define interface-range

To create an interface-range macro, use the **define interface-range** command.

define interface-range *macro-name interface-range*

Syntax Description

macro-name	Name of the interface range macro; the macro name can contain up to 32 characters.
interface-range	Interface range; for a list of valid values for interface ranges, see the "Usage Guidelines" section.

Command Default

This command has no default settings.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The macro name is a 32-character maximum character string.

A macro can contain up to five ranges. An interface range cannot span slots. When entering the *interface-range*, these formats can be used:

- *card-type* {*slot*}/{*first-interface*} - {*last-interface*}
- *card-type* {*slot*}/{*first-interface*} - {*last-interface*}

Valid values for *card-type* are as follows:

- **ethernet**
- **fastethernet**
- **gigabitethernet**
- **loopback**
- **tengigabitethernet**
- **tunnel**
- **vlan** *vlan-id* (valid values are from 1 to 4094)
- **port-channel** *interface-number* (valid values are from 1 to 256)

Examples

This example shows how to create a multiple-interface macro:

```
Router(config)# define interface-range macro1 ethernet 1/2 - 5, fastethernet 5/5 - 10
Router(config)#
```

Related Commands

Command	Description
interface range	Executes a command on multiple ports at the same time.

diagnostic bootup level

To set the bootup diagnostic level, use the **diagnostic bootup level** command. To skip all diagnostic tests, use the **no** form of this command.

diagnostic bootup level {**minimal** | **complete**}

default diagnostic bootup level

no diagnostic bootup level

Syntax Description

minimal	Specifies minimal diagnostics; see the "Usage Guidelines" section for additional information.
complete	Specifies complete diagnostics; see the "Usage Guidelines" section for additional information.
default	Returns to the default setting.

Command Default

minimal

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Setting the diagnostic level determines the level of testing that occurs when the system or module is reset. The two levels are as follows:

- Complete—Runs all tests.
- Minimal—Runs only EARL tests for the supervisor engine and loopback tests for all ports in the system.

Note Although the default is **minimal**, you can set the diagnostic level to **complete** for troubleshooting hardware problems.

In certain circumstances, you might want to skip the bootup online diagnostics completely. For example, you might skip the bootup online diagnostics to verify that a port is as bad as online diagnostics reports. To skip online diagnostic testing completely, enter the **no diagnostic bootup level** command.

For information on the diagnostic test types, see the **show diagnostic** command.

The new level takes effect at the next reload or the next time that an online insertion and removal is performed.

Examples

This example shows how to set the bootup diagnostic level:

```
Router(config)# diagnostic bootup level complete
Router(config)#
```

Related Commands

Command	Description
show diagnostic bootup level	Displays the coverage level for the configured boot-up diagnostics.

diagnostic cns

To configure the CNS diagnostics, use the **diagnostic cns** command. To disable sending diagnostic results to the CNS event bus, use the **no** form of this command.

diagnostic cns {**publish** | **subscribe**} [*subject*]

default diagnostic cns {**publish** | **subscribe**}

no diagnostic cns {**publish** | **subscribe**} [*subject*]

Syntax Description

publish	Sends diagnostic results to a remote network application to make decisions and take corrective actions that are based on the diagnostic results.
subscribe	Receives messages from remote network applications to perform diagnostic tests or retrieve diagnostic results.
subject	(Optional) Event subject name.
default	Sets the default.

Command Modes

This command has no default settings.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The online diagnostics receive events by subscribing to an event *subject* name. The *subject* is the event that you subscribe (receive) or publish (generate) through the CNS bus.

The **diagnostic cns publish** command sends diagnostic results to a remote network application to make decisions and take corrective actions that are based on the diagnostic results.

The **diagnostic cns subscribe** command receives messages from remote network applications to perform diagnostic tests or retrieve diagnostic results.

Examples

This example shows how to enable the publishing of diagnostic results:

```
Router(config)# diagnostic cns publish
Router(config)#
```

This example shows how to receive messages from remote network applications to perform diagnostic tests or retrieve diagnostic results:

```
Router(config)# diagnostic cns subscribe
Router(config)#
```

This example shows how to set the default to **publish**:

```
Router(config)# default diagnostic cns publish
Router(config)#
```

Command Default

Command	Description
show diagnostic cns	Displays the information about the CNS subject.

diagnostic event-log size

To modify the diagnostic event-log size dynamically, use the **diagnostic event-log size** command. To return to the default settings, use the **no** form of this command.

diagnostic event-log size *size*

default diagnostic event-log size

no diagnostic event-log size

Syntax Description

size	Diagnostic event-log size; valid values are from 1 to 10000 entries.
default	Returns to the default setting.

