校园网运行与安全管理论坛技术沙龙

802.1X和准入控制简介

段海新

2008年1月9日，清华大学

提纲

- 校园网接入安全的需求
- 802.1X 技术简介
- 网络准入控制（NAC和NAP)
- 清华802.1X实例
- 问题分析

校园网身份认证的需求

- 开放访问，没有认证
- 校内开放，网关认证
  - Web
  - 专用客户端
- 基于DHCP MAC的认证
- 其他认证技术……
- 基于802.1X的端口认证

- 计费、追踪、责任认定？？

802.1X的背景与需求

- 无线上网和Ethernet LAN的需求
- IEEE 802.1X 起源于无线局域网标准IEEE 802.11，但现在更多应用于LAN环境
- 基于端口的访问控制（Port-Based Access Control），基于身份（identity-based）

802.1X Framework

Supplicant ---------EAPOL---- **Authenticator** -----RADIUS--- **Authentication Server**

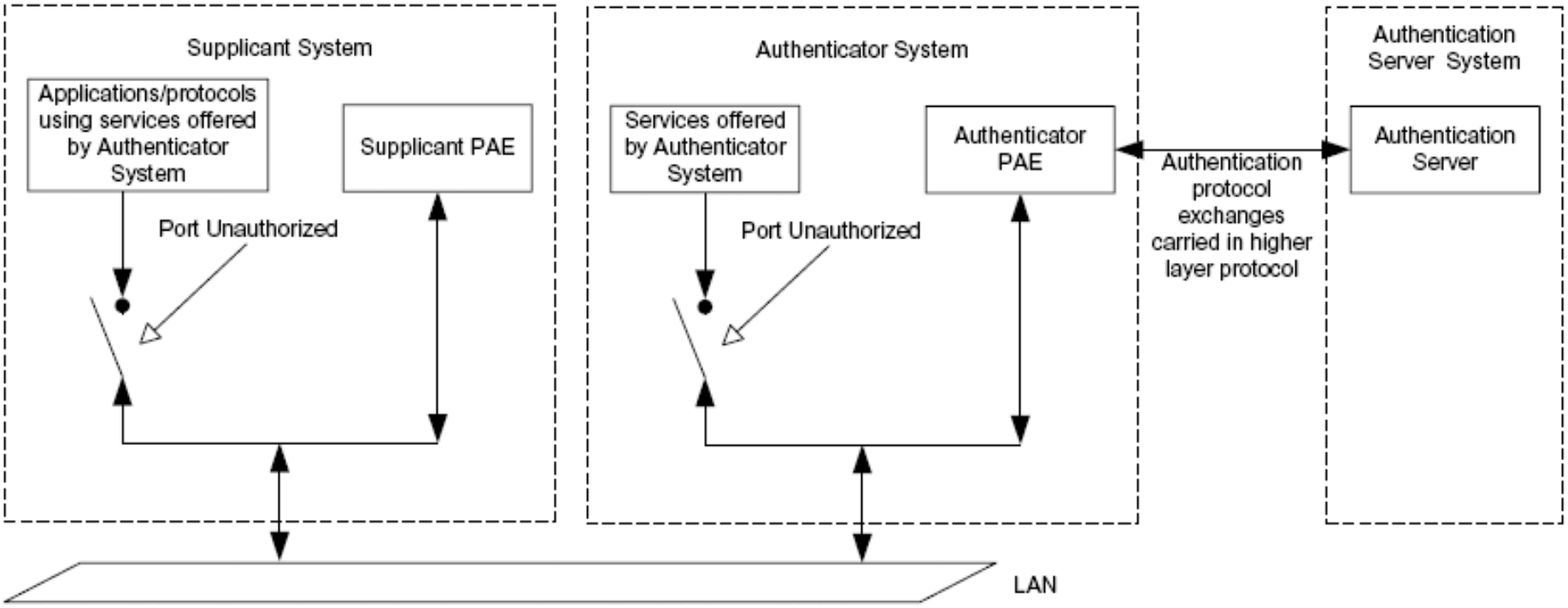


Figure 6-5—Authenticator, Supplicant, and Authentication Server roles

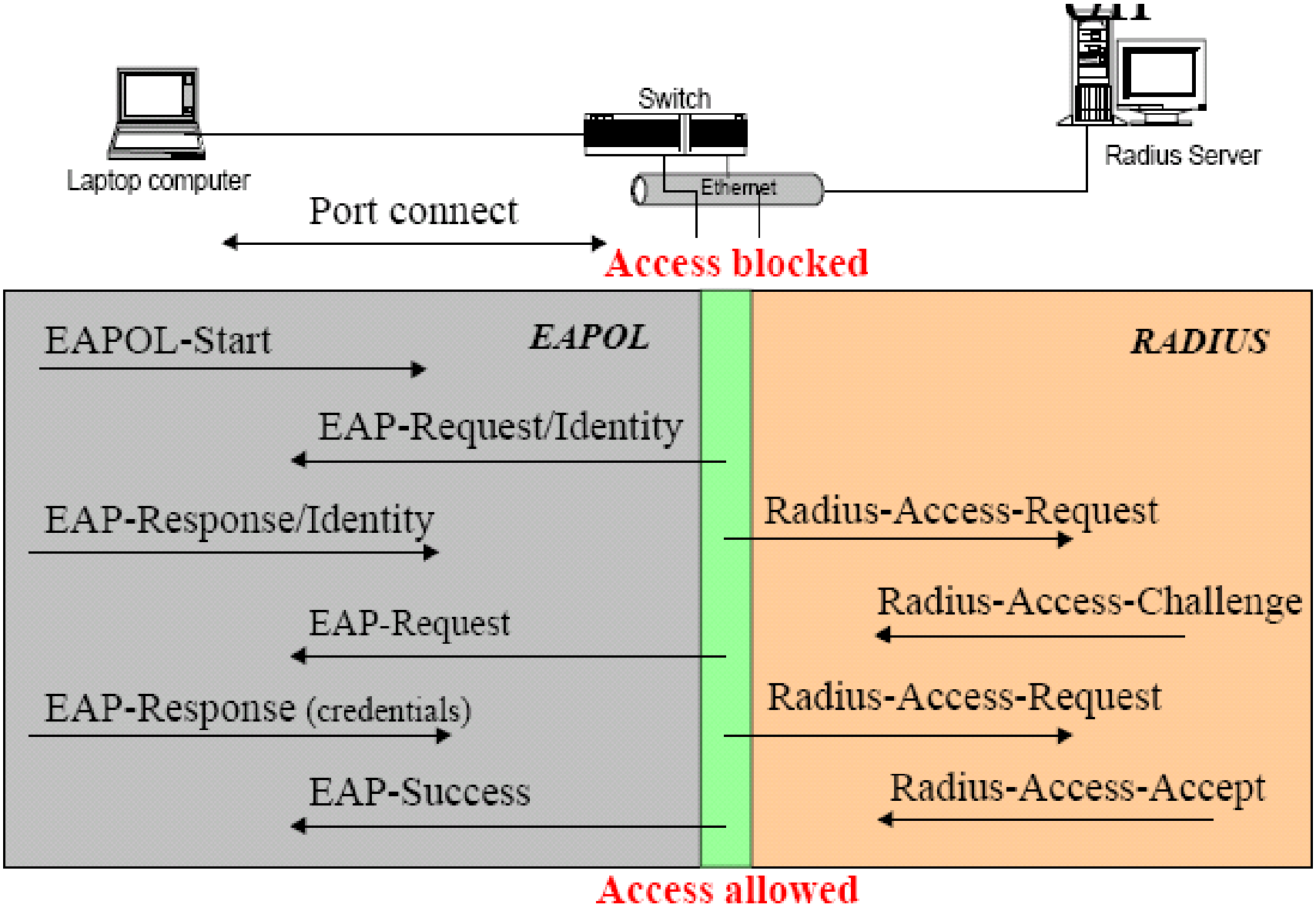
802.1X Framework

IEEE 802.1X 2004

http://standards.ieee.org/getieee802/download/802.1X-2004.pdf

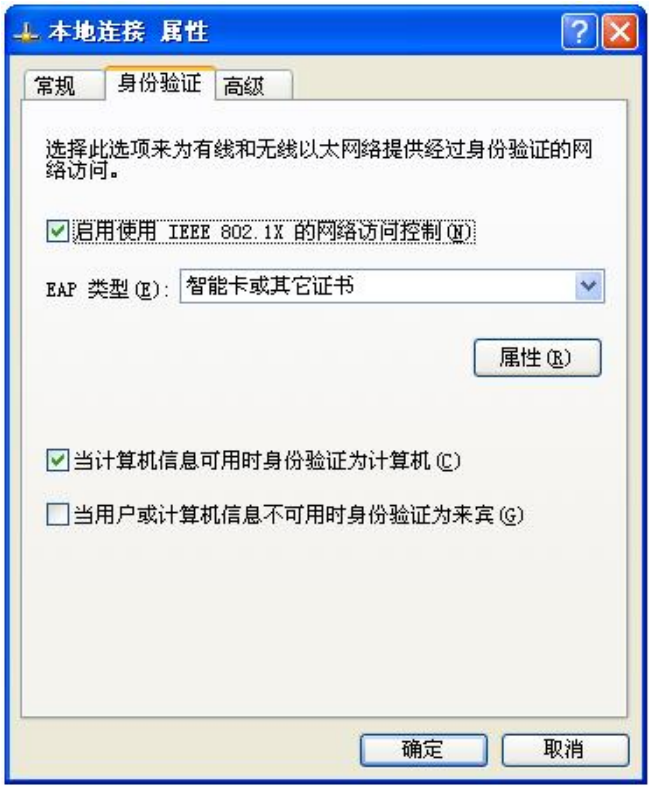
- Supplicant （PC 等）
- Authenticator（Switch, Access Point ）
- Authentication Server （RADIUS Server）
- EAPOL(RFC 2284)
- RADIUS(RFC 2138, 2139,)

