… System Set up for IEEE 802.1x Operation

Avaya Wireless Technical Bulletin **September 2001**

Introduction

With the introduction of the new Avaya Wireless AP-3 access point, IEEE 802.1x-based security has been made available for wireless (mobile) users to prevent unauthorized access to network resources, and to increase the protection against eavesdropping by using dynamic assigned encryption keys. IEEE 802.1x provides security authentication and encryption schemes, involving three major network elements:

- An authentication server to validate the authenticity of a user that requests access to a network. A user is validated based on a unique "certificate" its client PC provides and that is registered at the authentication server. The authentication server typically is implemented in the form of a RADIUS server.
- Provisions in wireless Access Points, to allow uncontrolled access to an authentication server only and controlled access to the rest of the network, once authentication by the server has been successfully completed, and encryption keys between the client and the Access Point are established. In the Avaya Wireless product family this uncontrolled/controlled access facility is implemented in the new AP-3 access point.
- Facilities within the client station to initiate the authentication process and the establishment of the encryption keys. In standard terms this is known as a "Supplicant" function. At the time of drafting this paper the only implementation of such a supplicant is within Microsoft's new Windows/XP Operating System. However it is expected that more OS versions will include this functionality over time.

Because of the complexity of these schemes and the configuration of the various systems involved, the need for a step-by-step configuration guideline/instruction was felt. This bulletin contains those instructions for a specific set of implementations.

Requirements on Authentication server and supplicant

At this point in time the actual configuration requires specific versions of operating systems.

- The only currently available RADIUS implementation that supports 802.1x is the Microsoft Windows 2000 Advanced Server Build 2195 with service pack 2 installed.
- The currently available supplicant is implemented in Microsoft Windows XP Professional (we used for the testing Release Candidate 2 build 2526)

Detailed instructions of a set configuration

Step 1: Preparations

a) Get a cross connect cable (or a hub with two patch cords)
b) Get a client system with Windows XP Professional RC2 (build 2526) on it
c) Use built-in XP client manager instead of Avaya Wireless client manager
d) Get a server with Windows 2000 Advanced Server Build 2195 on it.

- Install Service Pack 2 on the server

e) Make sure on the server that the C drive is formatted with the NTFS file system:

- Check the properties of the C drive under "My Computer" to determine the current file system
- If is not NTFS, run "convert C:/fs:ntfs" from a DOS window and then reboot.

Step 2: Name your server computer:

a) Right click My Computer → Network ID → Properties
b) Name the computer "radius"

Step 3: Install Active Directory on the server (start the Active Directory wizard) with default options:

a) Attach the server to a hub or connect the server to the AP with a cross connect cable. If this is not done, installing AD on the server will fail.
b) Start-Programs → Administrative Tools → Configure Your Server to start the Configure Your Server Wizard or:
c) Click on the "Active Directory" link on the left pane or click Start → Run and type "DCPROMO" (DCPROMO is the default command from a DOS window to start the AD wizard on W2k server)
d) Click on the "Start the Active Directory Wizard" link at the bottom of the page.
e) Select "Domain Controller for a New Domain", then "Create a New Domain Tree", and then "Create a New Forest of Domain Trees".
f) For the DNS name use "wireless.com"
g) For Domain NetBIOS name use "wireless"
h) Data base locations: WINNT\NTDS (default) → Next
i) Next
j) Select "OK" on the warning message, the select "Yes" to install DNS.
k) Select pre-Windows 2000 servers
l) No Admin password is needed, leave blank
m) Next. Advanced Server CD ROM will be required (exit CD autorun if it starts)
n) Reboot

Step 3: Install DHCP on the server:

a) Start → Programs → Settings → Control Panel
b) Add/Remove Programs → Windows Components
c) Select Networking Services and check DHCP
d) Assign a Static IP address for the NIC of the server: example 20.0.0.1, sub-mask 255.0.0.0, Default Gateway 20.0.0.1
e) Assign the DNS server to use 20.0.0.1, no secondary needed.

