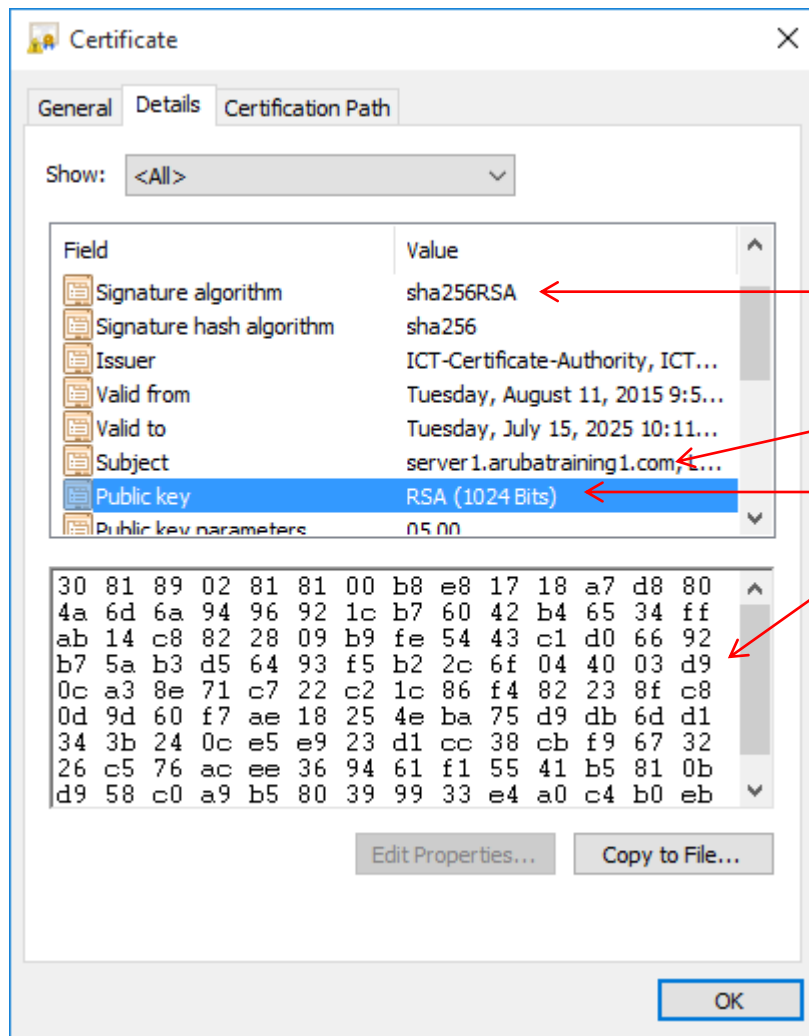




Wireless Networks
**Lab 4: 802.1X PEAP
Authentication**

Overview of a Digital Certificate



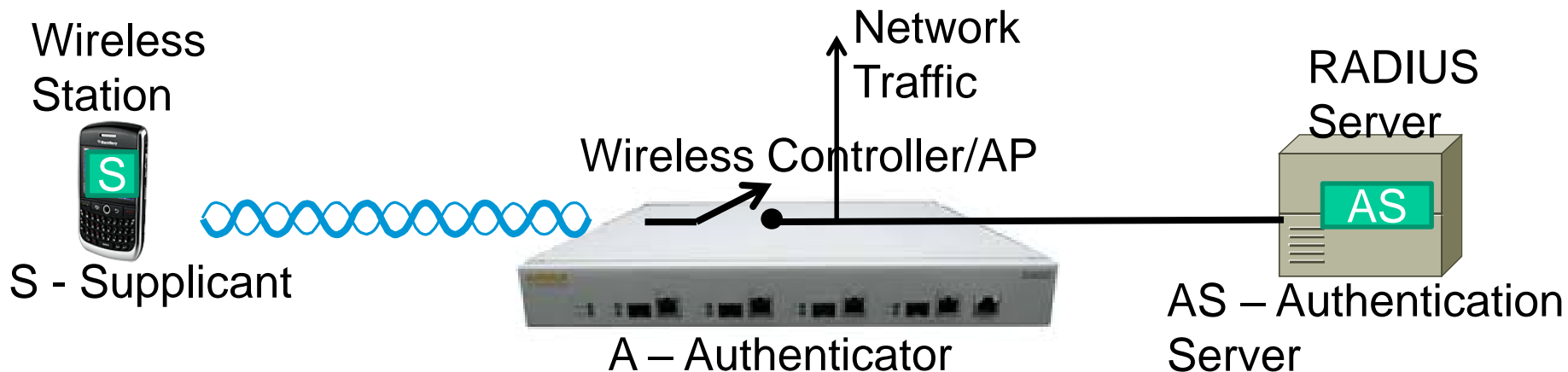
Hash Algorithm = SHA256
Encryption Algorithm = RSA

