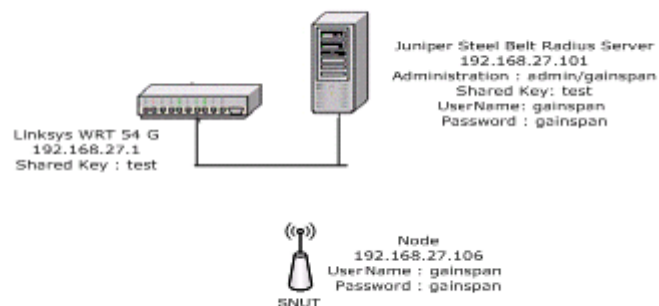


EAP Server Setup and Certificate Generation

EAP FAST SETUP

EAP, EXTENSIBLE AUTHENTICATION PROTOCOL configurations need to be completed on the Radius server and the access points. In this application note the radius server that is used in the configuration example is the Juniper Steel Belt Radius Server (Global Enterprise Edition Version 6.1.0) and the access point used is Linksys-WRT54G. The usernames, etc. are just for example purposes. To install Juniper Steel Belt Radius Server (SBR), please refer to the Juniper website:

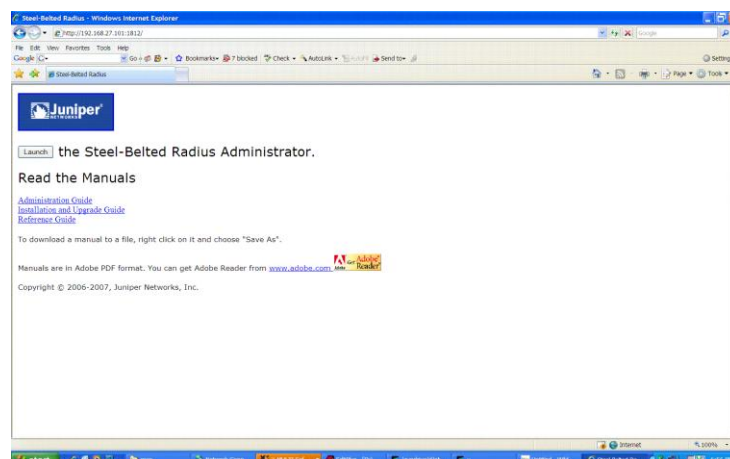
http://www.juniper.net/techpubs/software/aaa_802/sbr.html#GEE61



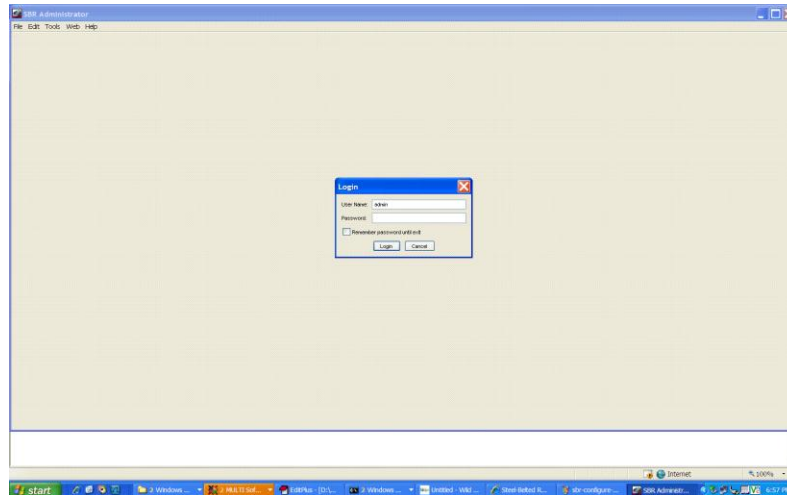
Configure the RADIUS Server

The following are the steps to configure:-

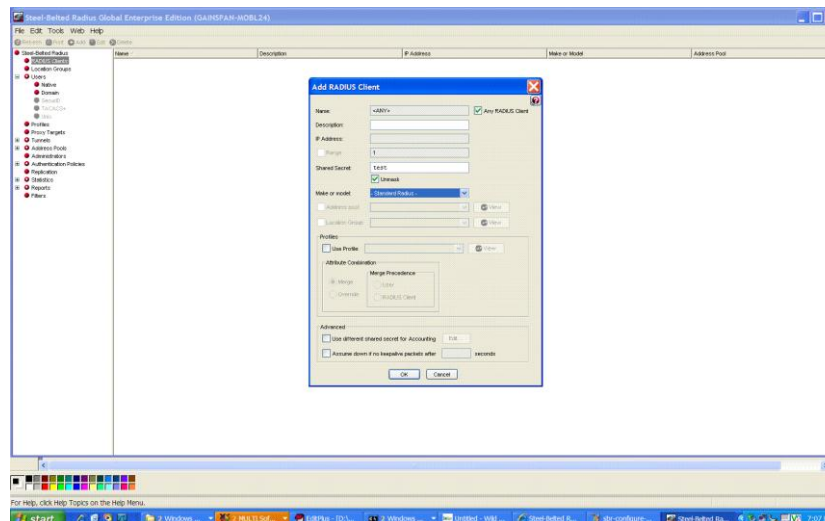
- After SBR installation and the starting of the SBR service, open the SBR from anywhere within the same network using a standard web browser with port number 1812. Launch the SBR application by clicking launch button.



