IEEE 802.1 Working Group

Port Based Network Access Control

Vipin Jain (3Com)
Paul Congdon (HP)
Andrew Smith (Extreme Networks)

March 9, 1999

Introduction

- Problem Statement
- Existing Solutions
- Why Is It Interesting To Us
- Goals and Objectives
- Discussion
- Possible Solution
- Summary

Problem Statement

- 802 LANs deployed in semi-public areas
- LAN access accounting is often only done at L3
- Physical access allows access to enterprise networks and data
- Easy to carry out attacks on corporate networks
- Examples:
  - attaching a sniffer to a network port and capturing sensitive data
  - rebooting a desktop and accessing the network via a web browser
  - adding a rogue server to the network
  - replacing an existing workstation with another workstation

Existing Solutions

- DHCP based authentication
- Snooping on end system communication
- Proprietary server based authentication
- Proprietary MAC protocol
- TELNET-based login process
- End-to-end encryption

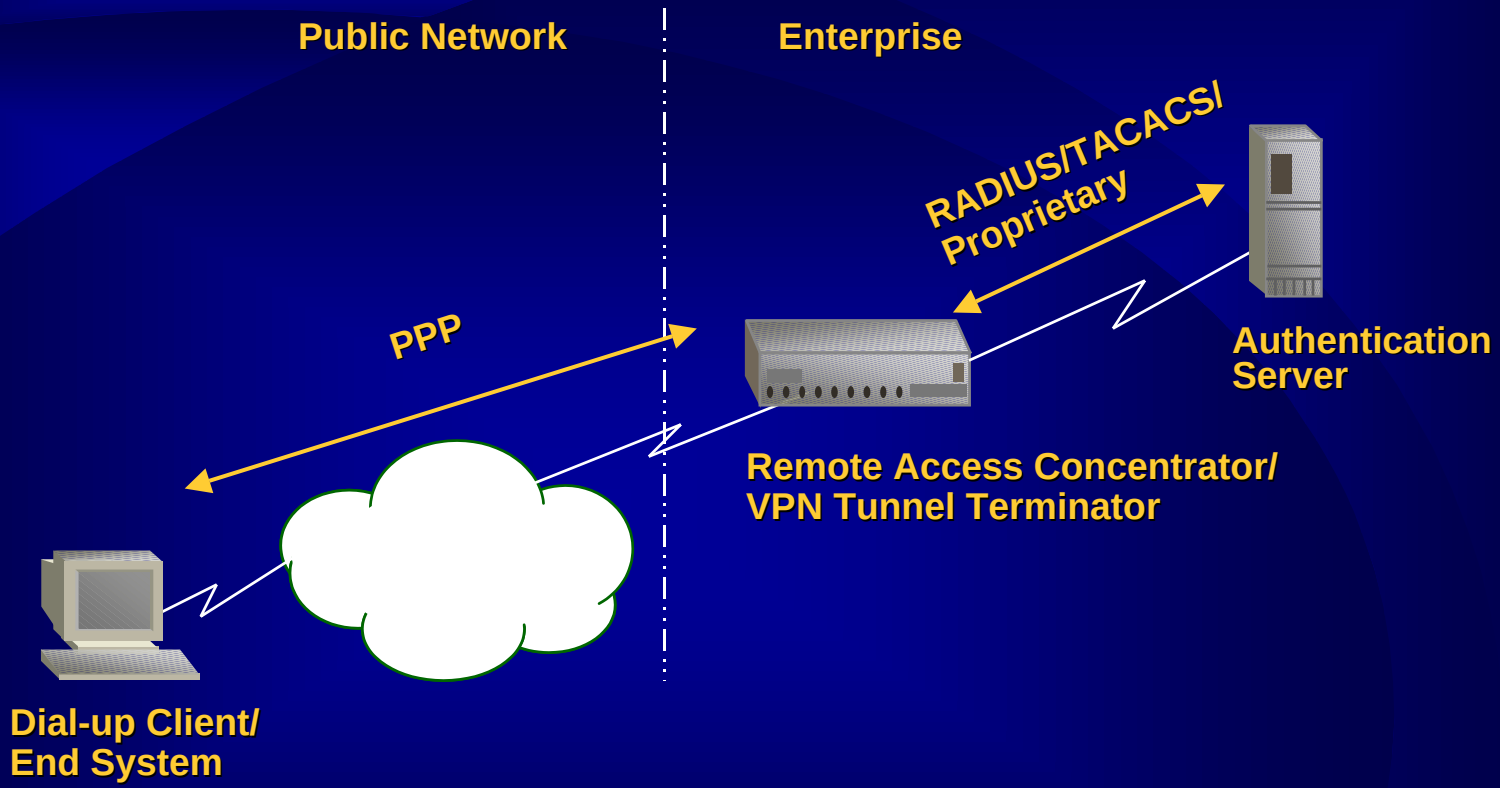
Why Is It Interesting to Us

- 802 LANs have become pervasive
- New market opportunities: semi public areas
- Customers looking for simpler solutions
- A cost effective solution for a complex problem
- It is dirty work, somebody has got to do it :-)

