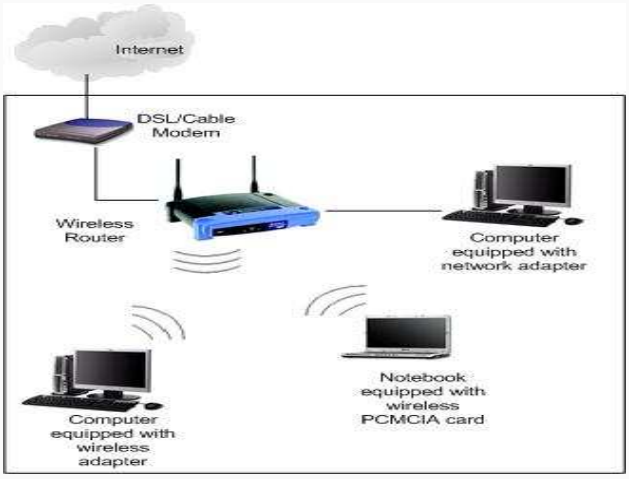
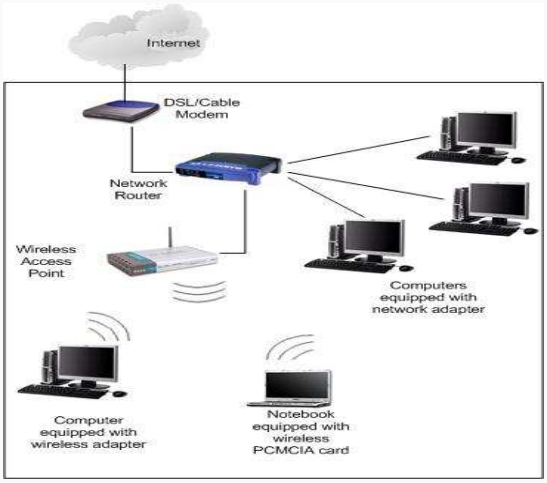
Enterprise Wireless Fidelity implementations using port based network access control(IEEE 802.1x)

Wireless Network



Detailed Figure



Security issues with IEEE 802.11

- No per-packet authentication
- Vulnerability to disassociation attacks
- No user identification and authentication
- No central authentication, authorization, accounting
- RC4 stream cipher
- Some implementations derive WEP keys

Threats in Wi-Fi implementations

- Access point(AP) is open
- directly log in to the access point using default credentials
- The attacker can sniff the network for SSID,BSSID
- Install a fake access point
- Disrupt the normal functioning of the network.

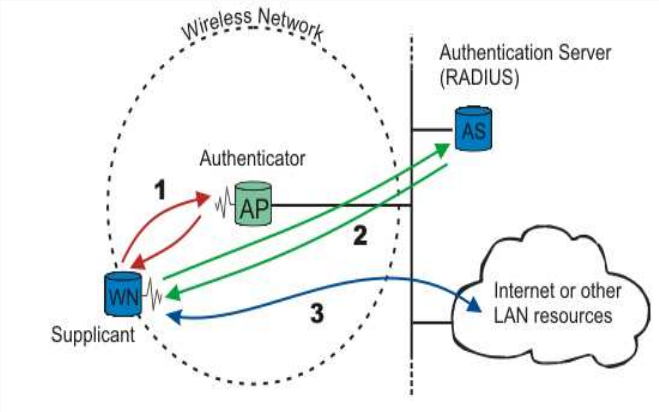
IEEE 802.1x

- Extensible authentication protocol(eap)
- Adapted for ieee 802.11 wireless lans
- Point to point connection
- Preventing access from the port