Common Name = FQDN of server

Public Key
Private Key remains with server or CA

Digital Signature signed by Certificate Authority (not shown)

802.1X / PEAP Authentication



802.1X – Provides an authorization framework that allows or disallows traffic to pass through a port to access network resources

EAP - Extensible Authentication Protocol: Authentication Protocol framework built on 802.1X. Enables more complex authentication negotiation between the Supplicant and the Authentication Server.

Supplicant: A host that is requesting authentication and access to network resources

Authenticator: A device that blocks or allows traffic to pass through its port

Authentication Server: A server validates the credentials of the supplicant and notifies the authenticator

WPA2 Enterprise: 802.1X/PEAP (highlights)

Wireless Station



S - Supplicant

Controller/AP



A – Authenticator
(802.1X port switch)



AS – Authentication Server

Part A: Association

Probe, Authentication, Association

Part B: 802.1X/EAP Negotiation

Start Auth (Auth Method) → Access Request

1. Server Authentication (Client Requests and Validates Certificate)
2. Create Secure Connection (i.e. Encrypted TLS Tunnel)
3. Client Authentication (Validate Credentials i.e. password)
4. Create Pairwise Master Key PMK
5. Tear down TLS Tunnel

EAP Success (Failure) ← Access Accept (or Deny)

Send PMK to Authenticator

Part C: 4-way Handshake

Four Messages to Create PTK

Encrypted Data Flow using PTK

PMK – Pairwise Master Key
PTK – Pairwise Transient Key

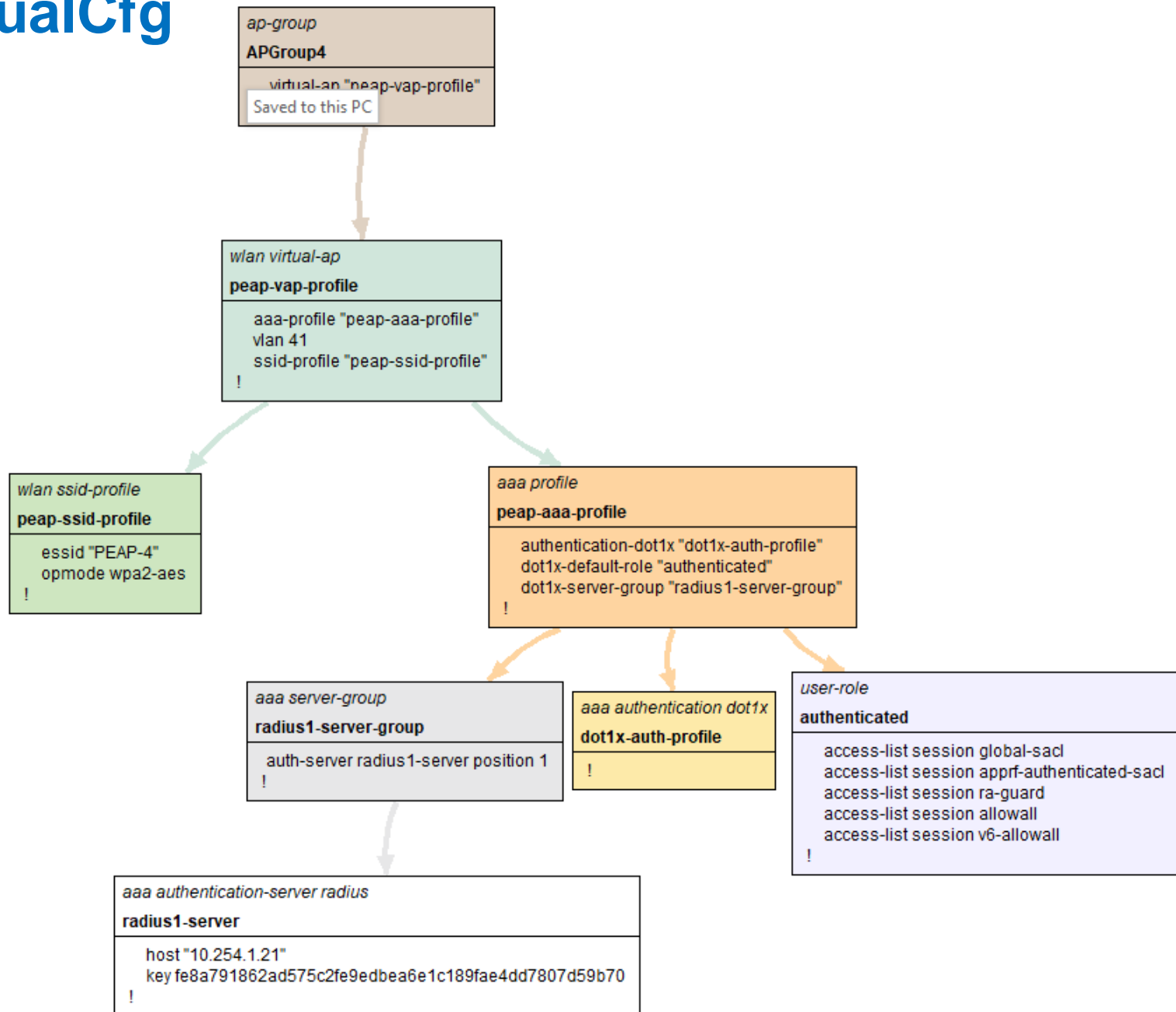
WPA2-802.1X with PEAP Auth Configuration

```
# This profile uses default parameters
aaa authentication dot1x profile-name
exit
```

```
aaa profile profile-name
  initial-role role-name
  authentication-dot1x profile-name
  dot1x-server-group profile-name
  dot1x-default-role role-name
exit
```