Goals and Objectives

- Simple access control on a bridge port
- Use existing authentication infrastructure (AAA)
- Use existing protocols wherever possible
- Do not modify or interpret authentication Information
- Do not modify user data frames to secure conversations
- Do not filter frames based on layer 2 or higher layer addressing or protocol information
- Minimize or avoid architectural changes to existing 802.1D/Q bridges - software only upgrade

Dial Up World



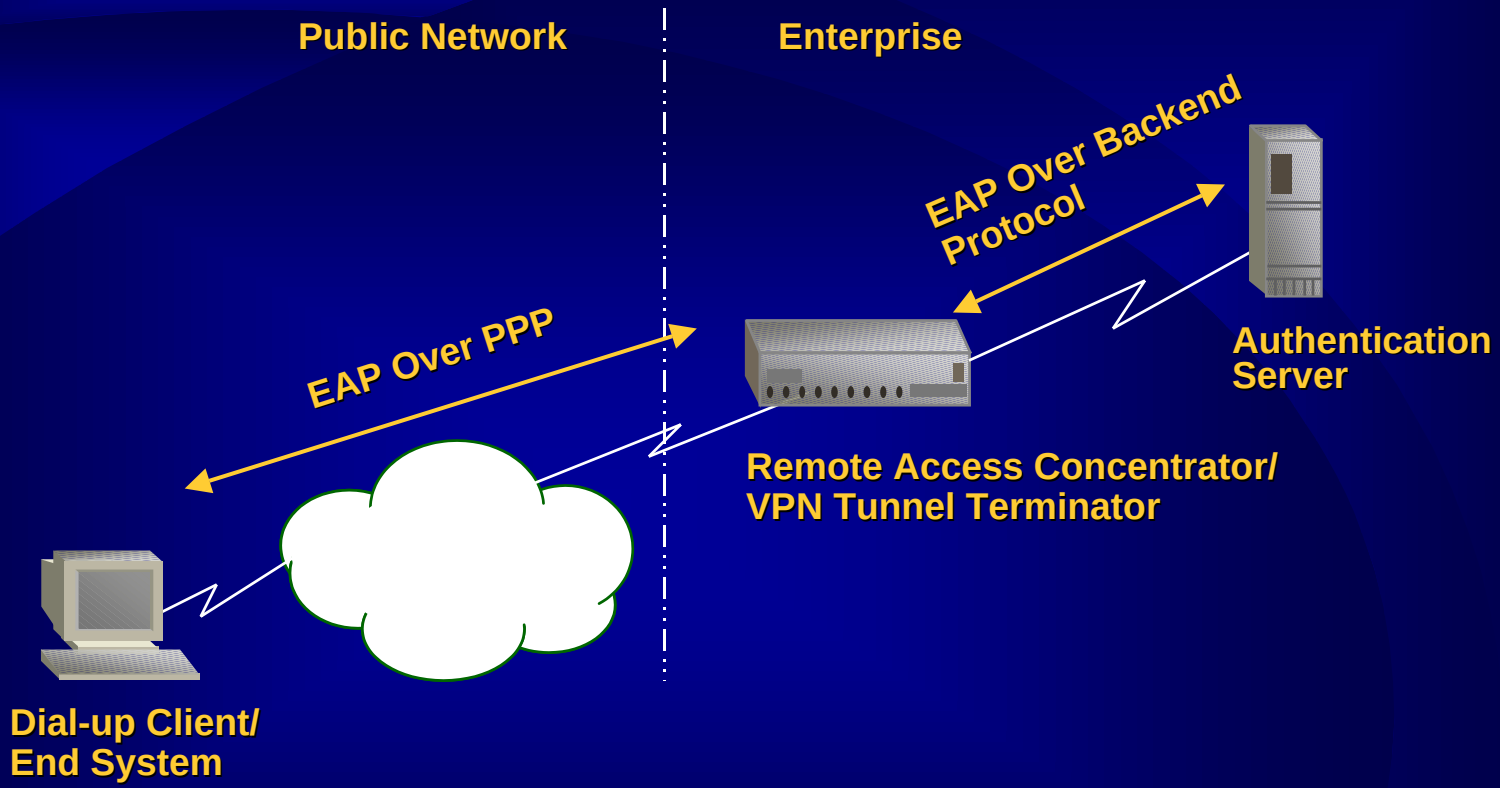
Dial Up World: Problems

- Heterogeneous AAA infrastructure
- Not extensible
  - Keep up with security vendors
  - Keep up with authentication methods
- Non-interoperable solutions
- Negotiate weak authentication
- Increased network support cost

