CONCEPT DESIGN

FOR

WIRELESS NETWORK

FOR

MYCOM

Table of Contents

0. Document control

- An electronic document will be filed at Z:\ concept design for wireless for mycom.doc
- All change to this document must be recorded in the table below:

ChangedBy	Activity	Date
	Original initiate	Xx/xx/xxxx

1. Requirements for the implementation of MyCOm's wireless network

- All users (internal users/guests) have to authenticate with a server before gaining access to MyCom's network infrastructure.
- The use of the existing Active Directory infrastructure for authentication is necessary for scalability reason.
- Wireless traffic must be encrypted
- Minimize overhead on the helpdesk.

2. Security Strategy for wireless

- There is a number of options available for wireless deployment:
  i. Wide open WLAN: anyone with a wireless device can access the wireless network and therefore this is not an option in this case
  ii. Static Wired Equivalent Privacy (WEP): This security method is weak; easy to break and find the WEP key; it is also difficult to maintain the secret key.
  iii. MAC address authentication: This protects the wireless network from unauthorized users but does not protect data. Data is not encrypted and easy to sniff and MAC spoof.
  iv. Use no security on wireless segment and deploy VPN to secure access and traffic:
    - An additional device is required for VPN termination (e.g VPN concentrator)
    - Wireless computer is not secured and easy to be attacked.
  v. IEEE 802.1x security
  vi. Cisco EAP (LEAP)
    - This is a Cisco proprietary algorithm which requires Cisco ACS for authentication (costly) or Wireless AP Local Radius server (not scalable)
  vii. EAP-TLS
    - Wireless devices needs clients certificate for authentication. This requires a pubic key infrastructure in place.
  viii. EAP-TTLS
  ix. EAP-PEAP

x. Our concern is the last three options(EAP-TLS, EAP-TTLS, EAP-PEAP). A detail comparison is show in the table below:

Table 1: EAP security comparison

	TLS	TTLS	PEAP
Specification RFC	2716	Internet-Draft, 11/2002	Internet-Draft, 3/2003
Software			
Supported client platforms	Linux, Mac OS X,Windows 95/98/ME, Windows NT/2000/XP, Mac OS X	Linux, Mac OS X, Windows 95/98/ME, Windows NT/2000/XP	Linux, MacOS X, Windows
Client Software	Need to be installed	Need to be installed	Come with window XP
Authentication server	Cisco ACS, Funk Odyssey, Interlink Secure.XS, Meetinghouse AEGIS, Microsoft IAS, FreeRADIUS	Funk, Meetinghouse, Interlink	Cisco ACS, Microsoft IAS, Interlink Secure.XS, Meetinghouse, Funk
Authentication methods	X.509 Certificates only	CHAP, PAP, MS-CHAP, MS-CHAPv2, and EAP methods	EAP methods; commonly MS-CHAPv2, generic token card, and EAP-TLS
Protocol operations			
Basic protocol structure	Establish TLS session and validate certificates on both client and server	Two phases: (1) Establish TLS between client and TTLS server (2) Exchange attributevalue pairs between client and server	Two parts: (1) Establish TLS between client and PEAP server (2) Run inner EAP exchange over TLS tunnel
Fast session reconnect	No	Yes	Yes
PKI/Certificates			
Server certificate	Required	Required	Required
Client certificate	Required	Optional	Optional
Additional Software	Yes	Yes	No, Windows 2003 comes with a Radius server.