Step 4: Configure the DHCP server and create a scope:

a) Start → Programs → Administrative Tools → DHCP
b) Click on the server, then Action → New Scope. Set scope name = 'scopename'
c) Use scope range of 20.0.0.1 to 20.0.0.200
d) Skip Exclusions :
(We used exclusion : static 20.0.0.1 for server NIC and static 20.0.0.2 for AP)
e) Length = 8, sub-net mask = 255.0.0.0.
f) Lease Duration: 8 days
g) Configure DHCP options: Yes
h) Skip default gateway
i) Parent domain = wireless.com
j) For Server Name for DNS use "radius", then click Resolve
k) Click Add IP address
l) For WINS server, fill in the server name, Resolve, Add → Next.
m) Activate scope :Yes
n) Finish
o) Authorize the DHCP server,
   - Refresh screen [F5]
   - Action → Authorize
   - Refresh [F5]
p) Attach a wired client to the server and verify receipt of an IP address.
   - On the wired client machine, run IPCONFIG and verify the IP address.
   - Start → Programs → Accessories → Command Prompt
   - IPCONFIG /all <CR>
   - Verify IP address between 20.0.0.3 and 20.0.0.200

Step 5: Configure the Domain Controller (server) so that passwords are stored in reversible encrypted format for all users.

a) Start → Admin Tools → Open Active Directory for Users and Computers
b) Right click server name (wireless.com), then click properties
c) Highlight Group Policy and click Edit
d) Go to Windows Settings/Computer Configuration/Security Settings/Account Policy/ Password Policy/Store password using reversible encryption for all users in the domain.
   - Double click on 'Store password using reversible encryption for all users in the domain'

Set to Enabled.

Step 6: Create a new domain user on the Domain Controller:

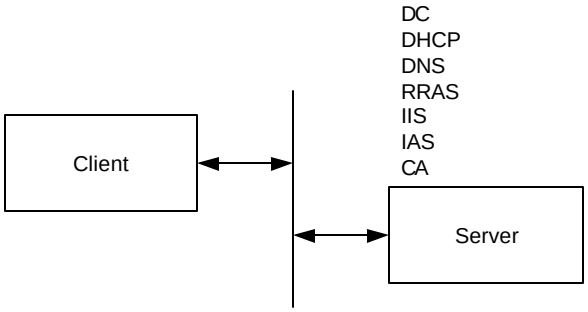
a) Log on to the DC as administrator

b) Start → Admin Tools → Open Active Directory of Users and Computers

c) Create a new username xxx
- Click Action → New → User xxx
- Pick a password xxx
- Finish the new user wizard

d) In the properties for the user, ensure that remote access dial-in is allowed and store reversibly encrypted password for the user.
- Right click on the user name that has just been created, and select properties.
- In the Account tab, click the box to store password using reversible encryption.
- In the Dial-in tab, allow access for Remote Access Permission.

Step 7: Make the machines (client shown in figure bebw) on network, members of the newly created domain.



a) Login as the Administrator of a XP client system

b) Edit the systems domain name to "wireless.com"
- Right click on My Computer → Properties → Computer Name → Change
- Domain Name: wireless.com
- Verify to see the 'Welcome to the domain' message
- Reboot the client
- Log on to "wireless.com" domain as administrator on the XP client

c) Now add the previously created domain user xxx from the server, to the local administrators group on the XP client (User Name: xxx and a password xxx, domain of "wireless.com")
- Start → Control Panel → User Accounts → Add
- User name: xxx
- Domain: wireless.com
- Other: Administrator
- Finish

Step 8: Ensure login is possible from XP client to the domain with user profile stored on Domain Controller (= roaming profile).

a) Configure the roaming profile on the server within user-account properties. Share the user profile folder on the server and set the proper NTFS permissions otherwise it will not be possible to load the roaming profile from the server at logon
b) Log on to Domain as a domain user of wireless.com using user name xxx and password xxx that was created on Domain Controller.
c) Check in Control panel → System that a roaming profile exists

