

set udd

Use the **set udd** command to enable or disable the UDLD information display on specified ports or globally on all ports.

```
set udd enable | disable [mod/port]
```

Syntax Description

enable	Keyword to enable the UDLD information display.
disable	Keyword to disable the UDLD information display.
<i>mod/port</i>	(Optional) Number of the module and port on the module.

Defaults

The defaults are as follows:

- UDLD global enable state—Globally disabled.
- UDLD per-port enable state for fiber-optic media—Enabled on all Ethernet fiber-optic ports.
- UDLD per-port enable state for twisted-pair (copper) media—Disabled on all Ethernet 10/100 and 1000BaseTX ports.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to enable the UDLD message display for port 1 on module 2:

```
Console> (enable) set udd enable 2/1
UDLD enabled on port 2/1.
Warning:UniDirectional Link Detection
should be enabled only on ports not connected to hubs,
media converters or similar devices.
Console> (enable)
```

This example shows how to disable the UDLD message display for port 1 on module 2:

```
Console> (enable) set udd disable 2/1
UDLD disabled on port 2/1.
Warning:UniDirectional Link Detection
should be enabled only on ports not connected to hubs,
media converters or similar devices.
Console> (enable)
```

This example shows how to enable the UDLD message display for all ports on all modules:

```
Console> (enable) set udd enable
UDLD enabled globally.

Console> (enable)
```

This example shows how to disable the UDL message display for all ports on all modules:

```
Console> (enable) set udd disable  
UDLD disabled globally  
Console> (enable)
```

Related Commands **show udd**

set udd aggressive-mode

Use the **set udd aggressive-mode** command to enable or disable the UDLD aggressive mode on specified ports or globally on all ports.

set udd aggressive-mode enable | disable *mod/port*

Syntax Description

enable	Keyword to enable UDLD aggressive mode.
disable	Keyword to disable UDLD aggressive mode.
<i>mod/port</i>	Number of the module and port on the module.

Defaults

The default is aggressive mode is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can use the aggressive mode in cases in which a port that sits on a bidirectional link stops receiving packets from its neighbor. When this happens, if aggressive mode is enabled on the port, UDLD will try to reestablish the connection with the neighbor. If connection is not reestablished after eight failed retries, the port is error disabled.

We recommend that you use this command on point-to-point links between Cisco switches only.

Examples

This example shows how to enable aggressive mode:

```
Console> (enable) set udd aggressive-mode enable 2/1
Aggressive UDLD enabled on port 5/13.
Warning:Aggressive Mode for UniDirectional Link Detection
should be enabled only on ports not connected to hubs,
media converters or similar devices.
Console> (enable)
```

Related Commands

set udd
show udd

set udd interval

Use the **set udd** command to set the UDDL message interval timer.

set udd interval *interval*

Syntax Description	<i>interval</i> Message interval in seconds; valid values are from 7 to 90 seconds.
---------------------------	---

Defaults	The default is 15 seconds.
-----------------	----------------------------

Command Types	Switch command.
----------------------	-----------------

Command Modes	Privileged.
----------------------	-------------

Examples	This example shows how to set the message interval timer:
-----------------	---

```
Console> (enable) set udd interval 90  
UDLD message interval set to 90 seconds  
Console> (enable)
```

Related Commands	set udd show udd
-------------------------	-----------------------------------

set vlan

Use the **set vlan** command set to group ports into a VLAN or set the private VLAN type.

```
set vlan {vlan_num} {mod/ports}
```

```
set vlan {vlan_num} [name {name}] [type {type}] [state {state}] [said {said}] [mtu {mtu}]
[bridge {bridge_num}] [mode {bridge_mode}] [stp {stp_type}] [translation {vlan_num}]
[aremaxhop {hopcount}] [pvlan-type {pvlan_type}] [ring {hex_ring_number}]
[decring {decimal_ring_number}] [parent {vlan_num}] [backupcrf {off | on}]
[stemaxhop {hopcount}] [rspan]
```

