Chapter 43

Port Authentication

Introduction

This chapter describes port authentication and its applications. The following mechanisms are supported:

■   IEEE Standard 802.1x authentication

■   MAC-based authentication

802.1x and MAC-based authentication may be enabled on the same router at the same time, however these two types of port authentication cannot be enabled on the same port at the same time.

Port authentication can be used to dynamically assign a port to a VLAN.

Dynamic VLAN assignment is only supported when using 802.1x authentication in single-supplicant mode.

802.1x ports can be configured with a limited access guest VLAN, which is used when no 802.1x supplicant is currently attached to the port.

802.1x Port Based Network Access Control

The IEEE Standard 802.1x provides a method of restricting access to networks based on authentication information. 802.1x provides port based network access control for devices connected to the Ethernet. This functionality allows a network controller to restrict external devices from gaining access to the network behind an 802.1x controlled port. External devices that wish to access services via a port under 802.1x control must firstly authenticate themselves and gain authorisation before any packets originating from, or destined for, the external device are allowed to pass through the 802.1x controlled port.

The 802.1x Implementation

802.1x port access control is achieved by making devices attached to a controlled port authenticate themselves via communication with an authentication server before these devices are allowed to access the network behind the controlled port.

Authentication is required on a per-port basis. The main components of an 802.1x implementation are:

■   the authenticator - the port that wishes to enforce authentication before allowing access to services that are accessible behind it.

■   the supplicant - the port that wishes to access services offered by the authenticator's system.

■   the authentication server - a device that uses the authentication credentials supplied by the supplicant, via the authenticator, to determine if the authenticator should grant access to its services.

The 802.1x configurations supported on each switch port and Eth port are:

■   supplicant

■   single-supplicant authenticator, where a single supplicant is directly
    connected to a single authenticator

■   authenticator. The VLAN ports each support a single supplicant, and the
    Eth ports each support up to 480 supplicants connected to the
    authenticating device. 802.1x port authentication is supported on all
    switch and Eth ports.

Configuration on a Single-Supplicant System

A single supplicant configuration giving true 802.1x functionality is shown in
. In this example, PC A wants to use services offered
by servers on the LAN behind the router acting as an authenticator. PC A is
connected to a port on the router that has 802.1x control enabled. Therefore, PC
A's own port acts in a supplicant role. Message exchanges take place between
the supplicant and the authenticator. The authenticator passes the supplicant's
credentials to the authentication server for verification, then the authentication
server informs the authenticator whether the attempt succeeded.
Consequently, PC A is either granted or denied access to the LAN behind the
router.

On a single supplicant system, the ability to allow or disallow the
piggybacking of network devices onto a device acting as a supplicant is
supported. The user can specify whether an authenticator with an attached
authenticated supplicant permits the passage of packets from any source or
only from the supplicant device itself.

On the AR415 and AR450S, piggybacking can be disabled on Ethernet ports
only.

Only one supplicant should be attached to the authenticator; adding more may
cause authentication problems.

Figure 43-1: Single supplicant 802.1x configuration
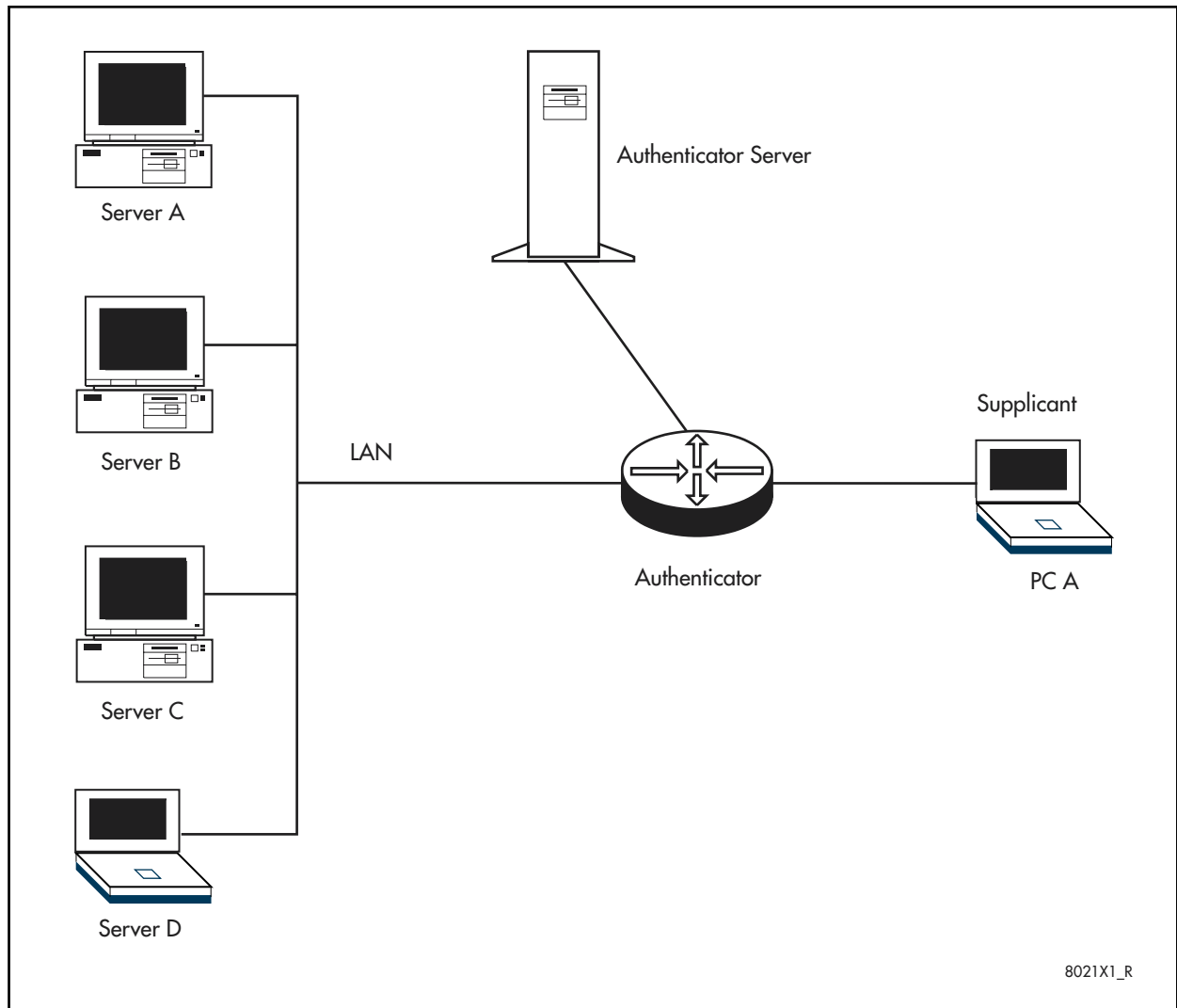
Configuration on a Multi-Supplicant System

A multi-supplicant configuration with 802.1x functionality is shown in Figure 43-2. In a multi-supplicant configuration, each supplicant is required to authenticate itself with the authenticator separately. Access to the port is granted only to supplicants that have successfully passed an authentication attempt.

Caution A multi-supplicant configuration is a departure from IEEE Standard 802.1x and introduces security risks. We recommend that 802.1x control not be used in a multi-supplicant configuration to minimise the risk of unauthorised access and denial-of-service attacks.

Figure 43-2: Multi-supplicant 802.1x configuration
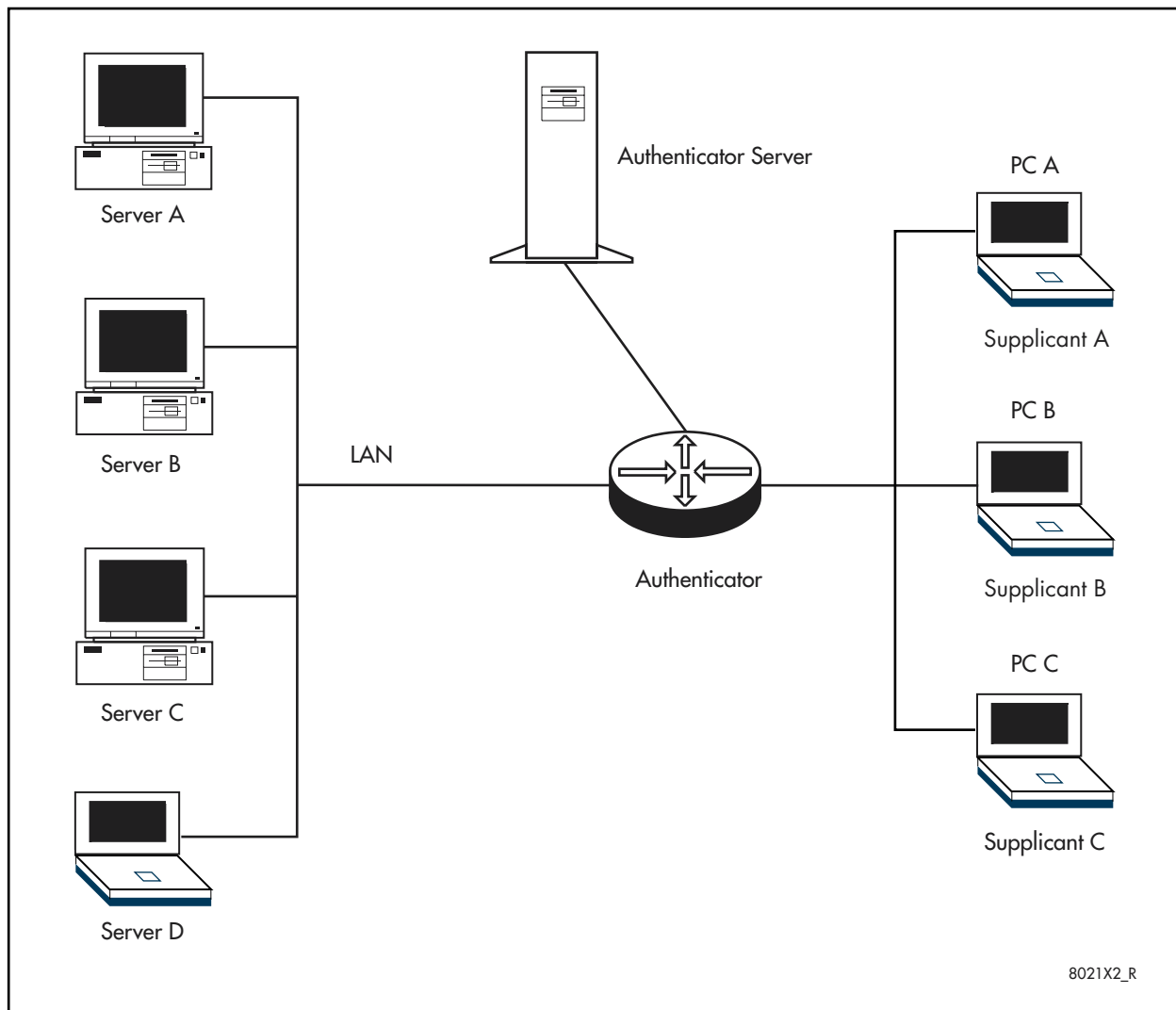
Supplicant and Authenticator Configuration

Routers acting as both supplicant and authenticator are shown in Figure 43-3. This configuration is typically seen in the backbone of a network where two routers are directly connected together. In this example, when traffic first attempts to cross from Router A to Router B, then Router B acts as an authenticator and Router A is the supplicant. When traffic first flows the other way, from Router B to Router A, then Router A acts as an authenticator and Router B is the supplicant.

Figure 43-3: Router as both supplicant and authenticator
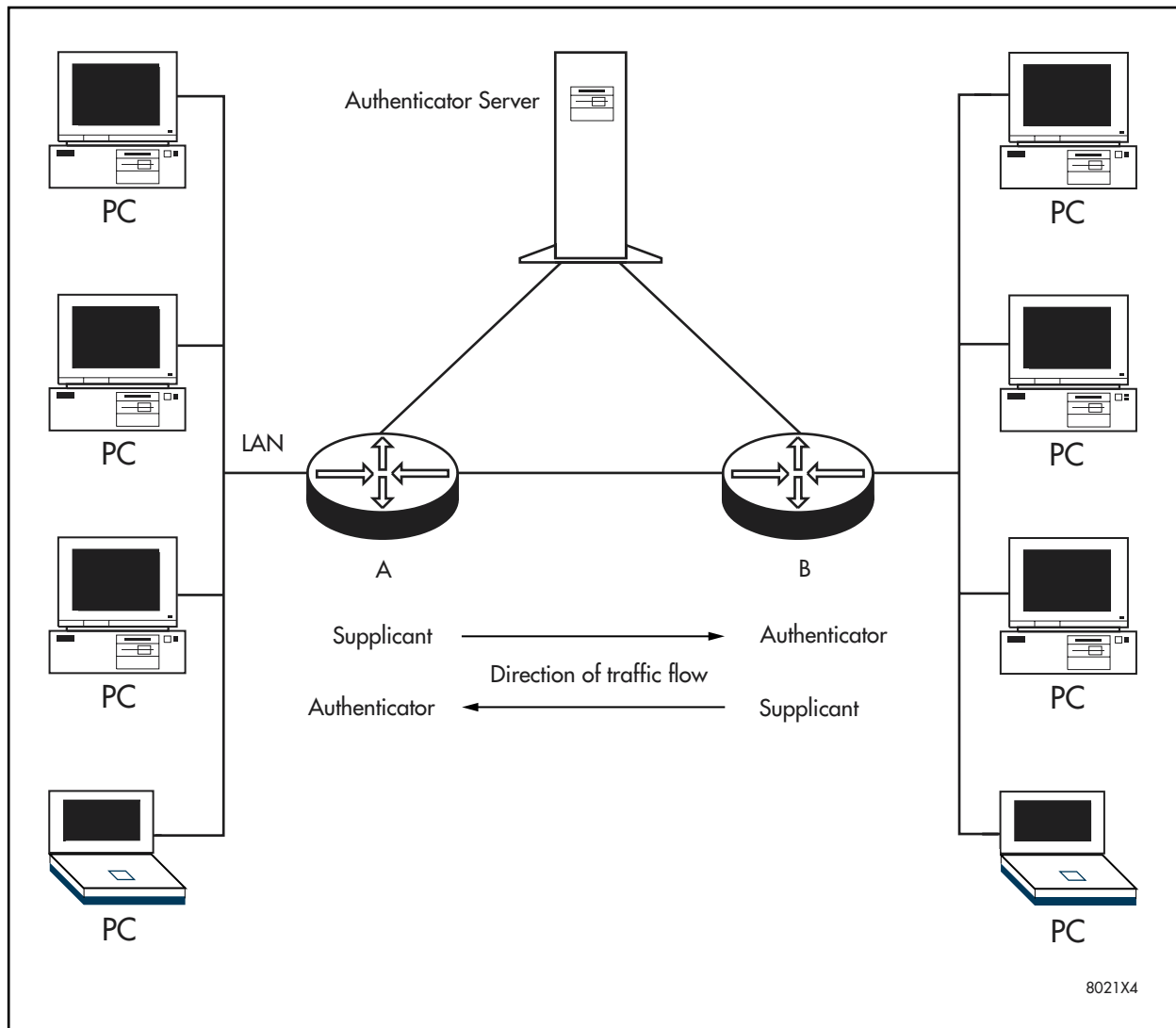
Port Authentication Control

A physical port under 802.1x control has associated with it a logical system known as a Port Access Entity (PAE). The PAE controls the authentication process. The authentication processes on the authenticator and on the supplicant are controlled by separate PAEs. The PAE controlling a port acting as a supplicant is called a Supplicant PAE. The PAE controlling a port acting as an authenticator is called an Authenticator PAE.

Ports under 802.1x control do not support static/dynamic learning and can be a member of only one VLAN.