Step 9: Install other necessary services on the servermachine.

a) Start → Control Panel → Add/Remove Programs → Add Windows components: Certificate services
   - Internet Information Services → (IIS) → Full Options
   - Networking services → Internet Authentication Service (IAS)
   - Click Next
   - Select Enterprise Root CA
   - CA name : radius
   - Next
   - Next
   - Select 'OK to stop IIS'
   - Finish

Step 10: Setup IAS server

a) Start → Admin Tools → IAS
b) Create Radius client for the server
   - Open IAS
   - Right click on Clients and select New Client
   - Client Name: radius
     IP address : 20.0.0.1 Use a shared secret key of "AP" (shared key could be anything)
   - Check 'Client must always send the signature attribute in the request.
   - Right click on Clients and select New Client
   - Client Name: AP-3
   - IP address: address assigned to the AP-3. (20.0.0.2)
   - shared secret key: of "AP"(shared key could be anything)
   - Check 'Client must always send the signature attribute in the request.
c) Create a client for RAS server, which needs to authenticate using IAS. Since RAS server will exist on the same machine as the IAS server, create a client for the server address.
   - Start → Admin Tools → Routing and Remote Access
   - Click on the server, then Action and Configure and Enable Routing and Remote Access
   - Use Manual Configured Server setting during the wizard.
   - Finish Wizard
   - Yes to start

- Right click on radius → Properties:
- General tab (Check Router)
- Select LAN and demand-dial routing
- Check Remote access server
- Security tab
- Authentication provider: "Radius Authentication"

d) Press the Configure button, Server name: 20.0.0.1
- Select the change button for the secret key, and type "AP" as the secret key.
- OK,OK, (including warning)
- Accounting provider: "Radius Accounting" .

e) Press the Configure button, Server name: 20.0.0.1
- Select the change button for the secret key, and type "AP" as the secret key.
- OK,OK, (including warning)
- Press the Authentication Methods button.
- Check "Extensible Authentication Protocol ".
- Deselect any other boxes in this window
- EAP Methods: "Smart Card or other Certificate" should be included in the list

Step 11: Create Remote Access policies and create a new profile for every authentication mechanism that is needed i.e., EAP-TLS.

a) Start → Admin Tools → IAS.
b) Select Remote Access policies.
c) Right click and select New Remote Access Policy.
d) Name: EAP-TLS.
e) Condition → Add → Day and Time Restriction → Add
f) Use 24hr access (blue colored screen)
g) Select Deny remote access permission
h) Edit the Profile:
- No Dial-in constraints
- IP: Select Server settings define policy
- Authentication: Select EAP only using smart card or other certificate.
- Uncheck all other boxes
- Configure the certificate by selecting Configure
- Select 'radius.wireless.com'
- Encryption: All boxes checked except for No Encryption.
- Dial-in Constraints: Check Restrict maximum session to: 200 minutes

Step 12: To ensure IAS server works, setup Routing and RAS server on the machine .

a) Ensure that on IAS, the EAP-TLS profile is the first one from top in order.
- Start → Admin Tools → IAS
- Click on Remote Access Policies
- Verify that EAP-TLS is the first profile listed

Step 13: Now on the Server machine:

a) Start → Admin Tools → Active Directory Users and Computers
   - Right click on Domain Controllers → properties
   - Group policy: Default domain policy → Edit
   - Computer Configuration → Windows Settings → Security Settings → Public Key Policies → Right Click on Automatic Certification Request Settings → New → Automatic Certificate Request
   - Default through the wizard.