IEEE 802.1X Conversation



Supplicant

- Windows



- 厂商或自己客户端

客户端软件要支持EAPOL，开放源代码实现http://open1x.sourceforge.net/

问题：如果使用DHCP，由于DHCP流量不能通过，启动过程很慢

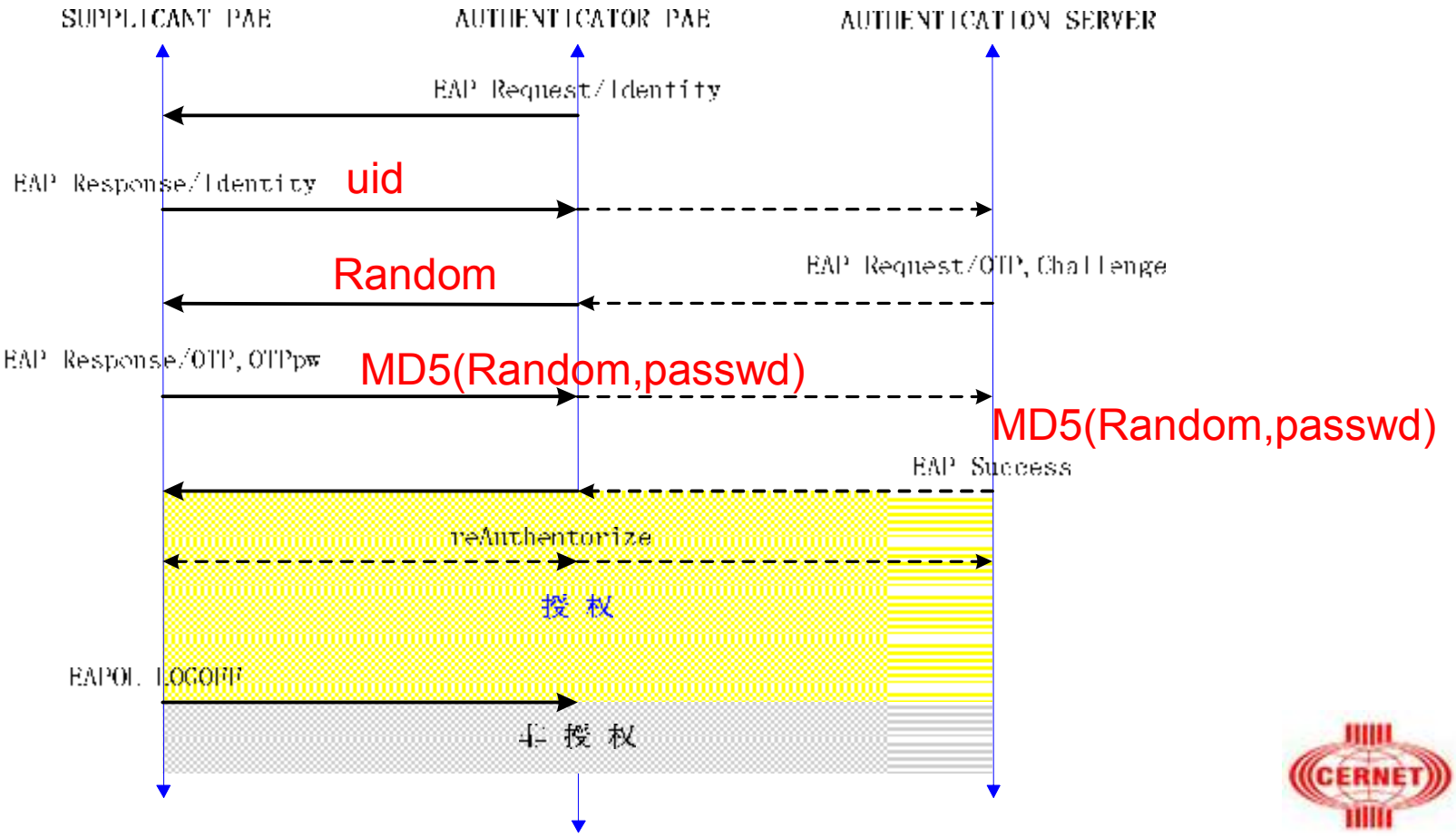
Authenticator

- Authenticator只起到代理的作用
- 以EAP与Supplicant交换认证信息
- 通过RADIUS等高层协议转交给Authentication Server（比如RADIUS）

