Post 5

Thursday, January 24, 2019 11:11 PM

VLAN CONFIGURATION IN IOS

Different switches support various #'s of VLANS: Normal/Extended Range VLANs

Normal Range	▪ Small/Medium sized business ▪ VLAN ID between: 1 – 1005 ▪ ID's: 1 and 1002 auto created: Can't be removed ▪ ID's: 1002 and 1005 auto created: Can't be removed **VLAN.dat**: DB where VLAN configs are stored in flash mem **VTP (VLAN Trunking Protocol)** helps manage VLAN configs bet switches: Only learn/store normal ranges
Extended Range	○ VLAN ID: between 1006-4094 ○ **Not written to VLAN.dat:** Fewer features than normal range ○ **Saved in running-config**: VTP doesn't learn extended range VLANs ○ 4096: Boundary: Number of VLANs avail on Catalyst switches ○ 12 bits in VLAN ID field of 802.1Q header frame

Config normal range VLANs

```
switch# config t
switch (config)# vlan [vlan-ID number]
or
switch (config)# vlan 100, 102, 105-107 [config multiple vlans]
switch (config-vlan)# name [give it a name]
switch (config-vlan)# end
switch# show vlan brief [display vlan.dat contents]
```

Assigning Ports to VLANs

- Access port can belong to 1 VLAN at time: 1 exception: IP phone: 2 VLAN's on 1 port: Voice/data
- switchport access: Forces VLAN creation if doesn't exist: *% Access VLAN does not exist. Creating vlan 30*
- int range to config multiple interfaces

```
switch# config t
switch(config)# interface [int ID fa0/blah]
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan [id]
switch(config-if)# end
```

Changing VLAN Port Membership

```
switch# config t
switch(config-if)# no switchport access vlan
switch(config-if)# end
```

```
show int fa/X switchport [verify output]
```

Delete VLAN info [reassign all member ports to diff VLAN when doing]

```
switch# config t
switch(config)# no vlan [vlan #]
switch(config)# end
switch# sh vlan brief
```

Delete vlan.dat

```
switch> enable
switch# delete flash: vlan.dat
or
```

```
switch# delete flash.vlan.dat [when not removed from original location]
```

- For Catalyst switch: erase startup-config must accompany delete vlan.dat prior to reload

show VLAN/INT cmds

```
show vlan (brief id [VID] | name [vlan name] | summary)
show int (int-id | vlan [VID] | switchport)
```

Trunk Links w/802.1Q

- L2 link between 2 switches: Carries traffic across switches that are trunked/belong to a specific VLAN

Enable Trunks: Config ports on either end of physical link w/parallel sets of cmds

switchport mode trunk Port enters permanent trunk mode/DTP (Dynamic Trunking Protocol) converts into trunk

- Even if the int doesn’t agree to the change

```
switch# config t
switch(config)# int [device id]
switch(config-if)# switchport mode trunk (force link to be a trunk)
switch(config-if)# switchport trunk native vlan (native VLAN for untagged 80.21Q trunks)
switch(config-if)# switchport trunk allow vlan [vlan list] (list of VLANs allowed on trunk)
switch(config-if)# end
```

Resetting Trunk to Default State: Removes allowed VLANs/reset native VLAN of trunk

- When reset: Trunk allows all VLANs/uses VLAN 1 as native

```
switch# config t
switch(config)# int [int id]
switch(config-if)# no switchport trunk allowed vlan (set trunk to allow all VLANs)
switch(config-if)# no switchport trunk native vlan (reset native VLAN to default)
switch(config-if)# end
```

```
show interfaces [int id] switchport
```

DTP (Dynamic Trunk Protocol)

- Trunk interface support different modes: Can be set to nontrunking or negotiate trunking w/neighbor int