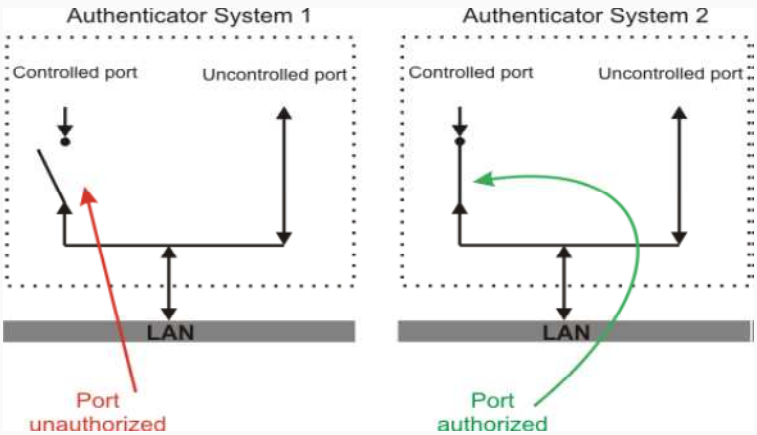
Participants in the IEEE 802.1x

- Supplicant
- Authenticator
- Authentication server
- Authentication protocol

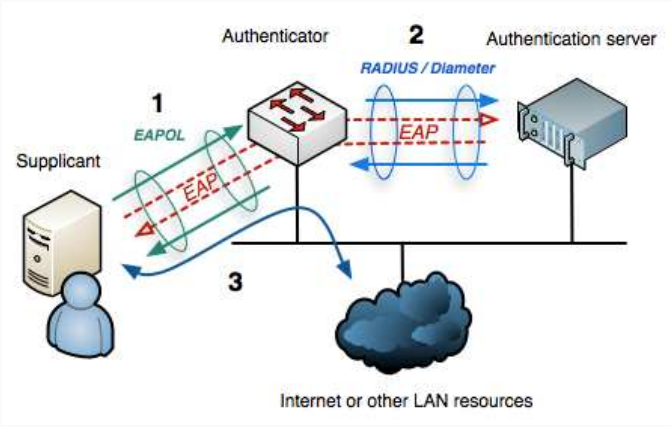
How to work IEEE 802.1x



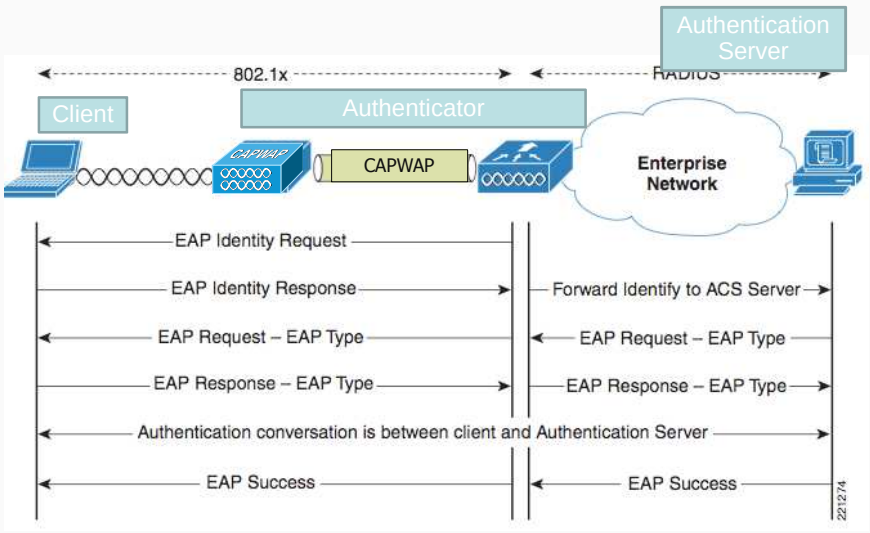
Port based authentication



Protocol operation



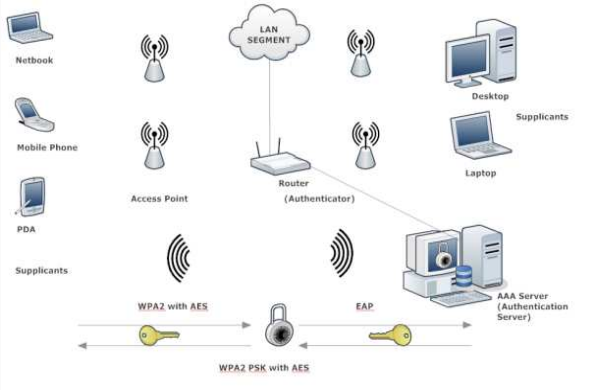
EAP — protocol flow



WPA2

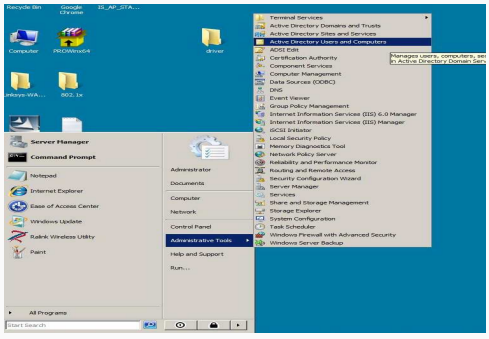
- Additional encryption and authentication mechanism
- AES
- Symmetric key
- Block size 128 and key size 128,192,256
- Multiple of 32