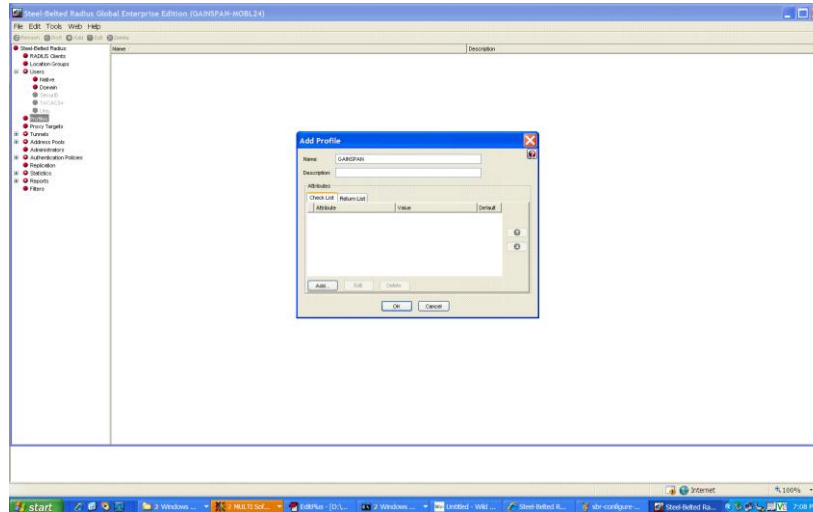
- Enter your Username and Password



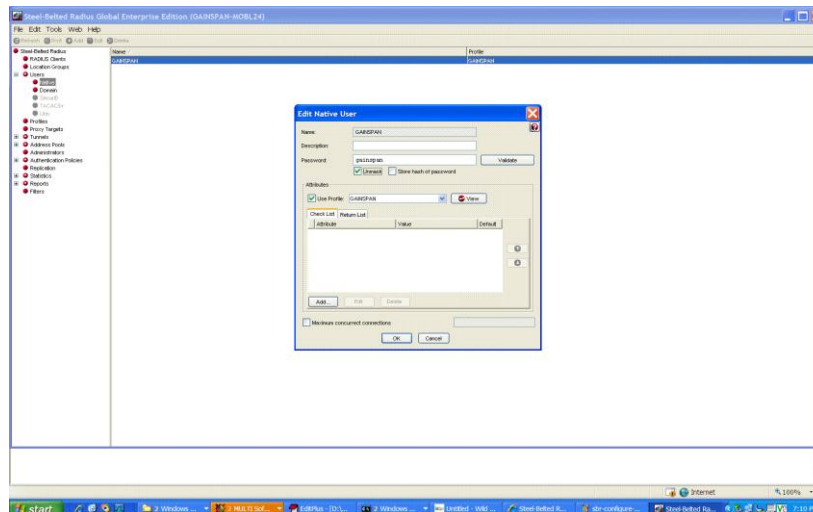
- Add new radius client by selecting any radius client. Configure the shared key (test) that will be configured on the AP.



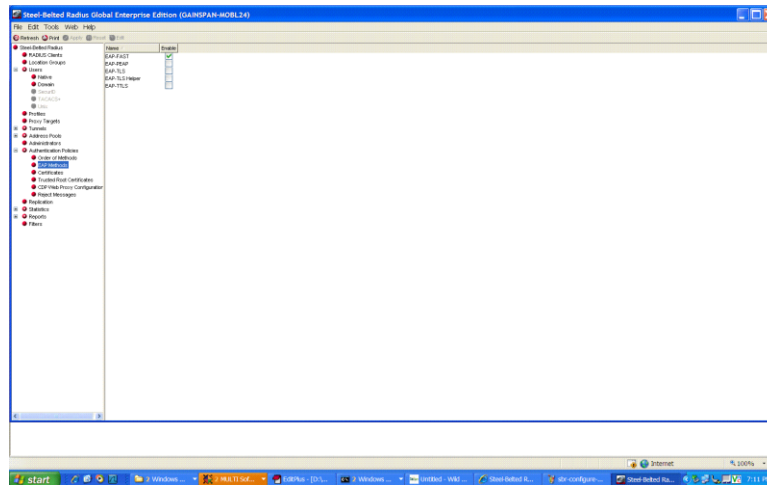
- Create a profile (gainspan)



