Chapter 4

Port Authentication

Introduction

This chapter explains the benefits of port authentication and its applications. The router supports the implementation of IEEE 802.1x.

802.1x Port Based Network Access Control

The IEEE 802.1x standard 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 a 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

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 and ETH port are:

- supplicant
- single-supplicant authenticator, where a single supplicant is directly connected to a single authenticator
- (AR410) authenticator. Ethernet ports each support up to 10 supplicants connected to the authenticator via a hub

  On the AR410, 802.1x port authentication is supported on eth ports only.
- (AR440S, AR441S, AR450S) authenticator. The VLAN ports each support a single supplicant, and the Ethernet ports each support up to 10 supplicants connected to the authenticator via a hub. 802.1x port authentication is supported on all switch and eth ports.

Configuration on a Single-Supplicant System

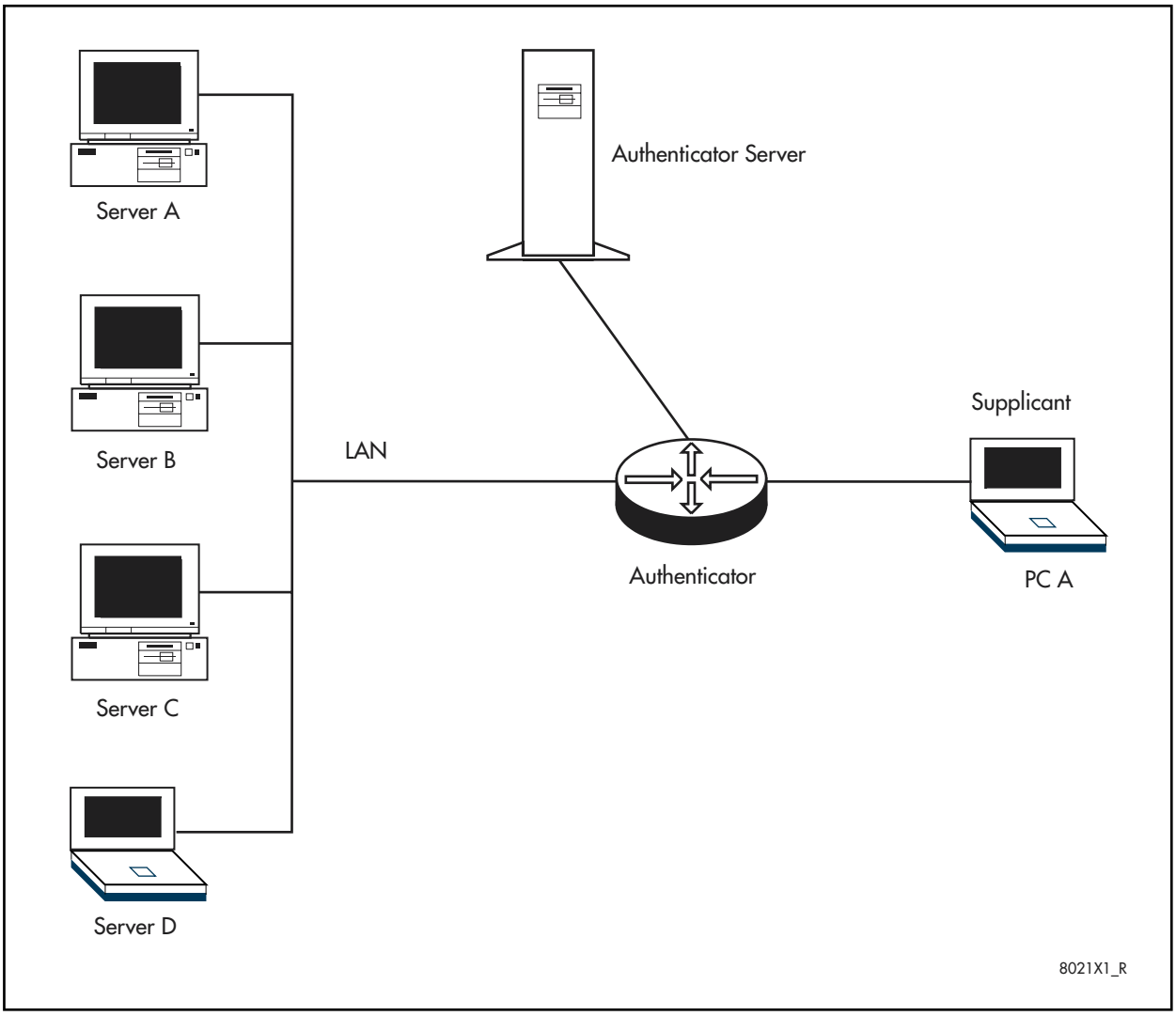
A single supplicant configuration giving true 802.1x functionality is shown in Figure 4-1 on page 4-4. In this example, PC A wants to use services offered by servers on the LAN behind the router acting as an authenticator. PC A is connected to a port on the router that has 802.1x control enabled. Therefore, 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 AR450, piggybacking can be disabled on Ethernet ports only.