Command Default

The *size* is **500** entries.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The events are dynamically allocated and stored in a circular queue.

You can enter either the **default diagnostic event-log size** command or the **no diagnostic event-log size** command to return to the default settings.

Examples

This example shows how to set the diagnostic event-log size:

```
Router(config)# diagnostic event-log size 600
Router(config)#
```

Related Commands

Command	Description
show diagnostic events	Displays the event log for the diagnostic events.

diagnostic monitor

To configure the health-monitoring diagnostic testing, use the **diagnostic monitor** command. To disable testing, use the **no** form of this command.

diagnostic monitor interval {**module** *num*} **test** {*test-id* | *test-id-range* | **all**} [**hour** *hh*] [**min** *mm*] [**second** *ss*] [**millisec** *ms*] [**day** *day*]

diagnostic monitor syslog

diagnostic monitor {**module** *num*} **test** {*test-id* | *test-id-range* | **all**}

no diagnostic monitor {**interval** | **syslog**}

Syntax Description

interval	Sets the interval between testing.
module *num*	Specifies the module number.
test	Specifies a test to run.
test-id	Identification number for the test to be run; see the "Usage Guidelines" section for additional information.
test-id-range	Range of identification numbers for tests to be run; see the "Usage Guidelines" section for additional information.
all	Runs all the diagnostic tests.
hour *hh*	(Optional) Specifies the number of hours between tests; see the "Usage Guidelines" section for formatting guidelines.
min *mm*	(Optional) Specifies the number of minutes between tests; see the "Usage Guidelines" section for formatting guidelines.
second *ss*	(Optional) Specifies the number of seconds between tests; see the "Usage Guidelines" section for formatting guidelines.
millisec *ms*	(Optional) Specifies the number of milliseconds between tests; see the "Usage Guidelines" section for formatting guidelines.
day *day*	(Optional) Specifies the number of days between tests; see the "Usage Guidelines" section for formatting guidelines.
syslog	Enables the generation of a syslog message when a health-monitoring test fails.

Command Default

The defaults are as follows:

- Depending on the test run, monitoring may be enabled or disabled.
- Depending on the test run, the default monitoring interval varies.
- **syslog** is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use these guidelines when scheduling testing:

- *test-id*—Enter the **show diagnostic content** command to display the test ID list.
- *test-id-range*—Enter the **show diagnostic content** command to display the test ID list. Enter the range as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6).
- *hh*—Enter the hours from 1 to 24.
- *mm*—Enter the minutes from 1 to 60.
- *day*—Enter the day of the week as a number from 1 to 7 (**1** is Sunday).
- *ss*—Enter the seconds from 1 to 60.
- *ms*—Enter the milliseconds from 1 to 1000.

Enter the [**no**] **diagnostic monitor test** {*test-id* | *test-id-range* | **all**} command to enable or disable the specified health monitoring test.

When entering the **diagnostic monitor** {**module** *num*} **test** {*test-id* | *test-id-range* | **all**} command, observe the following:

- Required
  - Isolate network traffic by disabling all connected ports and do not pump test packets during the test.
  - Remove all modules for testing FIB TCAM and SSRAM memory on the PFC of the supervisor engine.
  - Reset the system or the test module before putting the system back into the normal operating mode.
- Recommended
  - Turn off all background health-monitoring tests on the supervisor engine and the modules using the **no diagnostic monitor** {**module** *num*} **test** {*test-id* | *test-id-range* | **all**} command.

The FIB TCAM test for central PFC3B (on the supervisor engine) takes approximately 4 hours and 30 minutes.

The FIB TCAM test takes approximately 16 hours.