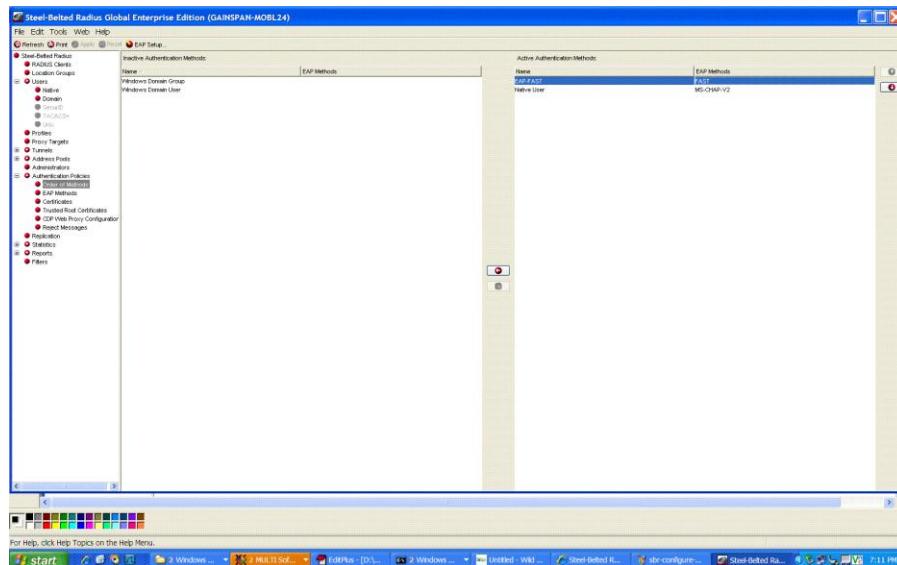
- Create username and password (gainspan/gainspan). Make sure the profile name and username matches. Add the users profile to the profile already created.



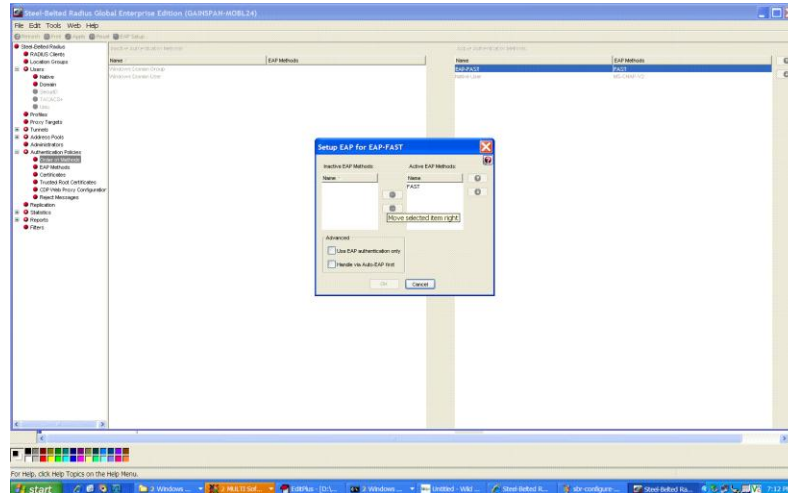
- Enable EAP-FAST in the EAP methods tab



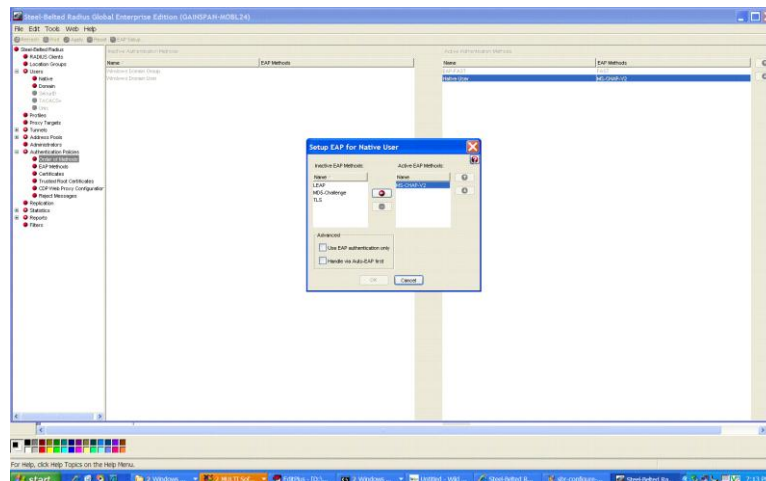
- Select FAST and MS-CHAP-V2 methods as the active authentication methods