DTP	▪ **Manages trunk negotiation:** Operates on point-to-point basis only between network devices ▪ **Cisco proprietary protocol:** Auto enabled on Catalyst 2960/3560 switches ▪ Other vendors don’t support: Some devices may fwd DTP frames improperly (misconfigs) ▪ Turn off DTP on interfaces connected to devices that don’t support DTP ▪ Manages trunk negotiation ONLY if port on switch is configured in trunk mode that supports it ▪ Default DTP config for 2960/3560 switches is dynamic auto Enable trunking from Cisco to device that doesn’t support DTP: ○ use switchport mode trunk and switchport nonegotiate interface config mode cmds ○ Causes the int to become a trunk, but not generate DTP frames

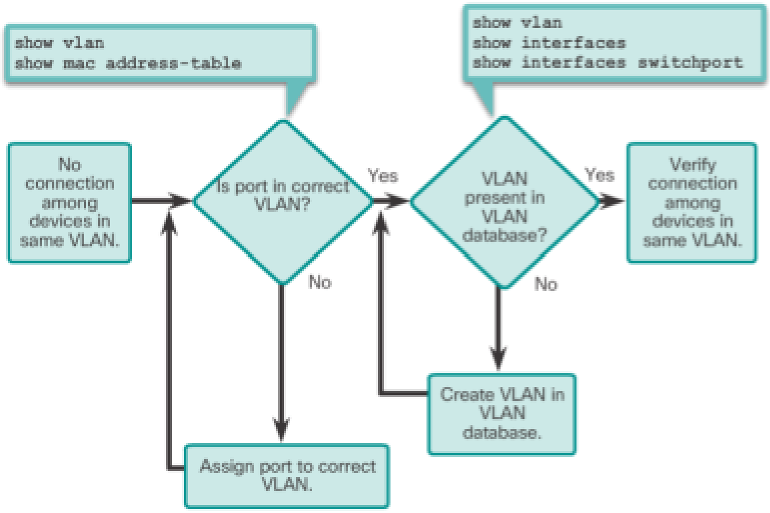
Negotiated Int Modes

switchport mode access	○ Puts interface (access port) into permanent nontrunking mode ○ Negotiates to convert link into nontrunk link ○ Interface becomes nontrunk int (whether/not neighboring int is a trunk)
switchport mode dynamic auto	○ Makes int a convertible to trunk link ○ Int becomes trunk int if neighboring interface is set to trunk/desirable mode ○ Default mode for all Ethernet interfaces
switchport mode dynamic desirable	○ Makes int actively attempt to convert link to trunk ○ Int becomes trunk int if neighboring int is set to trunk/desirable/auto mode ○ Default switchport mode (2950/3550 series)
switchport mode trunk	○ Puts int into permanent trunking mode ○ Negotiates to convert neighboring link into trunk link

	○ Int becomes a trunk int even if neighboring int isn’t a trunk int
switchport nonegotiate	○ Prevents int from generating DTP frames ○ can only use cmd when int switchport mode is access/trunk ○ Must manually configure neighboring int as trunk int to establish link

Determines current DTP mode show dtp int

Missing VLANs



```
show vlan
show mac address-table
```

```
show vlan
show interfaces
show interfaces switchport
```

No connection among devices in same VLAN.
Is port in correct VLAN?
Yes
No
VLAN present in VLAN database?
Yes
No
Verify connection among devices in same VLAN.
Create VLAN in VLAN database.
Assign port to correct VLAN.

Each VLAN must correspond to unique IP subnet: If 2 devices in same VLAN have different subnets: Can’t communicate.

Solve: ID incorrect config/changing subnet to correct one

No connection between devices in VLAN: IP ruled out:

- show vlan Check whether port belongs to expected VLAN

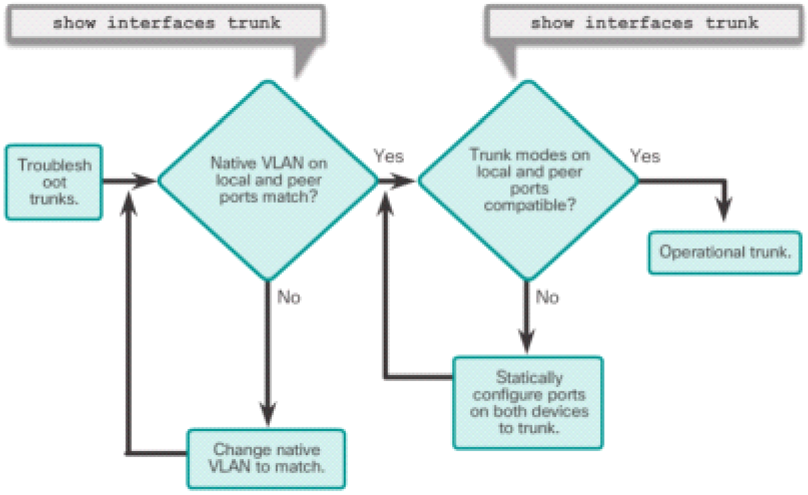
If unassigned/wrong VLAN

- switchport access vlan to correct
- show mac address-table to check which addresses learned on particular port/which VLAN port is assigned

If VLAN to which port assigned is deleted: Port becomes inactive

- show vlan or show int switchport cmds

Troubleshooting Trunks



```
show interfaces trunk
```

```
show interfaces trunk
```

Troublesh oot trunks.
Native VLAN on local and peer ports match?
Yes
No
Trunk modes on local and peer ports compatible?
Yes
No
Operational trunk.
Statically configure ports on both devices to trunk.
Change native VLAN to match.

VLAN leaking: When access port accepts frames from VLANs other than VLAN assigned

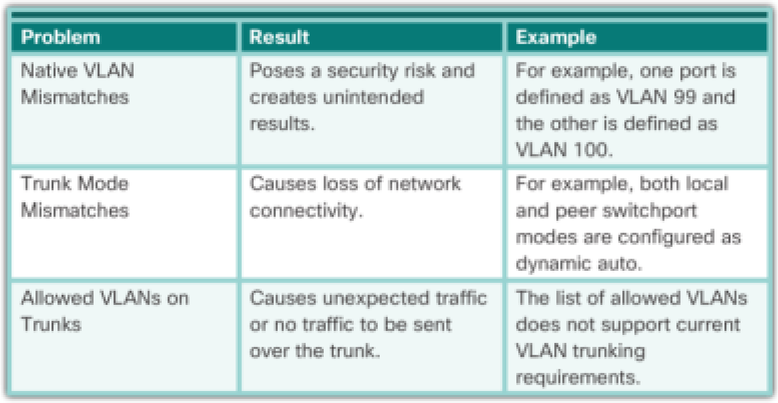
Trunk not forming/VLAN leak

- show interfaces trunk check if local/peer native VLANs match
- If native VLAN doesn’t match on both sides: **VLAN leaking**

Display status of trunk/native VLAN used on that trunk link/verify trunk establishment

- show interfaces trunk

Common Problems w/Trunks



Problem	Result	Example
Native VLAN Mismatches	Poses a security risk and creates unintended results.	For example, one port is defined as VLAN 99 and the other is defined as VLAN 100.
Trunk Mode Mismatches	Causes loss of network connectivity.	For example, both local and peer switchport modes are configured as dynamic auto.
Allowed VLANs on Trunks	Causes unexpected traffic or no traffic to be sent over the trunk.	The list of allowed VLANs does not support current VLAN trunking requirements.

- Incorrect config

Native VLAN mismatch	○ Trunk ports configured w/different native VLANs. ○ Config generates console notifications/causes inter-VLAN routing issues etc.. ○ Security risk
Trunk mode mismatches	○ 1 trunk port configured in a mode not compatible for trunking on corresponding peer port ○ Config error causes trunk link to stop working
Allowed VLANs on trunks	○ List of allowed VLANs on trunk not updated w/current VLAN trunking requirements ○ Unexpected/no traffic is sent over the trunk

Trunk Mode Mismatches

Normally configured statically with switchport mode trunk

- Cisco Catalyst switch trunk ports use DTP to negotiate state of the link
- When a port on a trunk link is configured w/a trunk mode that's incompatible with neighbor: fails to form

Incorrect VLAN list

switchport trunk allowed vlan [*vlan id*] traffic from a VLAN transmitted/allowed across trunk