Proposed Architecture

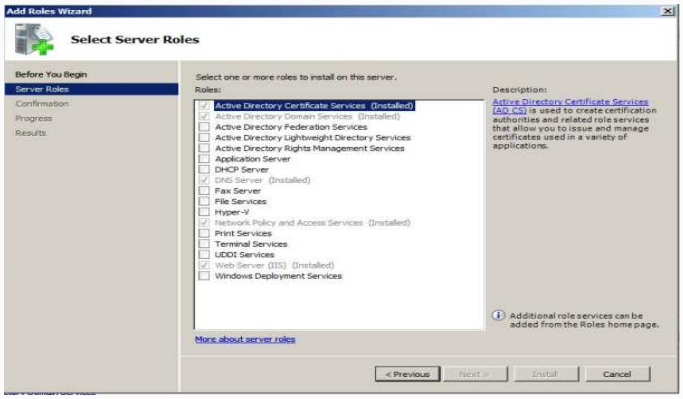


Implementation

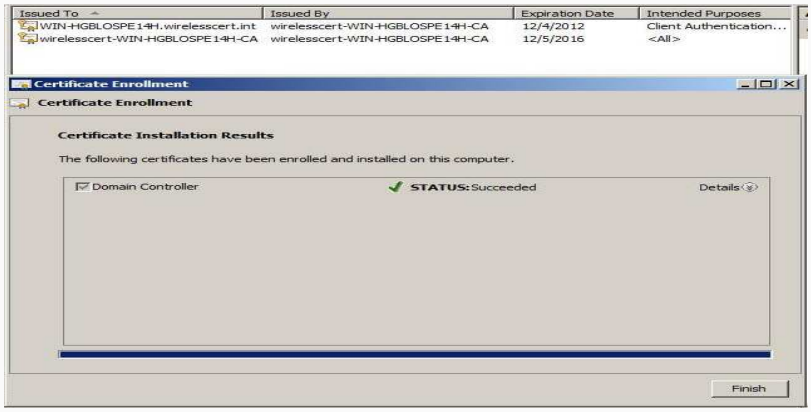
- Configure active directory domain services



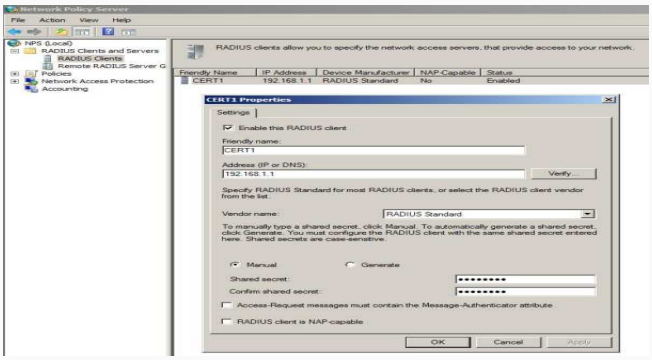
Configure active directory certificate services