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

Figure 4-1: Single Supplicant 802.1x Configuration

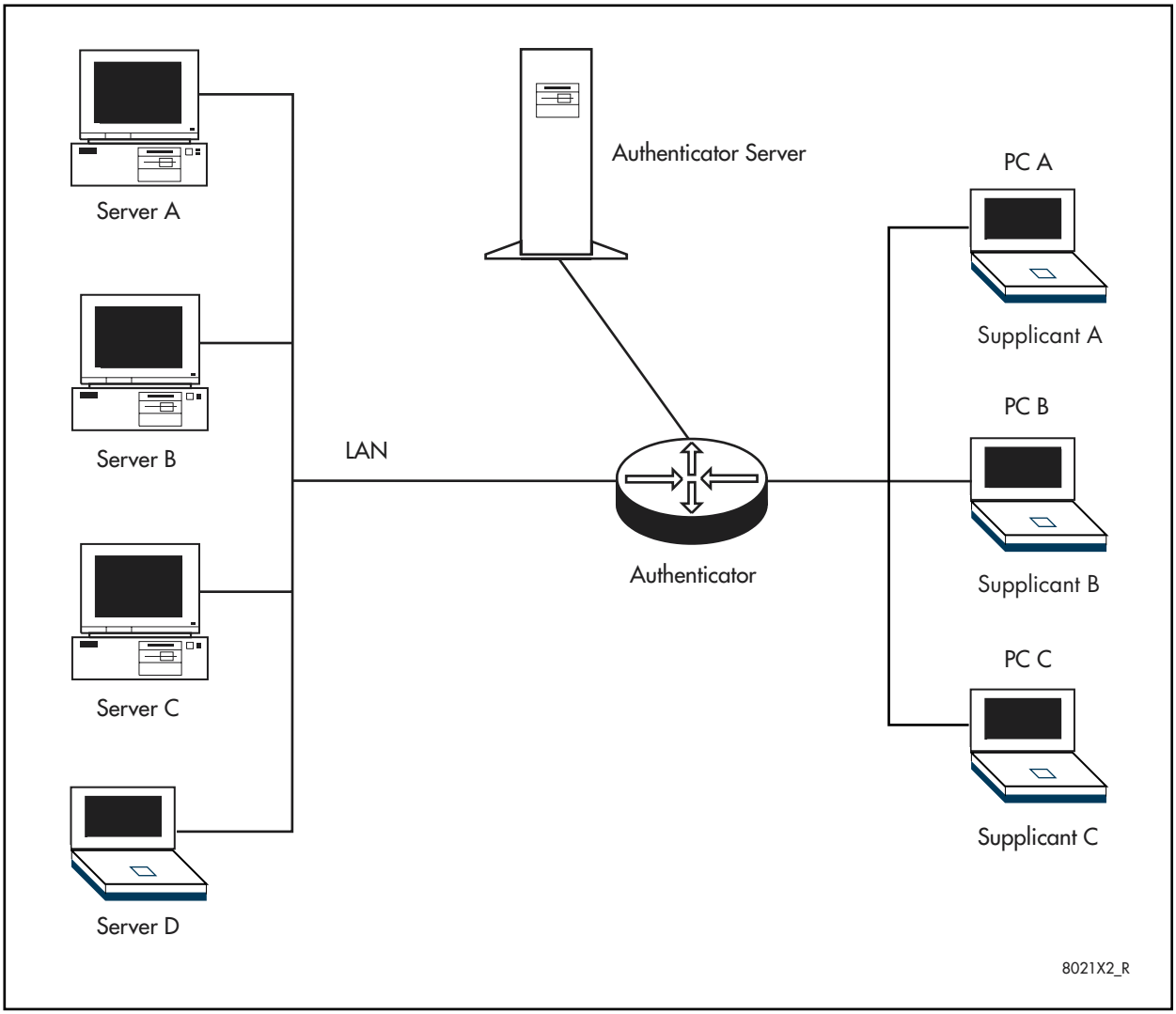


Configuration on a Multi-supplicant System

A multi-supplicant configuration with 802.1x functionality is shown in Figure 4-2 on page 4-5. 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.

