Allied Telesis

AlliedWare™ OS

How To | Configure Basic 802.1x Port Authentication

Introduction

This How To Note is a guide to 802.1x and Port Authentication. It outlines the implementation of the IEEE 802.1x standard for port-based network access control and the configuration of port authentication on Allied Telesis products and other required system components to enhance network security.

802.1x is an IEEE standard providing a mechanism for authenticating and authorising devices attached to a LAN port. Devices wishing to access services behind a port under 802.1x control must authenticate themselves before any Ethernet packets originating from the devices are allowed to pass through. In the cases of authentication failure, the device will be prevented from accessing the port and therefore will not be able to use the services behind the port.

What information will you find in this document?

This How To Note describes 802.1x in the following sections:

Which products and software versions does this information apply to?

This configuration applies to the following routers and switches, running AlliedWare Software Version 2.6.1 or later:

- AT-8800, AT-8600, AT-8700XL, Rapier i, and Rapier series switches

- AT-9900, x900, and AT-8900 series switches

- AR400 and AR700 series routers (note that AR410 routers only support 802.1x on their Eth ports)

Related How To Notes

You also may find the following How To Notes useful:

- *How To Create A Secure Network With Allied Telesis Managed Layer 3 Switches*

- *How To Use 802.1x EAP-TLS or PEAP-MS-CHAP v2 with Microsoft Windows Server 2003 to Make a Secure Network*

- *How To Use 802.1x Security with AT-WA7400 APs, AT-8624PoE Switches, and Linux's freeRADIUS and Xsupplicant*

- *How To use 802.1x VLAN assignment*

- *How To Configure A Secure School Network Based On 802.1x*

How To Notes are available from www.alliedtelesis.com/resources/literature/howto.aspx.

System Components

There are three main components to a system using 802.1x port authentication control:

Authenticator
The device that wishes to enforce authentication before allowing access to services that are accessible behind it. An example of this is an AT-8800 switch that has 802.1x port authentication control enabled.

Supplicant
The client that wishes to access services offered by the Authenticator's system. An example of this is a Windows XP Professional PC with 802.1x client.

Authentication Server
The device that uses the authentication credentials supplied by the Supplicant, to determine if the Authenticator should grant access to its services. The Allied Telesis implementation of 802.1x supports the use of RADIUS authentication server using EAP in conjunction with RADIUS.

A Typical Configuration

A typical configuration for a system under 802.1x control is shown in the following figure. In this scenario, PC "A" wishes to use services offered by servers on the LAN behind the switch. The PC is connected to a port on the switch that has 802.1x port authentication control enabled. The PC must therefore act in a supplicant role. Message exchanges take place between the supplicant and the authenticator, and the authenticator passes the supplicant's credentials to the authentication server for verification. The authentication server then informs the authenticator whether or not the authentication attempt succeeded, at which point PC "A" is either granted or denied access to the LAN behind the switch.
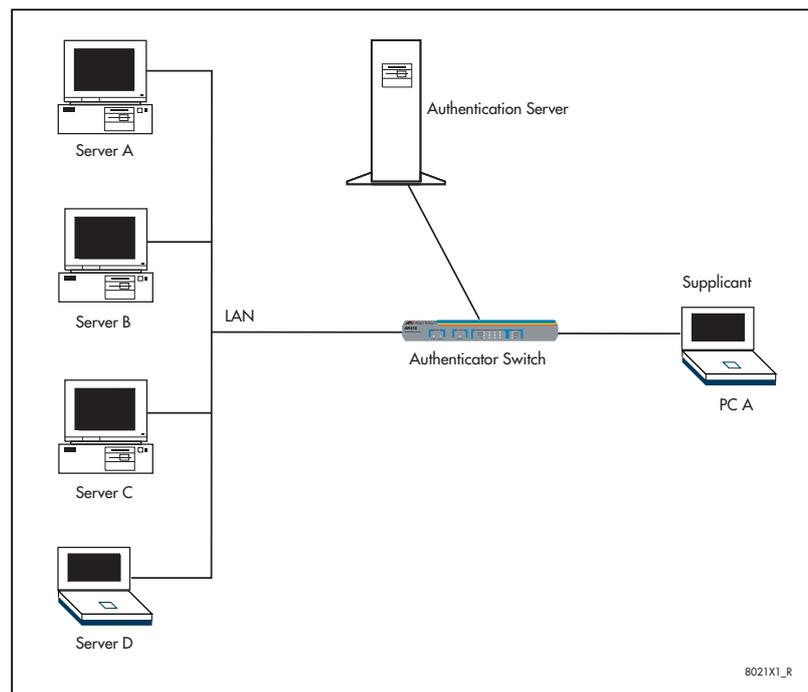
Steps in the Authentication Process

