Switchports for Trunking and Access; related display commands

switchport mode {access | trunk}
switchport access vlan vlan-number -- defines the VLAN interface resides in.
switchport trunk encapsulation [dot1q | isl] -- almost always use dot1q - you may have to do this first.
switchport mode dynamic auto | dynamic desirable
    dynamic auto - becomes a trunk if the neighboring interface is set to trunk or desirable- not if auto!
    dynamic desireable - becomes a trunk if neighboring interface is set to ANY trunk mode *(default!)*
switchport nonegotiate - prevents generating DTP frames, or converting dynamically to anything
switchport trunk allowed vlan 4,6,12,15 --this should eliminate vlans not specifically listed
switchport trunk allowed vlan [remove 4-8 | all | none]
no switchport trunk native vlan
no switchport trunk vlan 4
switchport trunk pruning vlan {add | except | none | remove} vlan-list Specify VLANs eligible for pruning

The proper way to remove VLANs from a Switch
If you delete a VLAN from a switch with "no vlan 30", it won't make it disappear from the interface configs that it was previously added to- it will remain in the swtchport configurations! (and cause confusion) First, run on those interfaces "switchport trunk allowed vlan remove 30' or "switch trunk allowed vlan 10,20,40,50' Then run "no vlan 30" on the switch to remove it.

show interfaces [type,#] switchport - settings, status, trunking, access/voice/native VLAN
show interfaces [type,#] trunk - lists info on trunks (or the specific trunk) and the VLANs
show vlan brief, show vlan - each VLAN and all assigned interfaces, but no trunks!
show vlan [vlan] - access and trunk ports in the VLAN.
show vtp status - VTP mode, configuration and status info

Expected Trunking Operational Mode Based on the Configured Administrative Modes w/ DTP

Administrative Mode	***Access***	***Dynamic Auto***	***Trunk***	***Dynamic Desirable***
access	Access	Access	Access	Access
dynamic auto	Access	Access	Trunk	Trunk
trunk	Access	Trunk	Trunk	Trunk
dynamic desirable	Access	Trunk	Trunk	Trunk

Port Security
As soon as you enable port-security, it defaults to violation shutdown and a maximum of 1 MAC address.
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address aa.bb.cc.dd.ee.ff [sticky, often used with maximum]
switchport port-security maximum value
    the max number of MAC addresses that can be assigned - default is one.
    A max value can also be set if it's a switch connected - recieving frames for multiple MACs
switchport port-security violation {protect | restrict | shutdown}
        protect: unauthorized frames would just be dropped
        restrict: authorized frames would be dropped and violations count toggled
        shutdown: disable the interface (err-disabled - this is the default action)
show port-security interface

To open an interface shut down with port-security, you first issue "shutdown", then "no shutdown"

Inter-VLAN Routing (IVR) and Switched Virtual Interfaces (SVIs)
VLANs can't bridge without a router or Inter-VLAN Routing (IVR). Implementing trunking and Inter-VLAN routing on a layer 3 switch uses Switched Virtual Interfaces (SVIs)

If each router interface is plugged into an access link, each of the routers' interfaces would be the default gateway address for each host in each respective VLAN. IVR in the "router on a stick" (ROAS) implementation puts VLANs into a trunk to a layer 3 device. which performs the routing on logical interfaces and send back out the trunk to the switch on the proper VLAN. This can be done without the external router with a layer 3 switch, which seems a bit more efficient, and relying on the one external router creates a potential bottleneck, as well as a single point of failure.

VLAN Trunking Protocol (VTP)

Designed as a method to manage VLANs across a large numbers of switches: addition, deletion, and renaming from a central point of control, and all switches participating can use any related VLANs. Add a VLAN on the server and it gets set up on others. Not used as much in modern networks, Cisco says best practice is having switches in "off" or "transparent" modes; you may never see it but may find it and want to disable or otherwise manage it.

A switch can belong to just one management domain, and there is no communication between domains.
VTP advertisements contain info about the domain itself (including revision number), it's VLANs and their info.

VTP Modes: vtp mode {server | client | transparent | off}

Server mode (is default)

- full control over management of it's domain. Each domain should have at least one server
- advertises updates to other switches in the domain, receives info to synchronize domain members
- The first server defined in a network defines the domain that will be used by future VTP servers and clients.
- Multiple VTP servers can coexist in a domain, and is recommended for redundancy.
- There is no election for primary or secondary server
- If one server is configured with a new VLAN or VTP parameter, other servers synchronize just as any client

Client mode:

- listen to VTP advertisements from other switches and modify configurations accordingly.
- forward/relay VTP messages out trunk links to neighboring switches in the domain

Transparent mode:

- do not participate in VTP, does not advertise or synchronize its VLAN database with received advertisements.
- can create and delete VLANs that are local only to itself without changes being advertised
- Works only as a relaying member.
- [VTP v1, transparent mode does not relay VTP info unless its domain and VTP version numbers match]
- [VTP v2 and 3, transparent mode does forward VTP advertisements regardless of the VTP domain name]

Off mode simply disables all VTP activity on the switch.

Revision Numbers - watch out when adding hardware!

VTP uses a revision number to track the most recent information.
Starts of at 0 and is incremented by the VTP server with each change in domain info it will advertise
An advertisement with a greater revision number than before says it has new and updated information.
That advertisement is stored and overwrites any previously stored VLAN information.

Important!

VTP VLAN data is saved in vlan.dat file in flash memory is retained even when the switch power is off.
It ensures a switch can recover last known VTP/VLAN configuration from its VTP database after it reboots. Even a device previously configured in client mode will send a summary advertisement using info from it's vlan.dat after powering up and discovering it has a higher revision number.
- Care must be taken to not plug in a VTP enabled switch containing a higher revision number, as it will obliterate existing VTP database information throughout the domain it matches to!