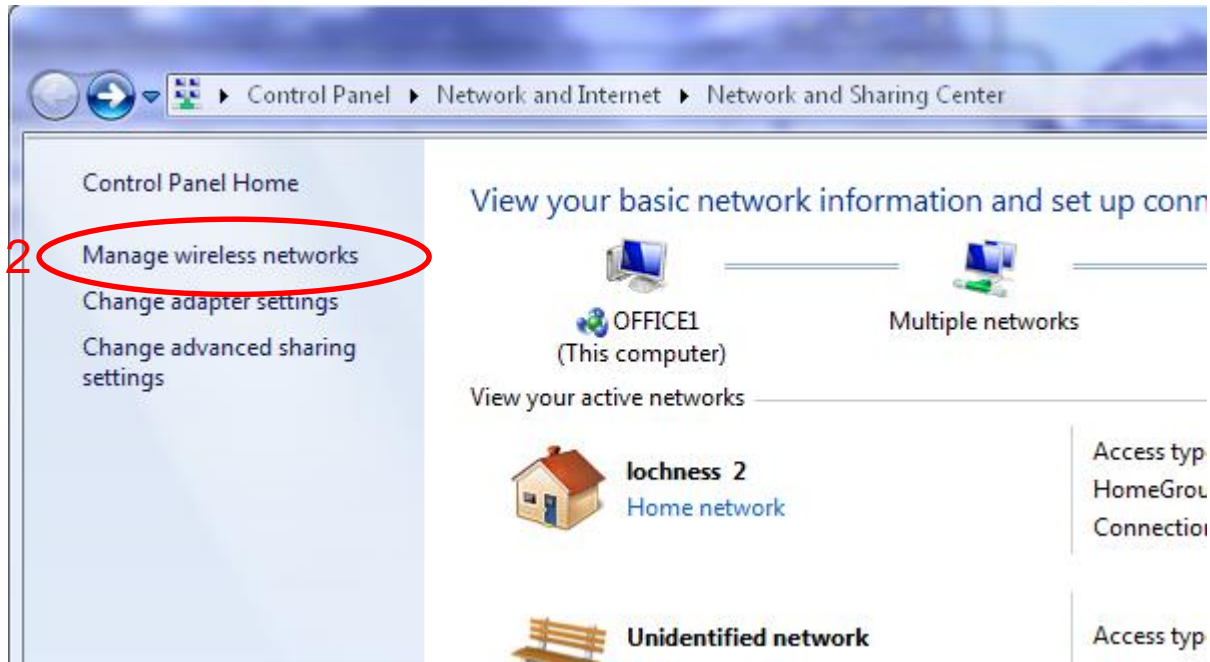
```
wlan ssid-profile profile-name
  essid ssid-name
  opmode wpa2-aes
```