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

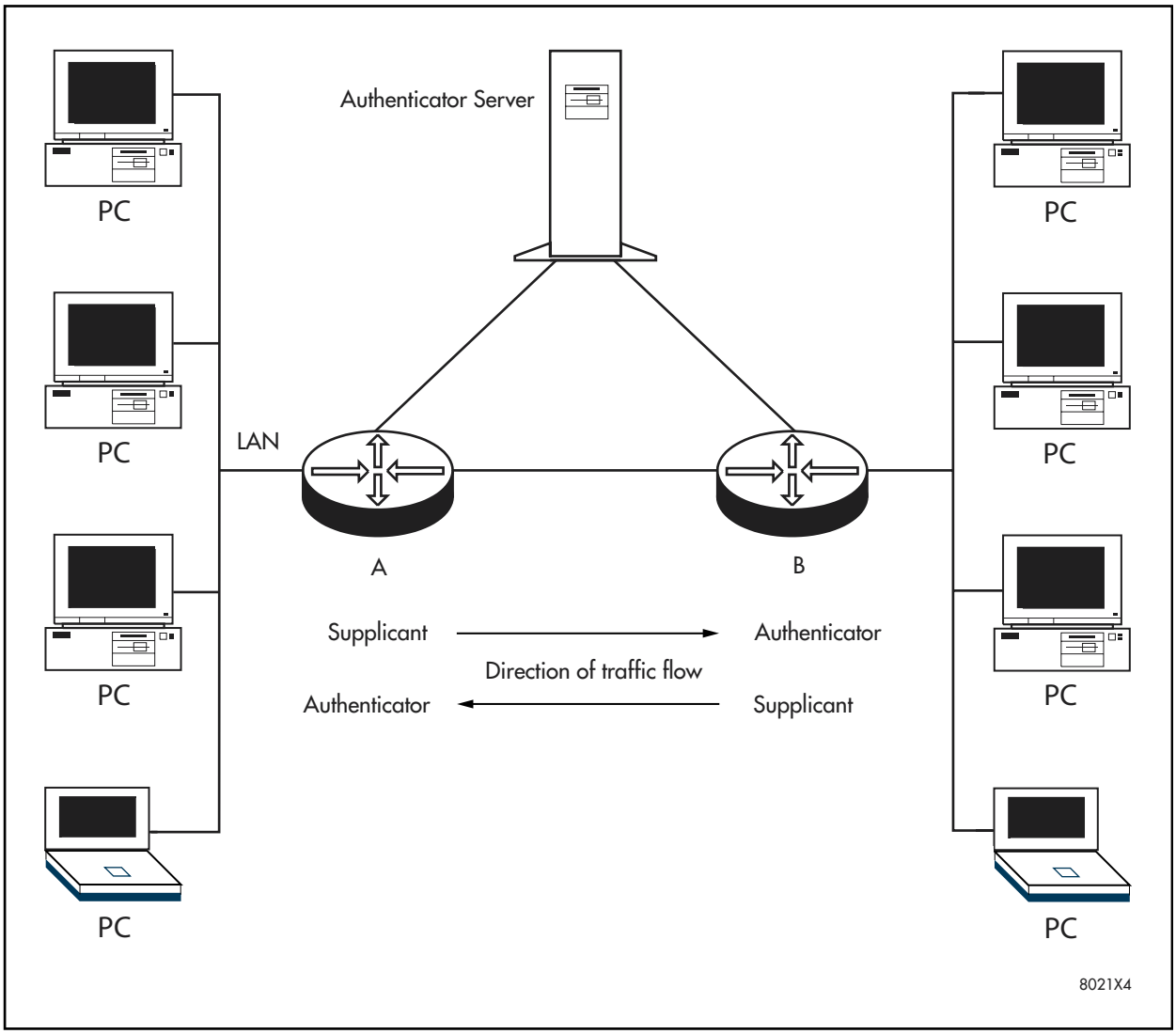
Figure 4-2: Multi-Supplicant 802.1x Configuration



Supplicant and Authenticator Configuration

Routers acting as both supplicant and authenticator are shown in Figure 4-3 on page 4-6. 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 4-3: 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 termed a Supplicant PAE. The PAE controlling a port acting as an authenticator is termed 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 Figure 4-4 on page 4-8. 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.