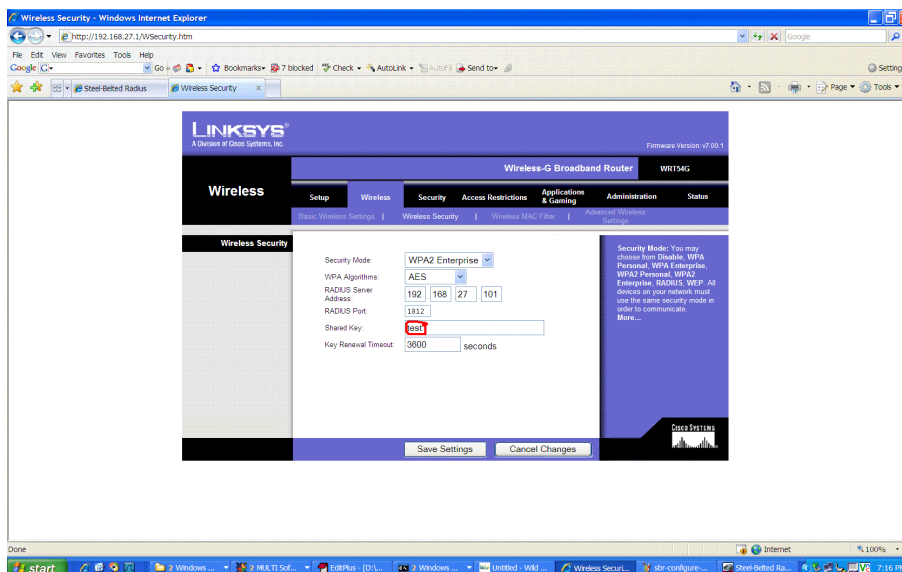
- Check if the EAP Setup of the EAP Methods has only FAST enabled. This is outer authentication type. Outer authentication is a mechanism to create the secure TLS tunnel.



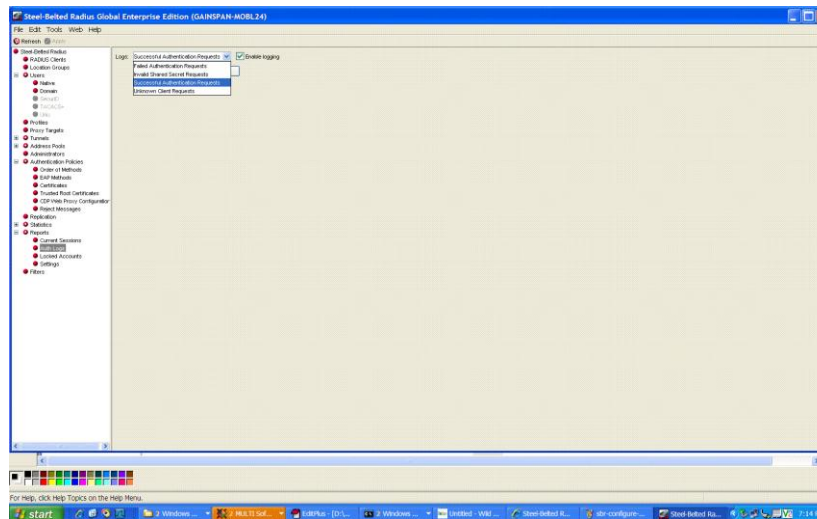
- Check if the EAP setup of the Native user has MS-CHAP-V2 selected. This inner authentication type based on the users' own device authentication protocols.



- Now that the SBR configuration is complete, configure the Linksys-WRT-54G security settings. Make sure the shared key configured on the access point is the same as the shared key (test) configured in the radius client tab in SBR



- Check the logs from the Report tab -> Auth Logs section. Logs are required for debugging purpose, only if authentication fails.



IMPORTANT POINTS

When the node authenticates for the first time, an EAP-FAILURE would be observed on the sniffer. This happens during the PAC (Protected Access Credential) receives. Later it creates a tunnel using PAC and gets associated to AP. This is not specific to our node and is same across all devices associating with EAP-FAST.

Microsoft Certificate Services

Microsoft Certificate Services is the built-in Certificate Authority software on Microsoft Server operating platforms. The Certificate Authority (CA) is the entity to issue certificates to end users (such as client certificates in EAP-TLS), for RADIUS servers (for EAP-PEAP, EAP-TLS or EAP-TTLS authentication) and to other clients requiring proof of identity.

There are 4 types of Microsoft CA:

- 1 Enterprise Root CA
- 2 Enterprise subordinate CA
- 3 Standalone Root CA
- 4 Standalone subordinate CA

The Enterprise CA includes integration with Active Directory (needed for IAS TLS client certificates). Before installing the Enterprise Root CA, make sure that Active Directory and IIS are installed. To install IIS, go to:

Control Panel-> Add/Remove Programs-> Add/Remove Windows Components

Select “Application Server” and then click on the Details button. Check the following:

To install IIS on a Win2003 server:

1. Click Start->Control Panel->Add or Remove Programs
2. In Add or Remove Programs, click Add/Remove Windows Components
3. Under Components, click on Application Server (but do NOT select it) and click Details
4. In the Application Server window, click to select IIS and click OK
5. Click Next

After the wizard completes the installation, click **Finish**. Also, check the current system date for accuracy. The current system date is the start date for when the CA is valid.