Syntax Description

<i>vlan_num</i>	Number identifying the VLAN.
<i>mod/ports</i>	Number of the module and ports on the module belonging to the VLAN.
name <i>name</i>	(Optional) Keyword and variable to define a text string used as the name of the VLAN; valid values are from 1 to 32 characters.
type <i>type</i>	(Optional) Keyword and variable to identify the VLAN type.
state <i>state</i>	(Optional) Keyword and variable to specify whether the state of the VLAN is active or suspended.
said <i>said</i>	(Optional) Keyword and variable to specify the security association identifier; valid values are from 1 to 4294967294.
mtu <i>mtu</i>	(Optional) Keyword and variable to specify the maximum transmission unit (packet size, in bytes) that the VLAN can use; valid values are from 576 to 18190.
bridge <i>bridge_num</i>	(Optional) Keyword and variable to specify the identification number of the bridge; valid values are hexadecimal numbers from 0x1 to 0xF.
mode <i>bridge_mode</i>	(Optional) Keyword and variable to specify the bridge mode; valid values are srt and srp .
stp <i>stp_type</i>	(Optional) Keyword and variable to specify the STP type; valid values are ieee , ibm , and auto .
translation <i>vlan_num</i>	(Optional) Keyword and variable to specify a translational VLAN used to translate FDDI or Token Ring to Ethernet; valid values are from 1 to 1005.
aremaxhop <i>hopcount</i>	(Optional) Keyword and variable to specify the maximum number of hops for All-Routes Explorer frames; valid values are from 1 to 13.
pvlan-type <i>pvlan-type</i>	(Optional) Keyword and options to specify the private VLAN type. See the “Usage Guidelines” section for valid values.
ring <i>hex_ring_number</i>	(Optional) Keyword to specify the VLAN as the primary VLAN in a private VLAN.
decring <i>decimal_ring_number</i>	(Optional) Keyword and variable to specify the decimal ring number; valid values are from 1 to 4095.
parent <i>vlan_num</i>	(Optional) Keyword and variable to specify the VLAN number of the parent VLAN; valid values are from 2 to 1005.

backupcrf off on	(Optional) Keywords to specify whether the TrCRF is a backup path for traffic.
stemaxhop <i>hopcount</i>	(Optional) Keyword and variable to specify the maximum number of hops for Spanning Tree Explorer frames; valid values are from 1 to 14.
rspan	(Optional) Keyword to create a VLAN for remote SPAN.

Defaults

The default values are as follows:

- Switched Ethernet ports and Ethernet repeater ports are in VLAN 1.
- *said* is 100001 for VLAN 1, 100002 for VLAN 2, 100003 for VLAN 3, and so forth.
- *type* is Ethernet.
- *mtu* is 1500 bytes.
- *state* is active.
- *hopcount* is 7.
- *pvlan type* is none.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

You cannot use the **set vlan** command until the Catalyst 6000 family switch is either in VTP transparent mode (**set vtp mode transparent**) or until a VTP domain name has been set (**set vtp domain name**). To create a private VLAN, UTP mode must be transparent.

You cannot set multiple VLANs for ISL ports using this command. The VLAN name can be from 1 to 32 characters in length. If you are adding a new VLAN, the VLAN number must be within the range 2 to 1001. When you are modifying a VLAN, the valid range for the VLAN number is from 2 to 1005.

If you use the **rspan** keyword for remote SPAN VLANs, you should not configure an access port (except the remote SPAN destination ports) on these VLANs. Learning is disabled for remote SPAN VLANs.

If you use the **rspan** keyword for remote SPAN VLANs, only the **name name** and the **state {active | suspend}** variables are supported.

The **stemaxhop hopcount** parameter is valid only when defining or configuring TrCRFs.

The **bridge bridge_num**, **mode bridge_mode**, **stp stp_type**, and **translation vlan_num** keywords and values are supported only when the Catalyst 6000 family switch is used as a VTP server for Catalyst 5000 family switches in the Token Ring and FDDI networks.

You must configure a private VLAN on the supervisor engine.

Valid values for *pvlan-type* are:

- **primary** specifies the VLAN as the primary VLAN in a private VLAN.
- **isolated** specifies the VLAN as the isolated VLAN in a private VLAN.

- **community** specifies the VLAN as the community VLAN in a private VLAN.
- **none** specifies that the VLAN is a normal Ethernet VLAN, not a private VLAN.