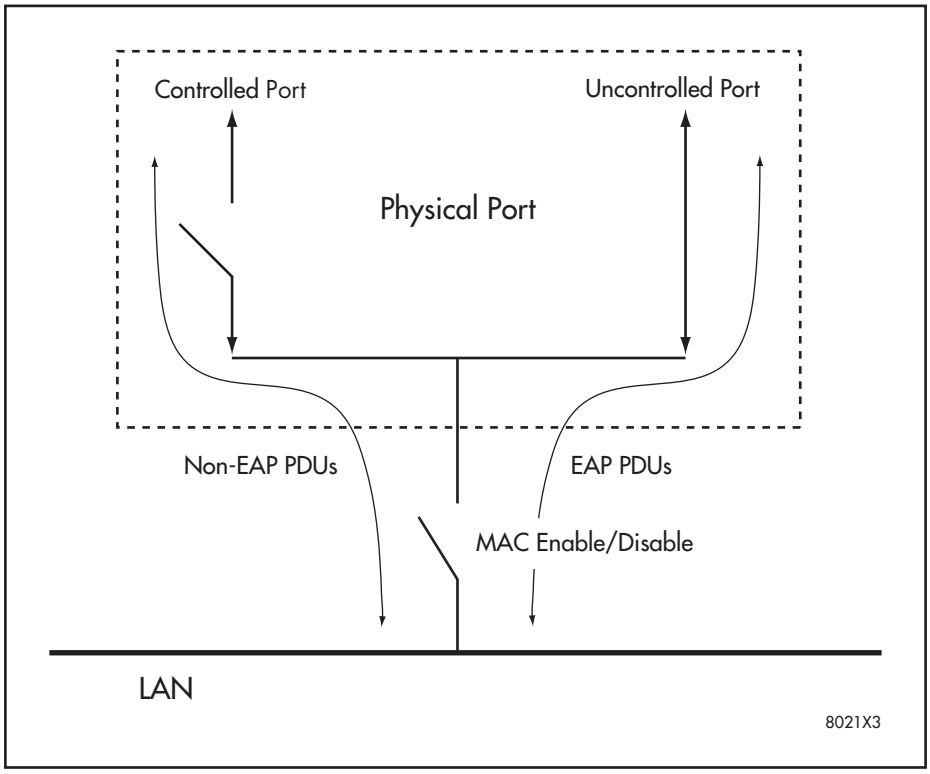
The Authenticator PAE can be configured to request that the Supplicant PAE reauthenticate itself at a configurable time period. During the process of reauthentication, the controlled port remains authorised until reauthentication fails.

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 10 Supplicant PAEs may be attached to a single Authenticator PAE.

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.

A multi-supplicant configuration does not conform to IEEE 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 4-4: 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 1-22 of Chapter 1, Operation.

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.
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.

On the AR450S, setting PIGGYBACK to FALSE is only valid on Ethernet ports.

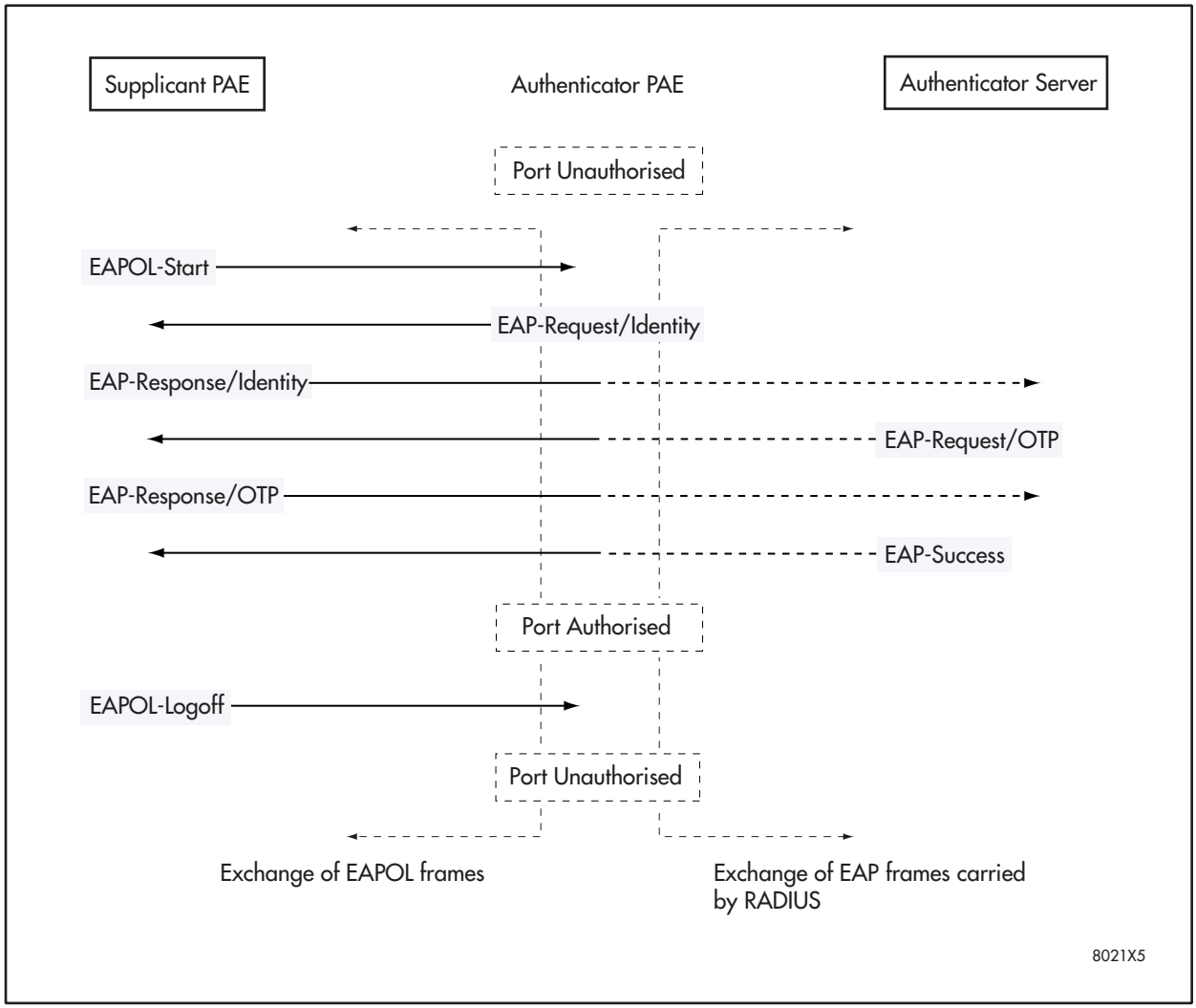
On the AR750S, setting PIGGYBACK to FALSE is only valid on Ethernet ports.