The Authenticator PAE

The role of the Authenticator PAE is to maintain the state of the controlled port based on the result of authentication message exchanges with a single Supplicant PAE.

A single physical port acting as an authenticator is considered to consist of two separate logical ports – an uncontrolled port and a controlled port, as shown in . An uncontrolled port allows authentication (EAPOL) protocol data units (PDUs) to pass at any time. A controlled port allows PDUs to pass only when the Authenticator PAE is authorised.

The uncontrolled port is necessary to allow communication to take place between the supplicant and the authenticator during the authentication process. During the authentication process, the Extensible Authentication Protocol (EAP) is used for message exchange. Packets are physically transported between an Authenticator PAE and a Supplicant PAE using the EAP over LAN (EAPOL) encapsulation.

The EAP packets transmitted during the authentication process contain a PAE group MAC address that identifies that they are allowed to pass through the uncontrolled port. The MAC associated with a port can be disabled or enabled, either physically or administratively. If the MAC associated with a port is disabled, the port automatically transits to an unauthenticated state. No message exchanges can take place on either the controlled or the uncontrolled port.

The Authenticator PAE can be configured to request that the Supplicant PAE reauthenticate itself at a configurable time period. During the process of reauthentication, the controlled port remains authorised until reauthentication fails.

In a multi-supplicant configuration, an Authenticator PAE can authenticate several Supplicant PAEs individually. In such a configuration, an authenticator is considered to consist of a single uncontrolled port and several controlled ports, one for each supplicant that is attempting authentication. Some supplicants may be granted access to the port, while others may not. A maximum of 480 Supplicant PAEs may be attached to a single authenticating device.

In a multi-supplicant configuration, the Authenticator PAE conducts EAP communications with individual Supplicant PAEs based on the MAC address of each supplicant. Therefore, it is possible for unauthorised devices to disguise themselves as authorised supplicants using stolen MAC addresses.

Caution A multi-supplicant configuration is a departure from IEEE Standard 802.1x and introduces security risks.We recommend that 802.1x control not be used in a multi-supplicant configuration to minimise the risk of unauthorised access and denial-of-service attacks.

Figure 43-4: An authenticator PAE
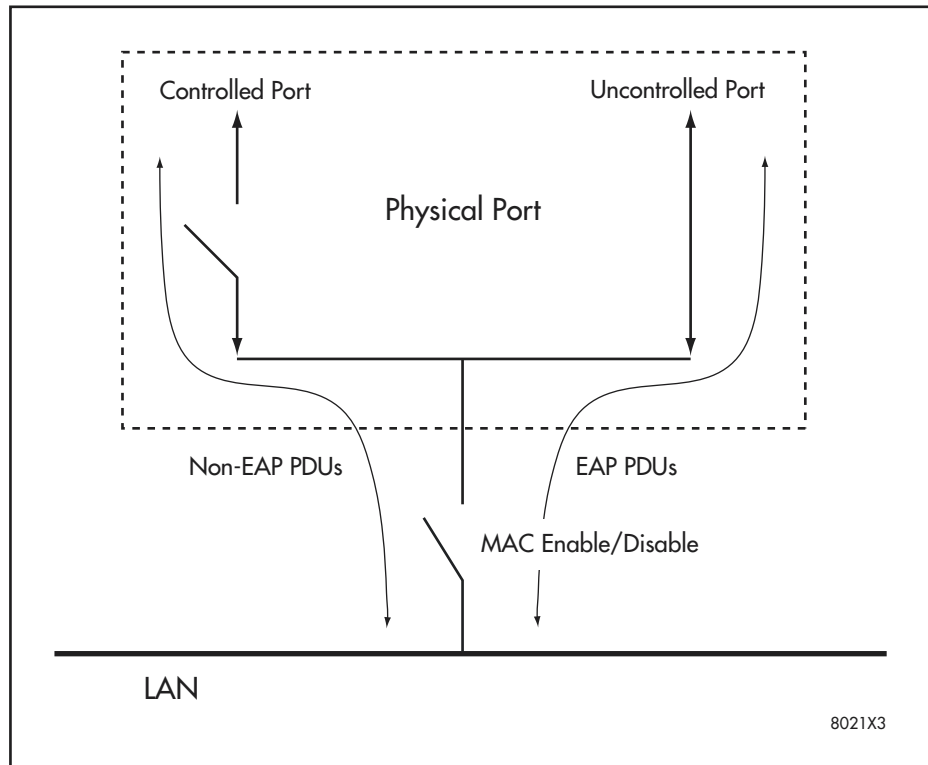
The Supplicant PAE

The role of the Supplicant PAE is to communicate the credentials of the supplicant to the Authenticator PAE when the Authenticator PAE requests them. The authentication message exchange between the Supplicant PAE and the Authenticator PAE can be initiated by the Supplicant PAE.

The Authentication Server

The authentication server verifies the supplicant's details, passed to it by the authenticator. This implementation of 802.1x control requires that a port acting as an authenticator must communicate with a RADIUS authentication server. The RADIUS server must be capable of receiving and deciphering EAP in RADIUS packets.

The authentication server must be connected to a port on the router which does not have port authentication enabled, or is set with **control=authorised**.

The supported supplicant encryption mechanisms for communication with the RADIUS server are EAP-MD5 and EAP-OTP. Encryption methods supported by authenticators are EAP-MD5, EAP-OTP, EAP-TLS, EAP-TTLS, and EAP-PEAP.

For more information about RADIUS, see "RADIUS" on page 41-15 of Chapter 41, User Authentication.

The Authentication Process

Until authentication is successful, the supplicant can only access the authenticator to perform authentication message exchanges, or access services not controlled by the authenticator's controlled port.

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.

1. Either the authenticator or the supplicant can initiate an authentication message exchange. The authenticator initiates the authentication message exchange by sending an EAPOL packet containing an encapsulated 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 EAPOL packet containing an encapsulated EAP-Request/Identity packet.

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

3. The authentication server selects an EAP authentication algorithm to verify the supplicant's identity, and sends an EAP-Request packet to the supplicant via the authenticator.

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

5. The authentication server either sends an EAP-Success packet or EAP-Reject packet to the supplicant via the authenticator. If VLAN assignment is enabled, then the authentication process is as described in "Single-supplicant mode" on page 43-12.

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. Also upon successful authorisation of the supplicant by the authenticator server, the supplicant is allowed full access to services offered via the controlled port. If piggybacking is enabled on the authorised authenticator port, any other device connected will also be give full access.

Note On the AR415S and AR450S, setting **piggyback** to **false** is only valid on Ethernet ports.

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 OTP authentication, is shown in Figure 43-5 on page 43-10.

Caution To minimise the risk of denial-of-service attacks by issuing EAPOL-Logoff messages to an Authenticator Port Access Entity (PAE) from a third party device, we recommend that 802.1x not be used in a shared media LAN.

Figure 43-5: Authentication Messaging Exchange Initiated by the Supplicant
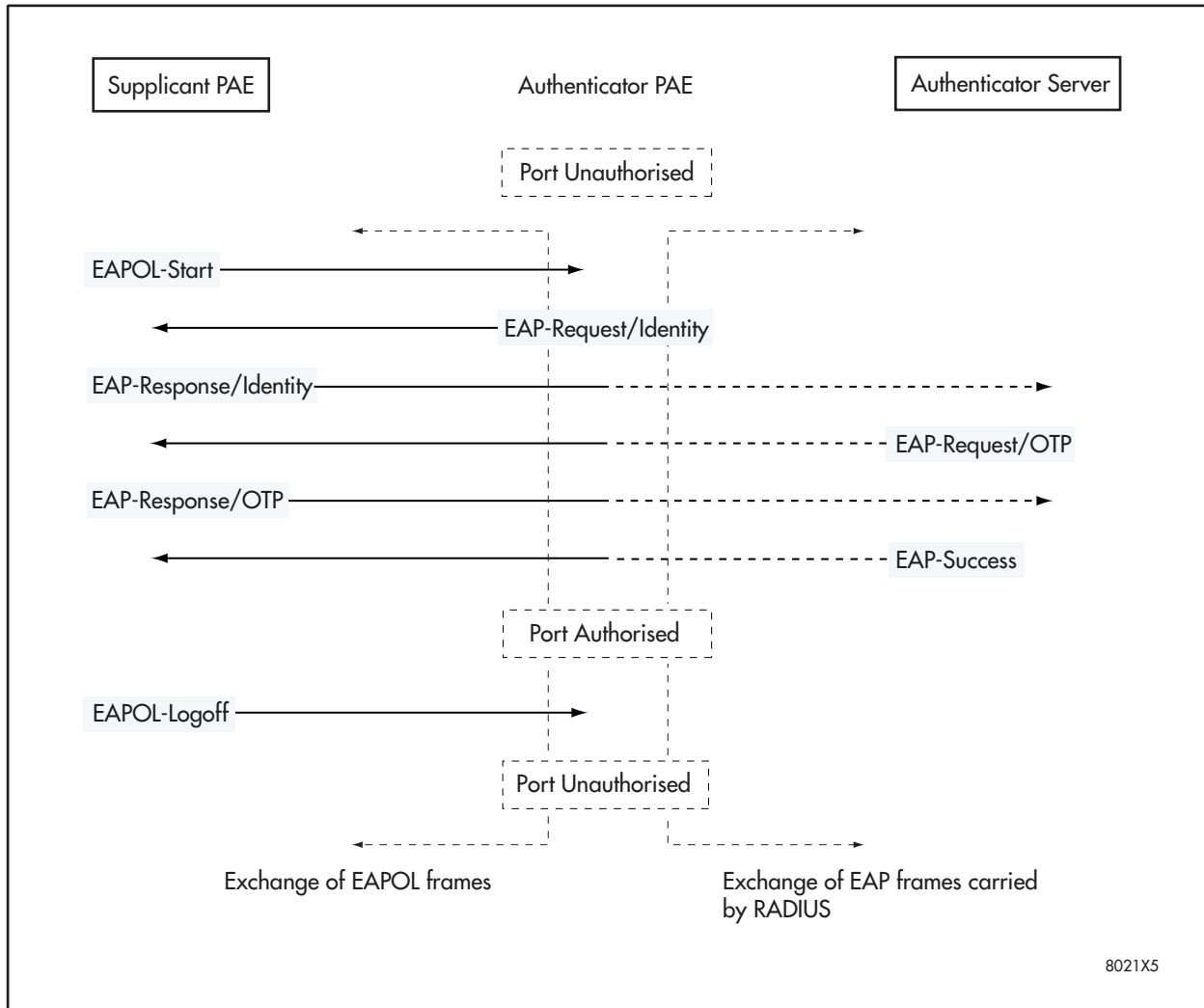
802.1x Guest VLAN

802.1x ports can be configured with a limited access guest VLAN, which is used when no 802.1x supplicant is currently attached to the port. This limited access VLAN is defined using the **guestvlan** parameter.

As soon as a single 802.1x packet is received on the port, the port is removed from the guest VLAN, and put into its configured access VLAN in the Unauthenticated state. This effectively disables the guest VLAN on the port until the port's link goes down.

A guest VLAN can only be configured for a port that is running in single-supplicant mode.

MAC-Based Authentication

MAC-based authentication is an alternative approach to 802.1x for authenticating supplicants connected to a port. It allows only clients with specified MAC addresses to access and pass data through a port. Clients with MAC addresses that are not in the list of allowed MAC addresses are denied access to the port (and any networks beyond).You can create a list of allowed MAC addresses in the RADIUS server used for MAC-based authentication.

MAC-based authentication allows non-802.1x capable clients such as network printers to be added securely.

The **portauth** parameter lets you configure either 802.1x or MAC-based authentication on a port. If no value is specified, 802.1x is used.

The MAC-Based Authentication Implementation

When authenticating based on the supplicant's source MAC address, the supplicant is not required to run a client for the 802.1x protocol. Port authentication is performed by the RADIUS server.

Authentication is required on a per-port basis. The main components of a MAC-based implementation are:

■   the authenticator - the port that enforces authentication before allowing access to services that are accessible behind it.

■   the supplicant - the port that accesses services offered by the authenticator's system.

■   the RADIUS authentication server - a device that authenticates based on the MAC address of the supplicant.

The MAC-Based Authentication Process

Authentication is required on a MAC-based authentication enabled port when it receives a packet that has an unknown source MAC address

1.   An Access-Request is sent to a RADIUS server with the source MAC address as the username and password

2.   If authentication is successful, the RADIUS server returns an Access-Accept packet with RADIUS tunnel attributes.

3.   If authentication fails, the RADIUS server returns an Access-Reject packet, and the supplicant is denied access.

After a port has been enabled for MAC-based authentication, and prior to any supplicants being authenticated, the port belongs to the configured access VLAN. This is the VLAN specified for the port in the **add vlan** command. It may be moved to another VLAN if dynamic VLAN assignment is enabled. See"Dynamic VLAN Assignment" on page 43-12.

If MAC-based authentication is disabled on a port, or all MAC-based authentication on the port expires, it returns to the configured access VLAN.

Dynamic VLAN Assignment

Dynamic VLAN assignment allows a supplicant to be placed into a specific VLAN based on information returned from the RADIUS server during authentication. This limits the network access of a supplicant to a specific VLAN that is tied to their authentication, and prevents supplicants from connecting to VLANs for which they are not authorised. A port's VLAN assignment is determined by the first supplicant to be authenticated on the port.

Dynamic VLAN assignment is only supported when using 802.1x authentication in single-supplicant mode.

VLAN assignment is enabled or disabled using the **vlanassignment** parameter of port authentication commands.

The Configured and Actual fields of the **show vlan** command show which ports are configured for the VLAN and which have been dynamically assigned to the VLAN.

RADIUS attributes   The RADIUS server provides information to the authenticator using RADIUS tunnel attributes, as defined in RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*. The tunnel attributes that must be configured for VLAN assignment are:

■   **Tunnel-Type**
    The protocol to be used for the tunnel specified by Tunnel-Private-Group-Id. VLAN (13) is the only supported value.

■   **Tunnel-Medium-Type**
    The transport medium to be used for the tunnel specified by Tunnel-Private-Group-Id. 802 (6) is the only supported value.

■   **Tunnel-Private-Group-ID**
    The ID of the tunnel the authenticated user should use. This must be the name or ID number of a VLAN on the router.

These tunnel attributes are included in the Access-Accept message from the RADIUS server to the Authenticator.

Single-supplicant   VLAN assignment can be run in single-supplicant mode for 802.1x
mode   authentication. In single supplicant mode, VLAN assignment is as follows:

■   If authentication fails, the supplicant is denied access to the port. The port is placed in its configured access VLAN, that is, the VLAN it was set up for in the **add vlan** command.

■   If the RADIUS server supplies valid VLAN information, the port is placed in the specified VLAN after configuration.

■   If the RADIUS server supplies invalid VLAN information, the port is returned to the Unauthorised state, and placed in its configured access VLAN.

■   If the RADIUS server supplies no VLAN information, the port is placed in its configured access VLAN after successful authentication.

■   When port authentication is disabled on the port, the port is returned to its configured access VLAN.

■   When the port is in the Force Authorized, Force Unauthorized or the Unauthorized state, it is placed in its configured access VLAN.

While the port is in a RADIUS server assigned VLAN, changes to the port's configured access VLAN do not take effect until the port leaves the assigned VLAN. This can occur if:

■ the last authentication session on the port expires

■ the link goes down

■ port authentication is disabled on the port

■ port authentication is disabled on the system

RADIUS accounting RADIUS accounting is included for:

■ MAC-based port authentication

■ 802.1x port authentication in single-supplicant mode.

When a supplicant has been authenticated for a port, a START Accounting-Request message is sent to the RADIUS server.

When a supplicant becomes unauthenticated, a STOP Accounting-Request message is sent to the RADIUS server.