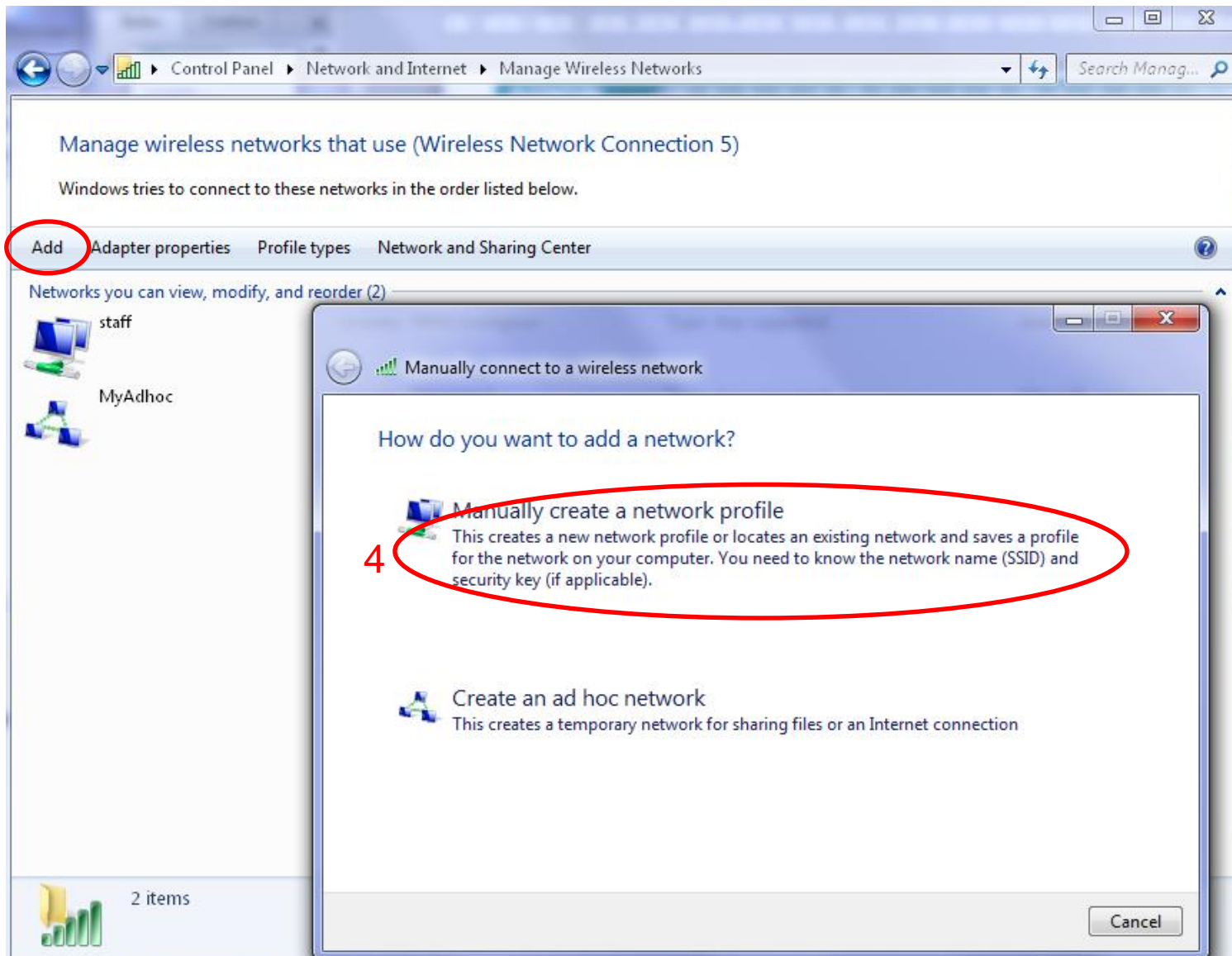
VisualCfg



How to Configure Windows 7 with 802.1X/PEAP

1. Open Network and Sharing Centre





Put your SSID here

Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name: 5

Security type:

Encryption type:

Security Key: Hide characters

Start this connection automatically

Connect even if the network is not broadcasting

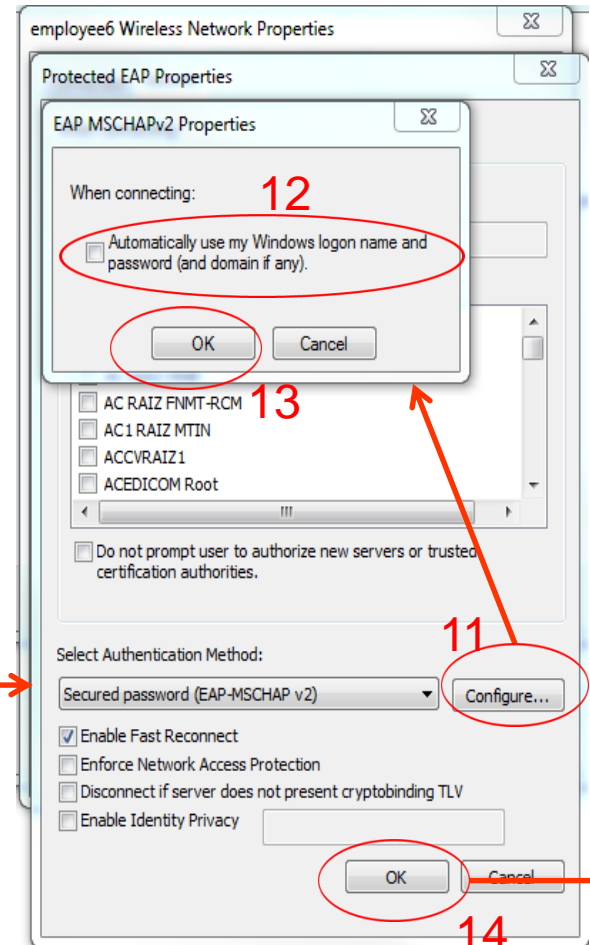
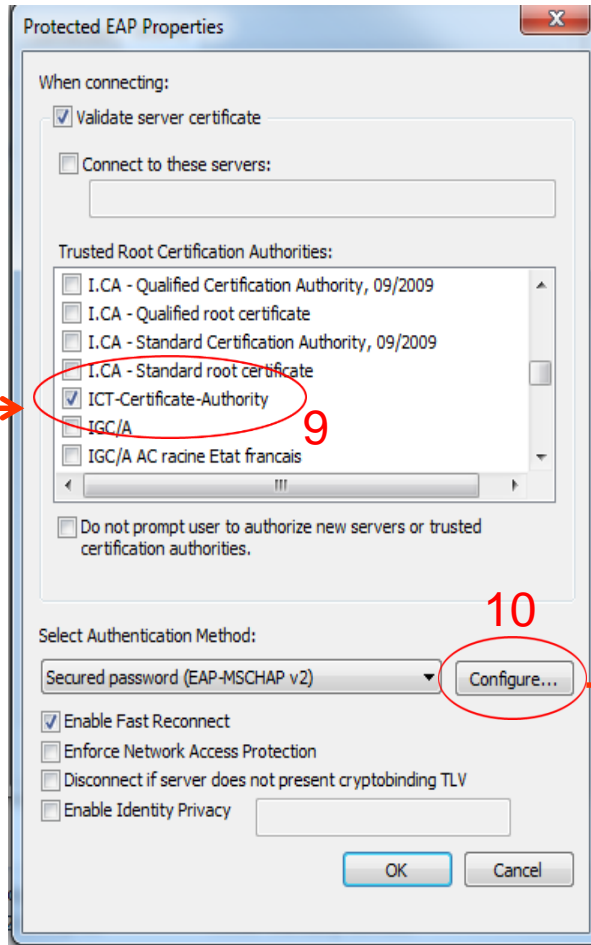
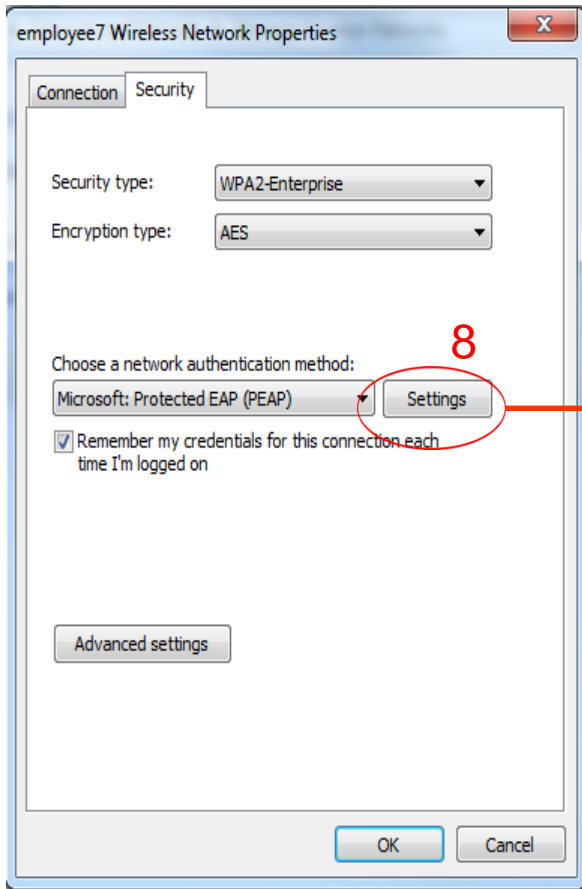
Warning: If you select this option, your computer's privacy might be at risk.