Examples

This example shows how to run the specified test every 3 days, 10 hours, and 2 minutes:

```
Router(config)# diagnostic monitor interval module 1 test 1 day 3 hours 10 min 2
Router(config)#
```

This example shows how to enable the generation of a syslog message when any health-monitoring test fails:

```
Router(config)# diagnostic monitor syslog
Router(config)#
```

Related Commands

Command	Description
show diagnostic content	Displays test information including test ID, test attributes, and supported coverage test levels for each test and for all modules.

diagnostic ondemand

To configure the ondemand diagnostics, use the **diagnostic ondemand** command.

diagnostic ondemand {**iteration** *iteration-count*} | {**action-on-error** {**continue** | **stop**} [*error-count*]}

Syntax Description

iteration *iteration-count*	Sets the number of times that the same test will be rerun when the command is issued.
action-on-error	Sets the execution action when an error is detected.
continue	Continues testing when a test failure is detected.
stop	Stops testing when a test failure is detected.
error-count	(Optional) Number of errors that are allowed before stopping; used with the **continue** option.

Command Default

The default settings are as follows:

- *iteration-count* is **1**.
- **action-on-error** is **continue**.
- *error-count* is **0**.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Entering **0** for the *error-count* sets the number of errors that are allowed to unlimited.

Examples

This example shows how to set the on-demand testing iteration count:

```
Router# diagnostic ondemand iteration 4
Router#
```

This example shows how to set the execution action when an error is detected:

```
Router# diagnostic ondemand action-on-error continue 2
Router#
```

Related Commands

Command	Description
show diagnostic ondemand	Displays the settings for the on-demand diagnostics.

diagnostic schedule test

To set the scheduling of test-based diagnostic testing for a specific module or schedule a supervisor engine switchover, use the **diagnostic schedule test** command. To remove the scheduling, use the **no** form of this command.

diagnostic schedule {**module** {*num* | *active-sup-slot*}} **test** {*test-id* | *test-id-range* | **all**} [**port** {*num* | *num-range* | **all**}] {**on** *mm dd yyyy hh*:*mm*} | {**daily** *hh*:*mm*} | {**weekly** *day-of-week hh*:*mm*}

no diagnostic schedule test

Syntax Description

module *num*	Specifies the module number.
module *active-sup-slot*	Specifies the slot number of the active supervisor engine.
test-id	Identification number for the test to be run; see the "Usage Guidelines" section for additional information.
test-id-range	Range of identification numbers for tests to be run; see the "Usage Guidelines" section for additional information.
all	Runs all diagnostic tests.
port	(Optional) Specifies the port to schedule testing.
num	Port number.
num-range	Range of port numbers, separated by a hyphen.
all	Specifies all ports.
on *mm dd yyyy hh*:*mm*	Specifies the scheduling of a test-based diagnostic task; see the "Usage Guidelines" section for formatting guidelines.
daily *hh*:*mm*	Specifies the daily scheduling of a test-based diagnostic task; see the "Usage Guidelines" section for formatting guidelines.
weekly *day-of-week hh*:*mm*	Specifies the weekly scheduling of a test-based diagnostic task; see the "Usage Guidelines" section for formatting guidelines.

Command Default

This command has no default settings.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use these guidelines when scheduling testing:

- *test-id*—Enter the **show diagnostic content** command to display the test ID list.
- *test-id-range*—Enter the **show diagnostic content** command to display the test ID list. Enter the range as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6).
- *num-range*—Enter the range as integers separated by a comma and a hyphen (for example, you can enter 1,3-6 to specify ports 1, 3, 4, 5, and 6).
- *mm*—Spell out the month such as january, february ... december (either uppercase or lowercase characters).
- *dd*—Enter the day as a 2-digit number.
- *yyyy*—Enter the year as a 4-digit number.
- *hh***:***mm*—Enter the time as a 2-digit number (for a 24-hour clock) for hours:minutes; the colon (**:**) is required.
- *day-of-week*—Spell out the day of the week, such as monday, tuesday... sunday (either uppercase or lowercase characters).
- **port** {*num* | *num-range* | **all**}—Is not supported when specifying a scheduled switchover.

Enter the **show diagnostic content** command to display the test ID list.

You can use the **diagnostic schedule module** *active-sup-slot* **test** *test-id* command to schedule a switchover from the active supervisor engine to the standby supervisor engine.

Enter the **show diagnostic content** *active-sup-slot* command to display the test ID list and look for the test ID in the ScheduleSwitchover field.