If no Accounting-Response is received from the RADIUS server after either a START or STOP Accounting message is sent, (and once the RADIUS module has reached its timeout and retry limit), the authorisation status of the supplicant remains unaffected, but an appropriate message is logged.

This allows the RADIUS server to track the time for which a user is logged in and authenticated, and to limit the number of ports on which a user can be authenticated at any one time. This provides greater security.

Port Authentication on the Router

This section describes how the router implements port authentication port control, and how to configure the router.

Enable Port Authentication on the Router

The implementation of 802.1x or MAC-based authentication on the router is disabled by default.

To enable 802.1x or MAC-based authentication, use the command:

```
enable portauth={8021x|macbased}
```

To disable 802.1x or MAC-based authentication, use the command:

```
disable portauth={8021x|macbased}
```

Enable Port Authentication on a Port

To enable a specific port to act as an 802.1x authenticator, use the command:

```
enable portauth=8021x port={all|port-name} type=authenticator
    [other-options...]
```

To enable a specific port to act as a MAC-based authenticator, use the command:

```
enable portauth=macbased port={all|port-name}
    [other-options...]
```

802.1x port authentication is supported on all switch and Eth ports.

When a router acts as an authenticator and port authentication is enabled on all ports, the router does not perform port authentication. This is because the router has no way of passing authentication requests from supplicants to the authentication server. Therefore, the authentication server must be connected to a port on the router which does not have port authentication enabled, or is set with **control=authorised**.

To enable the specified 802.1x port(s) to act as a supplicant, use the command:

```
enable portauth=8021x port={all|port-name} type=supplicant
    [other-options...]
```

To enable the specified 802.1x port(s) to act as both an authenticator and a supplicant, use the command:

```
enable portauth=8021x port={all|port-name} type=both
    [other-options...]
```

To enable the specified 802.1x port(s) to act as an authenticator, connected to either a single supplicant or multiple supplicants, use the command:

```
enable portauth=8021x port={all|port-name} type=authenticator
    [mode={multi|single}] [other-options...]
```

On the AR415S and AR450S, **multi** can be specified for Ethernet ports only.

Caution Setting the **mode** parameter to **multi** is a departure from IEEE Standard 802.1x and introduces security risks. We recommend that 802.1x control not be used in a multi-supplicant configuration to minimise the risk of unauthorised access and denial-of-service attacks.

To enable the piggybacking of network devices onto an authenticated supplicant, use the command:

```
enable portauth=8021x port={all|port-name} type=authenticator
    [mode=single] [piggyback={true|false}] [other-options...]
```

If **true** is specified, piggybacking is enabled and packets from any source are allowed to pass through the port once a supplicant has been authorised. If **false** is specified, piggybacking is disabled and packets from any source other than the authenticated supplicant are blocked. The default is **true**. On the AR415S and AR450S, piggybacking can only be disabled on Ethernet ports.

To change the configuration parameters for a port or ports under port authentication port control, use the commands:

```
set portauth={8021x|macbased} port={all|port-name}
    type=authenticator [other-options...]

set portauth=macbased port={all|port-name}
    [other-options...]

set portauth=8021x port={all|port-name} type=supplicant
    [other-options...]

set portauth=8021x port={all|port-name} type=both
    [other-options...]
```

To disable port authentication port control on a specified port(s), use the command:

```
disable portauth={8021x|macbased} [port={all|port-name}]
```

To reinitialise port authentication port control on a specified port(s), use the command:

```
reset portauth={8021x|macbased} port={all|port-name}
    [other-options...]
```

To purge all port authentication port configurations for a specified port(s), use the command:

```
purge portauth={8021x|macbased} port={all|portname}
```

To display information about each port's capabilities and protocol implementation detail, use the command:

```
show portauth={8021x|macbased}
```

To display counter information for ports on the router that have port authentication enabled, use the command:

```
show portauth=8021x counter port={all|port-name}
```

To display the current configuration for ports on the router that have port authentication enabled, use the command:

```
show portauth={8021x|macbased} port={all|port-name}
```

To display the amount of time remaining in seconds until the timeout is due for each timer associated with the specified port or ports, use the command:

```
show portauth={8021x|macbased} timer port={all|port-name}
```

Reauthenticate Supplicants

To force any supplicant currently authorised on a port acting as an authenticator to immediately reauthenticate itself, use the command:

```
activate portauth={8021x|macbased} port={all|port-name}
    reauthenticate [other-options...]
```

To specify that for a port(s) enabled as an authenticator any supplicants authorised for this port are periodically reauthenticated at a user-configurable period, use the commands:

```
enable portauth=8021x port={all|port-name} type=authenticator
    [reauthenabled={true|false}] [reauthperiod=1..86400]
    [other-options...]

enable portauth=macbased port={all|port-name}
    [reauthenabled={true|false}] [reauthperiod=1..86400]
    [other-options...]

enable portauth=8021x port={all|port-name} type=BOTH
    [reauthenabled={true|false}] [reauthperiod=1..86400]
    [other-options...]

set portauth=8021x port={all|port-name} type=authenticator
    [reauthenabled={true|false}] [reauthperiod=1..86400]
    [other-options...]

set portauth=macbased port={all|port-name}
    [reauthenabled={true|false}] [reauthperiod=1..86400]
    [other-options...]

set portauth=8021x port={all|port-name} type=both
    [reauthenabled={true|false}] [reauthperiod=1..86400]
    [other-options...]
```

If the **reauthenabled** parameter specifies **true**, then the authenticator requires the supplicant to undergo periodic reauthentication. The default **reauthenabled** value is **false**. The **reauthperiod** parameter specifies the time in seconds between reauthentications of the supplicant. The system uses the **reauthperiod** parameter when the **reauthenabled** parameter is **true**.

Setting Global 802.1x Username and Password

To configure a global username and global password for all Supplicant Port Access Entities (PAEs) to use during authentication, use the command:

```
set portauth=8021x username=login-name password=password
    [method={otp[encryption={md4|md5}]|standard}]
```

The default method is **standard**. The global settings may be overridden using the **set portauth port** command to set specific supplicant passwords and usernames.

Enter passwords in a secure environment because they appear on the screen as typed. We recommend also keeping configuration file backups secure because passwords are in plaintext in configuration files.

Debug Port Authentication

To enable port authentication debugging on a port or ports, use the command:

```
enable portauth=8021x debug={all|packet|state} port={all|
    port-name}

enable portauth=macbased debug={all|state} port={all|
    port-name}
```

To disable port authentication debugging on a port or ports, use the command:

```
disable portauth=8021x debug={all|packet|state} port={all|
    port-name}

disable portauth=macbased debug={all|state} port={all|
    port-name}
```

Multi-Supplicant Configuration

In a multi-supplicant configuration, a single authenticator is connected to more than one supplicant. Each supplicant is required to authenticate themselves with the authenticator separately. Multi-supplicant configuration is supported on Ethernet ports only.

Broadcast and multicast packets are transmitted to all stations connected to the multi-supplicant authenticator port, independent of authentication state.

Caution A multi-supplicant configuration is a departure from IEEE Standard 802.1x and introduces security risks. We recommend that 802.1x control not be used in a multi-supplicant configuration to minimise the risk of unauthorised access and denial-of-service attacks.

To enable and set the specified port(s) to act as an authenticator connected to multiple supplicants, use the commands:

```
enable portauth=8021x port={all|port-name} type=authenticator
    [mode=multi] [other-options...]

set portauth=8021x port={all|port-name} type=authenticator
    [mode=multi] [other-options...]
```

For MAC-based authentication, the only possible mode is multi-supplicant. To enable and set the specified port to act as an authenticator connected to multiple supplicants, use the command:

```
enable portauth=mac port={all|port-name}
```

The Authenticator PAE configuration for specified port(s) can be overridden for a specific supplicant. To override the Authenticator PAE configuration for a specific supplicant, use one of the commands:

```
set portauth[=8021x] port={all|port-name}
    supplicantmac=macadd [control={authorised|unauthorised|
    auto}] [maxreq=1..10] [quietperiod=0..65535]
    [reauthenabled={true|false}] [reauthmax=1..10]
    [reauthperiod=1..86400] [servertimeout=1..60]
    [supptimeout=1..60] [txperiod=1..65535]
    [vlanassignment={enabled|disabled}] [trap={success|
    failure|both|none}][default]
```

```
set portauth=macbased port={all|eth-port}
    [control={authorised|unauthorised|auto}]
    [reauthenabled={true|false}] [reauthperiod=1..86400]
    [quietperiod=0..65535] [vlanassignment={enabled|
    disabled}] [mibreset={enabled|disabled}] [trap={success|
    failure|both|none}]
```

Any supplicant that attaches to an Authenticator PAE configured for multi-supplicant support uses the parameters set by either the **set portauth port type=authenticator** command or **set portauth port type=both** command, unless the MAC address of the supplicant matches the **supplicantmac** parameter of a previously entered **set portauth port supplicantmac** command. At least one non-standard parameter value must be entered in the command. The **default** parameter removes the overridden settings for the specified supplicant MAC address.

To remove any multi-supplicant MIB instances relating to supplicants that are not currently authenticated by the specified ports, and that have not been specifically configured using the **set portauth port supplicantmac** command, use the command:

```
reset portauth={8021x|macbased} multimib port={all|port-name}
```

To specify for a port(s) enabled as an authenticator connected to multiple supplicants that any supplicants are to be immediately reauthenticated, use the command:

```
activate portauth={8021x|macbased} port={all|port-name}
    reauthenticate [supplicantmac=macadd]
```

To specify that for a port(s) enabled as an authenticator any supplicants authorised for this port are periodically reauthenticated at a user configurable period, use the commands:

```
enable portauth=8021x port={all|port-name} type=authenticator
    [mode=multi] [reauthenabled={true|false}]
    [reauthperiod=1..86400] [other-options...]

enable portauth=macbased port={all|port-name}
    [reauthenabled={true|false}] [reauthperiod=1..86400]
    [other-options...]

set portauth=8021x port={all|port-name} type=authenticator
    [mode=multi] [reauthenabled={true|false}]
    [reauthperiod=1..86400] [other-options...]

set portauth=macbased port={all|port-name}
    [reauthenabled={true|false}] [reauthperiod=1..86400]
    [other-options...]
```

If the **reauthenabled** parameter specifies **true**, then the authenticator requires the supplicant to undergo periodic reauthentication. The default **reauthenabled** value is **false**. The **reauthperiod** parameter specifies the time in seconds between reauthentications of the supplicant. The **reauthperiod** parameter is used when the **reauthenabled** parameter is **true**.

To reinitialise port authentication port control on a specified port(s) connected to multiple supplicants, use the command:

```
reset portauth={8021x|macbased} port={all|port-name}
    [supplicantmac={macadd}]
```

To display the configuration information about each supplicant connected to, or configured on, the specified port configured as a multi-supplicant authenticator, use the command:

```
show portauth={8021x|macbased} multisupplicant port={all|
    port-name}
```

Configuration Examples

Examples in this section show the following configurations:

■ **Port as Authenticator**

■ **Port as Supplicant**

Port as Authenticator

1. **Enable the IP module, add an IP interface, and add an IP route.**

   Enable IP by using the command:

   ```
   enable ip
   ```

   Add an IP interface by using the command:

   ```
   add ip interface=interface ipaddress=ipadd
       [other-options...]
   ```

   Add an IP route by using the command:

   ```
   add ip route=ipadd interface=interface nexthop=ipadd
       [mask=ipadd] [other-options...]
   ```

   where *interface* is an interface name formed by concatenating a Layer 2 interface type, an interface instance, and optionally a hyphen followed by a logical interface number from 0 to 15, and *ipadd* is an IP address in dotted decimal notation.

   For more information about configuring IP, see Chapter 22, Internet Protocol (IP).

2. **Add a RADIUS server.**

   Add a RADIUS server to process authentication requests from the supplicant sent via the port configured as an authenticator by using the command:

   ```
   add radius server=ipadd secret=secret port=port-number a
       cc port=port-number
   ```

   For more information about configuring a RADIUS server see **add radius server** command on page 41-30 of Chapter 41, User Authentication.

3. **Enable port authentication port control on the router.**

   Enable port authentication by using the command:

   ```
   enable portauth={8021x|macbased}
   ```

4. **Enable port authentication port control on a port.**

   Enable port authentication on the port you want to configure as an authenticator by using the command:

   ```
   enable portauth=8021x port=port-name type=authenticator
       [other-options...]
   ```

   ```
   enable portauth=macbased port=port-name
       [other-options...]
   ```

5. **Show the port authentication port control configuration for the port.**

   Show the port authentication port control configuration for the port by using the command:

   ```
   show portauth={8021x|macbased} port=port-name
   ```

Port as Supplicant

This example demonstrates how to configure a port on the router as a
supplicant using EAP-MD5 Authentication to communicate with the
authentication server.

1. **Enable the IP module, add an IP interface, and add an IP route.**

    Enable IP by using the command:

    ```
    enable ip
    ```

    Add an IP interface by using the command:

    ```
    add ip interface=interface ipaddress=ipadd
        [other-options...]
    ```

    Add an IP route by using the command:

    ```
    add ip route=ipadd interface=interface nexthop=ipadd
        [mask=ipadd] [other-options...]
    ```

    where *interface* is an interface name formed by concatenating a Layer 2
    interface type, an interface instance, and optionally a hyphen followed by a
    logical interface number from 0 to 15, and *ipadd* is an IP address in dotted
    decimal notation.

    For more information about configuring IP, see Chapter 22, Internet
    Protocol (IP).

2. **Enable port authentication port control on the router.**

    Enable port authentication by using the command:

    ```
    enable portauth=8021x
    ```

3. **Set the username and password that the supplicant should use during
    authentication.**

    Either set a global username and global password for all Supplicant Port
    Access Entities (PAEs) to use during authentication by using the command

    ```
    set portauth=8021x username=login-name password=password
        [method=standard]
    ```

    Alternatively, set a specific username and password for the port by using
    the **enable portauth port** command in the next step.

    Enter passwords in a secure environment because they appear on the
    screen as typed. Also, secure configuration file backups because passwords
    are in plaintext in configuration files.

4. **Enable port authentication port control on a port.**

    Enable port authentication on the port you want to configure as an
    supplicant by using the command:

    ```
    enable portauth=8021x port={all|port-name} type=supplicant
        [username=login-name password=password
        [method=standard]] [other-options...]
    ```

5. **Show the port authentication port control configuration for the port.**

    Show the port authentication port control configuration for the port by
    using the command:

    ```
    show portauth=8021x port=port-name
    ```

Command Reference

This section describes the commands available on the router to configure and manage port authentication.

The shortest valid command is denoted by capital letters in the Syntax section. See "Conventions" on page lxv of About this Software Reference in the front of this manual for details of the conventions used to describe command syntax. See Appendix A, Messages for a complete list of error messages and their meanings.

802.1x port authentication is supported on all switch and Eth ports.

activate portauth port reauthenticate

Syntax   ACTivate PORTAuth[={8021x|MACbased}] POrt={ALL|*port-name*}
          REAUTHENTicate [SUPPLicantmac=*macadd*]

where:

- *port-name* is an Ethernet interface (eth0 or eth1), a port number, a range of port numbers (specified as n-m), or a comma-separated list of port numbers and/or ranges. Port numbers start at n and end at m, where n is the lower value port number and m the upper value port number, including uplink ports.

- *macadd* is an Ethernet six-octet MAC address, expressed as six pairs of hexadecimal digits delimited by hyphens.

Description   This command causes the authenticator to reauthenticate supplicants authorised for the port using 802.1x or MAC-Based Authentication.

The **portauth** parameter specifies the type of port authentication to perform. The default is 802.1x.

The **port** parameter specifies the port where reauthentication is to occur. If **all** is specified, reauthentication occurs on all ports enabled as 802.1x Authenticator Port Access Entities (PAEs) or all ports enabled as MAC-based authentication PAEs, depending on the value of the **portauth** parameter.