Step 14: From the XP client machine, log in as a Domain User xxx of the domain.

a) Start → Run → mmc [MS Management Console]
b) File → Add/Remove Snap-in
c) Add → Certificates → Add → close
d) Click on Certificates, then hit Return
e) Certificates → Right click on Personal → All Tasks → Request New Certificate
f) Next → User
   - Check Advanced
   - Check MS Enhanced Crypto Prov 1.0
   - Uncheck Enable Strong Protection
g) Close MMC

Desktop

h) Right click on Internet Explorer on desktop → Properties → Content → Certificates →
i) Click on Certificates → Advanced
j) Check client authentication

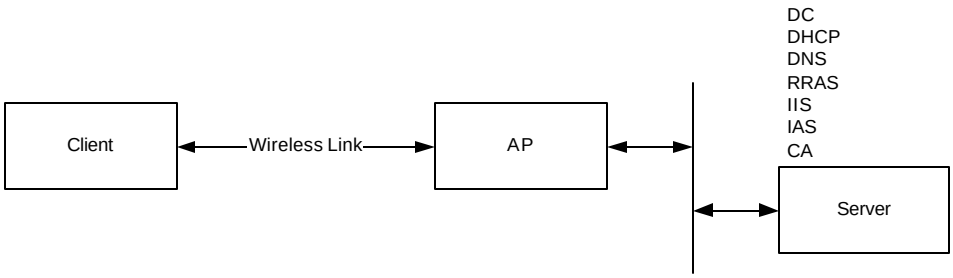
Step 15: Create a VPN on the Client for VPN access into the RRAS server:

a) Right click on My Network Places, select properties
b) Select Create a New Connection
c) Select Connection to the network at my workplace
d) Select VPN
e) Choose a company name
f) VPN Server Selection: 20.0.0.1
g) Connection Availability: My use only.
h) A "Connect Company name" screen will appear.
i) Finish
j) Click the properties → Security → Select Advanced (custom settings) → Settings
   - Data Encryption: Require Encryption
   - Use EAP: Smart Card or other Certificate
   - Select Properties
   - Select Use a Certificate on this computer
   - Uncheck Validate Server certificate
   - Check Use a different user name for the connection
k) Open Network Places → View Network Connections

- Right click on the VPN connection → properties
- Security: click on "Advanced (custom settings)
- Authentication mechanism : EAP-TLS – "Smart Card or other Certificate (encryption enabled)".
- Click on "Properties" tab for EAP-TLS.
- Check "Use a certificate on this computer" box.
- Uncheck "Validate server certificate" box.

l) Connect to the VPN server, by double-clicking on the connection.
m) User will be prompted to select a certification.
n) Select (the only) one and the user should be authenticated.
o) This ensures that a certificate on the client can be used for successful authentication with the server.

Step 16: Connect the AP -3 (with the Beta 2 fixed software) in the network (shown in figure below).



a) Use a wired connection between AP and server (preferable cross-cable) + a wireless link (Avaya Wireless PC Card with FW version 7.52) between XP client and AP

Step 17: Verify that your IP address for the AP and the DHCP address for the AP match on the server. Use IAS to change the address if needed.

a) Start → Admin Tools → DHCP → Scope → Address Leases
b) Start → Admin Tools → IAS
   - Clients → Check that the IP address for the AP-3 is correct
c) Open IE (Use the address of the AP = http://20.0.0.2)
d) User name is blank
e) AP password is 'public'
f) Configure → Interfaces →
   - Change Network name (not required)
   - Disable closed system
   - Ok → back
g) Configure → Security
   - Radius Authentication leave unchanged
   - Ok → back
h) Radius MAC Access Control Status → leave disabled
   - Change passwords to 'AP'
   - Ok → back
i) Radius Server → Server Status → Enable
   - IP address: 20.0.0.1

- Ok → back

j) Encryption:
   - Configuration: 802.1x
   - Enable used cards
   - Ok → back
k) Commands → Reboot → OK

Step 18: On the XP client logon as domain user xxx on domain

a) Right click on wireless connection → properties → authentication
b) Use certification
c) Uncheck 'Validate….'
d) Check 'Use a different name for connection'

Step 19: On the XP client, logon as domain user xxx on domain, connect to the VPN server, by double -clicking on the VPN connection.

a) User will be prompted to select a cert.
b) Select (the only !) one and the user should be authenticated.
c) This ensures that a certificate on the client can be used for successful authentication with the server via the AP.