You can specify a periodic switchover (daily or weekly) or a single switchover occurrence at a specific time using these commands:

- **diagnostic schedule module** *active-sup-slot* **test** *test-id* **on** *mm dd yyyy hh***:***mm*
- **diagnostic schedule module** *active-sup-slot* **test** *test-id* **daily** *hh***:***mm*
- **diagnostic schedule module** *active-sup-slot* **test** *test-id* **weekly** *day-of-week hh***:***mm*

Note To avoid system downtime if the standby supervisor engine cannot switch over the system, we recommend that you schedule a switchover from the standby supervisor engine to the active supervisor engine 10 minutes after the switchover occurs. See the “Examples” section for additional information.

Examples

This example shows how to schedule the diagnostic testing on a specific date and time for a specific module and port:

```
Router(config)# diagnostic schedule module 1 test 1,2,5-9 port 3 on january 3 2003 23:32
Router(config)#
```

This example shows how to schedule the diagnostic testing to occur daily at a certain time for a specific port and module:

```
Router(config)# diagnostic schedule module 1 test 1,2,5-9 port 3 daily 12:34
Router(config)#
```

This example shows how to schedule the diagnostic testing to occur weekly on a certain day for a specific port and module:

```
Router(config)# diagnostic schedule module 1 test 1,2,5-9 port 3 weekly friday 09:23
Router(config)#
```

This example shows how to schedule a switchover for the active supervisor engine every Friday at 10:00 pm, and switch the standby supervisor engine back to the active supervisor engine 10 minutes after the switchover occurs. For this example, these conditions apply:

- *test-id* is 32.
- The active supervisor engine is in slot 5.
- The standby supervisor engine is in slot 6.

Related Commands

Command	Description
show diagnostic content	Displays test information including test ID, test attributes, and supported coverage test levels for each test and for all modules.
show diagnostic schedule	Displays the current scheduled diagnostic tasks.

diagnostic start

To run the specified diagnostic test, use the **diagnostic start** command.

diagnostic start {**module** *num*} **test** {*test-id* | *test-id-range* | **minimal** | **complete** | **basic** | **per-port** | **non-disruptive** | **all**} [**port** {*num* | *port#-range* | **all**}]

Syntax Description

module *num*	Specifies the module number.
test	Specifies a test to run.
test-id	Identification number for the test to be run; see the "Usage Guidelines" section for additional information.
test-id-range	Range of identification numbers for tests to be run; see the "Usage Guidelines" section for additional information.
minimal	Runs minimal bootup diagnostic tests.
complete	Runs complete bootup diagnostic tests.
basic	Runs basic on-demand diagnostic tests.
per-port	Runs per-port level tests.
non-disruptive	Runs the nondisruptive health-monitoring tests.
all	Runs all diagnostic tests.
port *num*	(Optional) Specifies the interface port number.
port *port#-range*	Specifies the interface port number range; see the "Usage Guidelines" section for additional information.
port all	Specifies all ports.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Note We recommend that before you enable any online diagnostics tests that you enable the logging console/monitor to see all warning messages.

Note We recommend that when you are running disruptive tests that you only run the tests when connected through console. When disruptive tests are complete a warning message on the console recommends that that you reload the system to return to normal operation. Note: Strictly follow this warning.

Note While this test is running, all ports are shut down as a stress test is being performed with looping ports internally and external traffic might skew the test results. The entire switch must be rebooted to bring the switch to normal operation. When you issue the command to reload the switch, the system will ask you if the configuration should be saved. Note: Do not save the configuration.

Note If you are running the tests on a module that is not the supervisor engine, after the test is initiated and complete, you must reset the module.

Note Do not enter the **diagnostic start module** *x* **test all** command on systems that are configured with a DFC3A because this command causes the TCAM test to fail.

Enter the **show diagnostic content** command to display the test ID list.

Enter the *test-id-range* or *port#-range* as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6).

Use the **diagnostic stop** command to stop the testing process.