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 4-5 on page 4-10.

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 4-5: Authentication Messaging Exchange Initiated by the Supplicant



802.1x on the Router

This section describes how the router implements 802.1x port control and how to configure the router.

Enable 802.1x on the router

The implementation of 802.1x on the router is disabled by default. To enable 802.1x, use the command:

```
enable portauth
```

To disable 802.1x, use the command:

```
disable portauth
```

Enable 802.1x on a port

To enable specific ports to act as an authenticator, use the command:

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

On the AR410, 802.1x port authentication is supported on eth ports only. On the AR440S, AR441S and AR450, 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 port(s) to act as a supplicant, use the command:

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

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

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

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

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

*On the AR450S, **multi** can be specified for Ethernet ports only.*Setting the **mode** parameter to **multi** does not conform to IEEE 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 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 AR450S, piggybacking can only be disabled on Ethernet ports.

To change the configuration parameters for a port(s) under 802.1x port control, use the commands:

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

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

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

To disable 802.1x port control on a specified port(s), use the command:

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

To reinitialise 802.1x port control on a specified port(s), use the command:

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

To purge all 802.1x port configurations for a specified port(s), use the command:

```
purge portauth port={all|portname}
```

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

```
show portauth
```

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

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

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

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

set portauth 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**.

Set a global 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 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. Also, keep configuration file backups secure because passwords are in plaintext in configuration files.

Debug 802.1x

To enable the output of 802.1x debug information on a port or ports, use the command:

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

To disable the output of 802.1x debug information on a port or ports, use the command:

```
disable portauth debug={all|packet|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.

A multi-supplicant configuration does not conform to IEEE 802.1x and introduces security risks. To minimise the risk of unauthorised access and denial-of-service attacks 802.1x control in a multi-supplicant configuration is not recommended.

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

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

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

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 the command:

```
set portauth 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]]|[default]}
```

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

set portauth port={all|port-name} type=authenticator
    [mode=multi] [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 802.1x port control on a specified port(s) connected to multiple supplicants, use the command:

```
reset portauth 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:

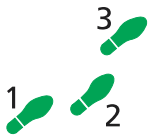
```
show portauth multisupplicant port={all|port-name}
```

Configuration Examples

The following examples illustrate how to configure 802.1x port authentication on the router. The first example shows how to configure a port as an authenticator; the second shows how to configure a port as a supplicant.

Port as an Authenticator

This example demonstrates how to configure a port on the router as an authenticator.



To configure a port on the router as an 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 14, 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 1-62 of Chapter 1, Operation.

3. **Enable 802.1x port control on the router.**

   Enable 802.1x by using the command:

   ```
   enable portauth
   ```

4. **Enable 802.1x port control on a port.**

   Enable 802.1x on the port you want to configure as an authenticator by using the command:

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

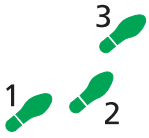
5. **Show the 802.1x port control configuration for the port.**

   Show the 802.1x port control configuration for the port by using the command:

   ```
   show portauth port=port-name
   ```

Port as a Supplicant

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



To configure a port on the router as an supplicant

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 14, Internet Protocol (IP).