The devices make use of the EAP (Extensible Authentication Protocol) packets for the port authentication process. Until authentication is successful, the supplicant can only access the authenticator to perform authentication message exchanges. Initial 802.1x control begins with an unauthenticated supplicant and an authenticator. A port under 802.1x control acting as an authenticator is in an unauthorised state until authentication is successful. The following steps outline the authentication process:

1. Either the authenticator or the supplicant can initiate an authentication message exchange. The authenticator initiates the authentication message exchange by sending an EAP-Request/Identity packet. The supplicant initiates an authentication message exchange by sending an EAPOL-Start packet, to which the authenticator responds by sending an EAP-Request/Identity packet.

2. The supplicant sends an EAP-Response/Identity packet to the authentication server via the authenticator, confirming its identity.

3. The authentication server uses a specific authentication algorithm to verify the supplicant's identity, for example EAP-MD5 (Message Digest 5) or EAP-OTP (One Time Password), and sends an EAP-Request packet to the supplicant via the authenticator.

4. The supplicant provides its authentication credentials to the authentication server via an EAP-Response.

5. The authentication server either sends an EAP-Success packet or EAP-Reject packet to the supplicant via the authenticator.

6. Upon successful authorisation of the supplicant by the authenticator server, a port under 802.1x control is in an authorised state, unless the MAC associated with the port is either physically or administratively inoperable, and the supplicant is allowed full access to services offered via the controlled port.

7. When the supplicant sends an EAPOL-Logoff message to the authenticator the port under 802.1x control is set to unauthorised.

A successful authentication message exchange, initiated and ended by a supplicant using the EAP OTP mechanism, is shown in the following figure.
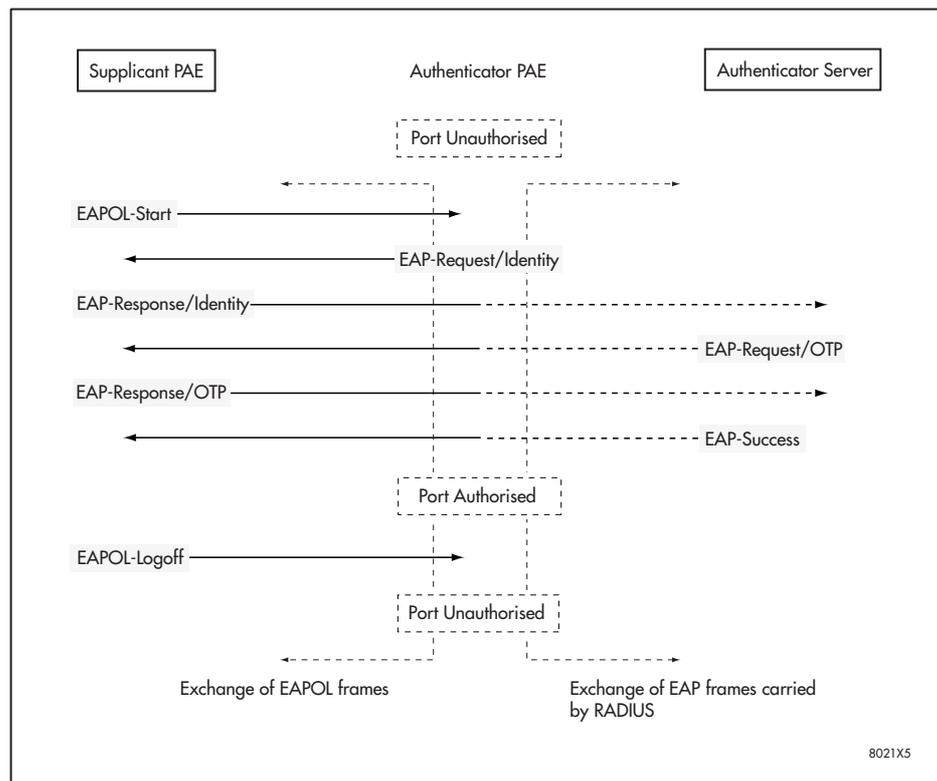
Setting up 802.1x Port Authentication