Examples

This example shows how to run the specified diagnostic test at the specified slot:

```
Router# diagnostic start module 1 test 5
Module 1:Running test(s) 5 may disrupt normal system operation
Do you want to run disruptive tests? [no]yes
00:48:14:Running OnDemand Diagnostics [Iteration #1] ...
00:48:14:%DIAG-SP-6-TEST_RUNNING:Module 1:Running TestNewLearn{ID=5} ...
00:48:14:%DIAG-SP-6-TEST_OK:Module 1:TestNewLearn{ID=5} has completed successfully
00:48:14:Running OnDemand Diagnostics [Iteration #2] ...
00:48:14:%DIAG-SP-6-TEST_RUNNING:Module 1:Running TestNewLearn{ID=5} ...
00:48:14:%DIAG-SP-6-TEST_OK:Module 1:TestNewLearn{ID=5} has completed successfully
Router#
```

Related Commands

Command	Description
diagnostic stop	Stops the testing process.
show diagnostic	Displays the test results of the online diagnostics and lists the supported test suites.

diagnostic stop

To stop the testing process, use the **diagnostic stop** command.

diagnostic stop {**module** *num*}

Syntax Description

module *num*	Module number.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use the **diagnostic start** command to start the testing process.

Examples

This example shows how to stop the diagnostic test process:

```
Router# diagnostic stop module 3
Router#
```

Related Commands

Command	Description
diagnostic start	Runs the testing process.
show diagnostic	Displays the test results of the online diagnostics and lists the supported test suites.

disconnect qdm

To disconnect a QDM session, use the **disconnect qdm** command.

disconnect qdm [{**client** *client-id*}]

Syntax Description

client *client-id*	(Optional) Specifies a client to disconnect.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

QDM is not supported on OSM interfaces.

If you enter the **disconnect qdm** command without any arguments, all QDM sessions are disconnected. You can obtain the *client-id* by entering the **show qdm status** command.

Examples

This example shows how to disconnect a QDM session:

```
Router# disconnect qdm client 1
Router#
```

Related Commands

Command	Description
show qdm status	Displays information about the status for the currently active QDM clients who are connected to the Catalyst 6500 series switch.

do

To execute the EXEC-level commands from global configuration mode or other configuration modes or submodes, use the **do** command.

do *command*

Syntax Description

command	EXEC-level command to be executed.

Command Default

This command has no default settings.

Command Modes

Global configuration (config) or any other configuration mode or submode from which you are executing the EXEC-level command.

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Caution Do not enter the **do** command in EXEC mode. Interruption of service may occur.

You cannot use the **do** command to execute the **configure terminal** command because entering the **configure terminal** command changes the mode to configuration mode.

You cannot use the **do** command to execute the **copy** or **write** command in the global configuration or any other configuration mode or submode.

Examples

This example shows how to execute the EXEC-level **show interfaces** command from within global configuration mode:

```
Router(config)# do show interfaces serial 3/0

Serial3/0 is up, line protocol is up
  Hardware is M8T-RS232
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output 1d17h, output hang never
  Last clearing of "show interface" counters never
.
.
.
Router(config)#
```

dot1x default

To reset the configurable 802.1X parameters to the default settings, use the **dot1x default** command.

dot1x default

Syntax Description

This command has no arguments or keywords.

Command Default

The default values are as follows:

- The per-interface 802.1X protocol enable state is disabled (force-authorized).
- The number of seconds between reauthentication attempts is 3600 seconds.
- The quiet period is 60 seconds.
- The retransmission time is 30 seconds.
- The maximum retransmission number is 2 times.
- The multiple host support is disabled.
- The client timeout period is 30 seconds.
- The authentication server timeout period is 30 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to reset the configurable 802.1X parameters to the default values:

```
Router(config-if)# dot1x default
Setting the Default Configuration for Dot1x on this interface

Router(config-if)#
```

Related Commands

Command	Description
show dot1x	Displays 802.1X information.

dot1x max-req

To set the number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process, use the **dot1x max-req** command. To return to the default settings, use the **no** form of this command.

dot1x max-req *count*

no dot1x max-req

Syntax Description

count	Number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process; valid values are from 1 to 10.

Command Default

The *count* is **2**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You should change the default value only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Examples

This example shows how to set 5 as the number of times that the switch sends an EAP-request/identity request before restarting the authentication process:

```
Router(config-if)# dot1x max-req 5
Router(config-if)#
```

Related Commands

Command	Description
show dot1x	Displays 802.1X information.

dot1x multi-hosts

To allow multiple hosts (clients) on an 802.1X-authorized port, use the **dot1x multi-hosts** command. To disallow multiple hosts, use the **no** form of this command.

dot1x multi-hosts

no dot1x multi-hosts

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Before entering this command, ensure that the **dot1x port-control** command is set to **auto** for the specified interface.