Installing an Enterprise Root CA

1. Go to: Control Panel-> Add/Remove Programs-> Add/Remove Windows Components
2. Select “Certificate Services”
3. Select “Enterprise Root CA”
4. Specify a name for the CA; such as “MyNewCA” or the equivalent
5. Select the default options and complete wizard as directed.

Getting the Root CA Certificate

This section will detail the instructions to obtain the certificate representing the “MyNewCA” Certificate Authority. You would need to obtain the Trusted Root CA certificate (and install it on the client) if the supplicant on the client/station will be validating the server certificate presented as part of the two way handshake an EAP-TLS or EAP-PEAP authentication.

1. Using an IE browser, enter the following URL:

`http://<Test-Net IP address of server machine>/certsrv`

If you are prompted for a password, then enter a valid username/password pair for any user in the Active Directory (like administrator/<blank>). Click on “Download a CA certificate, certificate chain, or CRL”.

2. Click on “Download CA certificate” and save it as a “.cer” files type that can be copied and installed on clients/stations as needed.

Getting the Client Certificate

For EAP-TLS, the user presents a digital client certificate as their credentials. To obtain a client certificate, follow these steps:

1. Create a user in active directory that will receive this certificate. A user may have multiple certificates issued to them. Select “New” → “User” from the menu for the Users folder. Enter “console” for the First name, Full name and User logon name fields.

2. Enter “user1” as the password for the user “console” and select “Password never expires”.

NOTE: You may need to change the security policies on the server via Control Panel – Administrative Tools – Domain Security Settings – Password Policy if you are unable to enter “user1” as the password. A reboot is required after the change.

3. In an IE browser window, enter the following URL:

`http://<Test-Net IP address of server machine>/certsrv`

4. Enter “console” and “azimuth” for the Username and Password respectively.
5. Select “Request a certificate”.
6. Select “Advanced Certificate Request”.
7. Select “Create and Submit a Request to this CA”.
8. Select “User” from the Certificate Template dropdown. Check “Mark keys as exportable”. You may also increase the Key Size. The larger the key size the more secure the certificate. Really large keys such as 16384 bits for example do require more CPU time to calculate the crypto. Having client certificates with different sized keys will yield different benchmark performance numbers.
9. After Submitting the certificate request, you will be prompted to install the certificate.
10. Install the certificate and you should get a successful confirmation.

11. The client certificate for the user “console” has now been installed on the Microsoft current user certificate store. To view and access both the current user and local computer certificate store on the 2003 server, run “mmc” from Start->Run File → Add/Remove snap-in. Click the Add button. Highlight Certificates → Add → “My user account” → Finish. Highlight Certificates → Add → “Computer account” → Next → Local computer selected → Finish. Click on the Close button on the Add standalone snap-in dialog. Click OK on the Add/Remove Snap-in dialog to close. If you now navigate to Certificates – Current User – Personal – Certificates, you will see the “console” client certificate. As an alternative to using the mmc certificate snap-in to view the certificates in the Current User certificate store only, you may use IE (Tools → Internet Options → Content tab → Certificates button).

Exporting the Client Certificate

1. You will need to export the client certificate to a .pfx file that will then be installed on the client/station laptop for TLS. This is done via the mmc certificate snap-in or through IE.
2. Select “Yes, export the private key”.
3. *Optional.* You may select to include the Root CA certificate for MyNewCA in this exported .pfx file.
4. Select a password for this .pfx certificate file. This file is password protected since it contains the private key.
5. Enter full path and complete .pfx file name and finish export wizard.
6. “consoleClientCert.pfx” may now be installed on the Microsoft (XP, 2000, etc) client/station by double-clicking on the file. You will need to enter the password from step 4 during the installation.
7. You will need to modify the dial-in properties for the “console” user in Active Directory in order for client stations to be granted access when this client certificate is used for wireless network authentication. In Active Directory Users and Computers, view the properties of the assigned “console” user. Under the “Dial-in” tab, select the “Allow access” radio button.

Getting a Server Certificate

When EAP-TLS, EAP-PEAP, or EAP-TTLS is enabled on a RADIUS server, you will need to configure a server certificate with the RADIUS server software. A server certificate for the 2003 server machine is typically generated and installed automatically in the local computer certificate store when Certificate Services is installed. Steps for manually requesting and installing a server certificate are as follows:

1. Enter the URL `http://<Test-Net IP address of server machine>/certsrv`. Supply the username and password for a member of the domain administrators group. You will need to access the certificate server page as a domain admin user so that more certificate template options will be available.
2. Click on “Request a certificate”.
3. Click on “advanced certificate request.”
4. Click on “Create and submit a request to this CA”.