Only regular VLANs with no access ports assigned to them can be used in private VLANs. Do not use the **set vlan** command to add ports to a private VLAN; use the **set pvlan** command to add ports to a private VLAN.

VLANs 1001, 1002, 1003, 1004, and 1005 cannot be used in private VLANs.

VLANs in a suspended state do not pass packets.

Examples

This example shows how to set VLAN 850 to include ports 3 through 7 on module 3:

```
Console> (enable) set vlan 850 3/4-7
VLAN 850 modified.
VLAN Mod/Ports
-----
850 3/4-7
Console> (enable)
```

This example shows how to set VLAN 7 as a primary VLAN:

```
Console> (enable) set vlan 7 pvlan-type primary
Console> (enable)
```

This example shows how to set VLAN 901 as an isolated VLAN:

```
Console> (enable) set vlan 901 pvlan-type isolated
Console> (enable)
```

This example shows how to set VLAN 903 as a community VLAN:

```
Console>(enable) set vlan 903 pvlan-type community
Console>(enable)
```

Related Commands

```
set vlan mapping
show vlan
set pvlan
clear config pvlan
clear pvlan mapping
show pvlan
show pvlan mapping
clear vlan
```

set vlan mapping

Use the **set vlan mapping** command to map 802.1Q VLANs to ISL VLANs.

```
set vlan mapping dot1q 1q_vlan_num isl isl_vlan_num
```

Syntax Description	
dot1q <i>1q_vlan_num</i>	Keyword and variable to specify the 802.1Q VLAN; valid values are from 1001 to 4095.
isl <i>isl_vlan_num</i>	Keyword to specify the ISL VLAN; valid values are from 1 to 1024.

Defaults The default is all switched Ethernet ports and Ethernet repeater ports are in VLAN 1.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines IEEE 802.1Q VLAN trunks support VLANs 1 through 4095. ISL VLAN trunks support VLANs 1 through 1024 (1005 to 1024 are reserved). The switch automatically maps 802.1Q VLANs 1000 and lower to ISL VLANs with the same number.

Use this feature to map 802.1Q VLANs above 1000 to ISL VLANs.

You can map up to eight VLANs. Only one 802.1Q VLAN can be mapped to an ISL VLAN. For example, if 802.1Q VLAN 800 has been automatically mapped to ISL VLAN 800, do not manually map any other 802.1Q VLANs to ISL VLAN 800.

You cannot overwrite existing 802.1Q VLAN mapping. If the 802.1Q VLAN number already exists, the command is aborted. You must first clear that mapping.

If *vlan_num* does not exist, then either of the following occurs:

- If the switch is in server or transparent mode, the VLAN is created with all default values.
- If the switch is in client mode, then the command proceeds without creating the VLAN. A warning will be given indicating that the VLAN does not exist.

If the table is full, the command is aborted with an error message indicating the table is full.

Examples This example shows how to map VLAN 850 to ISL VLAN 1022:

```
Console> (enable) set vlan mapping dot1q 850 isl 1022
Vlan 850 configuration successful
Vlan mapping successful
Console> (enable)
```

This example shows the display if you enter a VLAN that does not exist:

```
Console> (enable) set vlan mapping dot1q 2 isl 1016
Vlan Mapping Set
Warning: Vlan 2 Nonexistent
Console> (enable)
```

This example shows the display if you enter an existing mapping:

```
Console> (enable) set vlan mapping dot1q 3 isl 1022
1022 exists in the mapping table. Please clear the mapping first.
Console> (enable)
```

This example shows the display if the mapping table is full:

```
Console> (enable) set vlan mapping dot1q 99 isl 1017
Vlan Mapping Table Full.
Console> (enable)
```

Related Commands

show vlan
clear vlan mapping

set vtp

Use the **set vtp** command to set the options for VTP.

```
set vtp [domain domain_name] [mode {client | server | transparent}] [passwd passwd]
[pruning {enable | disable}] [v2 {enable | disable}]
```

Syntax Description	
domain <i>domain_name</i>	(Optional) Keywords to define the name that identifies the VLAN management domain. The <i>domain_name</i> can be from 1 to 32 characters in length.
mode {client server transparent}	(Optional) Keywords to specify the VTP mode.
passwd <i>passwd</i>	(Optional) Keyword and variable to define the VTP password; the VTP password can be from 8 to 64 characters in length.
pruning {enable disable}	(Optional) Keywords to enable or disable VTP pruning for the entire management domain.
v2 {enable disable}	(Optional) Keywords to enable or disable version 2 mode.