Examples

This example shows how to allow multiple hosts:

```
Router(config-if)# dot1x multi-hosts
Router(config-if)#
```

This example shows how to disallow multiple hosts:

```
Router(config-if)# no dot1x multi-hosts
Router(config-if)#
```

Related Commands

Command	Description
dot1x port-control	Sets the port control value.
show dot1x	Displays 802.1X information.

dot1x port-control

To set the port control value, use the **dot1x port-control** command. To return to the default settings, use the **no** form of this command.

dot1x port-control *value*

no dot1x port-control

Syntax Description

value	Port-control value; valid values are **auto**, **force-authorized**, and **force-unauthorized**; see the "Usage Guidelines" section for more information.

Command Default

force-authorized

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The port-control *value* definitions are as follows:

- **force-authorized**—Disables 802.1X port-based authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client.
- **force-unauthorized**—Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. Authentication services are not provided to the client through the interface.
- **auto**—Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The system requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the system by using the client's MAC address.

To check the port-control configuration, enter the **show dot1x** command and check the Status column in the 802.1X Port Summary section. An *enabled* status means that the port-control value is set either to **auto** or to **force-unauthorized**.

Examples

This example shows how to set the port control to auto:

```
Router(config-if)# dot1x port-control auto
Router(config-if)#
```

Related Commands

Command	Description
show dot1x	Displays 802.1X information.

dot1x reauthentication

To enable periodic reauthentication of the client, use the **dot1x reauthentication** command. To return to the default settings, use the **no** form of this command.

dot1x reauthentication

no dot1x reauthentication

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Reauthentication does not disturb the status of an already authorized port.

Examples

This example shows how to enable periodic reauthentication of the client:

```
Router(config-if)# dot1x reauthentication
Router(config-if)#
```

This example shows how to disable periodic reauthentication of the client:

```
Router(config-if)# no dot1x reauthentication
Router(config-if)#
```

Related Commands

Command	Description
dot1x timeout	Sets the reauthentication timer.
show dot1x	Displays 802.1X information.

dot1x system-auth-control

To enable 802.1X globally, use the **dot1x system-auth-control** command. To disable 802.1X globally, use the **no** form of this command.

dot1x system-auth-control

no dot1x system-auth-control

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You must enable AAA and specify the authentication method list before enabling 802.1X. A method list describes the sequence and authentication methods to be queried to authenticate a user.

Examples

This example shows how to enable 802.1X globally:

```
Router(config)# dot1x system-auth-control
Router(config)#
```

This example shows how to disable 802.1X globally:

```
Router(config)# no dot1x system-auth-control
Router(config)#
```

Related Commands

Command	Description
aaa authentication dot1x	Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.
aaa new-model	Enables the AAA access-control model.
show dot1x	Displays 802.1X information.

dot1x timeout

To set the reauthentication timer, use the **dot1x timeout** command. To return to the default settings, use the **no** form of this command.

dot1x timeout {{**reauth-period** *seconds*} | {**quiet-period** *seconds*} | {**tx-period** *seconds*} | {**supp-timeout** *seconds*} | {**server-timeout** *seconds*}}

no dot1x timeout {**reauth-period** | **quiet-period** | **tx-period** | **supp-timeout** | **server-timeout**}

Syntax Description

reauth-period *seconds*	Specifies the number of seconds between reauthentication attempts; valid values are from 1 to 65535. See the "Usage Guidelines" section for additional information.
quiet-period *seconds*	Specifies the number of seconds that the system remains in the quiet state following a failed authentication exchange with the client; valid values are from 0 to 65535 seconds.
tx-period *seconds*	Specifies the number of seconds that the system waits for a response to an EAP-request/identity frame from the client before retransmitting the request; valid values are from 30 to 65535 seconds.
supp-timeout *seconds*	Specifies the number of seconds that the system waits for the retransmission of EAP-request packets; valid values are from 30 to 65535 seconds.
server-timeout *seconds*	Specifies the number of seconds that the system waits for the retransmission of packets by the back-end authenticator to the authentication server; valid values are from 30 to 65535 seconds.