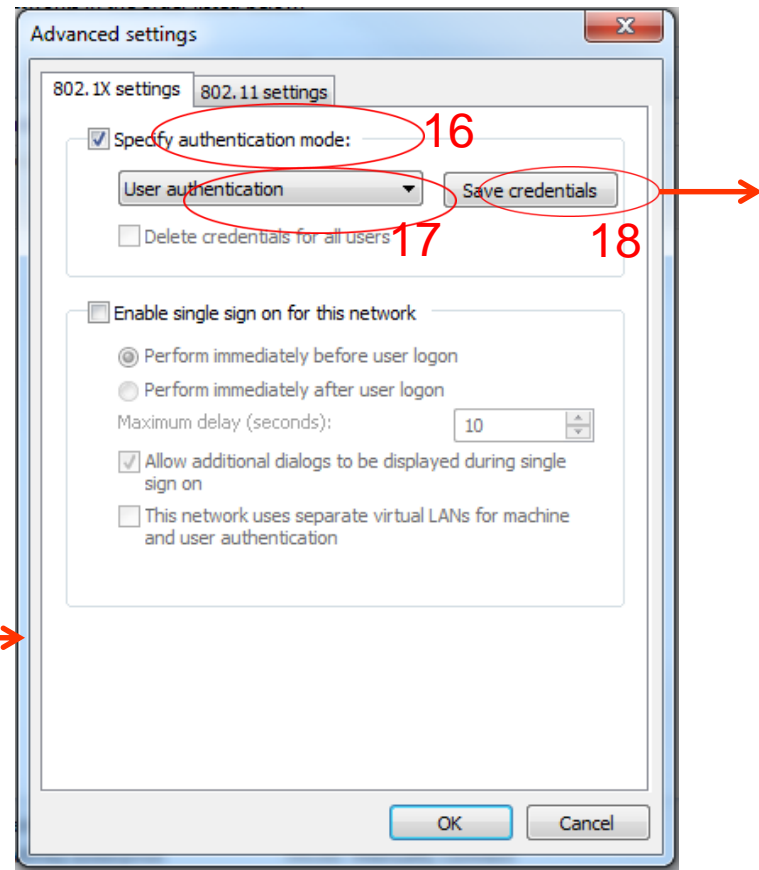
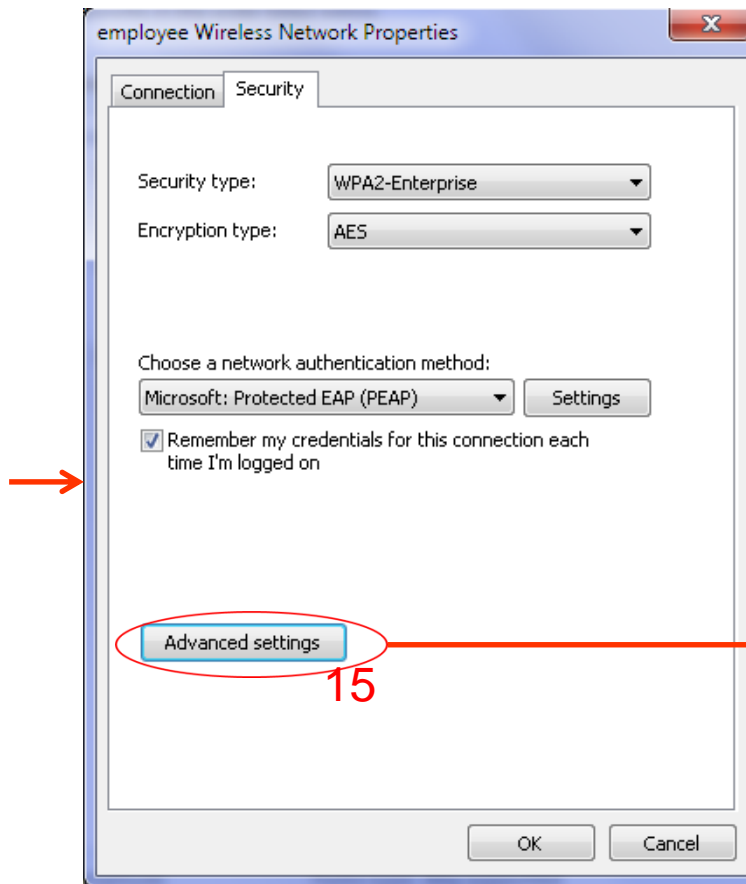
Manually connect to a wireless network