- Always force revision number 0 before being attaching *EVEN if previously configured as a only a VTP client*
- On a new device, set to VTP transparent and then later change back to server- or change the VTP domain to a bogus name
- For critical portions of your network, consider using VTP transparent or off mode to prevent synchronization problems
- Eliminate the chance for duplicate, overlapping VLANs in a large network with transparent mode. For example, two administrators might configure VLANs on switches in their respective areas but use the same VLAN identification or VLAN number. They could overlap if both administrators advertised them using VTP servers

Domains use unsecure advertisements (default), but a password can be required to participants (secure mode)

Cisco Catalyst switches - default is VTP mode server - Don't forget to disable!
It turns out that by default Cisco switches operate in VTP server mode for the management domain NULL (a blank string), no password. If it hears a VTP summary advertisement it automatically learns the VTP domain name, VLANs, revision number. This makes it easy to bring up a new switch in an existing VTP domain.
Be sure to remember that the new switch stays in VTP server mode until you change it..

show vtp status

```
Switch# show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aca0.164f.3f80
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
                                    0x56 0x9D 0x4A 0x3E 0xA5 0x69 0x35 0xBC
```

Advertisement types

Summary advertisements

- VTP domain servers send every 300 seconds and every time a VLAN database change occurs
- VTP version, domain name, revision number, MD5 hash, and number of subset advertisements to follow.
- When config changes, one or more subset advertisements with more details are sent afterwards

Subset advertisements

- list specific changes: add/ delete/ suspend/ activate a VLAN, changing of VLAN name, number, MTU.
- Even change in VLAN type (such as Ethernet or Token Ring), or security association identifier (SAID- 802.10)
- each VLAN gets it's own individual sequential subset advertisement per change, as needed.

VTP advertisements are multicast 01-00-0C-CC-CCCC and an SNAP type value of 0×2003.

Cisco switches default to v1. Versions are not fully backward compatible with each other
Versions 1 and 2 support VLAN numbers 1 to 1005. Only VTP v3 supports extended VLAN range 1-4094.

VTP v3 Features

Extended VLAN range VLANs 1 through 4094 can be advertised throughout a VTPv3 domain
Enhanced authentication - the password can be hidden (only a hash of the password is saved in the running configuration) or secret (the password is saved in the running configuration).
Database propagation - databases other than VTP can be advertised
By default, all VTPv3 switches operate as secondary servers and can send updates throughout the domain.
A primary server is only needed to take control of a domain.
Per-port VTP - VTPv3 can be enabled on a per-trunk port basis, rather than a switch as a whole

```
Switch(config)# vtp version 3
Switch(config)# vtp domain MyCompany
Switch(config)# vtp mode server
Switch(config)# vtp password bigsecret
```

VLAN Pruning
VTP pruning makes more efficient use of trunk bandwidth by reducing unnecessary flooded traffic.
Broadcast, multicast, and unknown unicast frames on a VLAN are forwarded over a trunk link only if the switch on the receiving end of the trunk has ports in that VLAN.
When a switch has an active port associated with a VLAN, the switch advertises that to its neighbor switches.
The neighbors then to decide whether flooded traffic from a VLAN should be allowed on certain trunk links.

Even when VTP pruning has determined that a VLAN is not needed on a trunk, an instance of the Spanning Tree will run for every VLAN that is **allowed** on the trunk link. To reduce the number of STP instances, you should manually "prune" unneeded VLANs from the trunk and allow only the needed ones. Use the **switchport trunk allowed vlan** command to identify the VLANs that should be added or removed from a trunk.

VTP pruning is disabled by default. To enable pruning, use **vtp pruning**
On a VTP server, it says pruning needs to be enabled for the entire domain (all will also enable pruning.
When pruning is enabled, all general-purpose VLANs become eligible for pruning on all trunk links, if needed.
However, you can modify the default list of pruning eligibility with the following interface-configuration command:

switchport trunk pruning vlan {{{add | except | remove} vlan-list} | none}

vlan-list	List of eligible VLAN numbers (2-1001), separate by commas or dashes, no spaces.
add	Will add to the already configured list
except	All VLANs are eligible except for the VLAN numbers
remove	VLAN numbers to remove from the already configured list
none	No VLAN will be eligible for pruning.

Obviously, VTP pruning has no effect on switches in the VTP transparent mode.
Those switches must be configured manually to "prune" VLANs from trunk links (same command)
VLAN 1 is never eligible for pruning, same with 1002-1005 (reserved for Token Ring and FDDI VLANs)

Troubleshooting VTP - Not updating information from a VTP server?
- Is the switch in VTP transparent mode
- If a VTP client, there might not be an VTP server. In this case, just make it a VTP server itself.
- Is the link to the VTP server a trunk? VTP advertisements are sent only over trunks.
- Is the VTP domain name is configured to match the one on the VTP server.
- Check if the VTP version is compatible matches the VTP domain.
- Does the VTP domain use a password? If the server doesn't, make sure the password is disabled or cleared.

VTP Troubleshooting Commands

show vtp status	Current VTP parameters, incl. the last VTP server
show vlan brief	Displays defined VLANs
show interface type member/module/number switchport	Displays trunk status, including pruning eligibility
show interface type member/module/number pruning	Displays VTP pruning state

VTP Configuration Commands

vtp domain domain-name	Define the VTP domain.
vtp mode {server | client | transparent | off}	Set the VTP mode.
vtp password password [hidden | secret]	Define an optional VTP password.
vtp version {1 | 2 | 3}	Configure VTP version.
vtp pruning	Enable VTP pruning.
switchport trunk pruning vlan {add | except | none | remove} vlan-list	Specify VLANs eligible for pruning