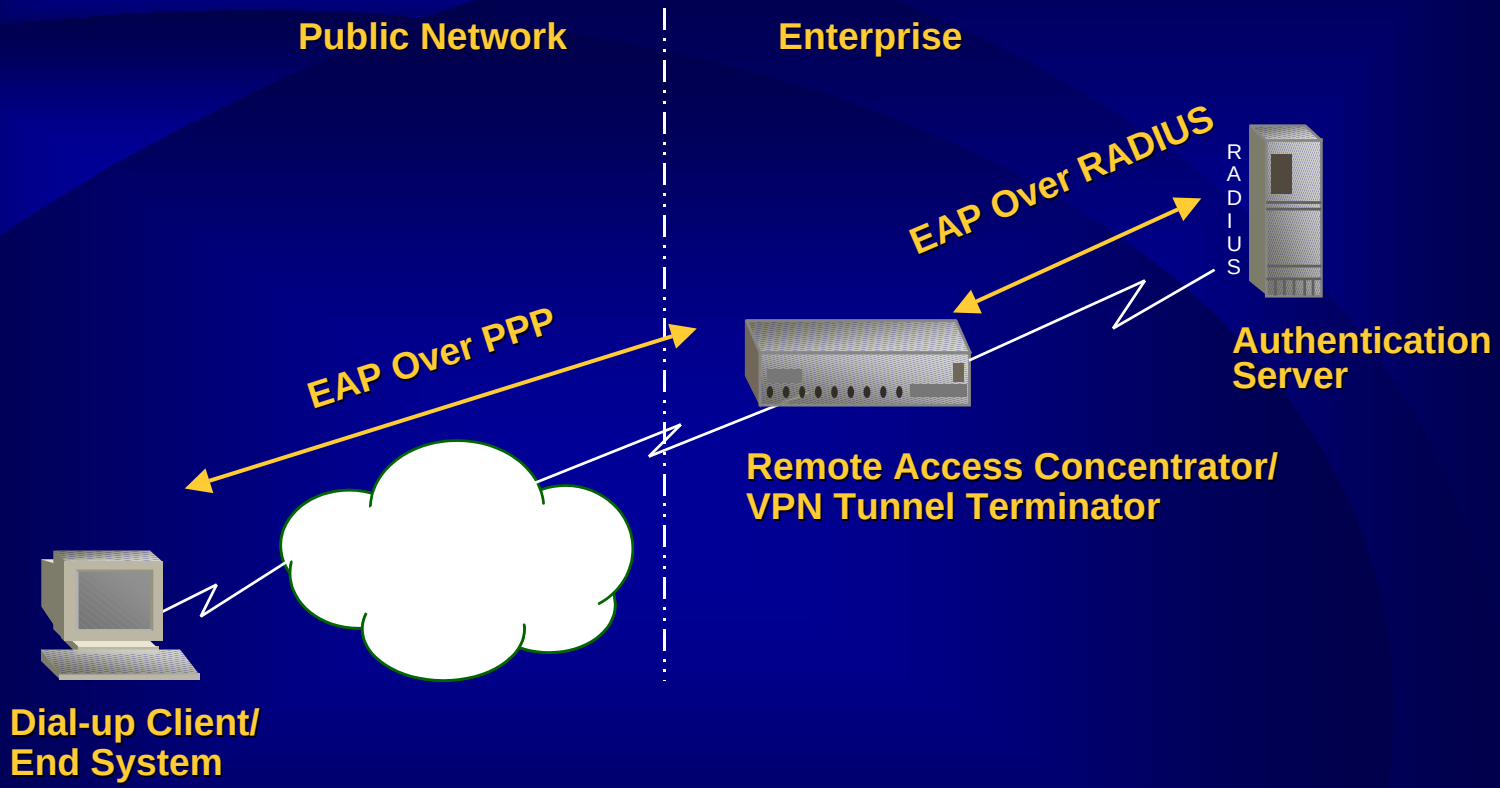
Dial Up World: EAP

- **E**xtensible **A**uthentication **P**rotocol
- Dis-associates authentication from link negotiation in PPP
- Transparent to network access device
- Authentication methods
  - MD5-challenge
  - One time password
  - Token card
- Additional methods can be supported by publishing EAP types in RFCs