2. **Enable 802.1x port control on the router.**

   Enable 802.1x by using the command:

   ```
   enable portauth
   ```

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 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.

   When you enter passwords ensure you do so in a secure environment as passwords appear on the screen as typed. Also, keep configuration file backups secure because passwords appear in plain text in configuration files.

4. **Enable 802.1x port control on a port.**

   Enable 802.1x on the port you want to configure as an supplicant by using the command:

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

5. **Show the 802.1x port control configuration for the port.**

   Show the 802.1x port control configuration for the port by using the command:

   ```
   show portauth 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 xcv of Preface 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.

On the AR410, 802.1x port authentication is supported on eth ports only. On the AR440S, AR441S and AR450, 802.1x port authentication is supported on all switch and eth ports.

activate portauth port reauthenticate

Syntax

```
ACTivate PORTAuth POrt={ALL|port-name} REAUTHENTicate
   [SUPPLicantmac=macadd]
```

where:

- 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.

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 (PAE's).

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 supplicants connected to eth 1, use the command:

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

Related Commands

disable portauth debug port
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
```

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 on page 4-20.

Examples

To disable 802.1x functionality on the router, use the command:

```
dis porta
```

Related Commands

disable portauth port
enable portauth
enable portauth port
purge portauth port
show portauth port

disable portauth debug port

Syntax

```
DISable PORTAuth 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 the display of debugging port authentication information on ports.

The DEBUG parameter specifies the type of 802.1x port authentication debug information to stop being output to the console. If STATE is specified the output of state changes in the 802.1x state machines for the specified port(s) is disabled. If PACKET is specified, the output of 802.1x EAP packet headers transmitted or received by a specific port is disabled. If ALL is specified all 802.1x debug output for the port is disabled.

The PORT parameter specifies the port for which debugging output is disabled. If ALL is specified, debugging information for all ports on the device is disabled.

Examples

To disable port authentication state machine debug output for eth 1, use the command:

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

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

disable portauth port

Syntax
```
DISable PORTAuth [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 on page 4-19.

The PORT parameter specifies the port(s) on which port authentication is disabled. If ALL is specified, port authentication is disabled on all ports.

Examples
To disable port authentication on eth 1, use the command:

```
dis porta 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
```

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 on page 4-22.

Examples
To enable 802.1x functionality on the router, use the command:

```
ena porta
```

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 port

Syntax

```
ENAble PORTAuth 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 the output of port authentication debug information on the specified port.

The DEBUG parameter specifies the type of debug information displayed. If ALL is specified both packet and state debugging for the specified port(s) 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. If STATE is specified, all state machine changes for the specified port(s) are echoed to the console.

The PORT parameter specifies the port for which debugging information is displayed. If ALL is specified, debugging information for all ports is displayed.

Examples

To show debug state information for eth 0, use the command:

```
ena porta deb=st po=eth1
```

Related Commands

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

enable portauth port

Syntax

```
ENAble PORTAuth POrt={ALL|port-name} 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]

ENAble PORTAuth POrt={ALL|port-name} 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}]]

ENAble PORTAuth POrt={ALL|port-name} 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}]]
```

where:

- 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.
- *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 the port authentication functionality on ports. A port can be enabled as an authenticator, supplicant, or both.

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

The PORT parameter specifies the port to enable with port authentication. If ALL is specified, all ports on the router are enabled.

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. 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 TYPE parameter specifies SUPPLICANT, or 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 MODE parameter is used when the TYPE parameter specifies AUTHENTICATOR or 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 TYPE parameter specifies SUPPLICANT, or 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 TYPE parameter specifies AUTHENTICATOR, or 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 TYPE parameter specifies SUPPLICANT, or 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 TYPE parameter specifies AUTHENTICATOR and the port(s) are acting in an authenticator role. 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.

Setting the MODE parameter to MULTI does not conform to IEEE 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 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 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 the TYPE parameter specifies AUTHENTICATOR, or 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 the TYPE parameter specifies AUTHENTICATOR, or 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 the TYPE parameter specifies AUTHENTICATOR, or 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 TYPE parameter specifies AUTHENTICATOR, or 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 TYPE parameter specifies AUTHENTICATOR, or 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 TYPE parameter specifies SUPPLICANT, or 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 TYPE parameter specifies AUTHENTICATOR, or 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 TYPE parameter specifies AUTHENTICATOR, or 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 TYPE parameter specifies SUPPLICANT, or 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 4-34 to set a global username and a global password for all supplicants.

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 TYPE parameter specifies SUPPLICANT, or 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 can is used when the TYPE parameter specifies SUPPLICANT, or 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.

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
show portauth
show portauth counter
show portauth port
show portauth port multisupplicant
show portauth timer

purge portauth port

Syntax `PURge PORTAuth 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 or ports.

The PORT parameter specifies which port to purge. Specifying the value ALL purges all ports on the router.

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