The **reauthenticate** parameter specifies that the connected supplicant must reauthenticate itself.

The **supplicantmac** parameter specifies the hardware address of the connected supplicant to reauthenticate, in standard MAC format, for example 11-22-33-44-55-66. The **supplicantmac** parameter is valid for ports configured as authenticators on a multi-supplicant system.

Examples   To reauthenticate 8021.x supplicants connected to port 1, use the command:

```
act porta=8021x po=1 reauthent
```

To reauthenticate MAC-based supplicants connected to port 1, use the command:

```
act porta=macbased po=1 reauthent
```

To reauthenticate 802.1x supplicants connected to Eth 1, use the command:

```
act porta=8021x po=eth1 reauthent
```

To reauthenticate MAC-based supplicants connected to Eth 1, use the command:

```
act porta=mac po=eth1 reauthent
```

Related Commands   disable portauth debug
enable portauth
enable portauth port
set portauth port
set portauth port supplicantmac
show portauth timer
show portauth port
show portauth port multisupplicant

disable portauth

Syntax   DISable PORTAuth[={8021x|MACbased}]

Description   This command disables port authentication functionality on the router. To disable port authentication functionality on a per-port basis use the **disable portauth port** command.

The **portauth** parameter specifies the type of port authentication to disable. The default is 802.1x.

Examples   To disable 802.1x authentication on the router, use the command:

```
dis porta=8021x
```

To disable MAC-based authentication on the router, use the command:

```
dis porta=mac
```

Related Commands   disable portauth port
enable portauth
enable portauth port
purge portauth port
show portauth port

disable portauth debug

Syntax   `DISable PORTAuth[={8021x|MACbased}] DEBug={ALL|PAcket|`
              `STate} POrt={ALL|port-name}`

where *port-name* is an Ethernet interface (eth0 or eth1), a port number, a range of port numbers (specified as n-m), or a comma-separated list of port numbers and/or ranges. Port numbers start at n and end at m, where n is the lower value port number and m the upper value port number, including uplink ports.

Description   This command disables port authentication debugging on the specified ports.

The **portauth** parameter specifies the type of port authentication port for which debugging is disabled. The default is 802.1x.

The **debug** parameter specifies the type of port authentication debugging to disable. If **state** is specified, the debugging of state changes in the state machines for the specified port(s) and port authentication type is disabled. If **packet** is specified, the debugging of 802.1x EAP packet headers transmitted or received by a specific port is disabled. Packet mode debugging is only valid for 802.1x authentication. If **all** is specified, all debugging for the specified port(s) and authentication type is disabled.

The **port** parameter specifies the port for which debugging is disabled. If **all** is specified, debugging is disabled for all ports.

Examples   To disable debugging of the 802.1x port authentication state machine for port 1, use the command:

        `dis porta=8021x de=st port=1`

To disable debugging of the MAC-based port authentication state machine for port 1, use the command:

        `dis porta=mac de=st port=1`

To disable debugging of the 802.1x port authentication state machine for Eth 1, use the command:

        `dis porta=8021x deb=st po=eth1`

To disable debugging of the MAC-based port authentication state machine for Eth 1, use the command:

        `dis porta=mac deb=st po=eth1`

Related Commands   **enable portauth**
                        enable portauth debug
                        enable portauth port
                        set portauth port
                        show portauth port

disable portauth port

Syntax   `DISable PORTAuth[={8021x|MACbased}] [POrt={ALL|port-name}]`

where *port-name* is an Ethernet interface (eth0 or eth1), a port number, a range of port numbers (specified as n-m), or a comma-separated list of port numbers and/or ranges. Port numbers start at n and end at m, where n is the lower value port number and m the upper value port number, including uplink ports.

Description   This command disables port authentication functionality on the specified port or ports. To disable port authentication functionality on the entire router, use the **disable portauth** command.

The **portauth** parameter specifies the type of port authentication to disable. The default is 802.1x.

The **port** parameter specifies the port(s) on which port authentication is disabled. If **all** is specified, port authentication is disabled on all ports enabled as either 802.1x authenticator Port Access Entities (PAEs), or MAC-based authenticator PAEs, depending on the value of the **portauth** parameter.

Examples   To disable 8021.x port authentication on port 1, use the command:

    dis porta=8021x po=1

To disable MAC-based port authentication on port 1, use the command:

    dis porta=mac po=1

To disable 802.1x port authentication on Eth 1, use the command:

    dis porta=8021x po=eth1

To disable MAC-based port authentication on Eth 1, use the command:

    dis porta=mac po=eth1

Related Commands   **disable portauth**
enable portauth
enable portauth port
reset portauth port multimib
set portauth port
set portauth port supplicantmac
show portauth port

enable portauth

Syntax	ENAble PORTAuth[={8021x|MACbased}]
Description	This command enables port authentication functionality on the router. To configure individual ports as authenticators and/or supplicants use the **enable portauth port** command.
	The **portauth** parameter specifies the type of port authentication to enable. The default is 802.1x.
Examples	To enable 802.1x port authentication on the router, use the command:

```
ena porta=8021x
```

To enable MAC-based port authentication on the router, use the command:

```
ena porta=mac
```

Related Commands activate portauth port reauthenticate
disable portauth
disable portauth port
enable portauth port
purge portauth port
reset portauth port
reset portauth port multimib
set portauth port
show portauth
show portauth port

enable portauth debug

Syntax   ENAble PORTAuth[={8021x|MACbased}] DEBug={ALL|PAcket|
             STate} POrt={ALL|*port-name*}

where *port-name* is an Ethernet interface (eth0 or eth1), a port number, a range of port numbers (specified as n-m), or a comma-separated list of port numbers and/or ranges. Port numbers start at n and end at m, where n is the lower value port number and m the upper value port number, including uplink ports.

Description   This command enables port authentication debugging on the specified port.

The **portauth** parameter specifies the type of port authentication port for which debugging is enabled. The default is 802.1x.

The **debug** parameter specifies the type of port authentication debugging to enable. If **all** is specified all debugging for the specified port(s) and authentication type is enabled. If **packet** is specified, all 802.1x related EAP and EAPOL packet headers are echoed to the router console as they are received or transmitted by the specified port. The packet contents are not displayed as they may contain sensitive username and/or password information. Packet mode debugging is only valid for 802.1x authentication. If **state** is specified, all state machine changes for the specified port(s) and port authentication type are echoed to the console.

The **port** parameter specifies the port for which debugging is enabled. If **all** is specified, debugging is enabled for all ports.

Examples   To show debug state information for MAC-based authentication on port 1, use the command:

    ena porta=mac deb=st po=1

To show debug state information for MAC-based authentication on Eth 0, use the command:

    ena porta=mac deb=st po=eth1

Related Commands   disable portauth debug
enable portauth
enable portauth port
reset portauth port
set portauth port
show portauth counter
show portauth port

enable portauth port

Syntax
```
ENAble PORTAuth[=8021x] POrt={ALL|eth-port|switch-port}
    TYpe=AUthenticator [CONTrol={AUTHorised|AUTO|
    UNauthorised}] [MAXReq=1..10] [MODe={MUlti|SIngle}]
    [PIGgyback={TRue|FAlse}] [QUIETperiod=0..65535]
    [REAUTHENAbled={TRue|FAlse}] [REAUTHMax=1..10]
    [REAUTHPeriod=1..86400] [SERVERTimeout=1..60]
    [SUPPTimeout=1..60] [TXperiod=1..65535]
    [GUEstvlan={1..4094|vlan-name|NONe}]
    [VLANAssignment={ENAbled|DIsabled}] [MIBReset={ENAbled|
    DIsabled}] [TRap={SUCcess|FAILure|BOTh|NONe}]

ENAble PORTAuth[=8021x] POrt={ALL|eth-port|switch-port}
    TYpe=BOth [AUTHPeriod=1..60] [CONTrol={AUTHorised|
    UNauthorised|AUTO}] [HELDPeriod=0..65535]
    [MAXReq=1..10] [MAXStart=1..10] [MODe={MUlti|SIngle}]
    [PIGgyback={TRue|FAlse}] [QUIETperiod=0..65535]
    [REAUTHENAbled={TRue|FAlse}] [REAUTHMax=1..10]
    [REAUTHPeriod=1..86400] [SERVERTimeout=1..60]
    [STARTperiod=1..60] [SUPPTimeout=1..60]
    [TXperiod=1..65535] [USERName=login-name
    PASSword=password [METhod={OTP[ENCryption={MD4|MD5}]|
    STandard}] [GUEstvlan={1..4094|vlan-name|NONe}]
    [VLANAssignment={ENAbled|DIsabled}] [MIBReset={ENAbled|
    DIsabled}] [TRap={SUCcess|FAILure|BOTh|NONe}]

ENAble PORTAuth[=8021x] POrt={ALL|eth-port|switch-port}
    TYpe=SUpplicant [AUTHPeriod=1..60]
    [HELDPeriod=0..65535] [MAXStart=1..10]
    [STARTperiod=1..60] [USERName=login-name
    PASSword=password [METhod={OTP[ENCryption={MD4|MD5}]|
    STandard}]]

ENAble PORTAuth=MACbased POrt={ALL|eth-port}
    [CONTrol={AUTHorised|UNauthorised|AUTO}]
    [REAUTHENAbled={TRue|FAlse}] [REAUTHPeriod=1..86400]
    [QUIETperiod=0..65535] [VLANAssignment={ENAbled|
    DIsabled}] [MIBReset={ENAbled|DIsabled}]
    [TRap={SUCcess|FAILure|BOTh|NONe}]
```

where:

■ *eth-port* is an Ethernet interface (for example, eth0 or eth1).

■ *switch-port* is a port number, a range of port numbers (specified as n-m), or a comma-separated list of port numbers and/or ranges. Port numbers start at n and end at m, where n is the lower value port number and m the upper value port number, including uplink ports.

■ *vlan-name* is a unique name for the VLAN, 1 to 32 characters in length. Valid characters are uppercase and lowercase letters, digits, the underscore character, and the hyphen character. The VLAN name cannot be a number or **all**.

■ *login-name* is a character string 1 to 64 characters long. Valid characters are uppercase and lowercase letters, and digits (0-9).

■ *password* is an character string. Valid characters are uppercase and lowercase letters, and digits (0–9).

Description   This command enables port authentication on the specified ports. The type of authentication to enable can be 802.1x or MAC-based authentication. For 802.1x, a port can be enabled as an authenticator, supplicant, or both.

Ports under port authentication control do not support static/dynamic learning and can be a member of only one VLAN.

The **portauth** parameter specifies the type of port authentication to enable. The default is 802.1x.

The **port** parameter specifies the port to enable with port authentication. If **all** is specified, all ports on the router that support the type of port authentication specified by the **portauth** parameter are enabled.

On the AR415S, MAC-based authentication is only available for ethernet interfaces, for example eth0.

The authentication server must be connected to a port on the router that does not have port authentication enabled, or is set with **control=authorised**.

The **type** parameter specifies whether the port is to act as an authenticator, supplicant, or both. **Type** can only be specified when **portauth=8021x**. **Both** cannot be specified when the **mode** parameter is **multi**.

The **authperiod** parameter specifies the period of time in seconds that the Supplicant PAE waits for a reply after sending out an EAP-Response frame to the Authenticator PAE. The **authperiod** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **supplicant**, or it specifies **both** and the port(s) are acting in a supplicant role. If no response is received within the specified time, a new authentication attempt may start. The valid range of integer values is 1 to 60. The default is 30.

The **control** parameter specifies the state of the controlled authenticator port. The **control** parameter is used when the **portauth** parameter specifies **macbased,** or when the **type** parameter either specifies **authenticator,** or it specifies **both** and the port(s) are acting in an authenticator role. If **authorised** is specified, the port acts as if it already passed authentication. If **auto** is specified, the port implements normal port authentication control. If **unauthorised** is specified, the port acts as if authentication of the supplicant failed. The default is **auto**.

The **heldperiod** parameter specifies the amount of time in seconds that the Supplicant PAE should refrain from re-contacting an Authenticator PAE after an authentication attempt fails due to an invalid username/password combination. The **heldperiod** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **supplicant**, or it specifies **both** and the port(s) are acting in a supplicant role. At the end of the specified time, further authentication attempts are permitted. The valid range of integer values is 0 to 65535. The default is 60.

The **maxreq** parameter specifies the maximum number of times the Authenticator PAE tries to retransmit an EAP request packet to the Supplicant PAE when no response is received. The **maxreq** parameter is used when the **portauth** parameter specifies **8021x,** and the **type** parameter either specifies **authenticator,** or it specifies **both** and the port(s) are acting in an authenticator role. The valid range of integer values is 1 to 10. The default is 2.

The **maxstart** parameter specifies the maximum number of successive EAPOL-Start messages sent before the supplicant assumes no authenticator is present. The **maxstart** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **supplicant,** or it specifies **both** and the port(s) are acting in a supplicant role. The valid range of integer values is 1 to 10. The default is 3.

The **mode** parameter specifies whether a port is connected to a single supplicant or to multiple supplicants. The **mode** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter specifies **authenticator**. If **multi** is specified, the port distinguishes between multiple supplicants attached to it and requires each supplicant to authenticate itself separately. If **single** is specified, the port is authenticated by the first supplicant attached to it. The default is **single**.

Caution Setting the **mode** parameter to **multi** is a departure from IEEE Standard 802.1x and introduces security risks. We recommend that 802.1x control not be used in a multi-supplicant configuration to minimise the risk of unauthorised access and denial-of-service attacks.

The **piggyback** parameter specifies whether the piggybacking of network devices onto an authenticated supplicant is allowed. The **piggyback** parameter is used when the **portauth** parameter specifies **8021x**, the **type** parameter specifies **authenticator** or **both,** and the **mode** parameter specifies **single**. If **true** is specified, piggybacking is enabled and packets from any source are allowed to pass through the port once a supplicant has been authorised on it. If **false** is specified, piggybacking is disabled and packets from any source other than the authenticated supplicant are blocked. The default is **true**. On the AR415S and AR450S, setting **piggyback** to **false** is only valid for Ethernet interfaces.

The **quietperiod** parameter specifies the amount of time in seconds that the Authenticator PAE should refuse additional authentication attempts after an attempt has already failed due to an invalid username/password combination supplied by the Supplicant PAE. The **quietperiod** parameter is used when **portauth=macbased**; or when the 802.1x **mode=multi**, and the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. In this state, all received EAPOL packets are discarded to prevent denial-of-service attacks. At the end of the specified time period further authentication attempts are permitted. The valid range of integer values is 0 to 65535. The default is 60.

The **reauthenabled** parameter specifies whether the Authenticator PAE requires the attached supplicants to undergo periodic reauthentication. The **reauthenabled** parameter is used when **portauth=macbased**; or when the 802.1x **mode=multi**, and the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. The default is **false**.

The **reauthmax** parameter specifies the maximum number of times the Authenticator PAE tries to establish contact with a Supplicant PAE when no response is received. The **reauthmax** parameter is used when **portauth=8021x** and the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. When the maximum number of attempts is reached, an EAPOL-failure message is transmitted and the Authenticator PAE resets itself before trying to contact a Supplicant PAE again. The valid range of integer values is 1 to 10. The default is 2.

The **reauthperiod** parameter specifies the time in seconds between reauthentications of the Supplicant PAE if the **reauthenabled** parameter is set to **true**. The **reauthperiod** parameter is used when the **portauth** parameter specifies **macbased**, or when the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. The valid range of integer values is 1 to 86400. The default is 3600.

The **servertimeout** parameter specifies the timeout period in seconds that the Authenticator PAE waits for a response from the authentication server after the Authenticator PAE has relayed an EAP response packet to it from the supplicant. The **servertimeout** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. The valid range of integer values is 1 to 60. The default is 30.