Authentication Server

- RADIUS Server (EAP with MD5)

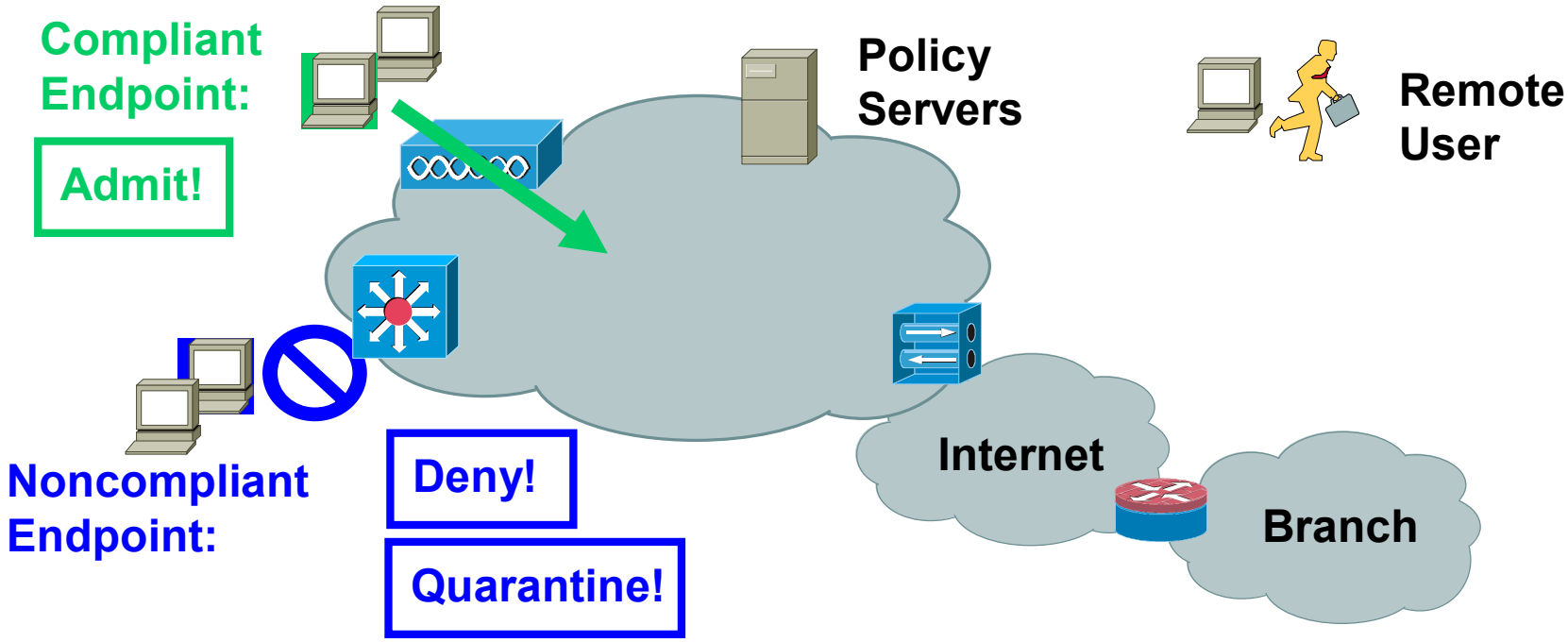
  FreeRadius



基于802.1X控制的其他功能

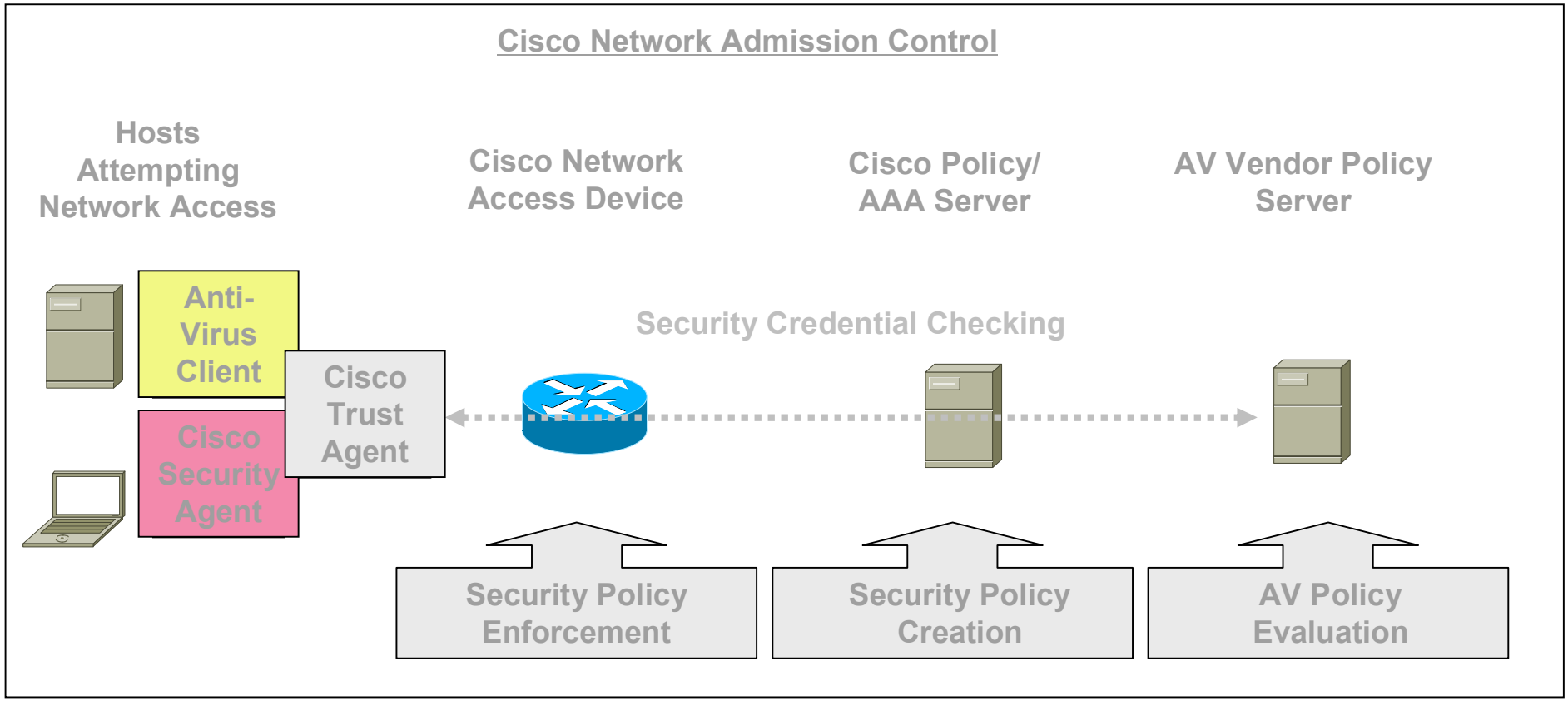
- Supplicant通过EAP 上传的其他信息
  - Identity
  - MAC Address
  - IP Address
  - Security Posture: Patch, Virus Signature, etc.
- 通过RADIUS传递给Authenticator的信息
  - VLAN ,其他属性（RFC 2868）
- Policy Enforcement
  - Client必须符合 Security Policy 才能接入
  - 集中管理

CISCO NAC: the Ideal Solution



- Multiple components are required for a complete solution