The following sections present an example for setting up 802.1x port-based network access control using Allied Telesis device as the Authenticator, Steel-Belted Radius server as the Authentication Server and Windows XP Professional as the Supplicant in the scenario depicted in "A Typical Configuration" on page 3. In this example, port 1 of a switch is configured to enable the port authentication.

Configuration for an Allied Telesis device as the Authenticator

The following steps are required to configure Allied Telesis device as the Authenticator and have port authentication enabled on port 1:

1. Configure switch/router to RADIUS server communication

        add radius server=192.168.1.254 secret=allied

2. Configure port authentication

        enable portauth

        enable portauth port=1 type=authenticator mode=single

---

Note: For detailed information on the command syntax and additional configuration information, please refer to the *Port Authentication* chapter of the Software Reference.

Configuration for a RADIUS server as the Authentication Server

The following steps provide a sample configuration for using the Steel-Belted RADIUS Enterprise Edition v4.0 as the Authentication Server:

1. Under Windows, double-click the RADIUS Administrator icon to run the Steel-Belted Radius Administrator program.

2. Click Connect to select the server under the Server Dialog.
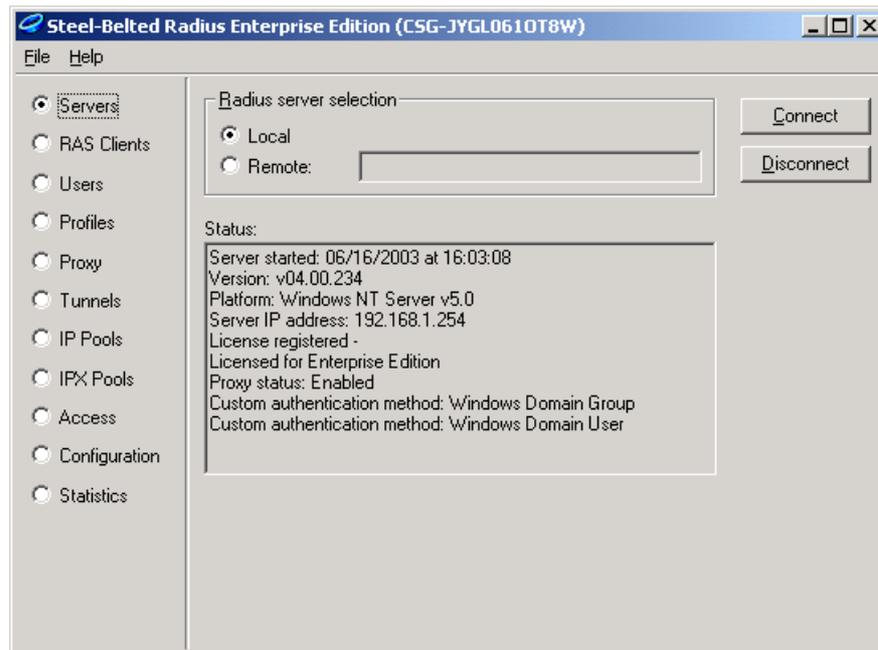
3. Add the RAS client information including the client (switch or router) name, IP address and authentication shared secret under the RAS Client Dialog.
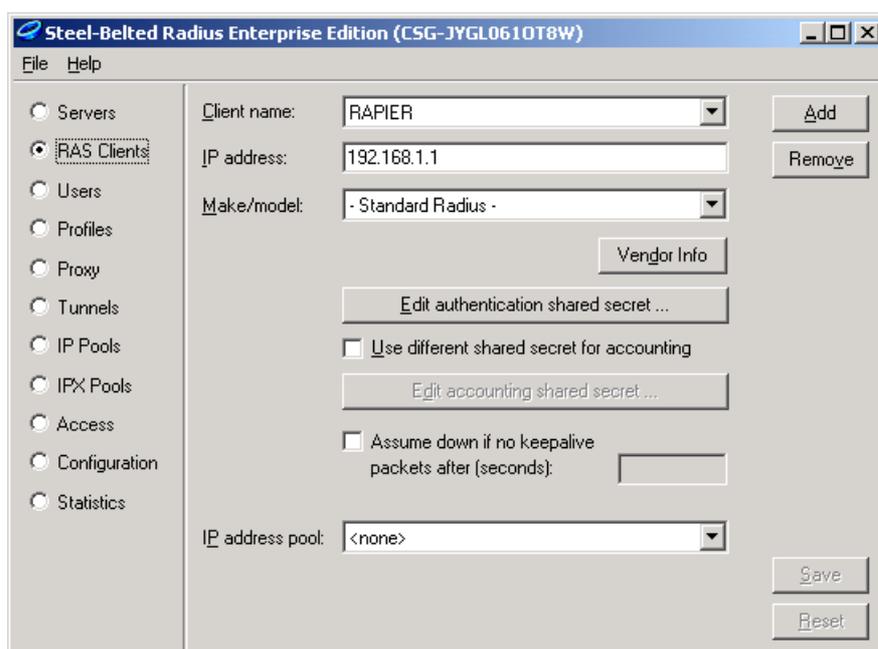
4. Add the users information including username and password under the Users Dialog.
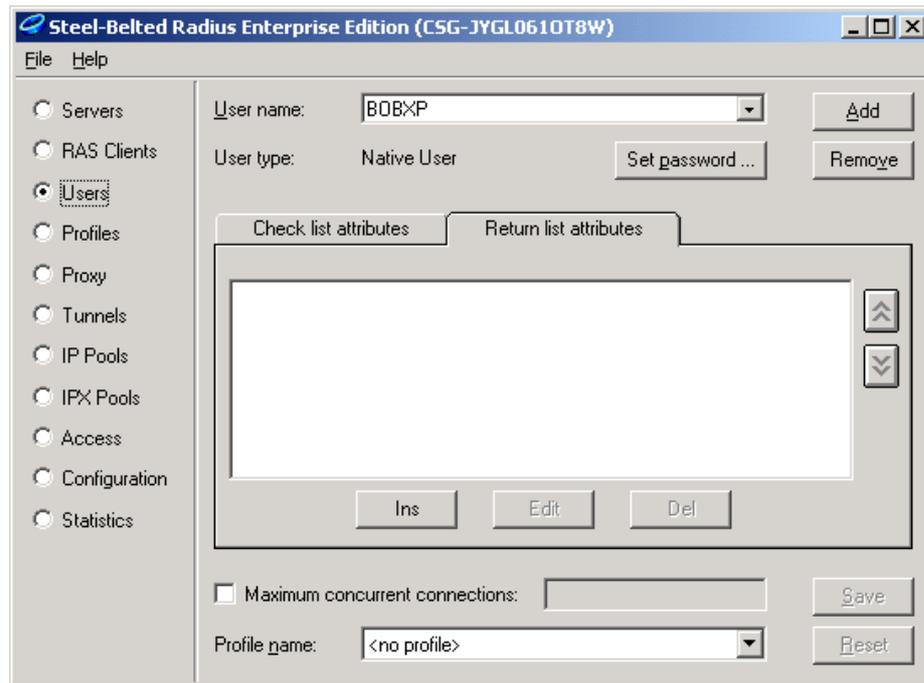
5. Edit the eap.ini configuration file to configure EAP MD5-Challenge as the authentication method for authenticating users.
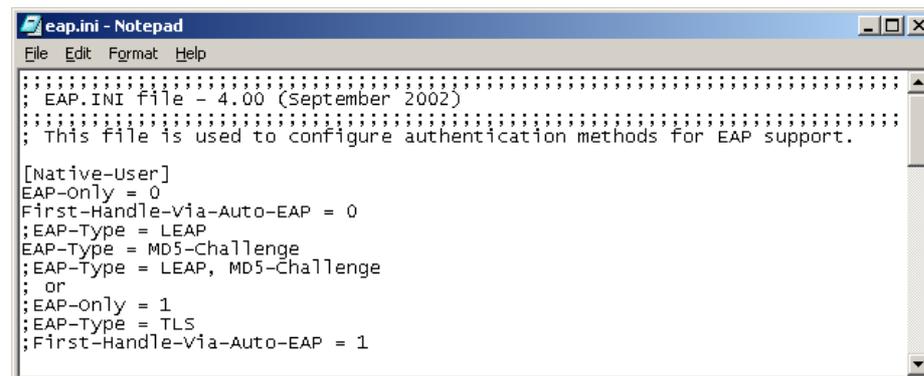
Note: This sample configuration only provides a basic setup for the use of Steel-Belted Radius server as 802.1x Authentication Server. For more information on the configuration of Steel-Belted Radius server, please refer to its documentation.

