

cnMatrix 802.1X Authentication Parameters and Commands

Commands	Description	CLI Mode
<code>aaa authentication dot1x default group { radius local}</code>	Enables the dot1x local authentication or RADIUS server based remote authentication method for all ports. The actual authentication of the supplicant happens at the authentication server.	Global Configuration
<code>dot1x local-database <username> password <password> permission {allow deny} [<auth-timeout (value(1-7200))>] [interface <interface-type> <interface-list>]</code>	Configures dot1x authentication server local database with user name and password.	Global Configuration
<code>set nas-id <identifier></code>	Sets the dot1x network access server id. Network Access Server Identifier is set in the RADIUS packets sent to the Remote Authentication Server Maximum length of the string is 16.	Global Configuration
<code>dot1x system-auth-control</code>	Enables dot1x in the switch. The dot1x is an authentication mechanism. It acts as mediator between the authentication server and the supplicant (client). If the client accesses the protected resources, it contacts the authenticator with EAPOL frames.	Global Configuration
<code>dot1x init-session <supp addr - aa:aa:aa:aa:aa:aa></code>	Initiates dot1x authentication session for the given MAC address of the supplicant. The supplicant requests for access to the protected network. It sends EAPOL (Extensible Authentication Protocol) frames to the authenticator. When the supplicant is authorized by the remote server, the session is initiated.	Global Configuration
<code>dot1x init session-reauth <supp addr - aa:aa:aa:aa:aa:aa ></code>	Initiates dot1x re-authentication session for the specified MAC address. When the supplicant has exceeded the time limit for accessing the protected network, the supplicant is forced for re-authentication. This is to ensure that the supplicant is the same entity that was initially authenticated.	Global Configuration
<code>dot1x default</code>	Configures dot1x with default values for this port. The previous configurations on this port are reset to the default values. These details are not displayed but are the basic settings for a port.	Interface Configuration (Physical interface)
<code>dot1x max-req <count(1-10)></code>	Sets the maximum number of EAP (Extensible Authentication Protocol) retries to the client by the authenticator before restarting authentication process. The count value ranges between 1 and 10.	Interface Configuration (Physical interface)

Commands	Description	CLI Mode
<code>dot1x max-start <count(1-65535)></code>	This command sets the maximum number of EAPOL retries to the authenticator. The value range is 1 to 65535.	Interface Configuration (Physical interface)
<code>dot1x reauthentication</code>	Enables periodic re-authentication from authenticator to client. The periodic re-authentication is requested to ensure if the same supplicant is accessing the protected resources. The amount of time between periodic re-authentication attempts can be configured manually.	Interface Configuration (Physical interface)
<code>dot1x timeout {quiet-period <value (0-65535)> {reauth-period server-timeout supp-timeout tx-period start-period held-period auth-period }<value (1-65535)>}</code>	Sets the dot1x timers. The timer module manages timers, creates memory pool for timers, creates timer list, starts and stops timer. It provides handlers to respective expired timers.	Interface Configuration (Physical interface)
<code>dot1x port-control {auto force-authorized force-unauthorized}</code>	Configures the authenticator port control parameter. The dot1x exercises port based authentication to increase the security of the network. The different Modes employed to the ports offer varied access levels. The 802.1x protocol is supported on both Layer 2 static-access ports and Layer 3 routed ports	Interface Configuration (Physical interface)
<code>dot1x access-control {active inactive}</code>	Configures the supplicant access control. This setting is for the application of the Supplicant authorization state when the port is operating as both Supplicant and Authenticator.	Interface Configuration (Physical interface)
<code>dot1x control-direction {in both}</code>	Configures port control direction.. The switch port authenticates incoming packets and outgoing packets. The direction can be configured manually by selecting either in or both. By default the value is both.	Interface Configuration (Physical interface)
<code>dot1x host-Mode {multi-host single-host}</code>	Configures the port authentication Mode of a port as either multi-host (which is also known as port-based) or single-host (which is also known as mac-based). Multi host authentication has different Modes of authentication. Single host authentication allows secured mac addresses to pass through the port. Non secure mac addresses are dropped.	Interface Configuration (Physical interface)
<code>dot1x re-authenticate [interface <interface-type><interface-id>]</code>	Initiates re-authentication of all dot1x-enabled ports or the specified dot1x-enabled port. This initializes the state machines and sets up the environment for fresh authentication. Re-authentication is manually configured if periodic re-authentication is not enabled. Re-authentication is requested by the authentication server to the supplicant to furnish the identity without waiting for the configured number of seconds (re-authperiod). If no interface is specified, re-authentication is initiated on all dot1x ports	Privileged EXEC

Commands	Description	CLI Mode
<pre>dot1x initialize [interface <interface-type> <interface-id>]</pre>	<p>Initializes the state machines and sets up the environment for fresh authentication. This initiates re-authentication of all dot1x-enabled ports or the specified dot1x-enabled port.</p> <p>Re-authentication is manually configured if periodic re-authentication is not enabled. Re-authentication is requested by the authentication server to the supplicant to furnish the identity without waiting for the configured number of seconds (re-authperiod). If no interface is specified, re-authentication is initiated on all dot1x ports</p>	Privileged EXEC
<pre>debug dot1x {all errors events packets state-machine redundancy registry }</pre>	<p>This command enables debugging of dot1x module. The failure messages and error information are captured by the debug traces. Different traces are enabled to capture particular performance failures. Only one trace can be enabled at a time.</p>	Privileged EXEC
<pre>show dot1x [{ interface <interface-type> <interface-id> statistics interface <interface-type> <interface-id> supplicant-statistics interface <interface-type> <interface-id> local-database mac-info [address <aa.aa.aa.aa.aa.aa>] mac- statistics [address <aa.aa.aa.aa.aa.aa>] all]}]</pre>	<p>Displays dot1x information. The configured information can be viewed by running this show command. When there is any change in the configuration to ensure that the port is configured as desired, the show command is used.</p>	Privileged EXEC
<pre>dot1x clear statistics [interface <iftype> <ifnum>][mac-statistics address <mac_addr>]</pre>	<p>Clears dot1x statistics information.</p>	Privileged EXEC