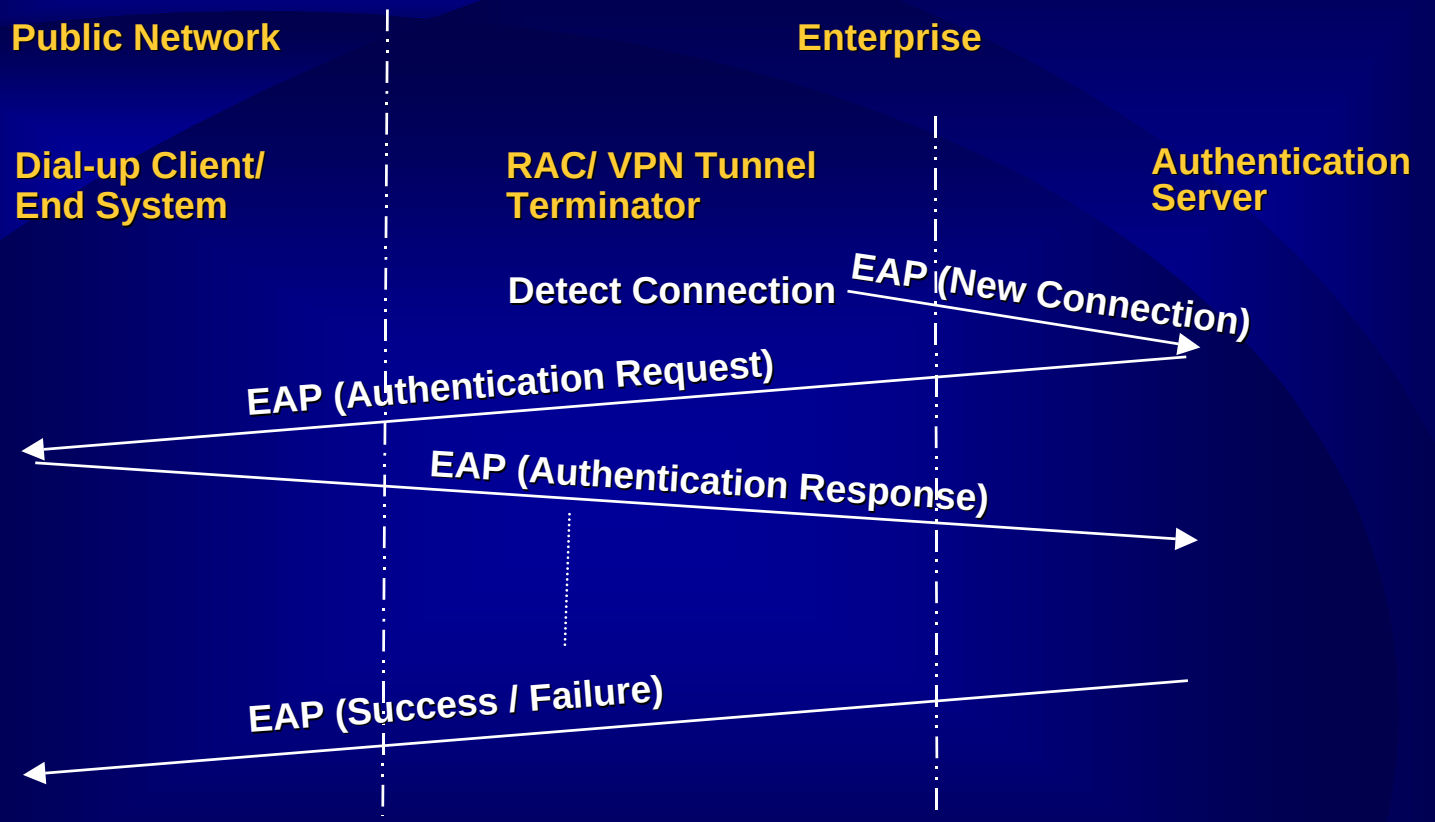
Dial Up World: Interface to EAP



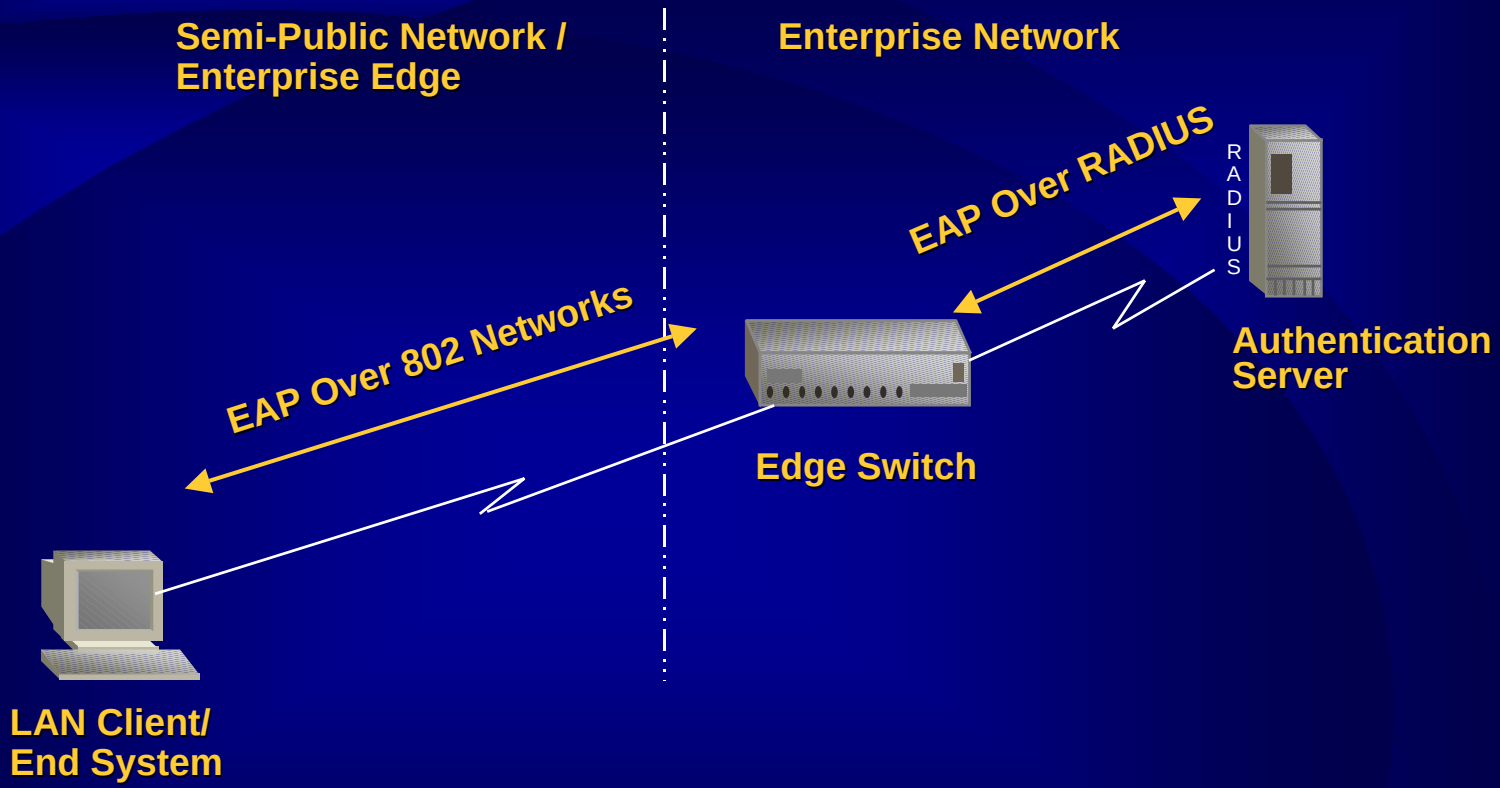
Dial Up World: Reference Interface to EAP