Configuration for Windows XP Professional as the 802.1x Supplicant

The following steps provide a sample configuration for using the Microsoft Windows XP Professional as the 802.1x Client/Supplicant:

1. Open Network Connections and right click the connection for which you want to enable 802.1x authentication, and then click Properties.

2. On the General tab, click to select the Show icon in notification area when connected check box
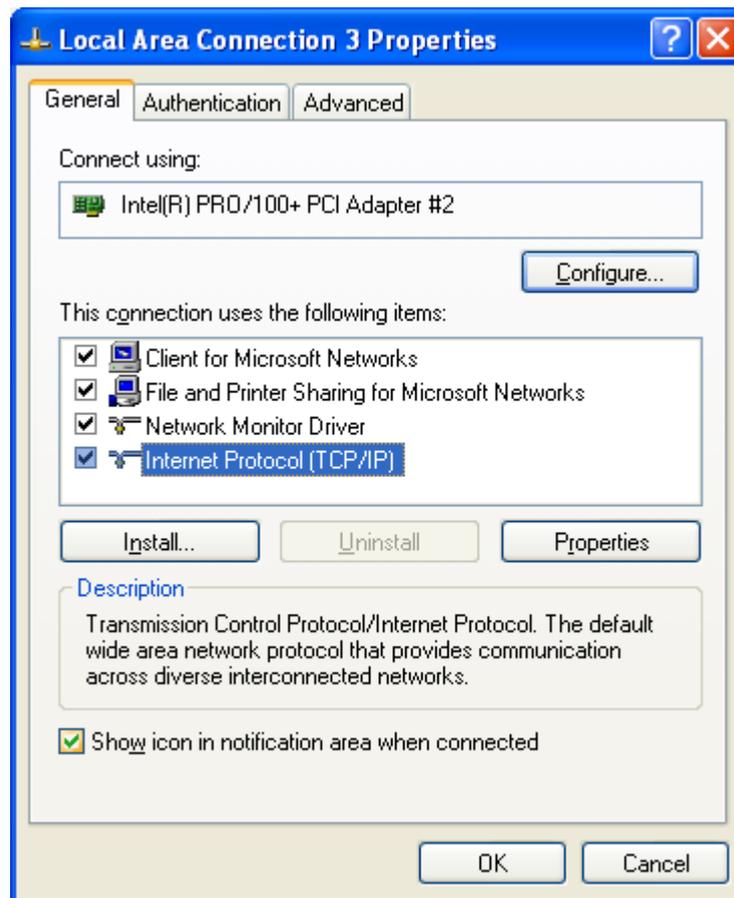
> **Note:** This will enable the "balloon" notifications feature on Windows XP Professional which provides balloon messages to request user action for entering username and password and displays error information for authentication failure.

3. On the Authentication tab, select the Network access control using IEEE 802.1x check box to enable the IEEE 802.1x authentication for the connection.