  - Endpoint security solutions knows security condition: type/compliance/etc
  - Policy servers know compliance/access rules
  - Network access devices (routers, switches) enforce admission policy
- Virus/worm prevention and containment requires industry collaboration

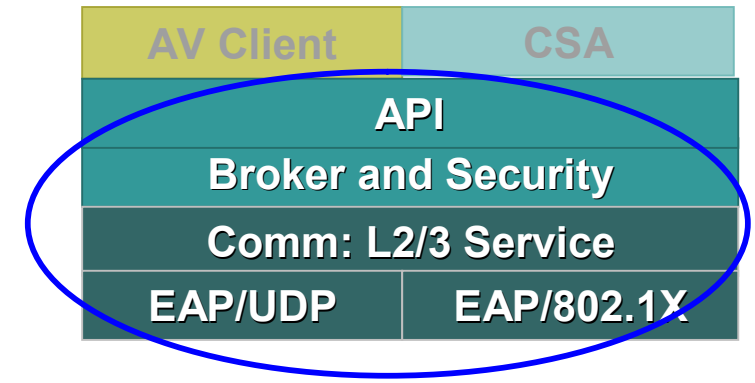
Cisco NAC
(Network Admission Control)



- **Based on endpoint security posture, appropriate admission policy will be enforced in the network**
- **Cisco® & NAC co-sponsors to deliver this collaborative solution**