Defaults The defaults are as follows: server mode, no password, pruning disabled, and v2 disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines All switches in a VTP domain must run the same version of VTP. VTP version 1 and VTP version 2 do not operate on switches in the same VTP domain.

If all switches in a domain are VTP version 2-capable, you only need to enable VTP version 2 on one switch (using the **set vtp v2 enable** command); the version number is then propagated to the other version 2-capable switches in the VTP domain.

If the VTP password has already been defined, entering **passwd 0** (zero) clears the VTP password.

VTP supports three different modes: server, client, and transparent. If you make a change to the VTP or VLAN configuration on a switch in server mode, that change is propagated to all of the switches in the same VTP domain.

If the receiving switch is in server mode and its revision number is higher than the sending switch, the configuration is not changed. If the revision number is lower, the configuration is duplicated.

VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.

If the receiving switch is in server mode, the configuration is not changed.

If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. Make sure to make all VTP or VLAN configuration changes on a switch in server mode.

If the receiving switch is in transparent mode, the configuration is not changed. Switches in transparent mode do not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to the other switches in the network.

The **pruning** keyword is used to enable or disable VTP pruning for the VTP domain. VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN out a particular switch port. Use the **set vtp pruneeligible** and **clear vtp pruning** commands to specify which VLANs should or should not be pruned when pruning is enabled for the domain.

To disable VTP, enter the **set vtp mode transparent** command. This command disables VTP from the domain but does not remove the domain from the switch. Use the **clear config all** command to remove the domain from the switch.

**Caution**

Be careful when you use the **clear config all** command. This command clears the entire switch configuration, not just the VTP domain.

Examples

This example shows how to use the **set vtp** command:

```
Console> (enable) set vtp domain Engineering mode client
VTP domain Engineering modified
Console> (enable)
```

This example shows what happens if you try to change VTP to server or client mode and dynamic VLAN creation is enabled:

```
Console> (enable) set vtp mode server
Failed to Set VTP to Server. Please disable Dynamic VLAN Creation First.
Console> (enable)
```

Related Commands

show vtp domain
set vlan
clear vlan
show vlan
set vtp pruneeligible
clear vtp pruning

set vtp pruneeligible

Use the **set vtp pruneeligible** command to specify which VTP domain VLANs are pruning eligible.

set vtp pruneeligible *vlan_range*

Syntax Description	<i>vlan_range</i> Range of VLAN numbers; valid values are from 2 to 1000.
---------------------------	---

Defaults	The default is VLANs 2 through 1000 are eligible for pruning.
-----------------	---

Command Types	Switch command.
----------------------	-----------------

Command Modes	Privileged.
----------------------	-------------

Usage Guidelines	VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN out a particular switch port. Use the set vtp command to enable VTP pruning.
-------------------------	--

By default, VLANs 2 through 1000 are pruning eligible. You do not need to use the **set vtp pruneeligible** command unless you have previously used the **clear vtp pruning** command to make some VLANs pruning ineligible. If VLANs have been made pruning ineligible, use the **set vtp pruneeligible** command to make them pruning eligible again.

Examples	This example shows how to configure pruning eligibility for VLANs 120 and 150:
-----------------	--

```
Console> set vtp pruneeligible 120,150
Vlans 120,150 eligible for pruning on this device.
VTP domain nada modified.
Console>
```

In this example, VLANs 200–500 were made pruning ineligible using the **clear vtp pruning** command. This example shows how to make VLANs 220 through 320 pruning eligible again:

```
Console> set vtp pruneeligible 220-320
Vlans 2-199,220-320,501-1000 eligible for pruning on this device.
VTP domain Company modified.
Console>
```

Related Commands	show vtp domain set vlan clear vtp pruning
-------------------------	---