4. In the EAP type drop-down box, select MD5-Challenge.
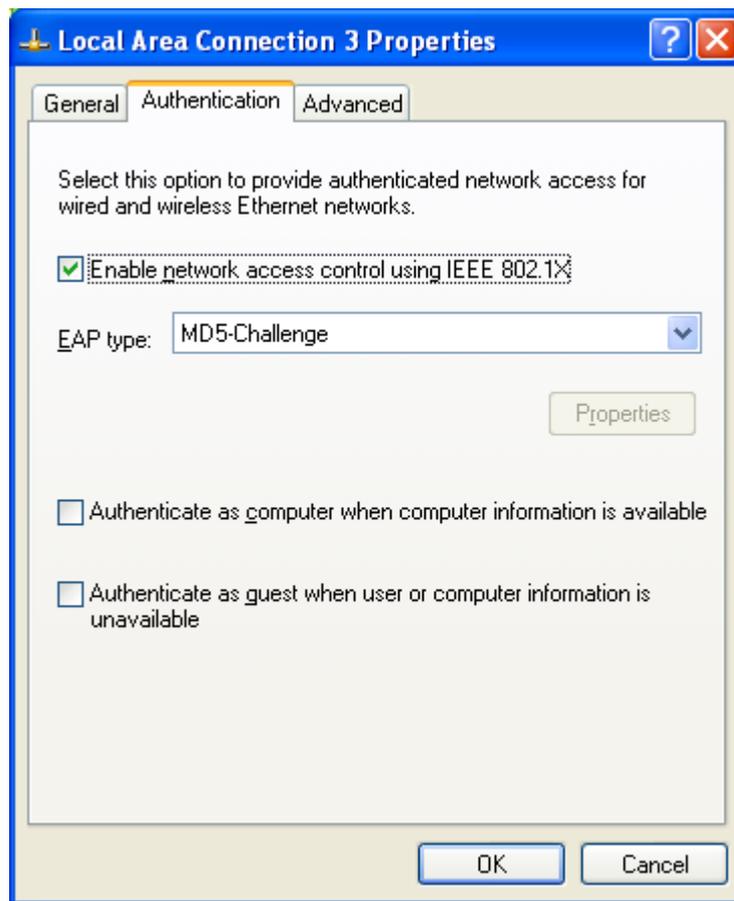
For basic configurations, it is your choice whether or not you select the check boxes "Authenticate as computer when computer information is available" and "Authenticate as guest when user or computer information is unavailable". However, if you have configured VLAN assignment with a guest VLAN, you must not check the second box. This is because VLAN assignment with a guest VLAN only works if guest users do not send any 802.1x information.

5. Click the OK button to save the settings.

6. Connect the Windows XP device to port 1 of the Allied Telesis router or switch that has port authentication enabled.

   The devices will initiate the port authentication process. After a short period of time, a balloon message on the task bar will prompt you for authentication action.

7. Click on the balloon message. A Local Area Connection dialog box will pop up.

8. Enter the username and password on the Local Area Connection dialog box and click the OK button. In this example, the Logon Domain information is not required.

After the Authentication Server verifies the authentication credentials, the port status on the Authenticator device will change to Authorised. The supplicant device is now able to access the services behind the port. In the event that authentication fails, the port status on the Authenticator device will remain Unauthorised. The supplicant device will be prevented from accessing the services behind the port.

Note: Microsoft Windows XP Professional has built-in support for IEEE 802.1x. Microsoft Windows 2000 Professional does not have built-in support for IEEE 802.1x. To enable this support requires SP3 and the Q313664_W2K_SP4_X86_EN patch. See support.microsoft.com/kb/313664.

Troubleshooting

The following sections provide some useful steps for trouble shooting the 802.1x functionality on the system components:

Authenticator—Allied Telesis device:

Use the **show portauth port** command to check the current configuration of 802.1x enabled ports on the device.

```
802.1X Configuration
--------------------------------------------------------------------------
Interface: port1
PAE Type............... Authenticator
Authenticator PAE State....... AUTHENTICATED
Port Status................... authorised
Backend Authenticator State... IDLE
AuthControlPortControl........ Auto
quietPeriod................... 60
txPeriod...................... 30
suppTimeout................... 30
serverTimeout................. 30
maxReq........................ 2
reAuthMax..................... 2
reAuthPeriod.................. 3600
reAuthEnabled................. False
piggyBack..................... True
keyTransmissionEnabled........ False (not supported)
adminControlledDirections..... Both (not supported)
```