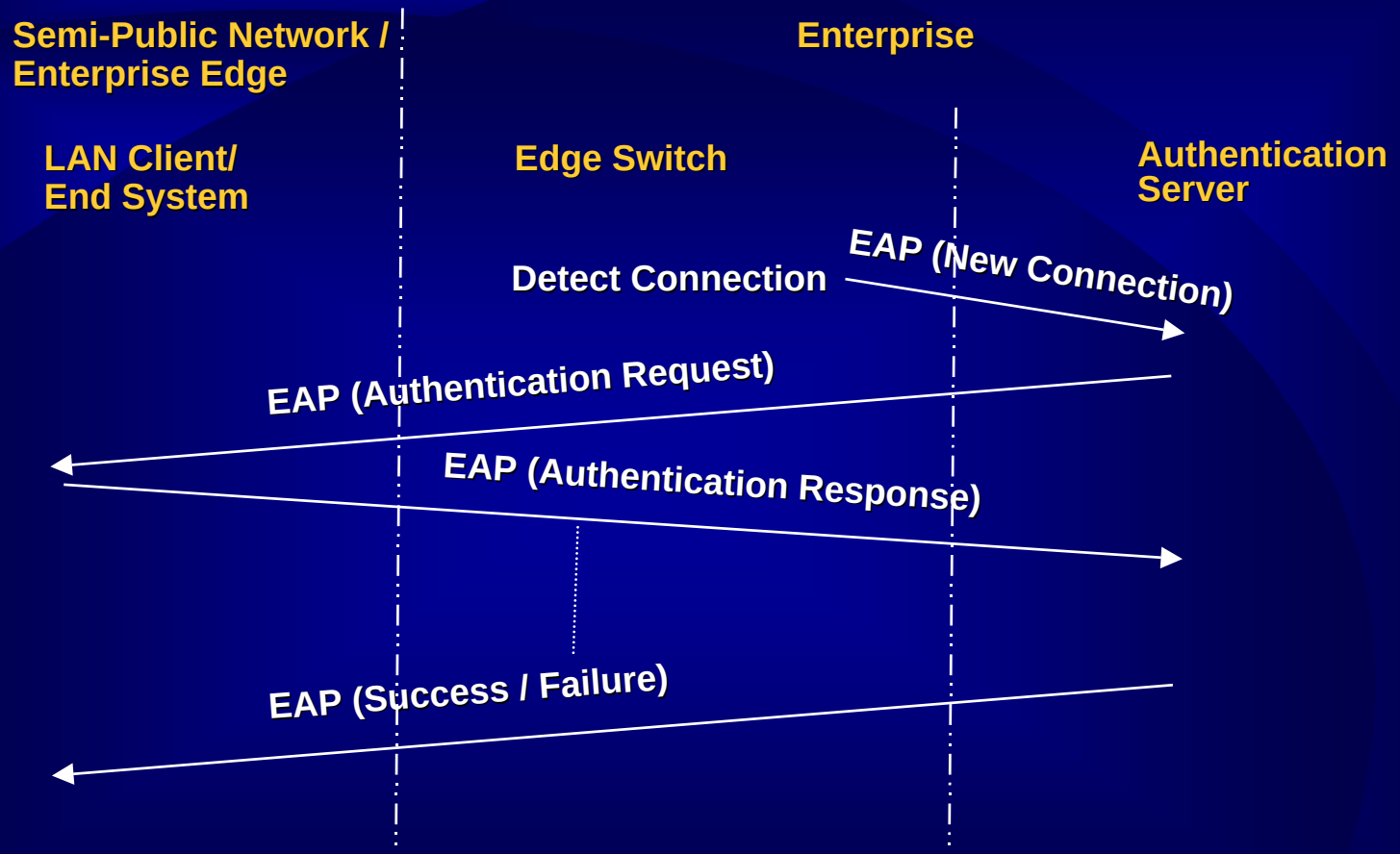
Dial Up World: Operation With EAP



LAN World: Is EAP the Solution



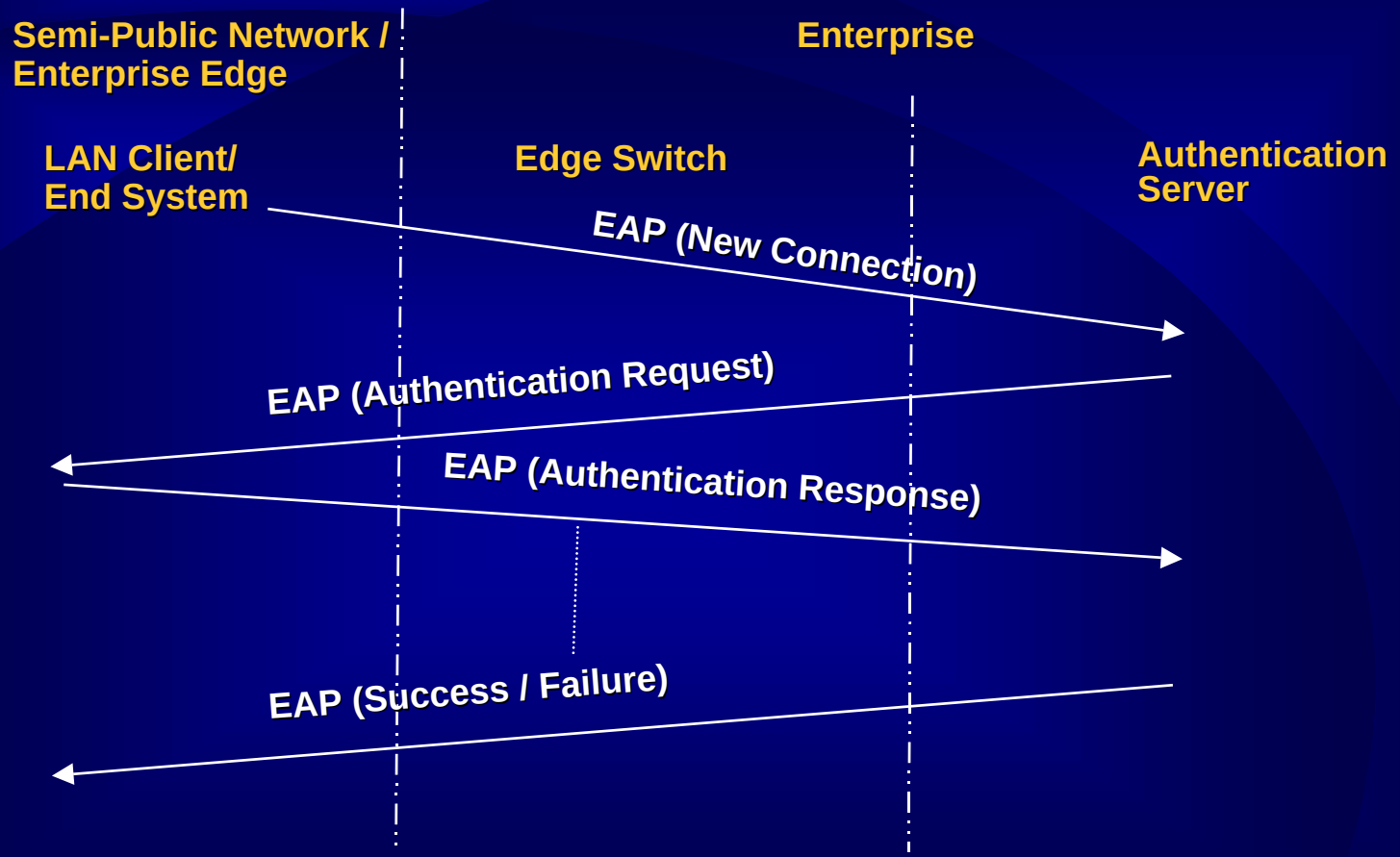
LAN World: Operation With EAP



Revisiting Problem Statement

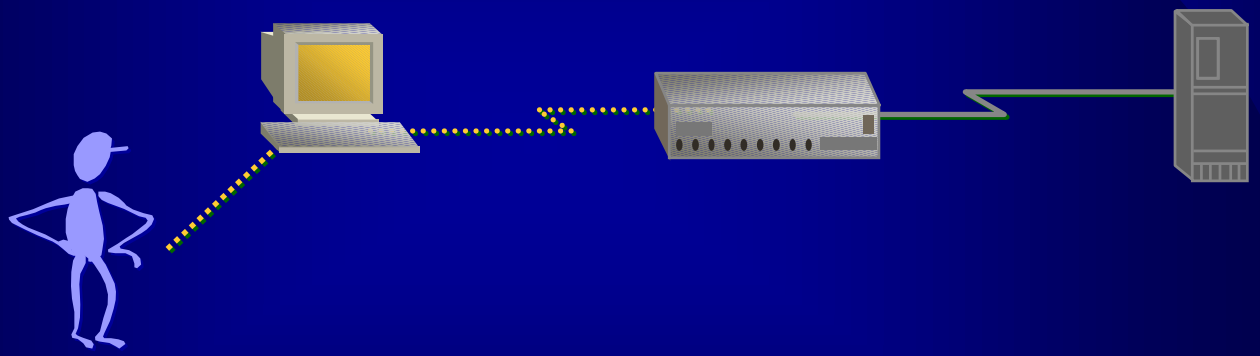
- 802 LANs deployed in semi-public areas
- LAN access accounting is often only done at L3
- Physical access allows access to enterprise data and networks