NAC Program Overview

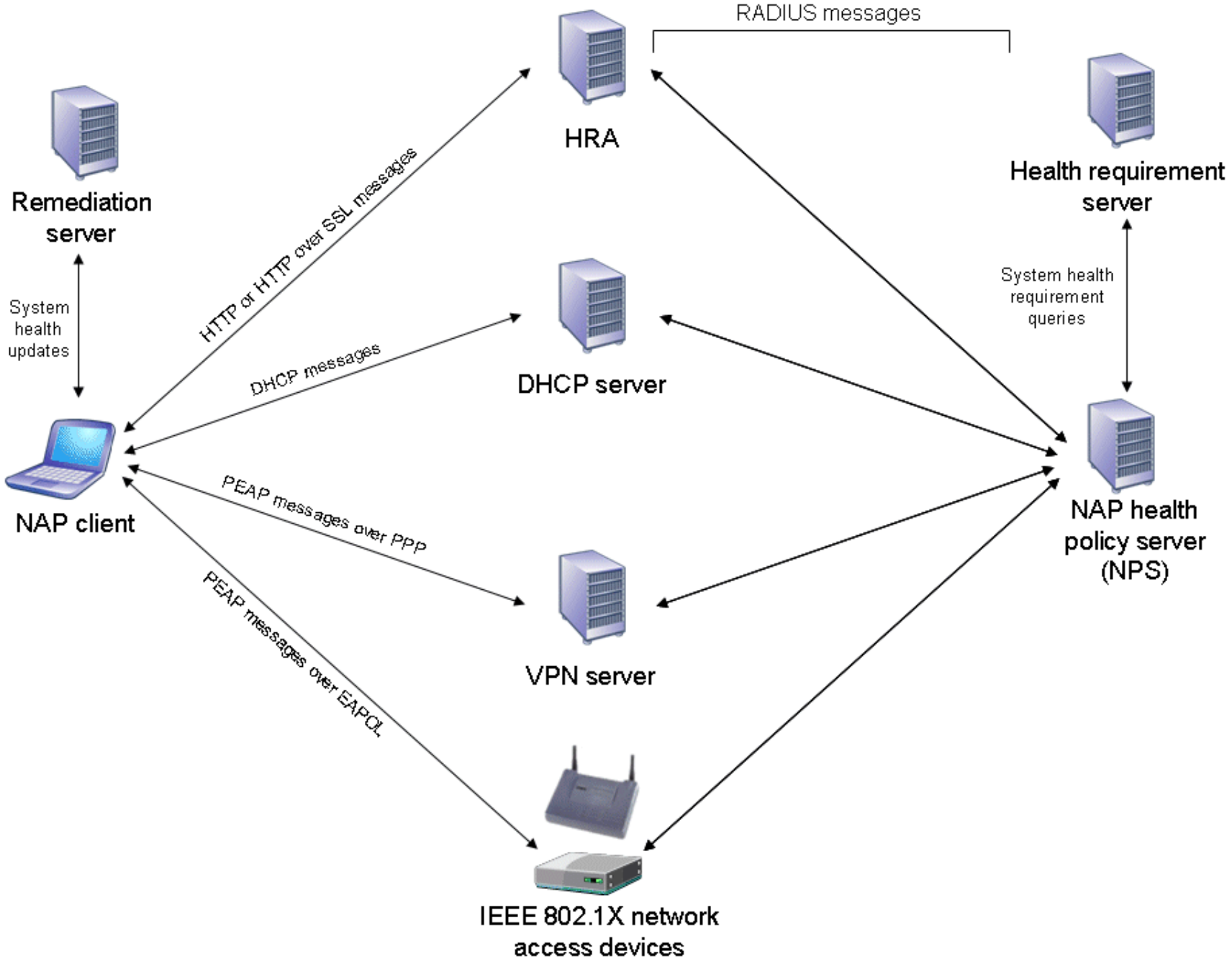
- Cisco® is driving the architectures, specifications, and guidelines of NAC
- Initial NAC co-sponsors include the major antivirus vendors: Network Associates, Symantec, and Trend Micro
- **Cisco Security Agent and NAC co-sponsor AV solutions will use Cisco Trust Agent for intelligent admission control**
- **Initial NAC capability to be delivered in Q2 CY04 in Cisco routers**
- **Future NAC extensions:**
  - **More Cisco network devices**
  - **More endpoint security software and endpoint platforms (OSs)**
  - **More industry co-sponsors**
  - **Solution "opened", timing and extent TBD**