The **startperiod** parameter specifies the time in seconds between successive attempts by the Supplicant PAE to establish contact with an Authenticator PAE when there is no response. The **startperiod** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **supplicant**, or it specifies **both** and the port(s) are acting in a supplicant role. Attempts to establish contact continue until the number of attempts reaches the value set by the **maxstart** parameter. When the value set by the **maxstart** parameter is reached, the Supplicant PAE assumes it is attached to a system that is not EAPOL aware and enters the authenticated state. The valid range of integer values is 1 to 60. The default is 30.

The **supptimeout** parameter specifies the timeout period in seconds to wait for a response from the Supplicant PAE after the Authenticator PAE has relayed an EAP request packet to it from the authentication server. The **supptimeout** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. The Authenticator PAE retransmits the packet to the Supplicant PAE upon timeout, up to the number of times defined by the **maxreq** parameter. The valid range of integer values is 1 to 60. The default is 30.

The **txperiod** parameter specifies the time in seconds between successive attempts by the Authenticator PAE to establish contact with a Supplicant PAE when there is no response. The **txperiod** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. The valid range of integer values is 1 to 65535. The default is 30.

The **username** parameter specifies the login name to use when the port is acting in a supplicant role. The **username** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **supplicant**, or it specifies **both** and the port(s) are acting in a supplicant role. If the **username** parameter is present, it overrides the global port authentication username for the specified port(s) only. The **password** parameter must also be specified. Omitting or specifying the **username** and **password** parameters without a specific value causes the global username and password to be used during authentication attempts. The login name is not case sensitive.

The **username** and **password** parameters set the username and password for an individual supplicant. Use the **set portauth username** command on page 43-45 to set a global username and a global password for all supplicants.

Caution Enter passwords in a secure environment because they appear on the screen as you type. Also, all configuration file backups should be kept secure because passwords are in plaintext in configuration files.

The **password** parameter specifies the password to be used when the port acts in a supplicant role during the authentication process. The **password** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **supplicant**, or it specifies **both** and the port(s) are acting in a supplicant role. If the **password** parameter is present, it overrides the global port authentication password for the specified port(s) only. The **username** parameter must also be specified. Omitting or specifying the **username** and **password** parameters without a specific value causes the global username and password to be used during authentication attempts. A password may contain uppercase letters (A–Z), lowercase letters (a–z), and decimal digits (0–9), and a configurable minimum password length is enforced. The password is case sensitive. If the **method** parameter is **standard**, the password must be at least 6 characters long. If the **method** parameter is **otp**, the password must contain no less than 10 characters and no more than 63 characters. If **otp** is specified, then the password should match the OTP initialisation password used when configuring the user on the authentication server.

The **method** parameter specifies the method used to encrypt the username and password during authentication attempts. The **method** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **supplicant**, or it specifies **both** and the port(s) are acting in a supplicant role. If the **method** parameter is specified, then the **username** and **password** parameters must also be specified. If **standard** is specified, authentication attempts are conducted by encrypting a standard username and password using EAP-MD5. If **otp** is specified, authentication attempts use one-time passwords via EAP-OTP. The default is **standard**.

The **encryption** parameter specifies the method for generating one-time passwords. The **encryption** parameter can only be specified if the **method** parameter specifies **otp**, i.e. when authentication is taking place using EAP-OTP messaging. If **md4** is specified, one-time passwords are generated using a MD4 one-way function, commonly known as S/Key. If **md5** is specified, one-time passwords are generated using a MD5 one-way function, commonly known as OTP.

The **guestvlan** parameter specifies any VLAN that exists on the switch. Prior to receiving any 802.1x BPDUs on the port, the port is configured in the specified **guestvlan**. Once any EAPOL packets have been received, the port is removed from the **guestvlan** and placed in the configured access VLAN. The **guestvlan** parameter is used when **portauth=macbased**; or when the 802.1x **mode=single**, and the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. This parameter is only valid in Single-Supplicant mode.

The **vlanassignment** parameter specifies whether or not to use the VLAN assignment mechanism on this port. Dynamic VLAN assignment is only supported when using 802.1x authentication in single-supplicant mode. When the **vlanassignment** parameter is set to **enabled**, the router uses any VLAN information returned by the RADIUS server to place the port in a VLAN. When it is set to **disabled**, the router ignores all VLAN information returned by the

RADIUS server. The **vlanassignment** parameter is used when **portauth=macbased**; or when the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. The default is **enabled**.

VLAN assignment cannot be enabled on any port that is one or more of the following:

- tagged

- a mirror port

- in more than one VLAN

- an uplink for a private VLAN

- in a group with other ports for private port VLANs

- in a nest vlan

- in a vlan that has a rule type other than port

The **mibreset** parameter provides a mechanism for ageing out stored information about old supplicants. When **enabled** is specified, MIB information for old supplicants is automatically destroyed. This allows new supplicants to be added. When **disabled** is specified, the MIB information remains until it is manually cleared via the **reset portauth port multimib** command. As long the MIB information remains for a supplicant, that supplicant counts towards the supplicant limit. This parameter can only be used in MAC-based authentication and 802.1x Multi-Supplicant mode. It does not affect supplicants explicitly added through the supplicant MAC command. The default is **enabled**.

The **trap** parameter specifies the events that cause SNMP traps to be sent. When either **success** or **both** is specified, traps are sent when a supplicant is successfully authenticated, and when the authentication expires. When either **failure** or **both** is specified, traps are sent when a supplicant fails authentication. When **none** is specified, no traps are sent. The **trap** parameter is used when **portauth=macbased**; or when the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. The default is **none**.

Examples   To enable Eth 0 as a authenticator, use the command:

```
ena porta po=eth0 ty=au
```

Related Commands   **activate portauth port reauthenticate**
disable portauth
disable portauth port
enable portauth
set portauth port
set portauth port supplicantmac
set radius
show portauth
show portauth counter
show portauth port
show portauth port multisupplicant
show portauth timer

purge portauth port

Syntax   PURge PORTAuth[={8021x|MACbased}] POrt={ALL|*port-name*}

where *port-name* is an Ethernet interface (eth0 or eth1), a port number, a range of port numbers (specified as n-m), or a comma-separated list of port numbers and/or ranges. Port numbers start at n and end at m, where n is the lower value port number and m the upper value port number, including uplink ports.

Description   This command purges all port authentication configurations for the specified port(s) and authentication type.

The **portauth** parameter specifies the type of port authentication to purge. The default is 802.1x.

The **port** parameter specifies which port to purge. If **all** is specified, all ports on the router that support the type of port authentication specified by the **portauth** parameter are purged.

Examples   To remove all current 802.1x port authentication settings on the router, use the command:

```
pur porta=8021x po=all
```

To remove all current MAC-based settings on the router, use the command:

```
pur porta=mac po=all
```

Related Commands   disable portauth
enable portauth
show portauth port

reset portauth port

Syntax
```
RESET PORTAuth[={8021x|MACbased}] POrt={ALL|port-name}
    [SUPPLicantmac=macadd]
```

where:

■   *port-name* is an Ethernet interface (eth0 or eth1), a port number, a range of port numbers (specified as n-m), or a comma-separated list of port numbers and/or ranges. Port numbers start at n and end at m, where n is the lower value port number and m the upper value port number, including uplink ports.

■   *macadd* is an Ethernet six-octet MAC address, expressed as six pairs of hexadecimal digits delimited by hyphens.

Description   This command reinitialises port authentication on the specified port(s) for the specified authentication type.

The **portauth** parameter specifies the type of port authentication to reset. The default is 802.1x.

The **port** parameter specifies the port or ports to be reset. If **all** is specified, all ports on the router that support the type of port authentication specified by the **portauth** parameter are reset.

The **supplicantmac** parameter specifies the hardware address of a single connected supplicant to reset, in standard MAC format, e.g. `11-22-33-44-55-66`. The **supplicantmac** parameter is valid for ports configured as authenticators on a multi-supplicant system.

Examples   To reset the 802.1x PAE associated with port 1, use the command:

```
reset porta=8021x port=1
```

To reset the MAC-based PAE associated with port 1, use the command:

```
reset porta=mac port=1
```

To reset the 8021.x PAE associated with Eth 0, use the command:

```
reset porta=8021x po=eth0
```

To reset the MAC-based PAE associated with Eth 0, use the command:

```
reset porta=mac po=eth0
```

Related Commands   disable portauth port
enable portauth
set portauth port supplicantmac
show portauth counter
show portauth port

reset portauth port multimib

Syntax   RESET PORTAuth[={8021x|MACbased}] POrt={ALL|*port-name*}
               MULTImib

where *port-name* is an Ethernet port

Description   This command removes any multi-supplicant MIB instances relating to
supplicants that are not currently authenticated by the specified ports and that
have not been specifically configured using the **set portauth port
supplicantmac** command on page 43-42.

This command applies only when using MAC-based authentication; or, when
using 802.1x authentication, to ports that act as authenticators in a
multi-supplicant configuration.

The **portauth** parameter specifies the type of port authentication to reset. The
default is 802.1x.

The **port** parameter specifies the port or ports for which MIB entries are
removed. If **all** is specified, all multi-supplicant MIB entries are removed from
all ports on the router that support the type of port authentication specified by
the **portauth** parameter.

Examples   To remove all unused 8021.x multi-supplicant MIB entries associated with Eth
0, use the command:

    reset porta=8021x po=eth0 multi

To remove all unused MAC-based multi-supplicant MIB entries associated
with Eth 0, use the command:

    reset porta=mac po=eth0 multi

Related Commands   **disable portauth port**
enable portauth
set portauth port
set portauth port supplicantmac
show portauth port

set portauth port

Syntax
```
SET PORTAuth[=8021x] POrt={ALL|eth-port|switch-port}
    TYpe=AUthenticator [CONTrol={AUTHorised|AUTO|
    UNauthorised}] [MAXReq=1..10] [MODe={MUlti|SIngle}]
    [PIGgyback={TRue|FAlse}] [QUIETperiod=0..65535]
    [REAUTHENAbled={TRue|FAlse}] [REAUTHMax=1..10]
    [REAUTHPeriod=1..86400] [SERVERTimeout=1..60]
    [SUPPTimeout=1..60] [TXperiod=1..65535]
    [GUEstvlan={1..4094|vlan-name|NONe}]
    [VLANAssignment={ENAbled|DIsabled}] [MIBReset={ENAbled|
    DIsabled}] [TRap={SUCcess|FAILure|BOTh|NONe}]

SET PORTAuth[=8021x] POrt={ALL|eth-port|switch-port}
    TYpe=BOth [AUTHPeriod=1..60] [CONTrol={AUTHorised|
    UNauthorised|AUTO}] [HELDPeriod=0..65535]
    [MAXReq=1..10] [MAXStart=1..10] [MODe={MUlti|SIngle}]
    [PIGgyback={TRue|FAlse}] [QUIETperiod=0..65535]
    [REAUTHENAbled={TRue|FAlse}] [REAUTHMax=1..10]
    [REAUTHPeriod=1..86400] [SERVERTimeout=1..60]
    [STARTperiod=1..60] [SUPPTimeout=1..60]
    [TXperiod=1..65535] [USERName=login-name
    PASSword=password [METhod={OTP[ENCryption={MD4|MD5}]|
    STandard}]] [GUEstvlan={1..4094|vlan-name|NONe}]
    [VLANAssignment={ENAbled|DIsabled}] [MIBReset={ENAbled|
    DIsabled}] [TRap={SUCcess|FAILure|BOTh|NONe}]

SET PORTAuth[=8021x] POrt={ALL|eth-port|switch-port}
    TYpe=SUpplicant [AUTHPeriod=1..60]
    [HELDPeriod=0..65535] [MAXStart=1..10]
    [STARTperiod=1..60] [USERName=login-name
    PASSword=password [METhod={OTP[ENCryption={MD4|MD5}]|
    STandard}]]

SET PORTAuth=MACbased POrt={ALL|eth-port}
    [CONTrol={AUTHorised|UNauthorised|AUTO}]
    [REAUTHENAbled={TRue|FAlse}] [REAUTHPeriod=1..86400]
    [QUIETperiod=0..65535] [VLANAssignment={ENAbled|
    DIsabled}] [MIBReset={ENAbled|DIsabled}]
    [TRap={SUCcess|FAILure|BOTh|NONe}]
```

where:

■ *eth-port* is an Ethernet interface (for example, eth0 or eth1).

■ *switch-port* is a port number, a range of port numbers (specified as n-m), or a comma-separated list of port numbers and/or ranges. Port numbers start at n and end at m, where n is the lower value port number and m the upper value port number, including uplink ports.

■ *vlan-name* is a unique name for the VLAN, 1 to 32 characters in length. Valid characters are uppercase and lowercase letters, digits, the underscore character, and the hyphen character. The VLAN name cannot be a number or **all**.

■ *login-name* is a character string 1 to 64 characters long. Valid characters are uppercase and lowercase letters and digits (0-9).

■ *password* is an character string. Valid characters are uppercase and lowercase letters and digits (0–9).

Description   This command sets port authentication on the specified ports. Port authentication must already be enabled on the port for the specified **portauth** type, which can be either **8021x** or **macbased**. If **portauth** is **8021x** a port can be set as an authenticator, supplicant, or both.

Ports under port authentication control do not support static/dynamic learning and can be a member of only one VLAN.

The **portauth** parameter specifies the type of port authentication to set. The default is 802.1x.

The **port** parameter specifies the port to set with port authentication. If **all** is specified, all ports on the router that support the type of port authentication specified by the **portauth** parameter are set.

On the AR415S, MAC-based authentication is only available for Ethernet interfaces, for example eth0.

The authentication server must be connected to a port on the router that does not have port authentication enabled, or is set with **control=authorised**.

The **type** parameter specifies whether the port is to act as an authenticator, supplicant, or both. **type** can only be specified when **portauth=8021x**. **both** cannot be specified when the **mode** parameter is **multi**.

The **authperiod** parameter specifies the period of time in seconds that the Supplicant PAE waits for a reply after sending out an EAP-Response frame to the Authenticator PAE. The **authperiod** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies supplicant, or it specifies **both** and the port(s) are acting in a supplicant role. If no response is received within the specified time, a new authentication attempt may start. The valid range of integer values is 1 to 60.

The **control** parameter specifies the state of the controlled authenticator port. The **control** parameter is used when the **portauth** parameter specifies **macbased**, or when the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. If **authorised** is specified, the port acts as if it already passed authentication. If **auto** is specified, the port implements normal port authentication control. If **unauthorised** is specified, the port acts as if authentication of the supplicant failed.

The **heldperiod** parameter specifies the amount of time in seconds that the Supplicant PAE should refrain from trying to re-contact an Authenticator PAE after an authentication attempt fails due to an invalid username/password combination. The **heldperiod** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **supplicant**, or it specifies **both** and the port(s) are acting in a supplicant role. At the end of the specified time, further authentication attempts are permitted. The valid range of integer values is 0 to 65535.

The **maxreq** parameter specifies the maximum number of times the Authenticator PAE attempts to retransmit an EAP request packet to the Supplicant PAE if no response is received. The **maxreq** parameter is used when the **portauth** parameter specifies **8021x**, and the type parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. The valid range of integer values is 1 to 10.

The **maxstart** parameter specifies the maximum number of successive EAPOL-Start messages that are sent before the supplicant assumes no authenticator is present. The **maxstart** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **supplicant**, or it specifies **both** and the port(s) are acting in a supplicant role. The valid range of integer values is 1 to 10.

The **mode** parameter specifies whether a port is connected to a single supplicant or to multiple supplicants. The **mode** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter specifies **authenticator**. If **multi** is specified, the port distinguishes between multiple supplicants attached to it, and requires each supplicant to authenticate itself separately. If **single** is specified, the port is authenticated by the first supplicant attached to it.