Successfully added employee7

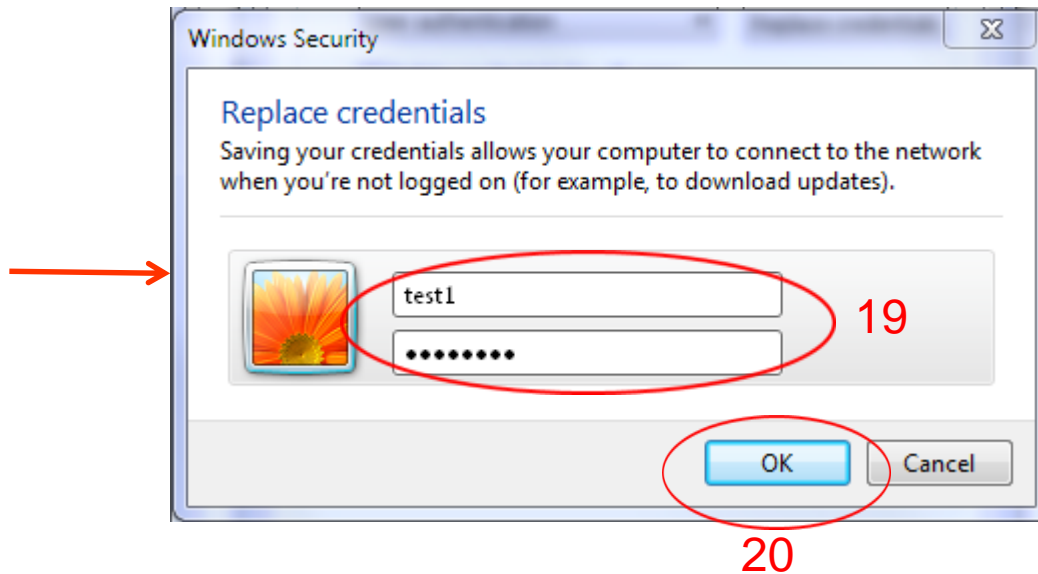
7 Open the connection properties so that I can change the settings.