5. For Certificate Template, select “Web Server”. Enter values for server certificate in the Information section. Check “Store certificate in the local computer certificate store”. Click on Submit to request certificate.
6. Click on Install this certificate.
7. You will get confirmation for a successful install.
8. To view the server certificate, you will need to use the mmc certificate snap-in with the local computer store certificate. Navigate to the “Certificates (Local Computer) – Personal – Certificates and double-click the “myradsvr” certificate.

NOTE: Dates are valid within the “from” and “to” range. Certificate contains private key. Enhanced Key Usage is “Server Authentication (1.3.6.1.5.5.7.3.1)”. For a complete list of other server and client certificate requirements when using IAS as the RADIUS server, see:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;814394>

Microsoft Internet Authentication Service (IAS)

1. Install Microsoft IAS if it is not already installed on the Windows 2003 Server machine.
Control Panel-> Add/Remove Windows Components
Networking Components-> Details-> Internet Authentication Services
2. Select the “Properties” menu from the Internet Authentication Service icon (left panel).
3. On the Ports tab, enter the RADIUS authentication port configured on your access points.
4. For each AP that will send requests to this IAS RADIUS server, you will need to configure a RADIUS Client.
Control Panel-> Administrative Tools-> Internet Authentication Service
5. Enter a new RADIUS Client for each Access Point under test in the system.
6. Select “RADIUS Standard” for the Client-Vendor. The Shared secret configured on the AP should match the shared secret here. Click on “Finish” to add RADIUS client.
7. You will now create a Remote Access Policy for EAP-TLS and EAP-PEAP/EAP-MS-CHAP-V2. You may create a remote access policy for each protocol separately or create one remote access policy that has both EAP-TLS and PEAP configured. The following directions will create 1 policy and then it will edit that policy to include both protocols. Select New Remote Access Policy from the left pane tree.
8. Enter “TLS or PEAP” for the policy name.
9. Select “Wireless” for Access Method.
10. Add the “Domain Users” group for your Active Directory Domain.
11. Select “Smart Card or other certificate” for EAP-TLS first and then click on “Next” to complete the Wizard.
12. Double click on your “TLS or PEAP” policy to edit. Navigate to the Authentication tab and click on EAP Methods.

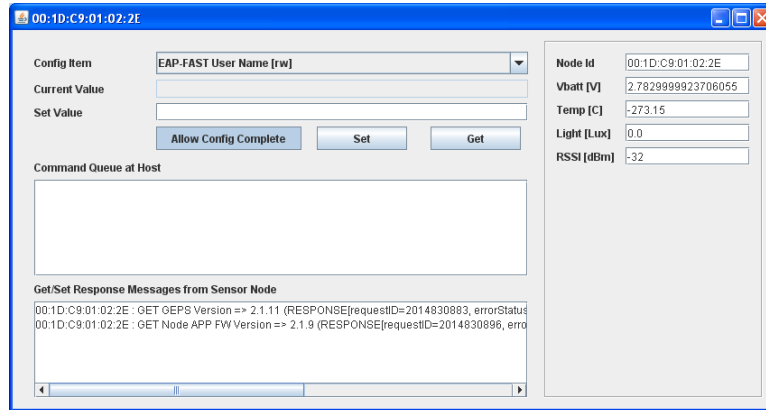
13. Click on “Add:” and select “Protected EAP (PEAP)”. Click on “OK” on the Add EAP.
14. Depending on the EAP type that the client/station is configured, you may want to list that EAP type first. *Note that it is likely that having the desired EAP type listed first, as opposed to second, will produce different benchmark performance results.*
15. Click “OK” on the Select EAP Providers and Edit Dial-in Profile dialogs to accept changes.
16. Select “Register Server in Active Directory” in the main menu.
17. Configure IAS to log details about authentication requests received. In addition, IAS will log authentication requests in the Control Panel-> Administrative Tools-> Eventviewer. This would be a good place to start debugging authentication problems with IAS.

NOTE: To view the server certificate configured on IAS, select “Properties” on the “TLS or PEAP” policy. Click on Edit Profiles, then select the Authentication tab and click on the “EAP Methods” button. Each EAP protocol listed may be configured to use a different server certificate. Highlight the desired EAP type and click “Edit” to view a properties dialog which lists the server certificate used. The “Certificate issued to” list is populated by certificates installed in the local computer certificate store.