- Easy to carry out attacks on corporate networks
- Examples:
  - attaching a sniffer to a network port and capturing sensitive data
  - rebooting a desktop and accessing the network via a web browser
  - adding a rogue server to the network
  - replacing an existing workstation with another workstation

LAN World: Extending Initiation With EAP



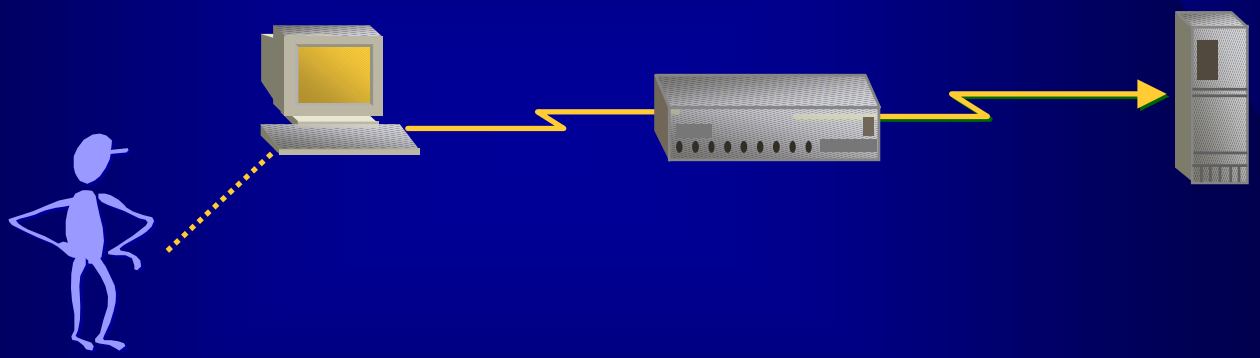
EAP in Action