Command Default

The defaults are as follows:

- **reauth-period** is **3600** seconds.
- **quiet-period** is **60** seconds.
- **tx-period** is **30** seconds.
- **supp-timeout** is **30** seconds.
- **server-timeout** is **30** seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You must enable periodic reauthentication before you enter the **dot1x timeout reauth-period** command. Enter the **dot1x reauthentication** command to enable periodic reauthentication. The **dot1x timeout reauth-period** command affects the behavior of the system only if periodic reauthentication is enabled.

Examples

This example shows how to set the number of seconds between reauthentication attempts to 4000:

```
Router(config-if)# dot1x timeout reauth-period 4000
Router(config-if)#
```

This example shows how to set the quiet time on the system to 30 seconds:

```
Router(config-if)# dot1x timeout quiet-period 30
Router(config-if)#
```

This example shows how to set 60 as the number of seconds to wait for a response to an EAP-request/identity frame from the client before retransmitting the request:

```
Router(config-if)# dot1x timeout tx-period 60
Router(config-if)#
```

This example shows how to set the system-to-client retransmission time for the EAP-request frame to 25 seconds:

```
Router(config-if)# dot1x timeout supp-timeout 25
Router(config-if)#
```

This example shows how to set the system-to-authentication-server retransmission time for transport layer packets to 25 seconds:

```
Router(config-if)# dot1x timeout server-timeout 25
Router(config-if)#
```

This example shows how to return to the default reauthorization period:

```
Router(config-if)# no dot1x timeout reauth-period
Router(config-if)#
```

Related Commands

Command	Description
dot1x reauthentication	Enables periodic reauthentication of the client.
show dot1x	Displays 802.1X information.

duplex

To configure the duplex operation on an interface, use the **duplex** command. To return the system to half-duplex mode, use the **no** form of this command.

duplex {**full** | **half**}

no duplex

Syntax Description

full	Specifies full-duplex operation.
half	Specifies half-duplex operation.

Command Default

half

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Table 2-7 lists the supported command options by interface.

Table 2-7 Supported duplex Command Options

Interface Type	Supported Syntax	Default Setting	Usage Guidelines
10/100-Mbps module	**duplex** [**half** | **full**]	See the "Usage Guidelines" section.	If the speed is set to **auto**, you will not be able to set **duplex**. If the speed is set to **10** or **100**, and you do not configure the duplex setting, the duplex is set to **half.**
100-Mbps fiber modules	**duplex** [**half** | **full**]	**half**	—
Gigabit Ethernet Interfaces	**duplex full**	**full**	—
10-Mbps ports	**duplex** [**half** | **full**]	**half**	—

If the transmission speed on a 16-port RJ-45 Gigabit Ethernet port is set to 1000, the duplex mode is set to full. If the transmission speed is changed to 10 or 100, the duplex mode stays at half duplex. You must configure the correct duplex mode when the transmission speed is changed to 10 or 100 from 1000.

Gigabit Ethernet is full duplex only. You cannot change the duplex mode on Gigabit Ethernet ports or on a 10/100/1000-Mps port that is configured for Gigabit Ethernet.

When manually configuring the interface speed to either 10 or 100 Mbps, you should also configure the duplex mode on the interface.

Note Catalyst 6500 series switches cannot automatically negotiate the interface speed and duplex mode if either connecting interface is configured to a value other than **auto**.

Caution Changing the interface speed and duplex mode configuration might shut down and reenable the interface during the reconfiguration.

Table 2-8 describes the relationship and the results for the different combinations of the **duplex** and **speed** commands.

Table 2-8 Relationship Between duplex and speed Commands

duplex Command	speed Command	Resulting System Action
duplex half or **duplex full**	**speed auto**	Autonegotiates both speed and duplex modes
duplex half	**speed 10**	Forces 10 Mbps and half duplex
duplex full	**speed 10**	Forces 10 Mbps and full duplex
duplex half	**speed 100**	Forces 100 Mbps and half duplex
duplex full	**speed 100**	Forces 100 Mbps and full duplex

Examples

This example shows how to configure the interface for full-duplex operation:

```
Router(config-if)# duplex full
Router(config-if)#
```

Related Commands

Command	Description
interface	Selects an interface to configure and enters interface configuration mode.
show controllers	Displays information that is specific to the hardware on a module.
show interfaces	Displays the traffic that is seen by a specific interface.
speed	Sets the port speed for an Ethernet interface.