SET UP EAP-FAST CONNECTION

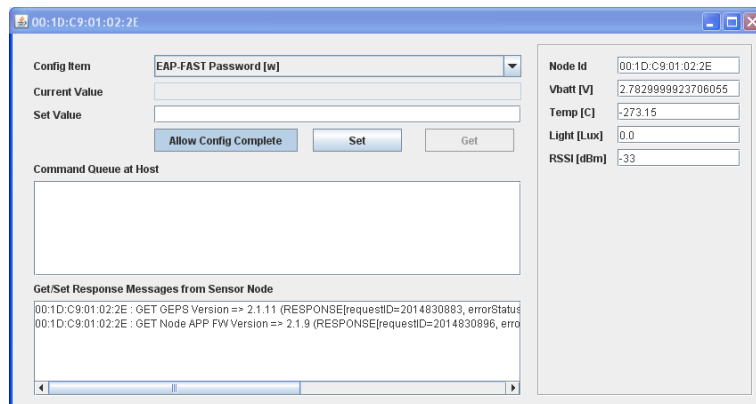
1. Compile the binaries with macros `GSN_SECURITY_ENTERPRISE_AVAILABLE` and `GSN_SECURITY_ENTERPRISE_FAST_MSCHAPV2_AVAILABLE` enabled in project file.
2. Load the binaries using WildConfigurator.
3. Configuration is to be done either while node is running in normal mode or by going to serial configuration mode by deploying GSDemo.
 - a. If using the Normal Mode for configuration, Configure AP with default settings for SSID <GainSpanDemo>, channel <6> and security <Open>. Run the node in order to associate it with the AP. The node will start sending the config trap to the SNMP server <192.168.3.200>.
 - b. If using the Serial Configuration Mode, the run the node and press the Alarm button to switch the node into Serial Configuration Mode. Run the NDIS driver and WildServer on the Configuration PC/Laptop. The node will start sending the config Trap to the PC through Serial interface.
4. After node starts sending the config trap to the configuration server, run the GSDemo.
5. Open the control window of the node and configure the required parameters such as SSID, channel, security parameters, Server IP address, etc.

6. To set the EAP-FAST user name, select the configuration item **EAP-FAST User Name** from the dropdown menu. Give the user name in the set value field and press set button.



The screenshot shows a configuration window titled "00:1D:C9:01:02:2E". The "Config Item" dropdown is set to "EAP-FAST User Name [w]". The "Current Value" field is empty. The "Set Value" field is empty. There are three buttons: "Allow Config Complete", "Set", and "Get". The "Command Queue at Host" section is empty. The "Get/Set Response Messages from Sensor Node" section shows two messages: "00:1D:C9:01:02:2E : GET GEPS Version => 2.1.11 (RESPONSE[requestID=2014830883, errorStatus=0])" and "00:1D:C9:01:02:2E : GET Node APP FW Version => 2.1.9 (RESPONSE[requestID=2014830896, errorStatus=0])". The right sidebar shows sensor data: Node Id (00:1D:C9:01:02:2E), Vbatt [V] (2.7829999923706055), Temp [C] (-273.15), Light [Lux] (0.0), and RSSI [dBm] (-32).

7. To set EAP-FAST password, select the configuration item **EAP-FAST Password** from the dropdown menu. Give the password in the set value field and press the set button.

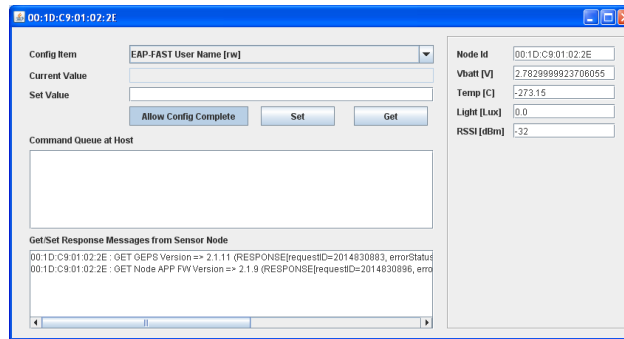


The screenshot shows a configuration window titled "00:1D:C9:01:02:2E". The "Config Item" dropdown is set to "EAP-FAST Password [w]". The "Current Value" field is empty. The "Set Value" field is empty. There are three buttons: "Allow Config Complete", "Set", and "Get". The "Command Queue at Host" section is empty. The "Get/Set Response Messages from Sensor Node" section shows two messages: "00:1D:C9:01:02:2E : GET GEPS Version => 2.1.11 (RESPONSE[requestID=2014830883, errorStatus=0])" and "00:1D:C9:01:02:2E : GET Node APP FW Version => 2.1.9 (RESPONSE[requestID=2014830896, errorStatus=0])". The right sidebar shows sensor data: Node Id (00:1D:C9:01:02:2E), Vbatt [V] (2.7829999923706055), Temp [C] (-273.15), Light [Lux] (0.0), and RSSI [dBm] (-33).