Caution Setting the **mode** parameter to **multi** is a departure from IEEE Standard 802.1x and introduces security risks. We recommend that 802.1x control not be used in a multi-supplicant configuration to minimise the risk of unauthorised access and denial-of-service attacks.

The **piggyback** parameter specifies whether the piggybacking of network devices onto an authenticated supplicant is allowed. The **piggyback** parameter is used when the **portauth** parameter specifies **8021x**, the **type** parameter specifies **authenticator** or **both**, and the **mode** parameter specifies **single**. If **true** is specified, piggybacking is enabled and packets from any source are allowed to pass through the port once a supplicant has been authorised on it. If **false** is specified, piggybacking is disabled and packets from any source other than the authenticated supplicant are blocked. On the AR415S and AR450S, setting **piggyback** to **false** is only valid for Ethernet interfaces.

The **quietperiod** parameter specifies the amount of time in seconds that the Authenticator PAE should refuse additional authentication attempts after an attempt has already failed due to an invalid username/password combination supplied by the Supplicant PAE. The **quietperiod** parameter is used when **portauth=macbased**; or when the 802.1x **mode=multi**, and the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. In this state, all received EAPOL packets are discarded to prevent denial-of-service attacks. At the end of the specified time, period further authentication attempts are permitted. The valid range of integer values is 0 to 65535.

The **reauthenabled** parameter specifies whether the Authenticator PAE requires the attached supplicants to undergo periodic reauthentication. The **reauthenabled** parameter is used when **portauth=macbased**; or when the 802.1x **mode=multi**, and the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role.

The **reauthmax** parameter specifies the maximum number of times the Authenticator PAE tries to establish contact with a Supplicant PAE when no response is received. The **reauthmax** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. When the maximum number of attempts is reached, an EAPOL-failure message is transmitted and the Authenticator PAE resets itself before trying to contact a Supplicant PAE again. The valid range of integer values is 1 to 10.

The **reauthperiod** parameter specifies the time in seconds between reauthentications of the Supplicant PAE if the reAuthEnabled parameter is set to **true**. The **reauthperiod** parameter is used when the **portauth** parameter specifies **macbased**, or when the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. The valid range of integer values is 1 to 86400.

The **servertimeout** parameter specifies the timeout period in seconds the Authenticator PAE waits for a response from the authentication server after the Authenticator PAE has relayed an EAP response packet to it from the supplicant. The **servertimeout** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. The valid range of integer values is 1 to 60.

The **startperiod** parameter specifies the time in seconds between successive attempts by the Supplicant PAE to establish contact with an Authenticator PAE when there is no response. The **startperiod** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **supplicant**, or it specifies **both** and the port(s) are acting in a supplicant role. Attempts to establish contact continue until the number of attempts reaches the value set by the **maxstart** parameter. When the value set by the **maxstart** parameter is reached, the Supplicant PAE assumes it is attached to a system that is not EAPOL aware and enters the authenticated state. The valid range of integer values is 1 to 60.

The **supptimeout** parameter specifies the timeout period in seconds to wait for a response from the Supplicant PAE after the Authenticator PAE has relayed an EAP request packet to it from the authentication server. The **supptimeout** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. The Authenticator PAE retransmits the packet to the Supplicant PAE upon timeout, up to the number of times defined by the **maxreq** parameter. The valid range of integer values is 1 to 60.

The **txperiod** parameter specifies the time in seconds between successive attempts by the Authenticator PAE to establish contact with a Supplicant PAE when there is no response. The **txperiod** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. The valid range of integer values is 1 to 65535.

The **username** parameter specifies the login name to use when the port acts in a supplicant role. The **username** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **supplicant**, or it specifies **both** and the port(s) are acting in a supplicant role. If the **username** parameter is present, it overrides the global port authentication username for the specified port(s) only. The **password** parameter must also be specified.

The **username** and **password** parameters set the username and password for an individual supplicant. Use the **set portauth username** command on page 43-45 to set a global username and a global password for all supplicants.

> **Caution** When you enter passwords, ensure you are in a secure environment because passwords appear on the screen as you type. Also, all configuration file backups should be kept secure because passwords appear in plaintext in configuration files.

The **password** parameter specifies the password to be used when the port acts in a supplicant role during the authentication process. The **password** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **supplicant**, or it specifies **both** and the port(s) are acting in a supplicant role. If the **password** parameter is present, it overrides the global port authentication password for the specified port(s) only. The **username** parameter must also be specified. A password may contain uppercase and lowercase letters and digits (0–9), and a configurable minimum password length is enforced. The password is case sensitive. If the **method** parameter is **standard**, the password must be at least 6 characters long. If the **method** parameter is **otp**, the password must contain no less than 10 characters and no more than 63 characters. Also, if **otp** is specified, then the password should match the OTP initialisation password used when configuring the user on the authentication server.

The **method** parameter specifies the method used to encrypt the username and password during authentication attempts. The **method** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **supplicant**, or it specifies **both** and the port(s) are acting in a supplicant role. If the **method** parameter is specified, then the **username** and **password** parameters must also be specified. If **standard** is specified, authentication attempts are conducted by encrypting a standard username and password using EAP-MD5. If **otp** is specified, authentication attempts use one-time passwords via EAP-OTP.

The **encryption** parameter specifies the method for generating one-time passwords. The **encryption** parameter can only be specified if the **method** parameter specifies OTP, i.e. when authentication is taking place using EAP-OTP messaging. If **md4** is specified, one-time passwords are generated using a MD4 one-way function, commonly known as S/Key. If **md5** is specified one-time passwords are generated using a MD5 one-way function, commonly known as OTP.

The **guestvlan** parameter specifies any VLAN that exists on the switch. Prior to receiving any 802.1x BPDUs on the port, the port is configured in the specified **guestvlan**. Once any EAPOL packets have been received, the port is removed from the **guestvlan** and placed in the configured access VLAN. The **guestvlan** parameter is used when **portauth=macbased**; or when the 802.1x **mode=single**, and the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. This parameter is only valid in Single-Supplicant mode.

The **vlanassignment** parameter specifies whether or not to use the VLAN assignment mechanism on this port. Dynamic VLAN assignment is only supported when using 802.1x authentication in single-supplicant mode.

 When the **vlanassignment** parameter is set to **enabled**, the router uses any VLAN information returned by the RADIUS server to place the port in a VLAN. When it is set to **disabled**, the router ignores all VLAN information returned by the RADIUS server. The **vlanassignment** parameter is used when **portauth=macbased**; or when the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role.

VLAN assignment cannot be enabled on any port that is one or more of the following:

■   tagged

■   a mirror port

■   in more than one VLAN

■   an uplink for a private VLAN

■   in a group with other ports for private port VLANs

■   in a nest vlan

■   in a vlan that has a rule type other than port

The **mibreset** parameter provides a mechanism for ageing out stored information about old supplicants. When **enabled** is specified, MIB information for old supplicants is automatically destroyed. This allows new supplicants to be added. When **disabled** is specified, the MIB information remains until it is manually cleared via the **reset portauth port multimib** command. As long the MIB information remains for a supplicant, that supplicant counts towards the supplicant limit. This parameter can only be used in MAC-based authentication and 802.1x Multi-Supplicant mode. It does not affect supplicants explicitly added through the supplicant MAC command.

The **trap** parameter specifies the events that cause SNMP traps to be sent. When either **success** or **both** is specified, traps are sent when a supplicant is successfully authenticated, and when the authentication expires. When either **failure** or **both** is specified, traps are sent when a supplicant fails authentication. When **none** is specified, no traps are sent. The **trap** parameter is used when **portauth=macbased**; or when the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role.

Examples   To modify the current **quietperiod** setting for 802.1x on Eth 0, use the command:

```
set porta=802.1x ty=au po=eth0 quiet=1024
```

To modify the current **quietperiod** setting for MAC-based authentication on Eth 0, use the command:

```
set porta=mac ty=au po=eth0 quiet=1024
```

Related Commands   **activate portauth port reauthenticate**
disable portauth port
enable portauth
enable portauth port
reset portauth port multimib
set portauth port supplicantmac
set radius
show portauth
show portauth counter
show portauth port
show portauth port multisupplicant
show portauth timer

set portauth port supplicantmac

Syntax   SET PORTAuth[=8021x] POrt={ALL|*port-name*}
        SUPPLicantmac=*macadd* [CONTrol={AUTHorised|UNauthorised|
        AUTO}] [MAXReq=1..10] [QUIETperiod=0..65535]
        [REAUTHENAbled={TRue|FAlse}] [REAUTHMax=1..10]
        [REAUTHPeriod=1..86400] [SERVERTimeout=1..60]
        [SUPPTimeout=1..60] [TXperiod=1..65535]
        [VLANAssignment={ENAbled|DIsabled}] [TRap={SUCcess|
        FAIlure|BOTh|NONe}][DEFAULT]

   SET PORTAUTH=MACbased POrt={ALL|portname}
        SUPPLicantmac=macadd [CONTrol={AUTHorised|UNauthorised|
        AUTO}] [REAUTHENAbled={TRue|FAlse}]
        [REAUTHPeriod=1..86400] [QUIETperiod=0..65535]
        [VLANAssignment={ENAbled|DIsabled}] [TRap={SUCcess|
        FAIlure|BOTh|NONe}][DEFAULT]

   where:

   ■   *port-name* is an Ethernet port.

   ■   *macadd* is an Ethernet six-octet MAC address, expressed as six pairs of
       hexadecimal digits delimited by hyphens.

Description   This command allows the Authenticator PAE configuration for specified
   port(s) to be overridden for a specific supplicant. Port authentication must
   already be enabled on the specified port(s) for the specified **portauth** type,
   which can be either **8021x** or **macbased**. Any supplicant that attaches to an
   Authenticator PAE configured for multi-supplicant support uses the
   parameters set by either the **set portauth port type=authenticator** command or
   set portauth port type=both command, unless the MAC address of the
   supplicant matches the **supplicantmac** parameter of a previously entered **set
   portauth port supplicantmac** command. At least one non-standard parameter
   value must be entered in the command.

   This command applies to ports that are authenticator capable on a
   multi-supplicant configuration.

   The **portauth** parameter specifies the type of port authentication to set. The
   default is 802.1x.

   The **port** parameter specifies for which port(s) the individual supplicant entry
   is to override the standard settings. If **all** is specified, the standard settings are
   overridden for all defined multi-supplicant authenticator ports on the router.

   The **supplicantmac** parameter specifies the hardware address of the connected
   supplicant to modify, in the standard MAC format of six pairs of hexadecimal
   digits delimited by hyphens. For example, 11-22-33-44-55-66.

   The **control** parameter specifies the state of the controlled authenticator port.
   The **control** parameter is used when the **portauth** parameter specifies
   macbased, or when the **type** parameter either specifies authenticator, or it
   specifies **both** and the port(s) are acting in an authenticator role. If **authorised**
   is specified, the port acts as if it has already passed authentication. If **auto** is
   specified, the port implements normal port authentication control. If
   unauthorised is specified, the port acts as if authentication of the supplicant
   failed.

The **default** parameter removes the individual settings for the specified supplicant MAC address.

The **maxreq** parameter specifies the maximum number of times the Authenticator PAE attempts to retransmit an EAP request packet to the Supplicant PAE if no response is received. The **maxreq** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. The valid range of integer values is 1 to 10.

The **quietperiod** parameter specifies the amount of time in seconds that the Authenticator PAE should refuse additional authentication attempts, if an attempt has already failed due to an invalid username/password combination supplied by the Supplicant PAE. The **quietperiod** parameter is used when **portauth=macbased**; or when **portauth=8021x**, and the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. In this state, all received EAPOL packets are discarded to prevent denial-of-service attacks. At the end of the specified time, further authentication attempts are permitted. The valid range of integer values is 0 to 65535.

The **reauthenabled** parameter specifies whether the Authenticator PAE requires the Supplicant PAE to undergo periodic reauthentication. The **reauthenabled** parameter is used when **portauth=macbased**; or when **portauth=8021x**, and the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role.

The **reauthperiod** parameter specifies the time between reauthentications of the Supplicant PAE if the **reauthenabled** parameter is set to **true**. The **reauthperiod** parameter is used when the **portauth** parameter specifies **macbased**, or when the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. The valid range of integer values is 1 to 86400.

The **servertimeout** parameter specifies the timeout period in seconds the Authenticator PAE waits for a response from the authentication server after the Authenticator PAE has relayed an EAP response packet to it from the supplicant. The **servertimeout** parameter is used when the **portauth** parameter specifies **8021x**, and **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. The valid range of integer values is 1 to 60.

The **supptimeout** parameter specifies the timeout period in seconds to wait for a response from the Supplicant PAE after the Authenticator PAE has relayed an EAP request packet to it from the authentication server. The **supptimeout** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. The Authenticator PAE retransmits the packet to the Supplicant PAE on timeout, up to the number of times defined by the **maxreq** parameter. The valid range of integer values is 1 to 60.

The **txperiod** parameter specifies the time in seconds between successive attempts by the Authenticator PAE to establish contact with a Supplicant PAE when there is no response. The **txperiod** parameter is used when the **portauth** parameter specifies **8021x**, and the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. The valid range of integer values is 1 to 65535.

The **vlanassignment** parameter specifies whether or not to use the VLAN assignment mechanism on this port. Dynamic VLAN assignment is only supported when using 802.1x authentication in single-supplicant mode. When the **vlanassignment** parameter is set to **enabled**, the router uses any VLAN information returned by the RADIUS server to place the port in a VLAN. When it is set to **disabled**, the router ignores all VLAN information returned by the RADIUS server. The **vlanassignment** parameter is used when **portauth=macbased**; or when the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role.

VLAN assignment cannot be enabled on any port that is one or more of the following:

- tagged

- a mirror port

- in more than one VLAN

- an uplink for a private VLAN

- in a group with other ports for private port VLANs

- in a nest vlan

- in a vlan that has a rule type other than port

The **trap** parameter specifies the events that cause SNMP traps to be sent. When either **success** or **both** is specified, traps are sent when a supplicant is successfully authenticated, and when the authentication expires. When either **failure** or **both** is specified, traps are sent when a supplicant fails authentication. When **none** is specified, no traps are sent. The **trap** parameter is used when **portauth=macbased**; or when the **type** parameter either specifies **authenticator**, or it specifies **both** and the port(s) are acting in an authenticator role. The default is **none**.

Examples   To modify the current **quietperiod** setting on Eth 0 of a multi-supplicant system with a supplicant MAC address of 22-22-22-22-22-22, use the command:

```
set porta po=eth0 suppl=22-22-22-22-22-22 quiet=1024
```

Related Commands   disable portauth port
enable portauth
enable portauth port
reset portauth port multimib
set portauth port
set radius
show portauth counter
show portauth port

set portauth username

Syntax   SET PORTAuth[=8021x] USERName=*login-name* PASSword=*password*
        [METhod={OTP[ENCryption={MD4|MD5}]|STandard}]

where:

- *login-name* is a character string 1 to 64 characters long. Valid characters are uppercase and lowercase letters and digits (0–9).

- *password* is a character string. Valid characters are uppercase and lowercase letters and decimal digits (0–9).

Description   This command allows the user to configure a global username and global password for all Supplicant Port Access Entities (PAEs) to use during authentication. The global settings may be overridden using the **set portauth port** to set specific supplicant passwords and usernames.

The **portauth** parameter specifies the type of port authentication the settings apply to. This command only applies to 802.1x, and defaults to 802.1x if no value is specified.

The **username** parameter specifies the global default login name to be used during authentication by any defined supplicant on the router that does not have its own username/password setting. The **password** parameter must also be specified. The **username** parameter is case insensitive. The default global username is "portAuthportAuth", but this should be reset as soon as possible for security reasons.