- Switch detects connection on the switch port



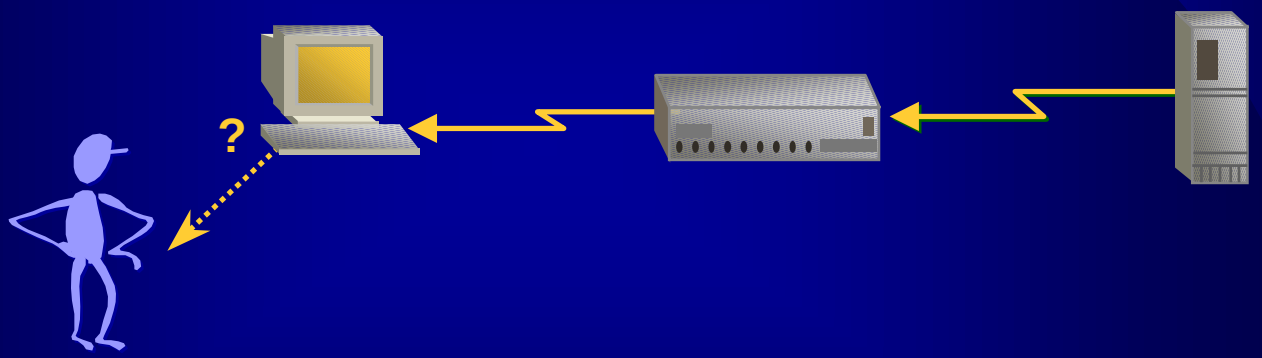
EAP in Action

- Switch detects connection or activity on the end system
- Switch tell the server about a new connection



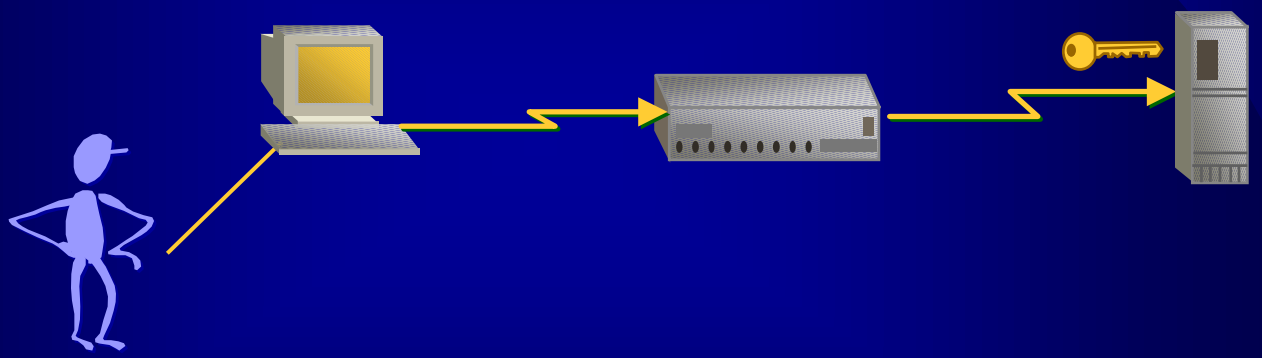
EAP in Action

- Switch detects connection or activity on the end system
- Switch tells the server about a new connection
- Server asks the end system to validate the user