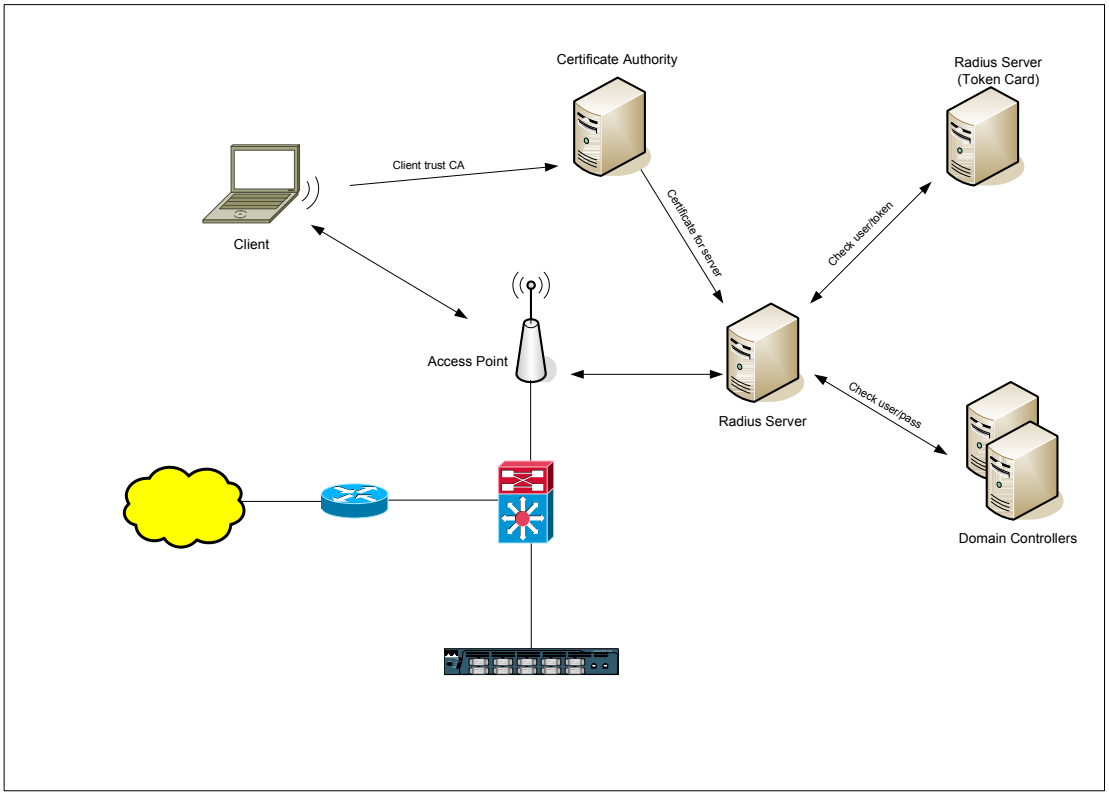
From the above table, EAP-PEAP is chosen to deploy in MyCom'swireless network

3. Required Components for PEAP implementation

- Windows 2003 domain controller
- Microsoft IAS radius server
- Certificate server for authentication server
- Cisco Access points
- Wireless clients (come with user wireless device)
- Group policy to automatically configure client computer
- Optional components:
  i Wireless LAN solution engine (WLSE): for wireless management and rogue AP detection.

4. Concept of Design

- Access Point
  ii. Access point name will be followed the normal format: MYCOMWx, where x is a number.
  iii. Two of the access point will be configured as Wireless Domain Service (WDS) for fast roaming. One of the two will be active and the other will be standby.
- Network IP Address
  i. There will be two VLANs for wireless network. One Vlan for internal users and the other for guests. These two VLANs will be routed via the 4507 router and ACL will be applied at router's interface to increase security between wireless and wired networks.
  ii. Access points' IP address will be one of available IP addresses in manangement VLAN.
  iii. Subnet xx.yy.zz.0/24 will be assigned for internal users
  iv. Subnet aa.bb.cc.0/24 will be assigned for guests
- SSID
  i. There are two SSID associated with the above VLANs. Two of them will not be broadcasted. SSID for internal users will be configured on user's PC/laptop by Domain Group Policy. Users are not authorised to modify that setting.
  ii. SSID for guest users will be given along with a setup instruction.
- Overall Network Diagram
  i. Network diagram is shown as below:



- User login
  i. Internal users with wireless access permitted use the domain username and password to access network. Users only key the username/password once at the login process
  ii. Guest users use a username provided in a format username@mycom.com and a token to login. The firewall might need to be modified so that these users (base on subnet) can access internet or a temporary proxy username/password is provided for internet usage.

5. Documents

- A detail implementation document will be provided at later stage.