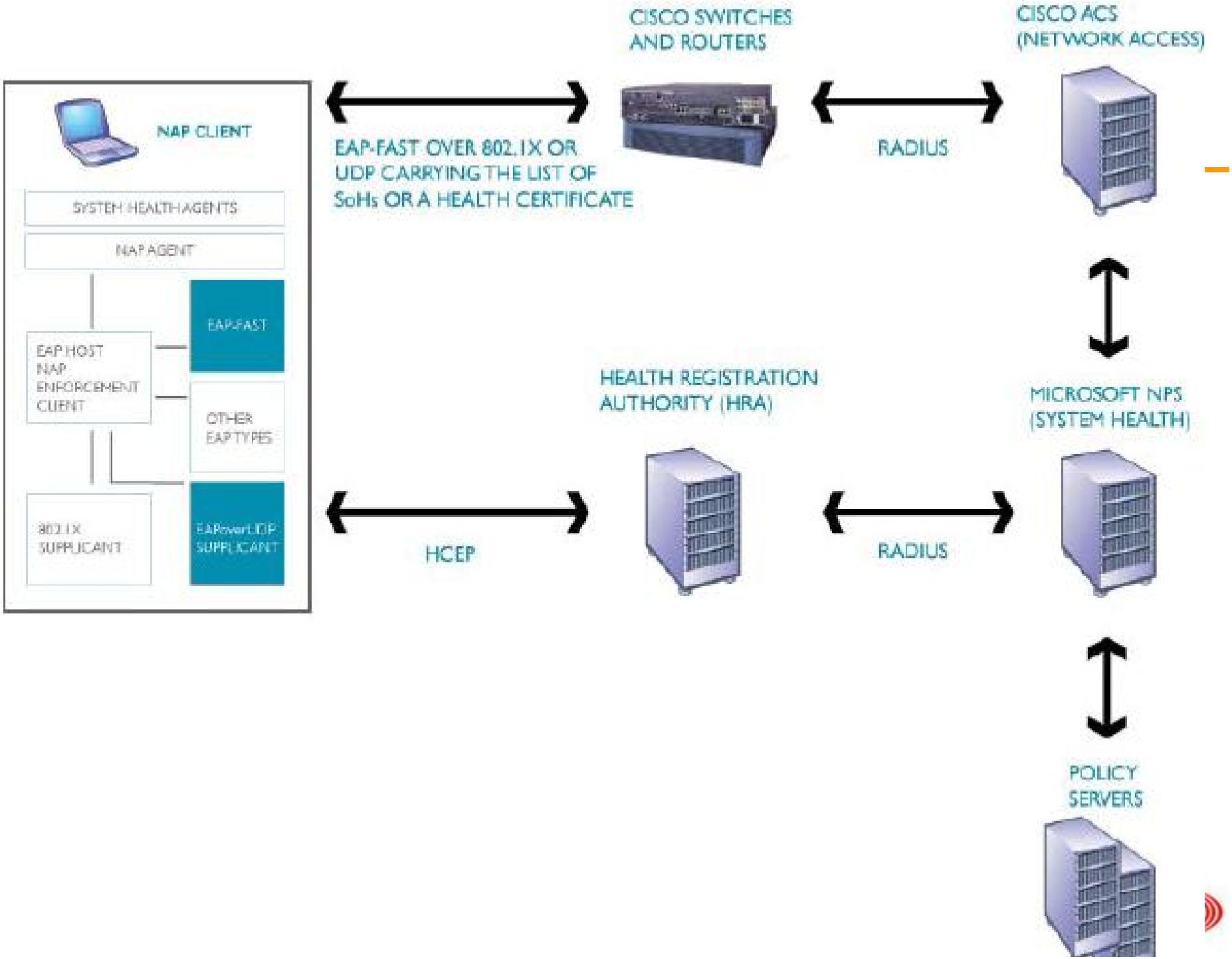


Cisco Trust Agent

Microsoft NAP

- 目的：验证接入网络的计算机的健康状态符合企业的安全政策，违反者可以被限制访问、更新等
- 组成
  - NAP Client
  - NAP Enforcement Point
  - NPS (Network Policy Server)
  - Remediation Servers
- Enforcement Point
  - IPSEC
  - VPN Sever
  - DHCP Server
  - 802.1X Switch or AP
- NAP 文档
  http://technet.microsoft.com/en-us/network/bb545879.aspx


RADIUS messages
HRA
Health requirement server
Remediation server
System health updates
HTTP or HTTP over SSL messages
DHCP messages
DHCP server
System health requirement queries
NAP client
PEAP messages over PPP
NAP health policy server (NPS)
PEAP messages over EAPOL
VPN server
IEEE 802.1X network access devices