Caution When you enter passwords ensure you do so in a secure environment because passwords appear on the screen as typed. Also, any configuration file backups should be kept secure as passwords appear in plaintext in configuration files.

The **password** parameter specifies the password to be used during the authentication process by any defined supplicant on the router that does not have its own username/password setting. The **username** parameter must also be specified. A password may contain uppercase and lowercase letters and digits (0–9), and a configurable minimum password length is enforced. The password is case sensitive. If the **method** parameter specified is **standard**, the password must be at least 6 characters long. If the **method** parameter is **otp**, the password must contain no less than 10 characters and no more than 63 characters. Also, if **otp** is specified, the password should match the OTP initialisation password used when configuring the user on the authentication server. The default global password is "portAuthportAuth", but this should be reset as soon as possible for security reasons.

The **method** parameter specifies the method used to encrypt the username and password during authentication attempts by any defined supplicant on the router that does not have its own username/password setting. If **standard** is specified, authentication attempts are conducted by encrypting a standard username and password using EAP-MD5. If OTP is specified, authentication attempts use one-time passwords via EAP-OTP. The default is **standard**.

The **encryption** parameter specifies the method for generating one-time passwords by defined supplicants on the router that do not have their own username/password setting when authentication takes place using EAP-OTP messaging. The **encryption** parameter is used when the **method** parameter specifies OTP. If **md4** is specified, one-time passwords are generated using a MD4 one-way function, commonly known as S/Key. If **md5** is specified, one-time passwords are generated using a MD5 one-way function, commonly known as OTP. The default is MD5 encryption.

Examples   To set the global port authentication username and password for 802.1x on the router, use the command:

```
set porta=8021x usern=manager pass=friend
```

To set the global port authentication username and password for MAC-based authentication on the router, use the command:

```
set porta=mac usern=manager pass=friend
```

Related Commands   disable portauth port
enable portauth port
set portauth port
set portauth port supplicantmac
show portauth counter
show portauth port
show portauth port multisupplicant

show portauth

Syntax   SHow PORTAuth[={8021x|MACbased}]

Description   This command displays information about each port's capabilities and protocol implementation (Figure 43-6, Table 43-1).

The **portauth** parameter specifies the type of port authentication that is displayed. The default is 802.1x.

Figure 43-6: Example output from the **show portauth=8021x** command

```
  802.1x System
  --------------------------------------------------
    SystemAuthControl............ ENABLED
    Global Username.............. portAuthPortAuth
    Global Password.............. portAuthPortAuth
    Global Encryption Method..... OTP
    Global Encryption Type....... MD5
    Number of Multi Supplicants.. 4 (limit 480)


    Port          PAE Capabilities      Protocol Version
  --------------------------------------------------
    eth0          None                  1
    eth1          None                  1
    port1         Supplicant            1
    port2         Authenticator         1
    port3         Both                  1
    port4         None                  1
    port5         None                  1
```

Table 43-1: Parameters in output of the **show portauth=8021x** command

Parameter	Meaning
SystemAuthControl	The 802.1x port authentication state; one of "ENABLED" or "DISABLED".
Global Username	The global port authentication username used by all Supplicant PAEs on the router that do not have their own unique username defined.
Global Password	The global port authentication password used by all Supplicant PAEs on the router that do not have their own unique password defined.
Global Encryption Method	The password transmission method used by all Supplicant PAEs using the global username and password - either "Standard" or "OTP".
Global Encryption Type	The password encryption method used by all Supplicant PAEs using the global username and password when the OTP encryption method is selected; either MD4 for S/Key support or OTP.
PAE Capabilities	The 802.1x functions available to a port; one of "Authenticator", "Supplicant", "Both", or "None".
Protocol Version	The EAPOL messaging protocol version supported by a port.
Number of Multi Supplicants	The number of 802.1x supplicants currently being handled by the system. The value in brackets indicates the maximum number of multi supplicants that the system will support.

Figure 43-7: Example output from the **show portauth=macbased** command

```
MAC Based Authentication System
  ----------------------------------------------------
   SystemAuthControl............ ENABLED
   Number of Supplicants.........4 (limit 480)


   Port                      PAE Status
  ----------------------------------------------------
   port1                     Enabled
   port2                     Enabled
   port3                     Enabled
   port4                     None
   port5                     None
   port6                     None
   port7                     None
   port8                     None
```

Table 43-2: Parameters in output of the **show portauth=macbased** command

Parameter	Meaning
SystemAuthControl	Whether MAC-based authentication is Enabled or Disabled.
PAE Status	Whether MAC-based authentication is Enabled or Disabled for a particular port.
Number of Supplicant	The number of MAC-based authentication supplicants currently being handled by the system. The limit value in brackets indicates the maximum number of multi supplicants that the system can handle.

Examples   To show the 802.1x capabilities of all ports on the router, use the command:

```
sh porta=802x
```

To show the MAC-based capabilities of all ports on the router, use the command:

```
sh porta=mac
```

Related Commands   **disable portauth port**
enable portauth
enable portauth port
set portauth port
set portauth port supplicantmac
show portauth counter
show portauth port
show portauth port multisupplicant
show portauth timer

show portauth counter

Syntax   SHow PORTAuth[=8021x] COUnter POrt={ALL|*port-name*}

where *port-name* is an Ethernet interface (eth0 or eth1), a port number, a range of port numbers (specified as n-m), or a comma-separated list of port numbers and/or ranges. Port numbers start at n and end at m, where n is the lower value port number and m the upper value port number, including uplink ports.

Description   This command displays counter information for ports on the router that have port authentication enabled (Figure 43-8 on page 43-50, Table 43-3 on page 43-50).

For Authenticator PAEs on a multi-supplicant system, the counters relating to each supplicant are shown separately. For PAEs acting as both a supplicant and an authenticator, the supplicant specific counters are shown separately from the authenticator specific counters.

The **portauth** parameter specifies the type of port authentication for which counters are displayed. This command only applies to 802.1x, and defaults to 802.1x if no value is specified.

The **port** parameter specifies for which port(s) information is displayed. If **all** is specified, information for all ports is displayed.

Figure 43-8: Example output from the **show portauth counter** command

```
802.1x Counters
----------------------------------------------------------------------------------
  port3
  PAE Type.................... Both

  Authenticator - Attached Supplicant(s)
    Last EAPOL Frame Source..... ff-ff-ff-ff-ff-ff
    MAC Address................... 12-34-56-78-90-12
    Last EAPOL Frame Version....... 0

        Receive                            Transmit
            EAPOL Frames...............  0   EAPOL Frames...............    0
            EAPOL Start Frames.........  0   EAP Req/Id Frames..........    0
            EAPOL Logoff Frames........  0   EAP Request Frames.........    0
            EAP Resp/Id Frames.........  0
            EAP Response Frames........  0
            EAP Length Error Frames....  0
            Invalid EAPOL Frames.......  0

    MAC Address................... ff-ee-dd-cc-bb-aa
    Last EAPOL Frame Version....... 0

        Receive                            Transmit
            EAPOL Frames...............  0   EAPOL Frames...............    0
            EAPOL Start Frames.........  0   EAP Req/Id Frames..........    0
            EAPOL Logoff Frames........  0   EAP Request Frames.........    0
            EAP Resp/Id Frames.........  0
            EAP Response Frames........  0
            EAP Length Error Frames....  0
            Invalid EAPOL Frames.......  0

  Supplicant
    Last EAPOL Frame Version.... 0
    Last EAPOL Frame Source..... ff-ff-ff-ff-ff-ff
    Receive                            Transmit
        EAPOL Frames...............  0   EAPOL Frames...............    0
        EAP Req/Id Frames..........  0   EAPOL Start Frames.........    0
        EAP Request Frames.........  0   EAPOL Logoff Frames........    0
        Invalid EAPOL Frames.......  0   EAP Resp/Id Frames.........    0
        EAP Length Error Frames....  0   EAP Response Frames........    0
```

Table 43-3: Parameters in output of the **show portauth counter** command

Parameter	Meaning
PAE Type	Whether the port is acting as an Authenticator PAE, Supplicant PAE, or Both.
Last EAPOL Frame Source	Source MAC address in the most recently received EAPOL frame.
Mac Address	An Ethernet six-octet MAC address, specifying the hardware address of the connected supplicant.
Last EAPOL Frame Version	Protocol version number in the most recently received EAPOL frame.
EAPOL Frames	The number of EAPOL frames received and transmitted.
EAPOL Start Frames	The number of EAPOL Start frames received and transmitted by the authenticator or supplicant.
EAP Resp/Id Frames	The number of EAP Resp/Id frames received and transmitted by the authenticator or supplicant.

Table 43-3: Parameters in output of the **show portauth counter** command (Continued)

Parameter	Meaning
EAP Response Frames	The number of EAP Resp/Id frames received and transmitted by the authenticator or supplicant.
EAP Length Error Frames	The number of EAP frames received by the authenticator or supplicant, where the packet body length field is invalid.
Invalid EAPOL Frames	The number of EAPOL frames received by the authenticator or supplicant, in which the frame type is not recognised.
EAP Request Frames	The number of EAP Request frames received and transmitted by the authenticator or supplicant.
EAP Req/Id Frames	The number of EAP Req/Id frames received and transmitted by the authenticator or supplicant.
EAPOL Logoff Frames	The number of EAPOL Logoff frames received and transmitted by the authenticator or supplicant.

Examples   To show the 802.1x counters associated with port 1, use the command:

```
sh porta=8021x cou po=1
```

To show the MAC-based counters associated with port 1, use the command:

```
sh porta=mac cou po=1
```

To show the counters associated with Eth 0, use the command:

```
sh porta cou po=eth0
```

Related Commands   disable portauth
enable portauth
enable portauth port
set portauth port
set portauth port supplicantmac
show portauth
show portauth port
show portauth port multisupplicant
show portauth timer

show portauth port

Syntax   SHow PORTAuth[={8021x|MACbased}] POrt={ALL|*port-name*}

where *port-name* is an Ethernet interface (eth0 or eth1), a port number, a range of port numbers (specified as n-m), or a comma-separated list of port numbers and/or ranges. Port numbers start at n and end at m, where n is the lower value port number and m the upper value port number, including uplink ports.

Description   This command displays the current configuration for ports with port authentication enabled (Figure 43-9, Table 43-4 on page 43-53).

The **portauth** parameter specifies the type of port authentication for which the port's configuration is displayed. The default is 802.1x.

The **port** parameter specifies individual ports. If **all** is specified, information for all ports is displayed.

Figure 43-9: Example output from the **show portauth=8021x port** command

```
802.1x Configuration
--------------------------------------------------------------------------------
Interface: eth0
  PAE Type.............. Both

  Multi-Supplicant Authenticator
    Default Settings
        AuthControlPortControl........ Auto
        quietPeriod................... 60
        txPeriod...................... 30
        suppTimeout................... 30
        serverTimeout................. 30
        maxReq........................ 2
        reAuthMax..................... 2
        reAuthPeriod.................. 3600
        reAuthEnabled................. False

    Attached Supplicant(s)
      MAC Address.................... 12-34-56-78-90-12
        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.................. 600
        reAuthEnabled................. False
        keyTransmissionEnabled........ False (not supported)
        operControlledDirections...... False (not supported)
```

Figure 43-9: Example output from the **show portauth=8021x port** command (Continued)

```
     Attached Supplicant(s)
       MAC Address.................... ff-ee-dd-cc-bb-aa
           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.................. 500
           reAuthEnabled................. False
           keyTransmissionEnabled........ False (not supported)
           operControlledDirections...... False (not supported)

     Supplicant
           heldPeriod.................... 60
           authPeriod.................... 30
           startPeriod................... 30
           maxStart...................... 3
           Supplicant PAE State.......... DISCONNECTED

 Interface: port1
   PAE Type.............. Supplicant
           heldPeriod.................... 60
           authPeriod.................... 30
           startPeriod................... 30
           maxStart...................... 3
           Supplicant PAE State.......... AUTHENTICATED

 Interface: port2
   PAE Type.............. Authenticator
           Authenticator PAE State....... CONNECTING
           Port Status................... unauthorised
           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)
```

Table 43-4: Parameters in output of the **show portauth=8021x port** command

Parameter	Meaning
PAE Type	The PAE Type of the port; one of "Authenticator PAE", "Supplicant PAE", or "Both".
heldPeriod	The delay period in seconds before the Supplicant PAE tries to acquire an Authenticator PAE.
authPeriod	The length of time in seconds when waiting for a reply from the Authenticator PAE.

Table 43-4: Parameters in output of the **show portauth=8021x port**
command (Continued)

Parameter	Meaning
startPeriod	The length of time in seconds between connection attempts by the Supplicant PAE.
maxStart	The maximum number of times an EAP Start message is retransmitted to the Authenticator PAE.
Supplicant PAE State	The current state of the Supplicant PAE; either "Authorised" or "Unauthorised".
Authenticator PAE State	The current state of the Authenticator PAE; one of "Initialise", "Disconnected", "Connecting", "Authenticating", "Authenticated", "Aborting", "Held", "ForceAuth", or "ForceUnAuth".
Port Status	The current state of the controlled port; either "Authorised" or "Unauthorised".
Backend Authentication State	The current state of the Backend Authentication; one of "Request", "Response", "Success", "Fail", "Timeout", "Idle", or "Initialize".
AuthControlPortControl	Whether the port's authorisation status is being administratively controlled; one of "Force Authorised", "Auto", or "Force Unauthorised".
quietPeriod	The delay period in seconds before the Authenticator PAE tries to acquire a Supplicant PAE.
txPeriod	The length in time between transmitting EAPOL PDUs.
suppTimeout	The time in seconds for which the Authenticator PAE waits for a reply from the Supplicant PAE.
serverTimeout	The time in seconds for which the Authenticator PAE waits for a reply from the authentication server.
maxReq	The maximum number of times an EAP Request packet is retransmitted to the Supplicant PAE.
reAuthMax	The maximum number of times the Authenticator PAE tries to establish contact with the supplicant PAE when no response is received.
reAuthPeriod	The time in seconds between reauthentication of the supplicant.
reAuthEnabled	Whether regular reauthentication takes place on this port.
piggyBack	An indication of whether the piggybacking of network devices onto a supplicant is allowed by an Authenticator PAE.
keyTransmissionEnabled	Whether transmission of 802.1x security keys is enabled. Not supported in this version.
OperControlledDirections	Incoming and outgoing communication is disabled on this port when the port is unauthorised.
Mac Address	An Ethernet six-octet MAC address, specifying the hardware address of the connected supplicant.
guestVlan	Displays the guest VLAN-ID if one has been specified. NONE is displayed otherwise.

Table 43-4: Parameters in output of the **show portauth=8021x port** command (Continued)

Parameter	Meaning
trap	Displays the types of events that cause SNMP traps to be sent. If Success or Both is specified, traps are sent when a supplicant is successfully authenticated and when the authentication expires. If Failure or Both is specified, traps are sent when a supplicant fails authentication. If None is specified, no traps are sent.
mibReset	Whether MIB information stored for supplicants will age out.
vlanAssignment	Whether the VLAN assignment mechanism is Enabled or Disabled. Dynamic VLAN assignment is only supported when using 802.1x authentication in single-supplicant mode.
Number of Supplicants	The number of 802.1x supplicants currently being handled by the port.