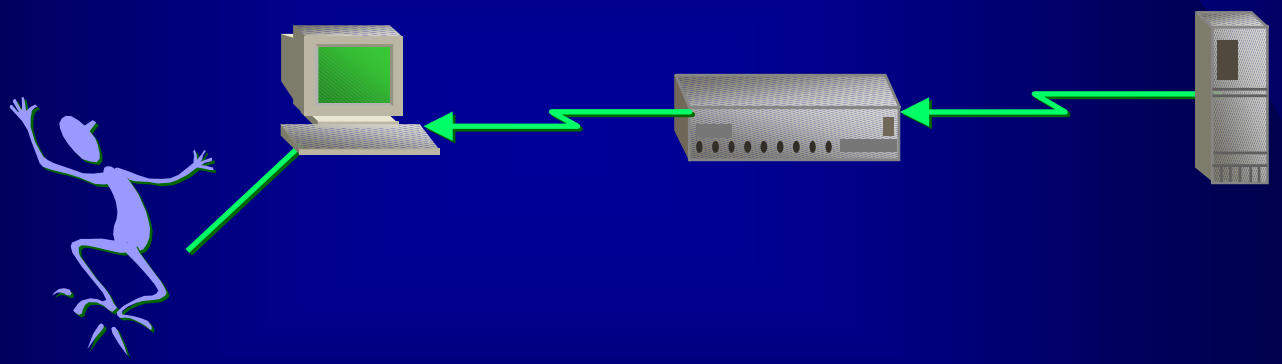
EAP in Action

- Switch detects connection or activity on the end system
- Switch tells the server about a new connection
- Server asks the end system to validate the user
- **End system gets the user credentials and sends them to the server**



EAP in Action

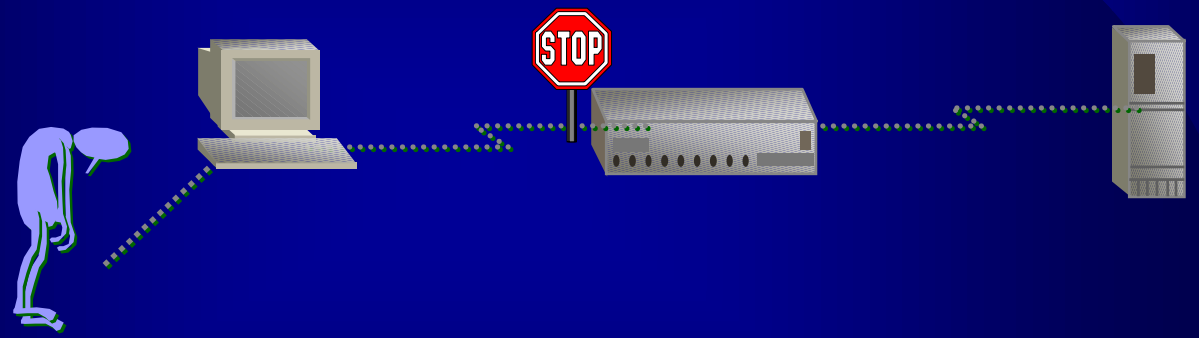
- Switch detects connection or activity on the end system
- Switch tells the server about a new connection
- Server asks the end system to validate the user
- End System gets the user credentials and sends them to the server



- **If user is validated, switch unblocks the port**

EAP in Action

- Switch detects connection or activity on the end system
- Switch tells the server about a new connection
- Server asks the end system to validate the user
- End System gets the user credentials and sends them to the server



- If user is validated, switch unblocks the port
- **Otherwise, access is denied**

Revisiting Goals and Objectives

- Simple access control on a bridge port
- Use existing authentication infrastructure (AAA)
- Use existing protocols wherever possible
- Do not modify or interpret authentication information
- Do not modify user data frames to secure conversations
- Do not filter frames based on layer 2 or higher layer addressing or protocol information
- Minimize or avoid architectural changes to existing 802.1D/Q bridges - software only upgrade

EAP in LAN World: What Does It Take

- Capability to open/close a port based on authentication
- Define EAP encoding over 802 LANs
- Backend server configuration
- Trust relationship between switch & server
- Extend 802.1 architecture to allow backend authentication clients: example, RADIUS

Summary

- Switch port access control important
- Existing solutions insufficient & proprietary
- EAP on switch ports a simple and less intrusive solution
- Works with existing AAA infrastructure
- Very lightweight
- Low processor overhead
- We can do it