Set up the certificate required by PEAP(protected EAP) for authentication server

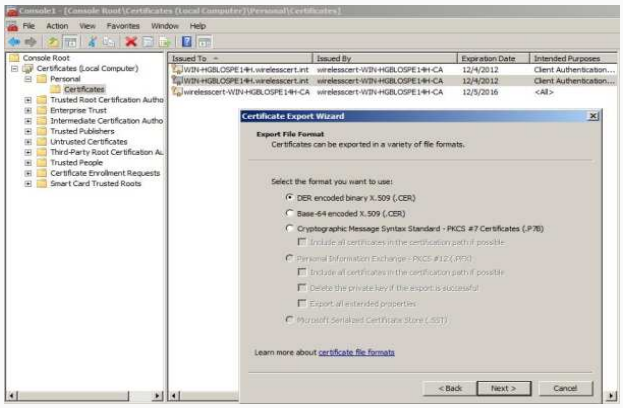


Configure network policy access services role and RADIUS

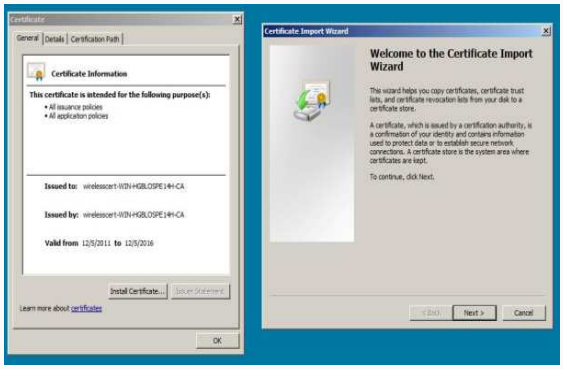


Configure wireless APs in IEEE 802.1X security mode

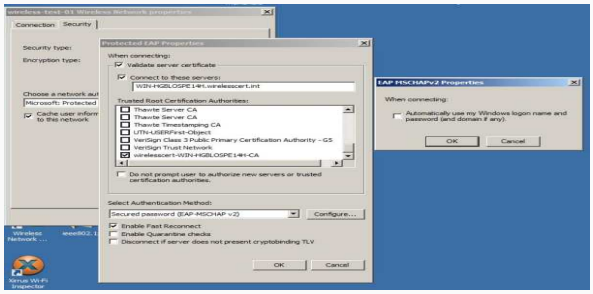
Export CA certificate to install it into client computers.



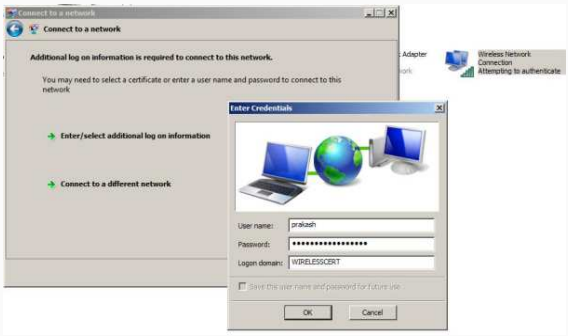
Copy the CA certificate generated to client machine and install.



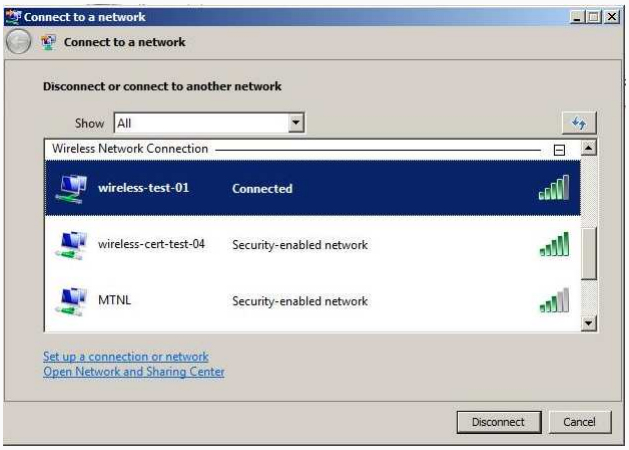
Manually create a network profile with WPA2 with AES. Validate the server certificate**.**



Login with proper domain credentials



Connection status



AAA features

- Proper authentication: the authentication is done through IEEE 802.1X RADIUS and EAP with WPA2/AES
- authorization: proper authorization can be set to the users in the domain.
- Accounting: relevant activities of the user is logged in the authentication server.

Intrusion detection system

- Identify the possible intrusion attempts.
- Identify the malicious(rogue) access points
- Kismet installed in the network.

Conclusion

- Change the default admin password on all the access points (aps).
- Implement a policy on (aaa) and encryption
- Authenticate the users with authentication protocols like 802.1X ,RADIUS and EAP.
- Use mac address filtering at the access points.

References

- [1] l. Zhou and ZJ. Haas, "securing ad hoc networks," IEEE network,

  Vol. 13, no. 6, 1999, pp. 24-30.

- [2] jinyang li, charles blake, douglas s. J. De couto, hu imm lee,robert morris, "capacity of ad hoc wireless networks," in proc. Of

  Mobicom (mobicomol) conference, 200l.