```
pur porta po=all
```

Related Commands
disable portauth
enable portauth
show portauth port

reset portauth port

Syntax

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

where:

- 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 the port authentication functionality on the specified port or ports.

The PORT parameter specifies the port or ports to be reset. If ALL is specified, all ports on the router 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 eth 0, use the command:

```
reset porta 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 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 4-32.

This command applies only to ports that act as an authenticator in a multi-supplicant configuration.

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.

Examples To remove all unused multi-supplicant MIB entries associated with eth 0, use the command:

```
reset porta 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 POrt={ALL|port-name} 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]

SET PORTAuth POrt={ALL|port-name} 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}]]

SET PORTAuth POrt={ALL|port-name} 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}]]
```

where:

- 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.
- *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 the port authentication functionality on ports. A port can be set as an authenticator, supplicant, or both. Port authentication must already be enabled on the port.

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

The PORT parameter specifies the port to set with port authentication. If ALL is specified, all ports on the router are set.

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. 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 TYPE parameter specifies SUPPLICANT, or 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 MODE parameter is used when the TYPE parameter specifies AUTHENTICATOR or 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 trying to re-contact an Authenticator PAE, if an authentication attempt fails due to an invalid username/password combination. The HELDPERIOD parameter is used when the TYPE parameter specifies SUPPLICANT, or 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 attempts to retransmit an EAP request packet to the Supplicant PAE if no response is received. The MAXREQ parameter is used when the TYPE parameter specifies AUTHENTICATOR, or 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 that are sent before the supplicant assumes no authenticator is present. The MAXSTART parameter is used when the TYPE parameter specifies SUPPLICANT, or 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 TYPE parameter specifies AUTHENTICATOR and the port(s) are acting in an authenticator role. 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.

Setting the MODE parameter to MULTI does not conform to IEEE 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 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 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 the TYPE parameter specifies AUTHENTICATOR, or 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 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 the TYPE parameter specifies AUTHENTICATOR, or 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 the TYPE parameter specifies AUTHENTICATOR, or 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 TYPE parameter specifies AUTHENTICATOR, or 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 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 TYPE parameter specifies AUTHENTICATOR, or 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 TYPE parameter specifies SUPPLICANT, or 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 TYPE parameter specifies AUTHENTICATOR, or 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 TYPE parameter specifies AUTHENTICATOR, or 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 acts in a supplicant role. The USERNAME parameter is used when the TYPE parameter specifies SUPPLICANT, or 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 4-34 to set a global username and a global password for all supplicants.

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 TYPE parameter specifies SUPPLICANT, or 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 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 TYPE parameter specifies SUPPLICANT, or 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 default is MD5 encryption.

Examples To modify the current QUIETPERIOD setting on eth 0, use the command:

```
set porta 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
show portauth
show portauth counter
show portauth port
show portauth port multisupplicant
show portauth timer

set portauth port supplicantmac

Syntax

```
SET PORTAuth 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]]]|[DEFault]}
```

where:

- 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). 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 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 device.

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. 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 is AUTO.

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 valid range of integer values is 1 to 10. The default is 2.

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. 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 default is 60.

The REAUTHENABLED parameter specifies whether the Authenticator PAE requires the Supplicant PAE to undergo periodic reauthentication. The default is FALSE.

The REAUTHPERIOD parameter specifies the time between reauthentications of the Supplicant PAE if the REAUTHENABLED parameter is set to TRUE. The valid range of integer values is 1 to 86400. The default is 3600.

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 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 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 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 valid range of integer values is 1 to 65535. The default is 30.

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
show portauth counter
show portauth port

set portauth username

Syntax

```
SET PORTAuth 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** command on page 4-28 to set specific supplicant passwords and usernames.

The USERNAME parameter specifies the global default login name to be used during authentication by any defined supplicant on the device 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.

When you enter passwords ensure you do so in a secure environment as 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 specified 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 entered 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 ENCRYPTION parameter specifies the method for generating one-time passwords by defined supplicants on the device 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.

The METHOD parameter specifies the method used to encrypt the username and password during authentication attempts by any defined supplicant on the device 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.