Figure 43-10: Example output from the **show portauth=macbased port** command

```
MAC Based Authentication Configuration
--------------------------------------------------------------------------------
Interface: port1
    PAE Status.................... Enabled
    Number of Supplicants ....... 2
    Default Settings
        AuthControlPortControl........ Auto
        quietPeriod ................... 60
        reAuthPeriod.................. 3600
        reAuthEnabled................. False
        trap ......................... None
        mibReset ..................... Enabled
        vlanAssignment ............... Enabled

    Attached Supplicant(s)
        MAC Address.................... 12-34-56-78-90-12
            Authenticator PAE State....... AUTHENTICATED
            Port Status................... authorised
            Backend Authenticator State... IDLE
            AuthControlPortControl........ Auto
            quietPeriod................... 60
            reAuthPeriod.................. 3600
            reAuthEnabled................. False
            trap ......................... None
            mibReset ..................... Enabled
            vlanAssignment ............... Enabled

        MAC Address.................... ff-ee-dd-cc-bb-aa
            Authenticator PAE State....... AUTHENTICATED
            Port Status................... authorised
            Backend Authenticator State... IDLE
            AuthControlPortControl........ Auto
            quietPeriod................... 60
            reAuthPeriod.................. 600
            reAuthEnabled................. False
            trap ......................... None
            mibReset ..................... Enabled
            vlanAssignment ............... Enabled
```

Table 43-5: Parameters in output of the **show portauth=macbased port** command

Parameter	Meaning
PAE Status	Whether MAC-based authentication is enabled.
Number of Supplicants	Number of MAC-based authentication supplicants currently being handled by the port.
AuthControlPortControl	Whether the port's authorisation status is being administratively controlled; one of "Force Authorised", "Auto", or "Force Unauthorised".
quietPeriod	The delay period in seconds before the Authenticator PAE tries to acquire a Supplicant PAE.
reAuthPeriod	The time in seconds between reauthentication of the supplicant.
reAuthEnabled	Whether regular reauthentication takes place on this port.
Mac Address	An Ethernet six-octet MAC address, specifying the hardware address of the connected supplicant.
Authenticator PAE State	The current state of the Authenticator PAE; one of "Initialise", "Disconnected", "Authenticating" "Authenticated"," Aborting", "Held", "ForceAuth", or "ForceUnauth".
Port Status	Whether the status of the controlled port is authorised or unauthorised.
Backend Authentication State	Current status of the Backend Authentication; either Request, Success, Fail, Timeout, Idle, or Initialise.
trap	Displays the types of events that will cause SNMP traps to be sent. When Success or Both is specified, traps are sent when a supplicant is successfully authenticated and when the authentication expires. When Failure or Both is specified, traps are sent when a supplicant fails authentication. When None is specified, no traps are sent.
mibReset	Determines whether MIB information stored for supplicants will age out.
vlanAssignment	Whether the VLAN assignment mechanism is Enabled or Disabled. Dynamic VLAN assignment is only supported when using 802.1x authentication in single-supplicant mode.
Number of Supplicants	Specifies the number of MAC-based authentication supplicants currently being handled by the port.

Examples To show the current configuration settings for port 1, use the command:

```
sh porta po=1
```

To show the current 802.1x configuration settings for Eth 0, use the command:

```
sh porta=8021x po=eth1
```

To show the current MAC-based configuration settings for Eth 0, use the command:

```
sh porta=mac po=eth1
```

Related Commands   activate portauth port reauthenticate
disable portauth
disable portauth port
enable portauth
enable portauth port
reset portauth port multimib
set portauth port
set portauth port supplicantmac
show portauth
show portauth counter
show portauth port multisupplicant
show portauth timer

show portauth port multisupplicant

Syntax SHow PORTAuth[={8021x|MACbased}] MULTIsupplicant
POrt={ALL|*port-name*} [SUPPlicantmac=*macadd*]

where *port-name* is an Ethernet port

■   *port-name* is an Ethernet interface (eth0 or eth1), a port number, a range of
port numbers (specified as n-m), or a comma-separated list of port
numbers and/or ranges. Port numbers start at n and end at m, where n is
the lower value port number and m the upper value port number,
including uplink ports.

■   *macadd* is an Ethernet six-octet MAC address, expressed as six pairs of
hexadecimal digits delimited by hyphens.

Description This command displays configuration information about each Supplicant Port
Access Entity (PAE) connected to, or configured on, the specified port. The port
must be configured as a multi-supplicant authenticator.

The default settings, representing the configuration used for all attached
supplicants that have not been configured individually using the **set portauth
port supplicantmac** command on page 43-42, along with actual settings for all
individually configured and currently attached supplicants, are displayed
(Figure 43-11 on page 43-58, Table 43-6 on page 43-59).

The **portauth** parameter specifies the type of port authentication that will have
its port's configuration displayed. The default is 802.1x.

The **port** parameter specifies the port for which port(s) information is
displayed. If **all** is specified, information for all ports is displayed.

The **supplicantmac** parameter specifies the hardware address of the connected
supplicant to display, in standard MAC format, for example 11-22-33-44-55-66.

Figure 43-11: Example output from the **show portauth=8021x port multisupplicant**
command

```
802.1x Multi-Supplicant Configuration
--------------------------------------------------------------
Interface: port1
  PAE Type...............Authenticator
  Multi-Supplicant Authenticator
    Number of Multi Supplicants......2
    Default Settings
      AuthControlPortControl........forceAuthorised
      quietPeriod...................60
      txPeriod......................30
      suppTimeout...................30
      serverTimeout.................30
      maxReq........................2
      reAuthMax.....................2
      reAuthPeriod..................120
      reAuthEnabled.................True
      trap ........................ None
      mibReset .................... Enabled
      vlanAssignment .............. Enabled
```

Figure 43-11: Example output from the **show portauth=8021x port multisupplicant** command (Continued)

```
        Attached Supplicant(s)
          MAC Address....................ba-09-87-65-43-21
           Authenticator PAE State.......AUTHENTICATED
           Port Status...................authorised
           Backend Authenticator State...INITIALISE
           AuthControlPortControl........forceAuthorised
           quietPeriod...................60
           txPeriod......................30
           suppTimeout...................30
           serverTimeout.................30
           maxReq........................2
           reAuthMax.....................2
           reAuthPeriod..................120
           reAuthEnabled.................True
           keyTransmissionEnabled........False (not supported)
           operControlledDirections......False (not supported)
           trap ........................ None
           mibReset .................... Enabled
           vlanAssignment .............. Enabled

        Attached Supplicant(s)
          MAC Address....................12-34-56-78-90-ab
           Authenticator PAE State.......AUTHENTICATED
           Port Status...................authorised
           Backend Authenticator State...INITIALISE
           AuthControlPortControl........forceAuthorised
           quietPeriod...................60
           txPeriod......................30
           suppTimeout...................30
           serverTimeout.................30
           maxReq........................2
           reAuthMax.....................3
           reAuthPeriod..................60
           reAuthEnabled.................True
           keyTransmissionEnabled........False (not supported)
           operControlledDirections......False (not supported
           trap ........................ None
           mibReset .................... Enabled
           vlanAssignment .............. Enabled
```

Table 43-6: Parameters in output of the **show portauth=8021x port multisupplicant** command

Parameter	Meaning
Mac Address	An Ethernet six-octet MAC address, specifying the hardware address of the connected supplicant.
Authenticator PAE State	The current state of the Authenticator PAE state machine.
Port Status	Whether the current status of the controlled port of an Authenticator PAE is Authorised or Unauthorised.
Backend Authenticator State	The current state of the Backend Authentication state machine.
AuthControlPortControl	The current management setting of the controlled port of an Authenticator PAE; one of "ForceUnauthorised", "Auto", or "ForceAuthorised".
quietPeriod	The delay period in seconds before the Authenticator PAE tries to acquire a Supplicant PAE.

Table 43-6: Parameters in output of the **show portauth=8021x port multisupplicant**
command (Continued)

Parameter	Meaning
txPeriod	The time in seconds between transmitting EAPOL PDUs.
suppTimeout	The time in seconds for which the Authenticator PAE waits for a reply from the Supplicant PAE.
serverTimeout	The time in seconds for which Authenticator PAE waits for a reply from the authentication server.
maxReq	The maximum number of times an EAP Request packet is retransmitted to the Supplicant PAE.
reAuthMax	The maximum number of times the authenticator PAE tries to establish contact with the supplicant PAE when no response is received.
reAuthPeriod	The time in seconds between reauthentication of the Supplicant.
reAuthEnabled	Whether regular reauthentication takes place on this port.
keyTransmissionEnabled	Whether transmission of 802.1x security keys is enabled. Not supported in this version.
adminControlledDirections	An indication of whether an unauthorised controlled port on an Authenticator PAE blocks inbound traffic or traffic in both directions.
trap	Specifies which type of events will cause SNMP traps to be sent. When Success or Both is specified, traps are sent when a supplicant is successfully authenticated and when the authentication expires. When Failure or Both, traps are sent when a supplicant fails authentication. When set to None, no traps are sent.
mibReset	Whether MIB information stored for supplicants will age out.
vlanAssignment	Specifies whether to use the VLAN assignment mechanism on this port; either "Enabled" or "Disabled". Dynamic VLAN assignment is only supported when using 802.1x authentication in single-supplicant mode.
Number of Supplicants	Specifies the number of 802.1x supplicants currently being handled by the port.

Figure 43-12: Example output from the **show portauth=macbased port multisupplicant** command

```
MAC Based Authentication Configuration
-------------------------------------------------------------------------------
Interface: port1
    PAE Status................... Enabled
    Number of Supplicants ....... 1
    Default Settings
            AuthControlPortControl........ Auto
            quietPeriod .................. 60
            reAuthPeriod.................. 3600
            reAuthEnabled................. False
            trap ......................... None
            mibReset ..................... Enabled
            vlanAssignment ............... Enabled

    Attached Supplicant(s)
        MAC Address................... 12-34-56-78-90-12
            Authenticator PAE State....... AUTHENTICATED
            Port Status................... authorised
            Backend Authenticator State... IDLE
            AuthControlPortControl........ Auto
            quietPeriod................... 60
            reAuthPeriod.................. 3600
            reAuthEnabled................. False
            trap ......................... None
            mibReset ..................... Enabled
            vlanAssignment ............... Enabled
```

Table 43-7: Parameters in output of the **show portauth=macbased port multisupplicant** command

Parameter	Meaning
PAE Status	Whether the port has been enabled for MAC-based authentication.
Number of Supplicants	The number of MAC-based authentication supplicants currently being handled by the port.
AuthControlPortControl	Whether the port's authorisation status is being administratively controlled; one of "Force Authorised", "Auto", or "Force Unauthorised".
quietPeriod	The delay period in seconds before the Authenticator PAE tries to acquire a Supplicant PAE.
reAuthPeriod	Seconds between reauthentication of the supplicant.
reAuthEnabled	Whether regular reauthentication takes place on this port.
Mac Address	An Ethernet six-octet MAC address, specifying the hardware address of the connected supplicant.
Authenticator PAE State	The current state of the Authenticator PAE; one of "Initialise", "Disconnected", "Authenticating", "Authenticated", "Aborting", "Held", "ForceAuth", or "ForceUnauth".
Port Status	The current state of the controlled port, either "Authorised" or "Unauthorised".
Backend Authentication State	The current state of the Backend Authentication; one of "Request", "Success", "Fail", "Timeout", "Idle", or "Initialize".

Table 43-7: Parameters in output of the **show portauth=macbased port multisupplicant** command (Continued)

Parameter	Meaning
trap	Specifies which type of events will cause SNMP traps to be sent. When Success or Both is specified, traps are sent when a supplicant is successfully authenticated and when the authentication expires. When Failure or Both is specified, traps are sent when a supplicant fails authentication. When set to None, no traps are sent.
mibReset	Determines whether MIB information stored for supplicants will age out.
vlanAssignment	Specifies whether to use the VLAN assignment mechanism on this port; either Enabled or Disabled. Dynamic VLAN assignment is only supported when using 802.1x authentication in single-supplicant mode.
Number of Supplicants	Specifies the number of MAC-based authentication supplicants currently being handled by the port.

Examples To show information about all Supplicant PAEs attached to the router, use the command:

```
sh porta po=all multi
```

Related Commands **activate portauth port reauthenticate**
enable portauth port
reset portauth port
set portauth port
set portauth port supplicantmac
show portauth
show portauth counter
show portauth port
show portauth timer

show portauth timer

Syntax   SHow PORTAuth[={8021x|MACbased}] TIMer POrt={ALL|
port-name}

where *port-name* is an Ethernet interface (eth0 or eth1), a port number, a range of port numbers (specified as n-m), or a comma-separated list of port numbers and/or ranges. Port numbers start at n and end at m, where n is the lower value port number and m the upper value port number, including uplink ports.

Description   This command displays the amount of time remaining in seconds until the timeout is due for each timer associated with the specified port or ports (Figure 43-13, Table 43-8).

For an authenticator Port Access Entity (PAE) on a multi-supplicant system, the timers related to each individually attached supplicant are displayed.

The **portauth** parameter specifies the type of port authentication for which port timer information is displayed. The default is 802.1x.

The **port** parameter specifies the port for which port timer information is displayed. If **all** is specified, information for all ports is displayed.

Figure 43-13: Example output from the **show portauth=8021x timer** command

```
802.1x Timers
--------------------------------------------------------------------------------
Interface: eth0                         PAE Type.............. Both
  Attached Supplicant: 12-34-56-78-90-12
     aWhile          quietWhile        reAuthWhen          txWhen
     00              00000             00000               00000

  Attached Supplicant: ff-ee-dd-cc-bb-aa
     aWhile          quietWhile        reAuthWhen          txWhen
     00              00000             00000               00000

  Supplicant
     authWhile       heldWhile         startWhen
     00              00000             00
```

Table 43-8: Parameters in output of the **show portauth=8021x timer** command

Parameter	Meaning
Attached Supplicant	An Ethernet six-octet MAC address, specifying the hardware address of the connected supplicant.
authWhile	A timer used by the Supplicant PAE state machine to determine how long to wait for a response from the authenticator before timing it out. The initial value of this timer is authPeriod.
aWhile	A timer used by the Backend Authentication state machine to determine timeout conditions in the exchanges between the authenticator and the supplicant or authentication server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.
heldWhile	A timer used by the Supplicant state machine to define periods of time during which it does not try to acquire an authenticator. The initial value of this timer is heldPeriod.
quietWhile	A timer used by the Authenticator state machine to define periods of time during which it does not try to acquire a supplicant. The initial value of this timer is quietPeriod.
reAuthWhen	A timer used by the Reauthentication Timer state machine to determine when reauthentication of the supplicant takes place. The initial value of this timer is reAuthPeriod.
startWhen	A timer used by the Supplicant PAE state machine to determine when an EAPOL-StartPDU is transmitted. The initial value of this timer is startPeriod.
txWhen	A timer used by the Authenticator PAE state machine to determine when an EAPOL PDU is transmitted. The initial value of this timer is txPeriod.

Figure 43-14: Example output from the **show portauth=macbased timer** command

```
MAC Based Authentication Timers
-------------------------------------------------------------------------------
Interface: port3

Supplicant            quietWhile        reAuthWhen
-------------------------------------------------
12-34-56-78-90-12     00000             00000
ff-ee-dd-cc-bb-aa     00000             00000

Interface: port4

Supplicant            quietWhile        reAuthWhen
-------------------------------------------------
12-34-56-12-34-56     00000             00000
aa-bb-cc-dd-ee-ff     00000             00000
```

Table 43-9: Parameters in output of the **show portauth=macbased timer** command

Parameter	Meaning
PAE Status	Whether the port has been enabled for MAC-based authentication.
Attached Supplicant	An Ethernet six-octet MAC address, specifying the hardware address of the connected supplicant.
quietWhile	A timer used by the Authenticator state machine to define periods of time during which it does not try to authenticate a supplicant. The initial value of this timer is quietPeriod.
reAuthWhen	A timer used by the Reauthentication Timer state machine to determine when reauthentication of the supplicant takes place. The initial value of this timer is ReAuthPeriod.

Examples   To show the timers for Eth 0, use the command:

```
sh porta tim po=eth0
```

Related Commands   **disable portauth port**
enable portauth
enable portauth port
set portauth port
set portauth port supplicantmac
show portauth
show portauth counter
show portauth port
show portauth port multisupplicant