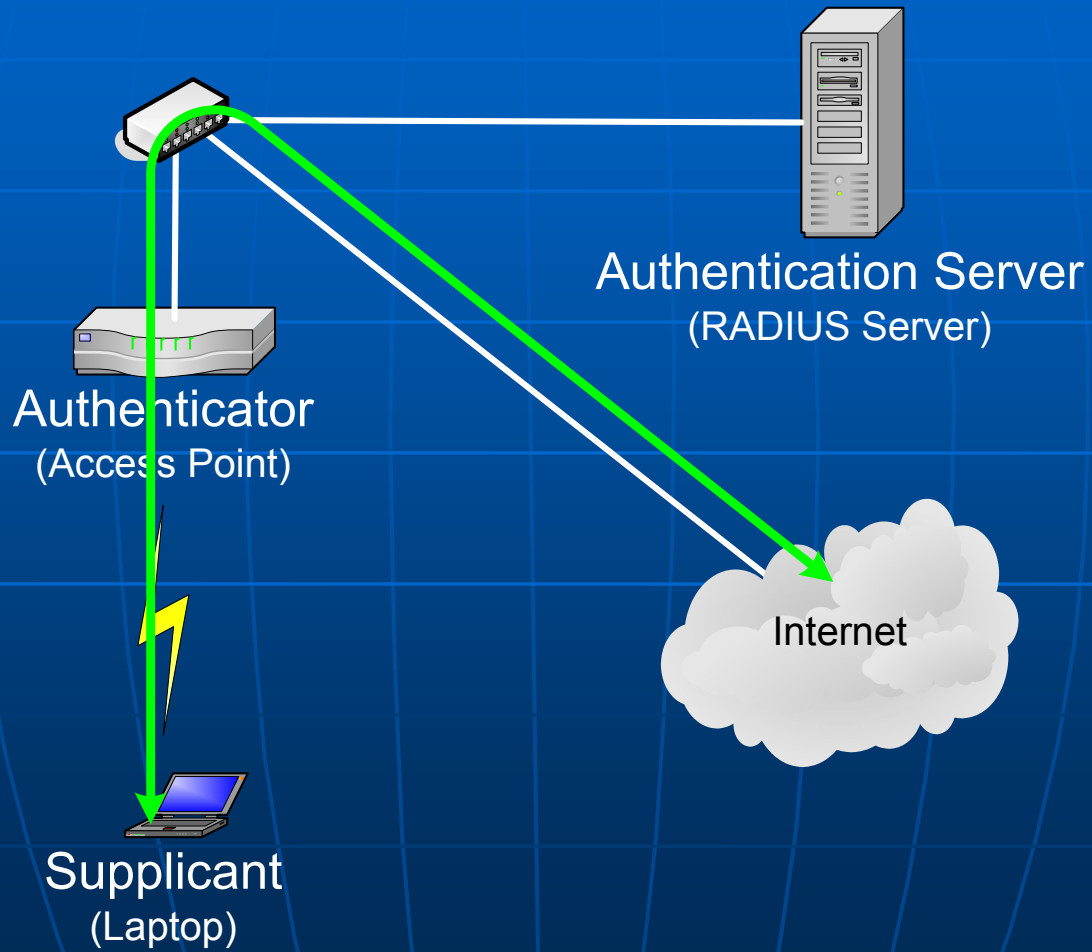
# 802.1X



# 802.1X



# 802.1X



# Why use 802.1X?

- Strong Authentication
  - User-based or machine-based
- Enable scalable over-the-air encryption
- Assign network profile by AuthN
  - Vlan, ACL, QoS
- Contain SSID spoofing (wireless)

# Why not use 802.1X

- Common alternatives: Web, VPN, MAC
- Long dependency chain
  - Client: supplicant, EAP, encryption (hardware)
  - Network: AP/switch support
  - Middleware: RADIUS, authentication server

# Authentication

- Choosing an EAP type
  - X.509 Certificates
    - EAP-TLS
  - Plaintext password (LDAP, Kerberos, OTP)
    - EAP-TTLS:PAP
  - Windows hashed password
    - PEAP:MSCHAPv2
    - EAP-TTLS:MSCHAPv2
- UserID format
  - userid vs userid@realm

# Authentication

- Guest login – 802.1X or other?
- AuthZ
  - Allow/deny
  - Access profile (ACL, vlan, ...)
- Credentials
  - Common
  - Dedicated
  - Merge of several sources

# Infrastructure

- RADIUS Server
  - Open Solution's Radiator
  - Funk Steelbelted RADIUS
  - Cisco ACS
  - Microsoft IAS
  - FreeRADIUS
- Multiple/Redundant RADIUS Servers
- RADIUS Transaction Rate
- Certificate for RADIUS Server
  - Purchase?
  - Self-signed?
- Logging, query tools

# Infrastructure

- AP / Switch support for 802.1X
- Wired 802.1X migration support
  - MAC Based
  - Default VLAN

# Deployment

- SSID name
- Broadcast SSID
- Multiple SSIDs
  - Open (current, guest, provisioning)
  - 802.1X
  - Client behavior
- Encryption: DynWEP, WPA, WPA2
  - Overloading SSID
- What about devices that don't support 802.1X?
- Client configuration
- Which supplicant?

# SupPLICANTS and Supported EAP Types

	EAP-TLS	EAP-FAST	LEAP	MD5	PEAP EAP-TLS	PEAP MSCHAPv2	EAP-TTLS PAP	EAP-TTLS MSCHAPv2	EAP-TTLS MSCHAP	EAP-TTLS CHAP
WinXP/2000/Vista Native	X			X	X	X				
MacOS 10.4 Native	X	X	X	X	X	X	X	X	X	X
wpa_supplicant	X	X	X	X	X	X	X	X	X	X
Odyssey	X	X	X	X	X	X	X	X	X	X
Aegis	X	X	X	X		X	X	X	X	X
SecureW2							X	X	X	X

# Management

- How quickly can you make changes on the wireless or wired network infrastructure?
- How do you encourage use of 802.1X in “dual mode” configurations?
- Can you disconnect authenticated users in your network hardware/software?
- Can you effectively troubleshoot a user connection problem?

# IT Participation

- IT Management / Oversight
- Security Officer
- Security Ops
- Wireless Network Ops
- RADIUS Server Ops
- Authentication, Authorization Service Ops
- Customer Support
- Customer Communications

# Checklist

- Network equipment (AP/switch) supports 802.1X (Wireless: WPA)
- EAP type decision
- RADIUS setup to AuthN, AuthZ
- Client-side experience known, documented, tested
- Tools to query logs for troubleshooting & security ops
- Process (tool?) to implement large scale network changes
- Communications plan to keep users apprised of changes

# Questions?