Examples

To set the global port authentication username and password on the router, use the command:

```
set porta 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`

Description This command displays information about the each port's capabilities and protocol implementation detail (See Figure 4-6 on page 4-36 and Table 4-1 on page 4-36).

Figure 4-6: Example output from the **show portauth** command

```
802.1X System
-------------------------------------------------
  SystemAuthControl.............. ENABLED
  Global Username................ portAuthPortAuth
  Global Password................ portAuthPortAuth
  Global Encryption Method..... OTP
  Global Encryption Type....... MD5


  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 4-1: Parameters in the output of the **show portauth** command

Parameter	Meaning
SystemAuthControl	Whether port authentication is enabled or disabled.
Global Username	The global port authentication username used by all Supplicant PAE's on the device that do not have their own unique username defined.
Global Password	The global port authentication password used by all Supplicant PAE's on the device that do not have their own unique password defined.
Global Encryption Method	The password transmission method used by all Supplicant PAE's using the global username and password - either Standard or OTP.
Global Encryption Type	The password encryption method used by all Supplicant PAE's 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 - either Authenticator, Supplicant, Both, or None.
Protocol Version	The EAPOL messaging protocol version supported by a port.

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

```
sh porta
```

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 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 (See Figure 4-7 on page 4-38 and Table 4-2 on page 4-39).

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

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

Figure 4-7: 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 4-2: Parameters in the 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 EAP frames received and transmitted.
EAPOL Start Frames	The number of EAP 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.
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 EAP 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 EAP Logoff frames received and transmitted by the authenticator or supplicant.

Examples 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 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 (See Figure 4-8 on page 4-41 and Table 4-3 on page 4-42).

The PORT parameter specifies individual ports. If ALL is specified, information for all ports is displayed.

Figure 4-8: Example output from the **show portauth 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....... INITIALISE
          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)

    Attached Supplicant(s)
      MAC Address..................... ff-ee-dd-cc-bb-aa
          Authenticator PAE State....... INITIALISE
          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
```

Figure 4-8: Example output from the **show portauth port** command (continued)

```
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 4-3: Parameters in the output of the **show portauth port** command

Parameter	Meaning
PAE Type	Whether the port is acting as an 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.
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	Whether the current state of the Supplicant PAE is Authorised or Unauthorised.
Authenticator PAE State	The current state of the Authenticator PAE: Initialize Disconnected Connecting Authenticating Authenticated Aborting Held Force authenticated Force unauthorised

Table 4-3: Parameters in the output of the **show portauth port** command (continued)

Parameter	Meaning
Port Status	Whether the current state of the controlled port is Authorised or Unauthorised.
Backed Authentication State	The current state of the Backed Authentication: Request Response Success Fail Timeout Idle Initialize
AuthControlPortControl	Whether the port's authorisation status is being administratively controlled; either 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 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 release.
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.

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

```
sh porta 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 MULTIsupplicant POrt={ALL|port-name}
```

where *port-name* is an Ethernet port

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 4-32, along with actual settings for all individually configured and currently attached supplicants, are displayed (See Figure 4-9 on page 4-45 and Figure 4-4 on page 4-45).

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

Figure 4-9: Example output from the **show portauth port multisupplicant** command

```
802.1X Multi-Supplicant Configuration
---------------------------------------------------------------
Interface: port1
  PAE Type..............Authenticator

  Multi-Supplicant Authenticator
    Default Settings
       AuthControlPortControl........forceAuthorised
       quietPeriod...................60
       txPeriod......................30
       suppTimeout...................30
       serverTimeout.................30
       maxReq........................2
       reAuthMax.....................2
       reAuthPeriod..................120
       reAuthEnabled.................True

    Attached Supplicant(s)
      MAC Address.....................ba-09-87-65-43-21
       Authenticator PAE State.......INITIALISE
       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)

    Attached Supplicant(s)
      MAC Address.....................12-34-56-78-90-ab
       Authenticator PAE State.......INITIALISE
       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)
```

Table 4-4: Parameters in the output of the **show portauth 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.

Table 4-4: Parameters in the output of the **show portauth port multisupplicant** command (continued)

Parameter	Meaning
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; either ForceUnauthorised, Auto, or ForceAuthorised.
quietPeriod	The delay period in seconds before the Authenticator PAE tries to acquire a Supplicant PAE.
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 release.
adminControlledDirections	An indication of whether an unauthorised controlled port on an Authenticator PAE blocks inbound traffic or traffic in both directions.

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 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 (See Figure 4-10 on page 4-47 and Table 4-5 on page 4-48).

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

The PORT parameter specifies for which port information is displayed. If ALL is specified, information for all ports is displayed.

Figure 4-10: Example output from the **show portauth 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 4-5: Parameters in the output of the **show portauth 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.

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