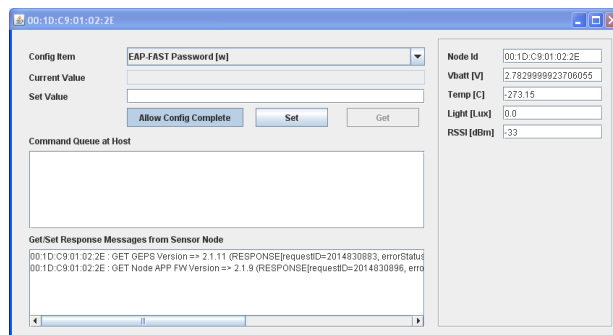
8. Reboot the node.
9. Configure the AP with the same configuration what is configured in the node. Configure the Authentication server with the same security credentials.
10. Restart the node to associate with the AP with EAP-FAST security.

SET UP EAP-TLS CONNECTION

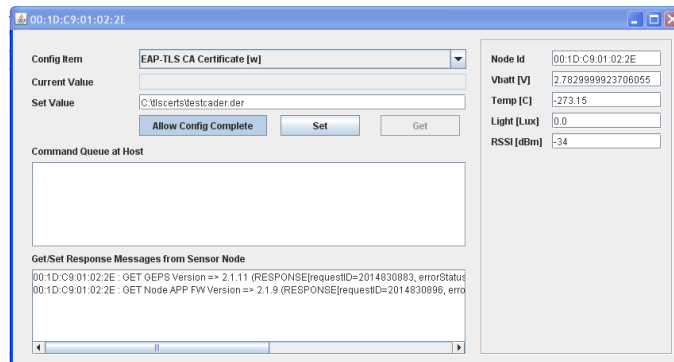
1. Compile the binaries with macros `GSN_SECURITY_ENTERPRISE_AVAILABLE` and `GSN_SECURITY_ENTERPRISE_TLS_AVAILABLE` enabled in project file.
2. Load the binaries using WildConfigurator.
3. Configuration is to be done either while node is running in normal mode or by going to serial configuration mode by deploying GSDemo.
 - a. If using the Normal Mode for configuration, Configure AP with default settings for SSID <GainSpanDemo>, channel <6> and security <Open>. Run the node in order to associate it with the AP. The node will start sending the config trap to the SNMP server <192.168.3.200>.
 - b. If using the Serial Configuration Mode, the run the node and press the Alarm button to switch the node into Serial Configuration Mode. Run the NDIS driver and WildServer on the Configuration PC/Laptop. The node will start sending the config Trap to the PC through Serial interface.
4. After node starts sending the config trap to the configuration server, run the GSDemo.
5. Open the control window of the node and configure the required parameters such as SSID, channel, security parameters, Server IP address, etc.
6. To set the EAP-TLS user name select the configuration item **EAP-FAST User Name** from the dropdown menu. Give the user name in the set value field and press set button.



7. To set EAP-TLS password select the configuration item **EAP-FAST Password** from the dropdown menu. Give the password in the set value field and press the set button.



8. To load the CA certificate select the configuration item **EAP-TLS CA Certificate**. Give the complete path of the certificate in the set value field and press the set value button.



9. Similarly load client and private key certificates by selecting configuration items EAP-TLS Client Certificate and EAP-TLS Private Key respectively.
10. Reboot the node.
11. Configure the AP with the same configuration what is configured in the node. Configure the Authentication server with the same security credentials.
12. Restart the node to associate with the AP with EAP-FAST security.

ADDITIONAL REFERENCES

1. GEPS2 APG
2. Serial to Wi-Fi Evaluation Kit Startup Guide.pdf
3. Serial to WiFi_Adapter_Guide.pdf
4. Serial to WiFi_Command_Reference.pdf
5. Serial to WiFi Bridge App Note AN025.pdf

The GainSpan Ultra-Low-Power Wi-Fi System-On-Chip may be used as a transparent bridge to carry serial (UART) traffic over an 802.11 wireless link. Serial commands are used to manage the wireless network configuration. This application note will give the details necessary to setup this bridge.

6. Firmware Update over Wi-Fi Interface using S2W App Note AN038.pdf

This document details the necessary steps and processes required for performing a firmware update over the Wi-Fi interface with the Serial2Wi-Fi Application.

Version	Date	Remarks
0.1	27 August 2010	Initial Release
1.0	9-Nov-10	GA

GainSpan Corporation • 1 (408) 673-2900 • info@GainSpan.com • www.GainSpan.com

Copyright © 2009-2010 by GainSpan Corporation.

All rights reserved.

GainSpan and GainSpan logo are trademarks or registered trademarks of GainSpan Corporation.
Other trademarks are the property of their owners.

Specifications, features, and availability are subject to change without notice.

SP-1.0

16-Nov-11