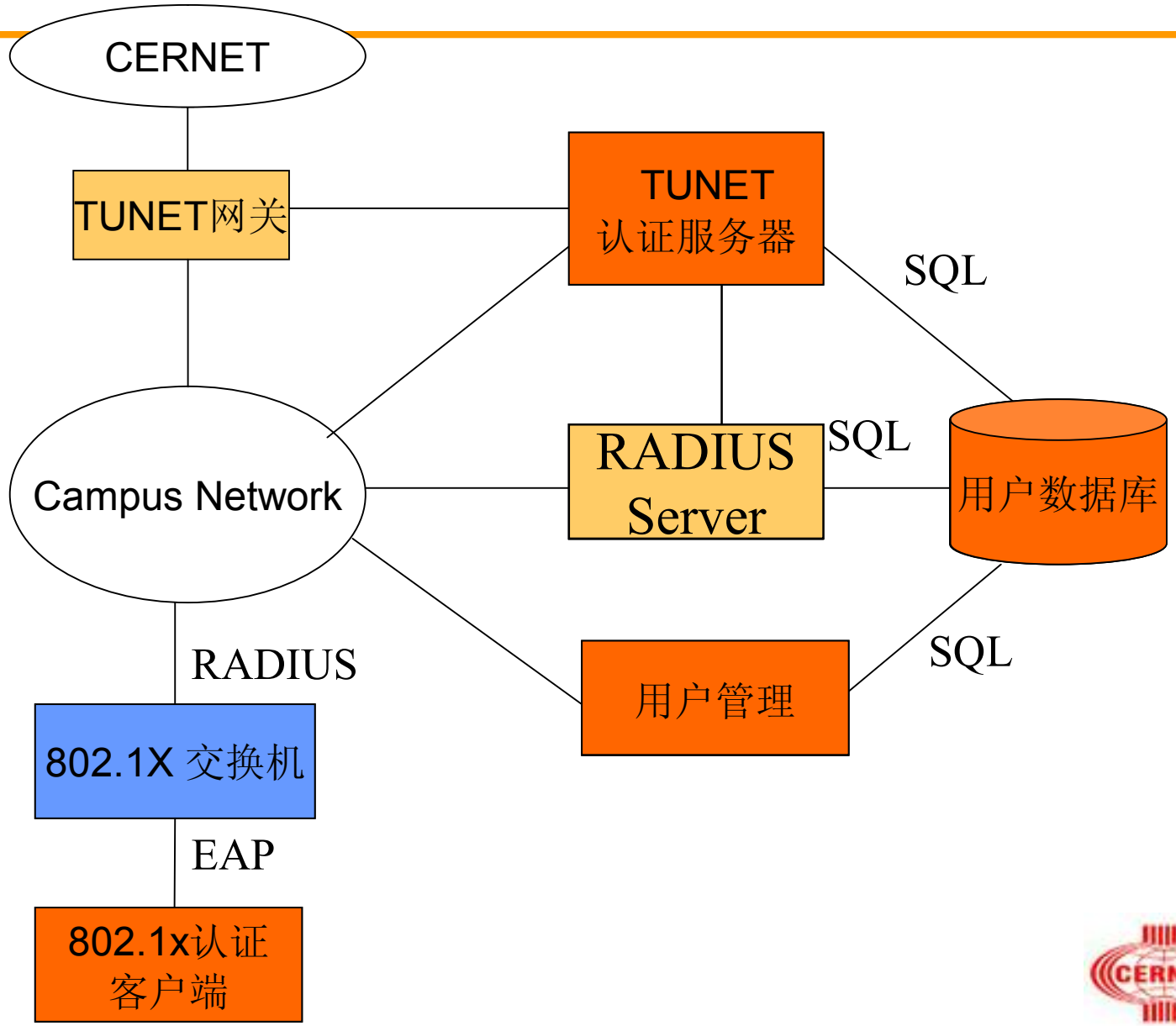

CISCO SWITCHES
AND ROUTERS
CISCO ACS
(NETWORK ACCESS)
NAP CLIENT
SYSTEM HEALTH AGENTS
NAP AGENT
EAP HOST
NAP
ENFORCEMENT
CLIENT
EAP-FAST
OTHER
EAP TYPES
802.1X
SUPPLICANT
EAPoverUDP
SUPPLICANT
EAP-FAST OVER 802.1X OR
UDP CARRYING THE LIST OF
SoHs OR A HEALTH CERTIFICATE
RADIUS
HEALTH REGISTRATION
AUTHORITY (HRA)
MICROSOFT NPS
(SYSTEM HEALTH)
HCEP
RADIUS
POLICY
SERVERS

IETF Activities

- **Network Endpoint Assessment (nea)**
- http://www.ietf.org/html.charters/nea-charter.html

- **EAP Method Update (emu)**
- http://www.ietf.org/html.charters/emu-charter.html

TUNET端口认证系统结构



校园网中应用802.1X的好处

- 细粒度的身份认证
- 细粒度的控制
- 安全事件的追踪
- 集中管理用户访问权限（通过VLAN设置）
- 用户安全状态的检查与更新

校园网中802.1X和准入控制的问题

- 技术问题
  - 位置移动的问题
  - DHCP的问题
  - 无线局域网中的问题
  - 技术成熟度问题
- 管理问题
  - 用户的接受程度？
  - 管理的复杂程度？

问题与讨论？