click the certificate



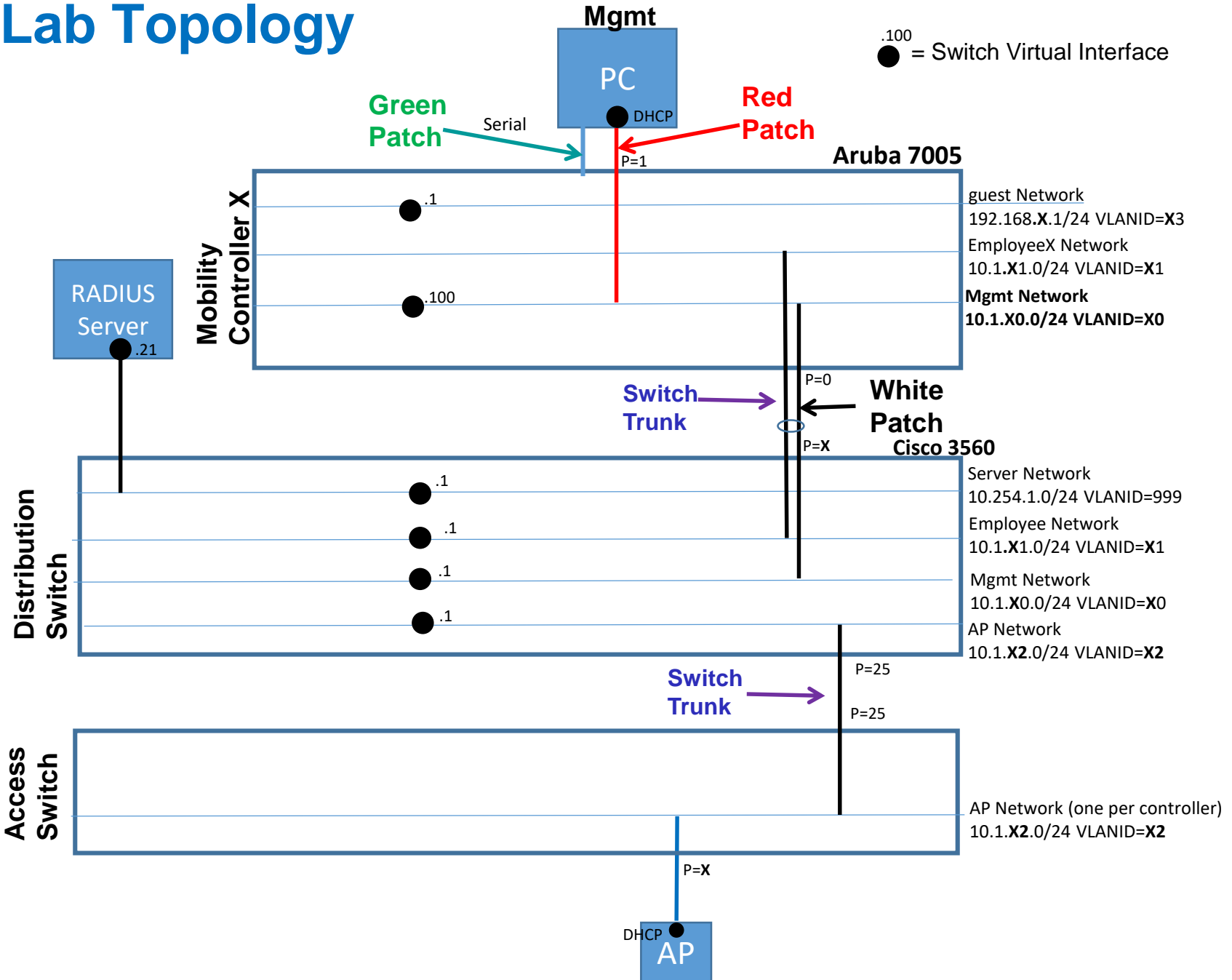


Enter Credentials:
username: test1
password: Aruba123



close all dialogue
boxes

Lab Topology



Lab Objectives

1. Create VAP1 with 802.1X and PEAP Authentication
2. Create a aaa profile with 802.1X Authentication
3. Create an SSID profile with WPA2 and AES encryption
4. Configure the PC Wireless Profile for 802.1X
5. Test the Configuration
6. Questions
7. Sign-off