Use the **show log** command to check the log of port state changes.

```
Date/Time   S Mod  Type  SType Message
--------------------------------------------------------------------------
25 12:13:12 4 ENCO ENCO  STAC  STAC SW Initialised
25 12:13:12 3 LOG               IGMP Snooping is active, L3FILT is activated
25 12:13:12 3 PORT PORTA PAE    Port Authentication enabled
25 12:13:12 3 PORT PORTA PAE    Config Change : port1 enabled
25 12:13:12 7 SYS  REST  NORM   Router startup, ver 2.6.0-00, 25-Oct-2000, Clock
                                Log: 12:12:17 on 25-Jun-2003
25 12:13:15 6 SWIT PINT  UP     Port1: interface is UP
25 12:13:15 3 PORT PORTA AUTH   State Change : Port=port1 New State=Unauthorised
25 12:13:15 6 SWIT PINT  UP     Port5: interface is UP
25 12:13:16 6 SWIT PINT  UP     Port24: interface is UP
25 12:13:36 3 PORT PORTA AUTH   Auth Success : Port=port1 User=bobxp
                                MAC=00-03-47-6b-93-fb
25 12:13:36 3 PORT PORTA AUTH   State Change : Port=port1 New State=Authorised
--------------------------------------------------------------------------
```

Use the **enable portauth debug port** command to debug the port authentication process.

```
Info (1118003): Operation successful.
Manager> EAPOL Auth Rx: ifIndex=1 src=00-03-47-6b-93-fb ver=1 type=EAP len=10
EAP Auth Rx: ifIndex=1 code=RESPONSE type=IDENTITY id=1 length=10
PORTAUTH : Int=port1 Authenticator Pae State Change
From : CONNECTING To : AUTHENTICATING
PORTAUTH : Int=port1 Backend Authentication State Change
From : IDLE To : RESPONSE
EAP Auth Tx: code=RESPONSE type=IDENTITY id=1 length=10
EAP Auth Rx: ifIndex=1 code=REQUEST type=MD5 id=2 length=22
PORTAUTH : Int=port1 Backend Authentication State Change
From : RESPONSE To : REQUEST
EAPOL Auth Tx: ifIndex=1 ver=1 type=EAP len=22
EAP Auth Tx: code=REQUEST type=MD5 id=2 length=22
EAPOL Auth Rx: ifIndex=1 src=00-03-47-6b-93-fb ver=1 type=EAP len=27
EAP Auth Rx: ifIndex=1 code=RESPONSE type=MD5 id=2 length=27
PORTAUTH : Int=port1 Backend Authentication State Change
From : REQUEST To : RESPONSE
EAP Auth Tx: code=RESPONSE type=MD5 id=2 length=27
EAP Auth Rx: ifIndex=1 code=SUCCESS id=3 length=4
PORTAUTH : Int=port1 Backend Authentication State Change
From : RESPONSE To : SUCCESS
EAPOL Auth Tx: ifIndex=1 ver=1 type=EAP len=4
EAP Auth Tx: code=SUCCESS id=3 length=4
PORTAUTH : Int=port1 Authenticator Pae State Change
From : AUTHENTICATING To : AUTHENTICATED
PORTAUTH : Int=port1 Backend Authentication State Change
From : SUCCESS To : IDLE
```

Authentication Server—Steel-Belted Radius server

- Check the communication between the Radius server and the authenticator device. For example, make sure that the devices can ping each other.

- Check to make sure that the authentication shared secret is the same on both the Radius server and authenticator device.

- Check to make sure that the appropriate EAP type has been configured properly on the eap.ini configuration file.

- Check to make sure that the user information such as username and password are correctly entered in the Radius server database.

Supplicant device—Windows XP Professional 802.1x Client

- Check to make sure that the IEEE 802.1x authentication functionality has been enabled on the Authentication tab via the Properties of the network connection.

- Check to make sure that the appropriate EAP type, for example MD5-Challenge, has been selected on the Authentication tab.

C613-16123-00 REV A

Connecting The (IP) World

Allied Telesis